Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas y Telemática

Anatomía de un ataque Informático

Tesis previo a la obtención del título de Ingeniero en Sistemas y Telemática.

Autor: Byron Vinicio Guamán Sinchi

Director: Ing. Fabián Carvajal

Cuenca, Ecuador

2014

DEDICATORIA:

Dedico esta tesis a mi mamá Gladys Guamán por haberme apoyado incondicionalmente en todo momento y gracias a ella poder cumplir esta meta. A toda mi familia y amigos que durante este camino me apoyaron de cierta manera y así poder lograrlo.

AGRADECIMIENTOS:

Agradecer primeramente a Dios por darme todo lo necesario y poner gente que en mi vida que me supo apoyar creyendo en mi y así lograr esta meta.

También agradecer de una manera especial al Ingeniero Fabián Carvajal que me brindo su apoyo y su amistad desinteresadamente en el transcurso de mi formación académica, profesional y a lo largo de este trabajo. Así mismo agradecer al Ingeniero Luis Ochoa que pese a no ser mi director me supo brindar su ayuda incondicionalmente.

Y por último agradecer al Ingeniero Javier Alvarado por su amistad y ser un mentor en mi formación profesional, apoyándome en todo momento incondicionalmente en la formación académica.

RESUMEN

El internet a través de los años ha evolucionado totalmente, siendo esta la red más grande del mundo por donde circula la mayor cantidad de información de cierto modo libremente, este crecimiento no solo en internet sino también en redes privadas genera una estrecha relación con la seguridad de la información debido a su vulnerabilidad. Para lograr mitigar riegos de una manera preventiva hay que conocer posibles atacantes, su escenario y vectores de ataque, en consecuencia se ha establecido este trabajo llamado "Anatomía de un ataque informático" demostrando como logran acceder a un sistema sin autorización y esquematizando sus pasos.

ABSTRACT

The internet has fully evolved through the years, being the world's largest network by which the greatest amount of information flows freely. This growth has not only happened online, but also in private networks generating a close relationship with information security due to its vulnerability. In order to diminish risks as a preventive measurement, it is necessary to identify possible attackers, their scenario and attack vectors. Consequently, we present this work entitled "Anatomy of a computer attack" in order to demonstrate how they gain access to a system without authorization by outlining the steps followed.

UNIVERSIDAD DEL
AZUAY
Dpto. Idiomas

Translated by,
Lic. Lourdes Crespo

INDICE DE CONTENIDOS

INDICE DE ILUSTRACIONES

CAPITULO 1

SEGURIDAD INFORMATICA

1.1 Introducción

En este capítulo se tratara los conceptos necesarios para comprender la seguridad informática así como también sus características y una breve historia de cómo ha evolucionado este concepto a través de los años.

1.2 Historia

A partir de los años 80 el campo de la computación ya tenía una gran acogida y había cierta preocupación por la integridad de los datos que se almacenaban en los ordenadores. Todo esto generado a un acontecimiento llamado "El Día en el que internet se detuvo".

Imagen 1 Robert Morris Jr.

Aunque en realidad solo se detuvo el 10% de los computadores conectados en esa época a ARPAnet[1], **Robert Morris Jr.** como se muestra en la imagen fue el causante de tan alarmante acontecimiento, estudiante de 23 años de la Universidad de Cornell, creo el software con una gran capacidad de reproducirse copiándose en cada máquina y luego escondiéndose en la red esto ocasionaba que más recursos de la CPU sean consumidos provocando el primer ataque de denegación de servicios (DoS). Por ellos surgió la necesidad de dotar medidas y profesionales que implementara procedimientos y políticas de seguridad, dando comienzo a la seguridad de la informática.

[1] ARPAnet.- es la red de computadoras creada por encargo del Departamento de Defensa (DOD) de Estados Unidos para utilizarla como medio de comunicación entre los diferentes organismos nacionales estadounidenses.

En la época de los noventa se empezó a escuchar términos de gusanos, virus y **hackers** asechando a los computadores y su información, conectados ya en la **Internet** como la conocemos hoy en día. Generando la necesidad ya de tomar conciencia del peligro que esto generaba y en la búsqueda de medidas preventivas para evitar esto.

A comienzos del siglo 21 ya se generan acontecimientos de mayor gravedad introduciéndose la palabra delito informático, algo común en el medio y haciendo que se tomen mucho más en serio la seguridad informática en la Cumbre Mundial de la sociedad de la información (Ginebra, 2003). También se dio lugar al Día Internacional de la Seguridad de la información (DISI) uno de los eventos que se realiza año tras año sobre Seguridad Informática y Sociedad de la Información en la ciudad de España.

1.3 Definición

La palabra seguridad como tal en el diccionario se define como algo que no registra peligros, daños ni riesgos considerándose como una certeza.

Seguridad Informática se definiría como; asegurar el acceso a los recursos de cualquier sistema de una manera autorizada sin afectar la confidencialidad, autenticidad o integridad de la información.

La seguridad informática no debe ser confundida con la seguridad de la información que solo trata de resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.[2]

Se podría definir a la seguridad informática como una disciplina encargada de diseñar normas procedimientos, métodos, técnicas con el objetivo de conseguir un sistema el cual cumpla los tres principios fundamentales de confiabilidad, integridad y disponibilidad.

[2] Wikipedia. «Wkipedia.» 20 de 07 de 2011. 20 de 03 de 2014. <http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n>.

Imagen 2 Seguridad Informática: Objetivos

Confidencialidad: Consiste en garantizar la privacidad de los elementos almacenados en un sistema de personas autorizadas negando así a quien no esté autorizado su acceso.

Disponibilidad: La información y los datos estén accesibles en el momento que se requiere.

Integridad: Es una característica que garantiza que se pueda detectar posibles modificaciones en los datos que se hayan hechos en dos momentos determinados en el tiempo.

1.4 Importancia

La seguridad informática debería ser tomada con un nivel de importancia tal que las empresas o personas adquieran una lema de "Debe ser seguro" y no un "Debería ser seguro" y así manteniendo los pilares de la seguridad la integridad, confidencialidad y disponibilidad.

Esto no debe convertirse en algo obsesivo sino considerar el nivel de seguridad que esté acorde a la magnitud de la información, ya que es muy diferente un usuario particular al de una empresa, o una empresa a una nación.

1.4.1 Para Particulares

Un usuario particular es aquella persona sin ninguna vinculación a una empresa o institución que hace uso de su computador o cualquier

dispositivo con conexión a internet intercambiando información con su familia o amigos, o sin conexión a internet solamente revisando su Información personal.

Hoy en día la mayor parte de usuarios particulares tienen acceso a internet en su hogar o en lugares públicos tales como parques, bibliotecas, etc. En los cuales hacen revisión de cuentas bancarias, información empresarial como su mail o accesos a programas de cualquier índole vinculado con la misma, medios Sociales como Facebook. Toda esta información se encuentra expuesta, ya que, no se toma medidas adecuadas de seguridad y por esta razón han sido víctimas de delitos informáticos u otro medio que exponga la seguridad de dicha información.

Con la aparición de redes sociales tales como Facebook, Twitter entre las más conocidas, son un medio de exposición de información que si bien es cierto es un vulnerabilidad que puede parecer un poco grave pero un **delincuente informático**[3] puede hacer uso de la misma.

La importancia de la seguridad informática para el particular radica en el nivel de exposición de información personal a través del internet y de qué forma está protegida.

Sabiendo todo esto se habla hoy en día el concepto de seguridad no solo para empresas o instituciones, sino para particulares que pueden ser víctimas de un delito informático y deben establecer medidas de seguridad para salvaguardad su información.

1.4.2 Para Empresas o Instituciones Educativas.

En nuestro país la importancia que se da a este tema de la seguridad de la información en una empresa o institución educativa pasa muy desapercibida puesto que es tomando como **"gasto"** o algo innecesario. Pero no consideran que la información es el núcleo de toda organización, el **activo más importante** y que es lo primordial protegerla con las medidas acordes a la magnitud de dicha información, al no contar con seguridad

[3] **Delincuente Informático.-** Es la persona que realiza actividades ilegales haciendo uso de las computadoras y en agravio de terceros, en forma local o a través de Internet.

adecuada puede ser una pérdida parcial o total, hasta el punto de no poder recuperarla de ninguna manera.

El riesgo de un ataque a un sistema podría darse a pesar de tener todas las medidas de seguridad pero no debe considerarse un obstáculo para no utilizar con confianza el sistema porque también hay factores como el humano o de hardware que pueden fallar en cualquier momento.

Para una empresa o institución la seguridad debe ser realizada y adquirir una importancia; a nivel de usuario, tecnologías usadas, nivel físico (infraestructura TI), nivel de datos como los permisos, autenticación o control que se mantiene sobre los mismo.

1.4.2 Para un país o una nación.

Para las clasificaciones anteriores planteadas en muchos casos no puede tener un nivel de importancia de mayor relevancia pero al tratarse de una nación esto debe ser considerado a tal punto que no exista inseguridad de ningún modo.

"Los procedimientos puestos en práctica tiene que estar a la altura de la información que se proteja, ya que está en juego la seguridad de toda una nación."[4]

La película de 1983 Estado Unidos llamada "Juegos de Guerra" alarmo sobre la seguridad informática en una época que no se tenía mucho conocimiento, pero dando a conocer que sea una nación se debe tomar de importancia el tema y desde aquella época ha venido tenido una evolución en esta materia.

Hoy en día se ha escuchado hablar sobre múltiples ataques a diferentes naciones en sus páginas gubernamentales u oficiales haciendo que esto

[4] Auditoría, Consejo. *Seguridad informática-ethical hacking : conocer el ataque para una mejor defensa*. Barcelona: Ediciones ENI, 2013.

sea de mucho más importancia en la actualidad. Dando cabida a un nuevo termino llamado terrorismo cibernético [5]

1.2.3 Tipo de Amenazas.

Las amenazas que puede tener un sistema informático son cuando se hace una planificación de seguridad mal elaborada, pero también no puede estar previstas. Ahí se deben elaborar medidas para protegerse de esas amenazas y sobre todo proteger como antes mencionado el activo más importante "la información". Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información, es necesario implementarla.

Aun ni con todas las medidas de seguridad respectivas se puede controlar todas las amenazas que pueden existir o eliminarlas totalmente.

Existen diversos factores y los podemos clasificar de la siguiente manera:

1. Factor Humano.

Para la seguridad de la información el factor humano es crítico y la principal fuente de amenaza debido a la negligencia con la que puede ser manejada una norma de seguridad preestablecida o simplemente mala intensión con el afán de causar algún tipo de daño. Este factor puede ser considerado al personal interno de una organización o personas ajenas como un hacker.

Un ejemplo es la técnica de Ingeniera Social que es muy utilizada para obtener información de carácter importante para una empresa u organización a través del propio personal.

1.1 Físicas.

El suministro de energía es una de las amenazas físicas más comunes, al no poner medidas de seguridad como reguladores de voltaje o un UPS, pero esta no es la mayor amenaza ya que existe también mala manipulación o uso por parte del usuario como por ejemplo cuando se desconectan la

[5] **Terrorismo Cibernético.-** Es el término genérico para aquellas operaciones ilícitas realizadas por medio de internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet.

alimentación de cualquier equipo sin apagarlo previamente. Falta de suministro eléctrico interno de la organización causado por un corto circuito o un problema en general, también puede darse el caso que sea este externo por parte de la compañía de suministro electro por motivos ajenos a la organización.

Amenaza física son incendios que pueden ser iniciados por diversos factores, pero hoy en día se cuenta con contramedidas y con equipos especializados que lo mitigan.

2. Software.

Existen posibles fallas de software por la falta de precaución en la inserción de código malicioso como pueden ser troyanos, bombas lógicas, virus, gusanos informáticos, etc. Pero también puede existir una inserción de código malicioso por parte de un programador por ejemplo en un sistema financiero y afectar de alguna manera el mismo.

Los errores de programación no son muy comunes hoy en día pero sin embargo cuenta como una amenaza pudiendo causar pérdida o modificación de la información.

De acuerdo a la información que se maneje si esta es crítica debería contar con un cifrado de datos que no ponga en amenaza la misma.

3. Redes de Datos.

Las redes de datos garantizan la transmisión de la información, son los canales por donde se entre conecta la misma. Pero sin embargo es el principal objetivo de un atacante o no cumplen con las normas necesarias de instalación y vienen a convertirse en una amenaza.

La principal amenaza a considerar en una red de datos es la no disponibilidad en la información.

4. Desastres Naturales.

Estos son factores a considerar también importantes ya que su origen es por parte de la naturaleza y al igual que los anteriores representan una amenaza, afectando sistemas enteros y su integridad en donde se toma en

cuenta la infraestructura, instalación, componentes, equipos y todo lo que sea parte del mismo.

Las amenazas de un desastre natural pueden ser de una inundación, terremoto, incendio, huracán, tormentas eléctricas, etc. Pero todo estas deberían ser consideradas como un factor de riesgo y así no se pueda mitigar en su totalidad, pero tomando precauciones se podría acarrear menos consecuencias.

1.2.4 Mecanismos de Seguridad

Los mecanismos de seguridad son herramientas, técnicas o métodos utilizados para mantener la disponibilidad, confidencialidad y la integridad de un sistema informático.

De acuerdo a la amenaza que tengamos existen muchos mecanismos que pueden ser utilizados, considerando que estas pueden ser **detectivo, correctivos o preventivos.**

Mecanismos **Preventivos** tiene como objetivo principal prevenir antes de que un ataque ocurra. Los mecanismos **detectivos** tienen la misma funcionalidad de prevenir antes de que un ataque ocurra pero con la diferencia de que se utiliza agentes o métodos que monitorean constantemente el sistema, informado el problema y registrando el mismo.

Los métodos **correctivos** a diferencia de los anteriores no previene sino ayuda a corregir las consecuencias que ha dejado el ataque esta como su función principal.

HACKERS

1.3.1 Definición

Existen muchas definiciones de hackers que pueden ser mal interpretadas, pero ¿quiénes son? , y a ¿cuáles se definen como hackers?, son las preguntas más frecuentes que al no tener conocimiento del tema se relaciona con personas que hacen virus o ingresan al ordenador para hacer daño, pero casi siempre relacionado con la cara mala de la informática.

La palabra se originó por estudiantes del M.I.T.[6] en los años 60's y 70's, hack que traducida al español significa hachar, entonces la relación que tiene un hacker es que en muchas técnicas se utiliza la fuerza bruta para ingresar a un sistema asemejando al hachazo que un leñador le daría a un árbol.

En el campo informático un "hacker" es una persona que tiene mucho conocimiento en redes, programación o cualquier tema relacionado con informática y lo maneje a tal punto que logre acceder a un sistema con o sin autorización vulnerando su seguridad y siendo su motivación una ideología con fines de lucro, modo de una protesta o simplemente la satisfacción de un logro personal.

En el diccionario enciclopédico se define como "Persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no se maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo".

1.3.2 Tipos de Hacker

El termino hacker se ha asemejado a la comunidad informática pero de una forma clandestina, pero estos últimos años este mismo término se manejado de una manera más abierta clasificando los tipos de hackers que existen. En el campo de la seguridad informática podemos clasificar 3 categorías como más relevantes como son hacker de sombrero blanco, de sombrero gris y de sombrero negro.

1.3.2.1 Black Hat (Sombrero Negro)

Hacker de sombrero negro es la persona que al descubrir una vulnerabilidad de un sistema lo explota e ingresa sin autorización pero siempre buscando un fin de lucro o su propia satisfacción de conocimiento.

También conocidos como crackers, llamados así porque en las películas antiguas del viejo oeste utilizaban sombrero negro. Pero su mala utilización

[6] El **Instituto Tecnológico de Massachusetts** (**MIT** por las iniciales de su nombre en idioma inglés, *Massachusetts Institute of Technology*)

de sus habilidades informáticas con métodos hacking hace de esto su mala reputación.

Al obtener la información pueden ser capaces de hacer chantajes, fraudes, hasta destruir la misma llegando a que el usuario, empresa o institución piensen que son todo lo que temen de un criminal informático.

Pero no todo lo malo se puede relacionar con ellos, ya que fomentan la investigación, y las empresas dedicadas a la seguridad de la información no fueran capaces de tener un avance si ellos no violaran las seguridades impuestas. Y los sistemas operativos no fueran capaces de mejorar sus fallas.

El avance en el campo de la seguridad informática hay que acreditarles también. Porque en un mundo donde cada día avanza la tecnología de la información y volviéndose por su velocidad de evolución más vulnerable a ataques su colaboración es implacable y directa, llevando a los sistemas a ser mejores y consistentes día a día.

1.3.2.2 Grey Hat (Sombrero Gris)

La combinación entre ético y no ético, entre lo bueno y lo malo es un hacker de sombrero gris, porque los métodos y técnicas no se diferencian de sus otros tipos pero su mentalidad de cómo hacer uso de la información que consiguen o sus habilidades informáticas se maneja de una forma diferente.

Cuando encuentran y explotan una vulnerabilidad de un sistema esto se lo hace una manera ilegal lo cual esta se asemeja a como un hacker de sombrero negro actuaria, pero cuando consiguen la información u otro tipo de beneficio de sus actos entonces los llevan a las empresas y los tratan de vender soluciones que ellos lograron vulnerar, esto actuando como un hacker de sombrero blanco ya que tiene el consentimiento para ingresar y solucionarlo. De ahí la combinación entre el blanco y lo negro para dar como resultado una ética hacker ambigua.

1.3.2.3 White Hat (Sombrero Blanco)

Con el afán de ayudar y la mentalidad no maliciosa es como se maneja un hacker de sombrero blanco quien es contratado y tiene todos los permisos necesarios para encontrar y explotar vulnerabilidades en el sistema. Luego de esto realizar un informe y un plan para mitigar dichos fallas, para en un futuro muy cercano dar solución.

Las técnicas utilizadas no tiene diferencia a los tipos anteriores, pero si radica la diferencia en sus objetivos y metas.

Al ayudar a la investigación muchos de ellos haciendo públicos artículos o código con el cual los ayudo los hackers de sombrero negro pueden hacer uso llevando a un círculo de no terminar entre éticos y no éticos.

CAPITULO 2

ANATOMIA DE UN ATAQUE INFORMATICO

2.1 Introducción

El siguiente capítulo se trata de esquematizar la metodología utilizada en un ataque. Desglosando cada una de las fases estandarizadas en la seguridad informática haciendo una descripción y comprendiendo cual es la forma de cómo se ejecuta.

2.2 Definición

Para establecer una definición hay que saber el de cada palabra que la compone.

Anatomía en el diccionario de la real academia de la lengua española nos indica que: "Estudio de la estructura, situación y relaciones de las diferentes partes del cuerpo de los animales o de las plantas"[7].

"Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático"[8].

Se podría establecer la definición como el estudio de la estructura de un ataque informático, sabiendo que métodos utilizaron para ingresar a un sistema sin autorización desestabilizando o dañando al mismo.

2.3 Etapas

Es importante tratar de definir las fases o etapas para conocer la forma ya se un hacker de sombrero blanco, gris o negro ingresara a un sistema.

---

[7] Real Academia Española. *Real Academia Española*. s.f. 01 de 06 de 2014. <http://lema.rae.es/drae/?val=anatom%C3%ADa>.

[8] Wikipedia. *Wikipedia*. s.f. 01 de 07 de 2014. <http://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico>.

Empresas y expertos en seguridad informática han establecido todas estas fases a las cuales se conocen también como **circulo hacker**. Los atacantes sean estos éticos o no éticos siempre seguirán esta secuencia pero puede variar las técnicas y herramientas que utilicen. Conocer esto ayudara a las buenas prácticas de la seguridad informática y sobrellevar sus desafíos.

Estas fases son Reconocimiento, Escaneo, Obtener Acceso, Mantener Acceso y Borrar Huellas en ese orden, estas pueden variar en un paso adicional que sería el de presentar un informe en el caso de un auditor informático, pero casi siempre se maneja solo las antes mencionadas.

El circulo hacker es el esqueleto que comprende una anatomía de un ataque informático.

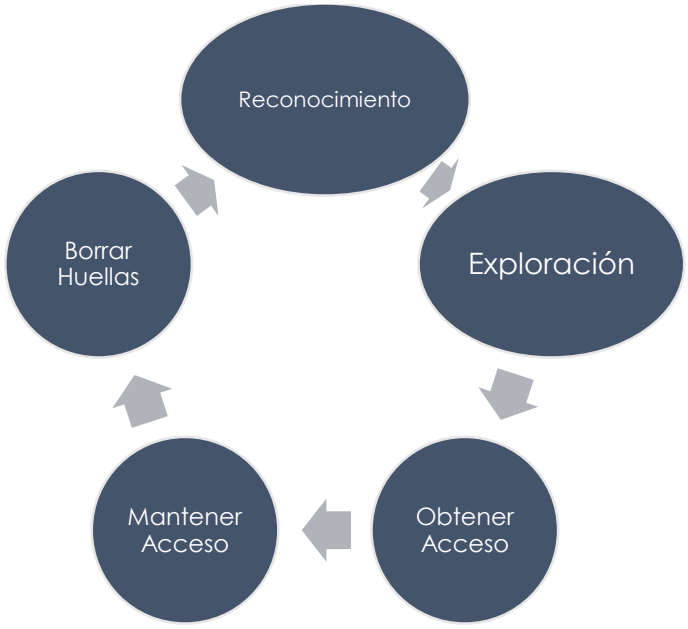


Imagen 3 Anatomía de un ataque Informático

2.3.1 Reconocimiento

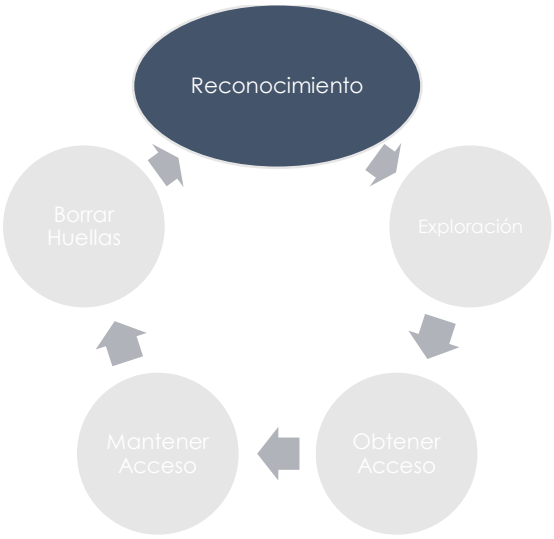


Imagen 4 Fase de Reconocimiento

El reconocimiento o también llamado **footpriting** es la primera fase del ya mencionado circulo hacker que compone la anatomía de un ataque informático, en donde el hacker ético o no ético investiga toda la información que pueda obtener con el uso de herramientas o métodos de la persona, institución o empresa a la cual va a atacar. Siendo esta información de dominio público o publicada a propósito por desconocimiento de seguridad.

Toda información sea muy importante o insignificante que se recopile servirá a la hora del ataque, obteniéndose de una forma activa cuando tenemos una interacción directa con el objetivo o de una manera pasiva cuando no se tiene interacción directa con el objetivo.

En esta fase se sabe si el ataque será o no exitoso.

Reconocimiento Activo

Es cuando se tiene una interacción directa con el objetivo es decir que el atacante envía algún tipo de acción y tiene una respuesta. De una manera técnica es él envió de paquete de datos a la víctima y se tiene una repuesta, por ejemplo cuando se realiza un ping, un mapeo de red, ingeniera social, barridos de ping entre otras.

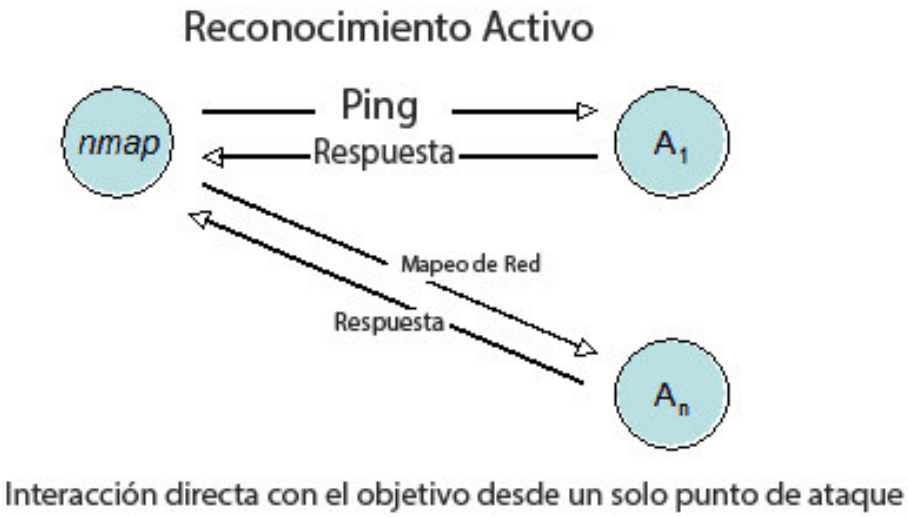


Imagen 5 Reconocimiento Activo

La herramienta más conocida por los hackers es Nmap[9] que en una de sus funciones ayuda a establecer que computadoras están conectadas en una red con un mapeo de red, y con esto podemos obtener sistema operativo, puertos abiertos, servicios ejecutándose e inclusive características de su hardware, como podemos observar en el siguiente gráfico.

[9] Nmap: es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon.

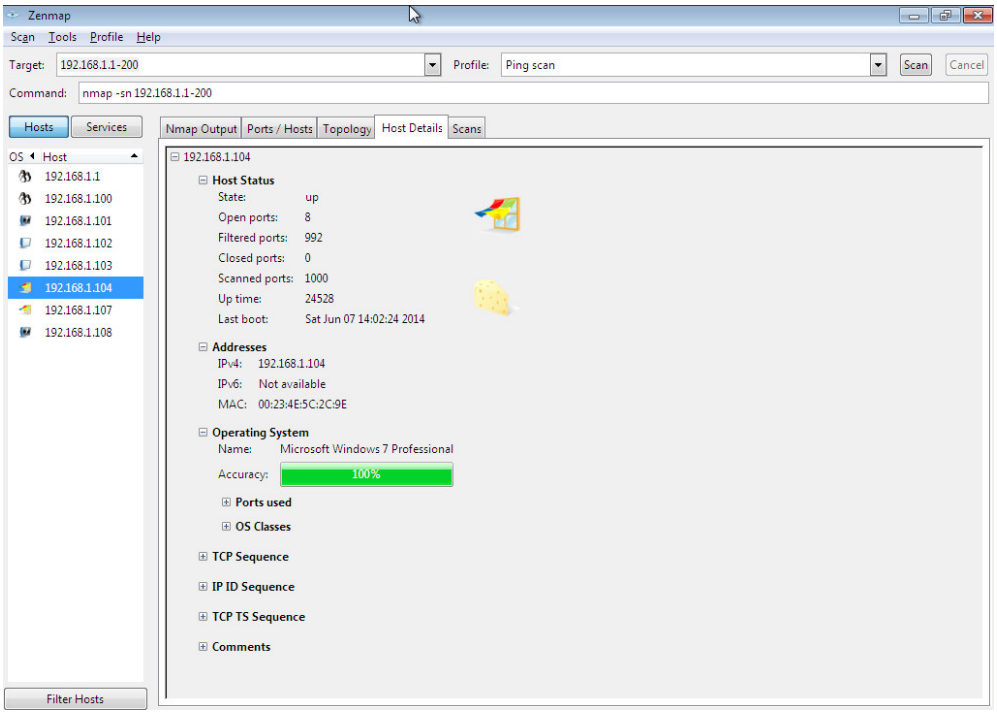


Imagen 6 Ejemplo Zenmap

Reconocimiento Pasivo

Este tipo de reconocimiento es cuando se obtiene información sin tener interacción directa con el objetivo.

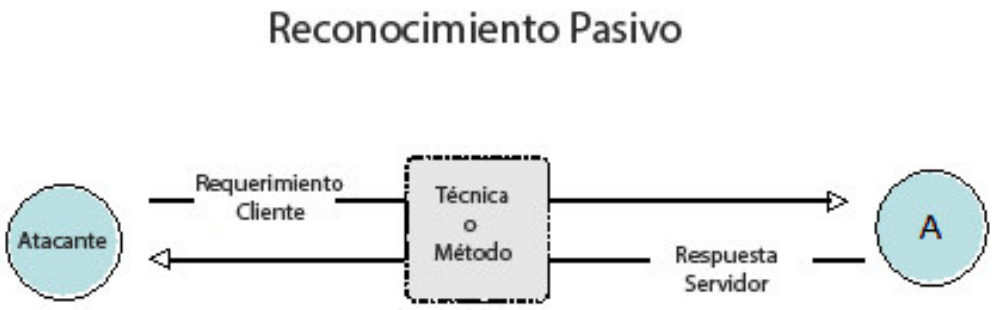


Imagen 7 Reconocimiento Activo

Todo absolutamente toda la información es necesaria y valida no importa la técnica que se utilice.

Es importante el papel toman los buscadores de internet especialmente Google que siendo el más utilizado y gracias a su clasificación de páginas web según su ranking es el que más información nos ayudara a obtener. La

técnica que se emplea se denomina "google hack" que con la ayuda de comodines de búsqueda se obtendrá resultados mucho más específicos.

Los comodines de búsqueda más comunes son los siguientes

Comodín	Función	Ejemplo de Uso
+	Forzar palabras para su búsqueda.	Noticia + de + la universidad + del Azuay
-	Excluir términos en la búsqueda.	Universidades Ecuador - Quito
""	Encontrar frases exactas.	"universidad del Azuay"
site	Indicar la búsqueda en determinado dominio	Site: www.uazuay.edu.ec
OR	Páginas que incluyan una palabra u otra.	Universidades Cuenca OR Quito
Link	Busca todas las páginas que tengan el link indicado.	Link: www.uazuay.edu.ec
allinurl	Indicada todas las paginas indexadas de un dominio indicado.	Allinurl:www.uazuay.edu.ec
allintitle	Todas las páginas que tengan el titulo indicado.	Allintitle: Universidad del Azuay
Info:	Muestra información del dominio indicado.	Info:www.uazuay.edu.ec
filetype	Busca un tipo de documento especificado.	Articulo x filetype:pdf

Tabla 1 Comodines de Búsqueda Google

Para realizar un reconocimiento no solo es importante la técnica sino el ingenio para encontrar información.

Otra forma de encontrar información es mediante el protocoló Whois que efectúa consulta a una base de datos y se obtiene información de un domino en específico o una dirección IP en internet.

Los datos que nos proporciona WHOIS son dirección IP, servidores DNS[10], Registrador del Dominio, Lenguaje de Programación, Idioma, País, Sistema Operativo del Servidor, Correos Electrónicos de Contacto, Números telefónicos entre otros datos que pueden ser recolectados y utilizados para un ataque. En este caso sería muy útil para realizar un ataque de Ingeniería Social la cual utiliza el eslabón más débil de la cadena de seguridad que es la persona y con el uso adecuado de esta información obtener aún más.

No es tan común en la actualidad pero otro método que cabe mencionar dentro de esta fase es el "dumpster dive" que es cuando un atacante revisa la basura de su víctima y en mucho de los casos obtiene información sensible de su objetivo.

2.3.2 Exploración

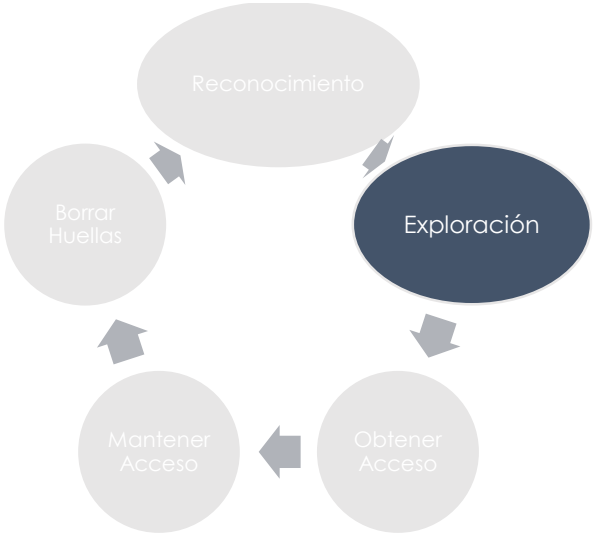


Imagen 8 Fase de Exploración

Una vez recopilada la información necesaria en la anterior etapa se actúa de una manera más activa con el objetivo, siendo necesario tener algún tipo de conexión, se realiza un reconocimiento activo teniendo respuesta del objetivo, aquí se introduce más a fondo el uso de herramientas como NMAP.

Al ser un reconocimiento activo se escanea la red para determinar hosts accesibles y activos, puertos abiertos, localización de routers, detalles de sistemas operativos y servicios del objetivo. Siendo esta último paso

[10] DNS: Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

recopilatorio de información para el ataque. El éxito del mismo depende del conocimiento y la aplicación con el que se realice las técnicas de escaneo.

Las herramientas utilizadas en esta fase se basan en el concepto del protocolo TCP (Protocolo de Control de Transmisión) y su saludo en tres vías o llamada también "three-way handshake" el cual establece la comunicación entre dos dispositivos. Esta técnica utiliza 3 tramas con mensajes de sincronismo (SYN) y reconocimiento (ACK) como se aprecia en el siguiente gráfico.

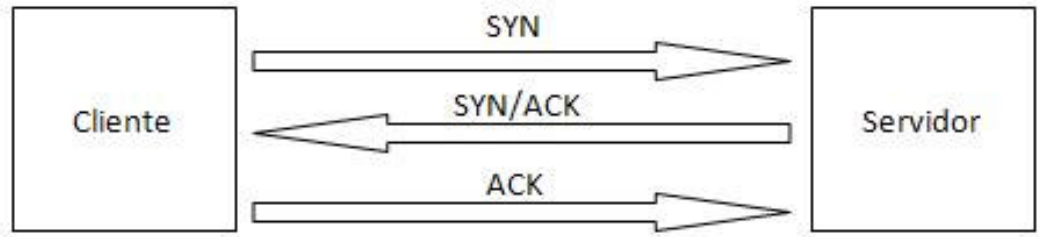


Imagen 9 Saludo en tres vías protocolo TCP

El cliente realiza una conexión enviando un paquete SYN al servidor, en el servidor se comprueba si el puerto está abierto, si el puerto no está abierto se le envía al cliente un paquete de respuesta RCT, esto significa un rechazo de intento de conexión. Si el puerto está abierto, el servidor responde con un paquete SYN/ACK. Entonces el cliente respondería al servidor con un ACK, completando así la conexión.

Para determinar si un objetivo está activo se utiliza herramientas con técnicas de barrido ping o escáneres de puertos usando el protocolo ICMP[11] enviando paquetes a todos los hosts y si uno de ellos da respuesta implica que está activo. En una red con las medidas de seguridad adecuadas el firewall tienen bloqueado por completo el ping para que no puedan hacer uso de esta técnica.

[11] ICMP.-El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas en inglés de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).

Una vez identificado el host activo se realiza un escaneo de puertos que tiene vulnerables. Una herramienta de las más útiles para realízalo es la mencionado NMAP y su versión gráfica de ZENMAP.

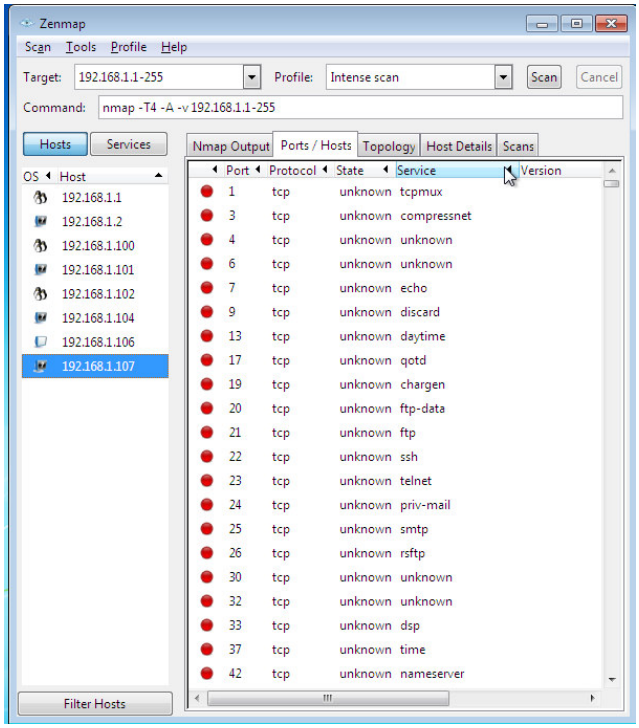


Imagen 10 Software Zenmap

Un puerto está abierto cuando está disponible y a la escucha de conexión, cerrado pero accesible sin ser asociado a un servicio y filtrado cuando no se tiene acceso por que existe un dispositivo filtrando paquetes de por medio que impide determinar su estado abierto o cerrado.

El proceso de identificación del sistema operativo determina su versión y que sistema es. P0f es la herramienta que realiza este trabajo, no posee un interfaz gráfico pero es indetectable ante firewalls al no generar tráfico en la red adicional. Dentro de este procedimiento se realiza una subfase llamada **enumeración** la cual se encarga de recopilar aún más información desde la parte interna de la red en el sistema operativo como usuarios y grupos, nombres de equipos y dispositivos, recursos compartidos y dispositivos.

La enumeración se realiza gracias a protocolos TCP/UDP que son susceptibles sean estos por fallas del fabricante del software o configuraciones débiles de parte de los administradores del sistema.

2.2.3 Obtener Acceso

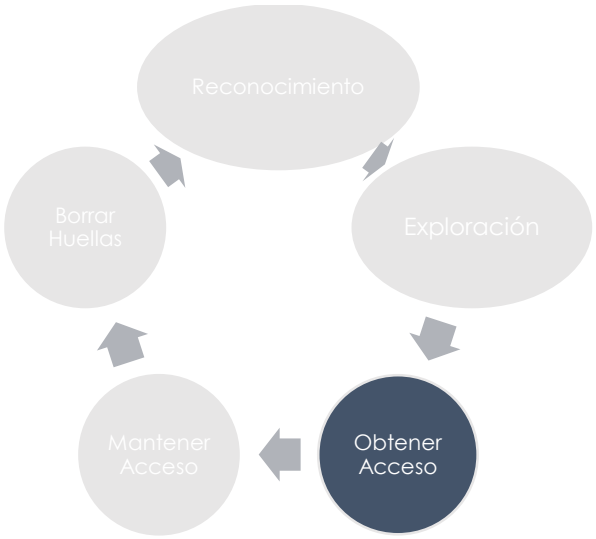


Imagen 11 Fase Obtener Acceso

Obtener acceso es la fase donde verdaderamente se realiza el ataque, el daño que ocasione está en función de la información recopilada y de las habilidades del atacante. El ataque puede ser a nivel de red, aplicación y de sistema donde no necesariamente puede implicar un acceso como dice en la fase ya que podría también ser por ejemplo un ataque de denegación de servicio.

Esta es la fase más importante porque se explota vulnerabilidades encontradas y se toma el control de la víctima mediante el uso de herramientas, tales como exploits[12] o un bugs[13] para lograrlo.

Un exploit al explotar una vulnerabilidad lo puede hacer de tres maneras:

-**Exploit Local.-** Se ejecuta dentro de la red de la víctima escalando privilegios a nivel de usuario.

[12] Exploit.-Es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

[13] Bug.- Un error de software, comúnmente conocido como bug («bicho»), es un error o fallo en un programa de computador o sistema de software que desencadena un resultado indeseado.

-Exploit Remoto.- Se ejecuta fuera de la red de la víctima tomando control del equipo objetivo, tambien pudiendo tomar control de otros equipos que tenga visibilidad desde este.

-Exploit ClientSide.- Explota la vulnerabilidad de aplicaciones instaladas en un computador como Microsoft Office, Pdf, programas utilitarios y este tiene que ser ejecutado por el usuario para que tenga resultado, si no es detenido por algún mecanismo de seguridad como un firewall o un antivirus se lograra tener el control del objetivo deseado.

Con la evolución en el campo de la seguridad informática también lo hizo el estudio de las vulnerabilidades, de hacer una explotación manual en donde el atacante escribe su propio código tornándolo muy costoso en tiempo y conocimiento resultando tedioso. Gracias a esto aparecen los frameworks de explotación que son paquetes de software que incluye todo tipo de herramientas para la construcción de exploits haciendo el trabajo más fácil tanto para un auditor o para un atacante.

En la actualidad existen frameworks de explotación como Inmunity Canvas y Core impact, que trabajan bajo una licencia de pago, sin embargo también existe herramientas bajo la licencia GNU como es el Metasploit Framework (MFS) haciendo de este un entorno multiplataforma.

2.2.4 Mantener Acceso

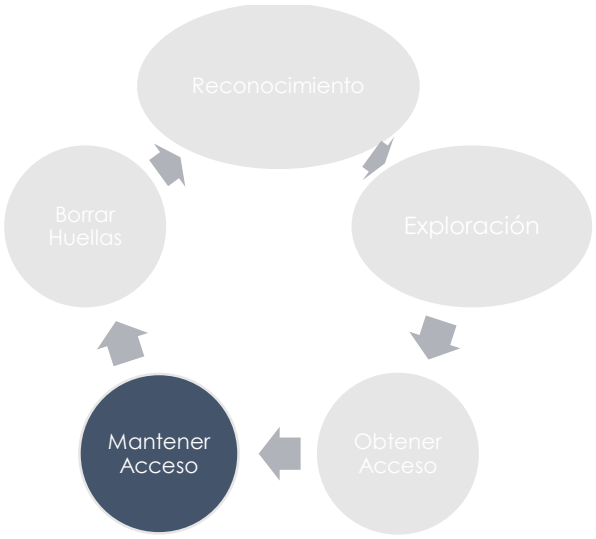


Imagen 12 Fase Mantener Acceso

El ingreso al sistema es solo un paso, ya que mantener el acceso es dar la continuidad del ataque con el fin de hacer más daño a la víctima, controlando el sistema que ya logro acceder.

Se puede decir es la fase más peligrosa para un atacante mal intencionado por que puede lograr robar información personal como números de tarjetas de crédito u otra información clave haciendo mucho daño a la víctima.

Pero existen diversas maneras de mantener el acceso como un malware (virus, troyano), sniffer, teniendo como principal factor la habilidad del atacante y la forma como quiera mantener el acceso. Esta fase se caracteriza por no solo hacer daño al equipo donde se ingresó, sino también infectando a otros equipos que se encuentra cerca en la misma red.

Mantener Acceso mediante el uso de Malwere

"El malware (del inglés malicious software), también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario."[14]

[14] —. *Wikipedia*. 06 de 06 de 2014. 13 de 07 de 2014. <http://es.wikipedia.org/wiki/Malware>.

Como su definición lo dice el malware tiene como único fin concretar un acción maliciosa para la que fue diseñada, como la eliminación de archivos del sistema operativo, eliminación de particiones de disco duro, pudiendo llegar hasta la manipulación de un mecanismo de seguridad como es un antivirus o un firewall.

En la siguiente tabla una breve clasificación de los malware más relevantes y sus características.

Malware	Características
Gusano	-Explota vulnerabilidades de una red e infecta a otros equipos. -Produce el máximo número de copias de sí mismo con el afán de facilitar su propagación.
Virus	-Necesitan la intervención del usuario para ejecutarse. -Pueden destruir archivos y corromper sistemas operativos. -Pueden llegar infectar a otros archivos de la misma tipo con el comenzó la infección.
Backdoors	-Establece una puerta trasera y a través de esta poder controlar el ordenador. -Una vez instalado el atacante pueden ingresar de una manera oculta.
Rootkits	-Técnica por la cual modifica el sistema operativo y hace que el malware permanezca oculto e indetectable, inclusive algunos logran evadir ser borrados.
Troyanos	-No son más que malwares disfrazados con algo atractivo al usuario y que hace que lo ejecute.

	-Una vez ejecutado es inminente generando consecuencias indeseables.
Spyware	-Recopila información del usuario y luego es enviada a un servidor remoto, esta es usada por agencias publicitarias o empresas que tengan interés en los datos recopilados.
Adware	-Tiene la misma característica que un spyware de recopilar información del usuario y luego enviar a un servidor remoto, la diferencia radica en que muestra publicidad no deseada.
Keyloggers	-Obtiene toda información digitada por teclado y luego enviada donde el creador lo ha programado. -Puede ser muy peligroso porque puede recopilar usuarios y contraseñas u otra información muy privada.
Stealers	-Roban Información almacena en el computador y es enviada al donde el creador lo ha programado.
Ransomware	-Cifran archivos importantes para el usuario y negando su acceso cuando lo requieran.
Rogue	-Su infección es a través de otro malware e induce al usuario a pagar por un software inútil o simplemente hace instalar otro programa malicioso.

Tabla 2 Clasificación de Malware

2.2.5 Borrar Huellas.

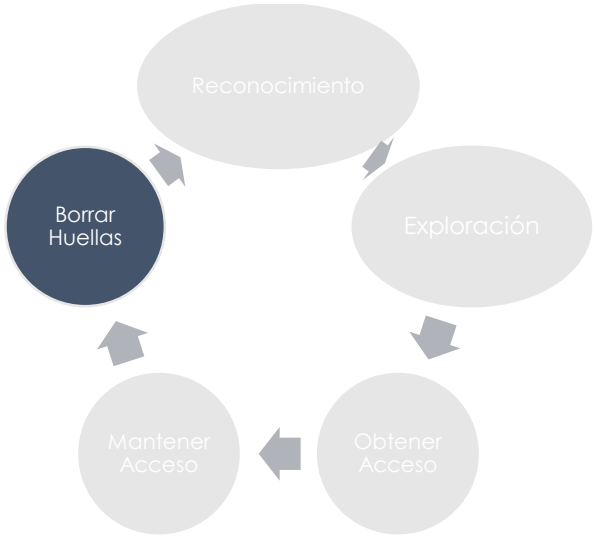


Imagen 13 Fase Borrar Huellas

La última fase del circulo hacker en donde se marca la diferencia entre un atacante con experiencia en no dejar ninguna huella y el atacante principiante que simplemente su objetivo es causar daño.

Es importante para un atacante destruir la información que lo implicaría esto le ayudaría a seguir manteniendo acceso al objetivo y el administrador de la red no tendría ninguna pista quien pudo haber causado el daño.

Cuando se ingresa a un sistema sea esta desde adentro o fuera de la red quedan paquetes trazando una ruta desde el punto del ataque hasta el objetivo. Por lo general cuando atacan lo hacen desde diferentes puntos justamente para evitar este rastro o a través de un software que cambie su ubicación cada vez.

Un método puede ser el imitar las actividades del usuario infectado para que no se dé cuenta de actividad sospechosa pero este teniendo control total del sistema para borrar sus huellas cuando sea necesario. Los archivos muchas veces modificados son los logs de registro, eliminar archivos temporales generados.

El uso de proxy anónimos es muy frecuente cuando se realiza el ataque por ejemplo el navegador TOR que fue hecho para mantener el anonimato ocultando IP, información que viaja a través del mismo y sobre todo su integridad.

Imagen 14 Navegador TOR

Hay que considerar que un software que realice el trabajo de borrar las huellas no siempre será confiable porque este en muchos casos eliminar registros de ubicaciones estándares, pero si el administrador de la red realizo un trabajo adecuado de seguridad dichas ubicaciones serian cambiadas dejando rastro para que pueda ser detectado. Estas herramientas se llaman zappers que elimina registros y logs una de las más conocidas es WinZapper.

CAPITULO 3

INYECCIÓN SQL

3.1 Introducción

En capitulo se trata de comprender los conceptos de Inyección SQL, método por el cual se basa nuestro primer caso de análisis hacia Sony Network. Este en la actualidad es muy utilizado por los atacantes, ya que es una de las vulnerabilidades más devastadoras que existe para impactar un negocio y se pueden ejecutar desde cualquier parte con una conexión a internet, pudiendo borrar o alterar datos y hasta la obtención o también conocido como el robo de información sensible almacenada como nombre de usuario, contraseña, números de teléfono, en muchos casos hasta números de tarjetas de crédito.

Para entender este método de ataque se debe comprender el concepto de SQL que es y para qué sirve.

"El lenguaje de consulta estructurado o SQL (por sus siglas en inglés Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas. Una de sus características es el manejo del álgebra y el cálculo relacional que permiten efectuar consultas con el fin de recuperar de forma sencilla información de interés de bases de datos, así como hacer cambios en ellas".[15]

3.2 Definición

Como se menciona anteriormente esta es una técnica de ataque con la que los hackers aprovechan las vulnerabilidades como el caso de Sony en su servicio de línea Play Station Network o. Esto mediante la alteración de sentencias SQL en una aplicación que pasa a una base de datos Back-End,

[15] WIKIPEDIA. *WIKIPEDIA*. 17 de 09 de 2014. 11 de 10 de 2014. <es.wikipedia.org/wiki/SQL>.

al ser capaz de influir en dicha sentencia aprovecha la sintaxis y la capacidad SQL.

Este método de ataque no solo se da en aplicaciones web sino también en cualquier programa, página web, etc. Que acepte una entrada que puede formar sentencias SQL es decir puede ingresar código SQL por ejemplo en una página de inicio de sesión (login) para un usuario y este a su vez es vulnerable pudiendo ser atacado.

Entonces se podría definir a la inyección SQL como la modificación del comportamiento de consultas SQL introduciendo parámetros en la sintaxis no deseados, siendo una vulnerabilidad muy letal en la validación de las entradas a la base de datos de una aplicación.

3.2 Método de ataque

Una inyección SQL no es más como bien dice la palabra inyectar código SQL dentro de una aplicación alterando el funcionamiento, y hacer que se ejecute el código malicioso insertado en la base de datos.

Este método tiene diferentes maneras de ejecutar esto de acuerdo al resultado que pretendamos obtener. Tales como elevar privilegios, suplantar usuarios, obtención de información y denegar un servicio al usuario.

Elevar Privilegios es cuando en el sistema se utiliza credenciales para cada usuario y este puede hacer ciertas funciones de acuerdo a su puesto o al privilegio que le haya sido asignado, todo esto almacenad en una base de datos en donde se realiza una inyección SQL obteniendo esas credenciales de privilegios y cambiándose así mismo hasta conseguir tener el permiso de acceso más alto con el que puede hacer modificación de la información u otras funciones de acuerdo como el crea conveniente.

Suplantar a un usuario es una que el atacante haya accedido a la información del mismo y haga uso de esa información realizando acciones con la identidad suplantada.

Denegar un servicio es cuando pudiendo generar un código el cual pare los servicios de una base de datos dejando esta inhabilitada y cuando un usuario legal quiera acceder no lo lograría ya que esta al estar inactiva no responde a la solicitud del servicio.

La capacidad llega hasta el punto de obtener información sensible siendo esta acción muy letal para el sistema en donde las técnicas de inyección SQL permiten que el atacante realice una modificación a los registros de la base de datos extrayendo su información y en el peor de los casos su información bancaria o tarjeta de crédito.

3.2.1 Escenario para la explotación del ataque.

Para que se de este tipo de ataques existen escenario para que se puedan dar que a su vez se convierten en vulnerabilidades.

El primero es el fallo en la comprobación al momento que el usuario ingresa lo datos considerando que es un cliente autentico, pero siendo utilizado por los atacantes enviando código malicioso. El programador debe considerar que cualquier medida de seguridad en este caso puede fallar. En los parámetros que son enviados para hacer consulta en la base de datos son en los campos de los formularios utilizando métodos de llamadas POST, campos donde se obtiene información de la base de datos con el método GET, en la caso de aplicaciones web datos que se pasan por la cabecera http y datos almacenados en Cookies.

La utilización de parámetros cuando se llama a una base de datos es un problema y un escenario donde se puede aplicar este tipo de ataque, dándose siempre en los parámetros que nos comprobados adecuadamente, por ejemplo al hacer una conexión entre el lenguaje de programación y el motor de base de datos utilizado.

El ultimo escenario que existe dentro de este tipo de ataque es cuando se genera una consulta y esta no es fiable, esto dependiendo tanto del lenguaje de programación como el motor de base de datos utilizados. Cuando se construye la sentencia SQL y se concatenan las cadenas de caracteres, por ejemplo se genera una consulta en la sé que concatena

datos de que vienen por medio de parámetros desde otra página web con datos que están fijos en la sentencia, esto implica que en la misma tanto en los datos que son recogidos como los parámetros tengan el mismo nivel dentro de la cadena, una vez generada la sentencia SQL no se diferencia de que parte vino desde el programador, o desde el sitio y los parámetros dentro de la misma.

3.3 Ataque de inyección SQL a ciegas (Blind SQL injection)

Este tipo de ataques se denominan a ciegas por que el atacante al momento de hacer un inyección SQL no puede ver los resultados de los comandos ejecutados ya que el programa acepta datos de un cliente y ejecuta consultas sin primero validar la entrada del cliente. Pero el que no pueda ver esa información no significa que no pueda modificarla.

El no poder ver los resultados de los ataques como los mensajes de error, cambia la manera de obtener esa información haciéndolo de una manera deductiva cuando se envía la sentencia y esta logra modificar los parámetros realizando conclusiones sobre esos cambios logrando obtener información en base a los resultados.

La vulnerabilidad es evidente cuando al realizar una consulta SQL con condicionales como "or 1=2", "and 1=1" y esta no muestra ningún cambio y muestra el mismo contenido que se mostraba antes por ejemplo en una página web que muestre una noticia.

http://www.webejemplo.com/noticia.php?id=1

Si en esta página web de ejemplo podemos de la siguiente manera.

http://www.webejemplo.com/noticia.php?id=1 and 1=1

Y está a su vez nos muestra el mismo resultado que antes mostraba quiere decir que es vulnerable y puede ser atacada y lograr inclusive extraer información de la misma, en muchos casos para lograr esto se utiliza ataques de fuerza bruta en donde se obtiene carácter por carácter de un usuario o algún dato importante.

Hoy en día no solo se lo realiza de una forma manual sino existen programas especializados que ayudan a estos tipos de ataques realizando los ataques de fuerza bruta de una manera automática así obteniendo mucho más rápido los resultados y los datos.

3.4 Ataque de inyección SQL a ciegas en función del tiempo (Blind SQL Time-Based).

Este método de inyección SQL es igual que el anterior, pero la diferencia es que los atacantes hacen uso de una pausa durante un periodo establecido en la base de datos, luego se da la devolución de los resultados consultados. Es decir es utilizado para extraer información generando en las consultas retardos de tiempo en base a un criterio de falso o verdadero. Por ejemplo criterios como si la primera letra de un nombre de usuario es B esperar 10 sin importar la base de datos.

En la siguiente consulta mandamos a comprobar si es que existe la tabla de usuarios esperar 10 segundos, esto nos ayudara a determinar si es que esa tabla existe en realidad.

http://www.miweb.com/noticias.php?id=1; if (exists (select * from usuarios)) waitfor delay '0:0:10'-

Este método puede ser aplicado en los siguientes motores de base de datos tales como Oracle, Mysql, Sqlserver menos en Access y DB2.

CAPITULO 4

CASO DE ANALISIS ATAQUE SONY

4.1 Introducción

Este capítulo recopilara información del ataque que sufrió Sony a su servicio Sony Network en el 2011, enfocando al análisis del ataque determinando su anatomía, su metodología, objetivos atacados, consecuencias y así establecer contramedidas, estas pudiendo ser aplicadas o tomadas en consideración como medida preventiva para cualquiera que lo disponga.

4.2 Antecedentes

Sony es una empresa multinacional japonesa que fabrica productos tecnológicos de consumo. En el 2011 para una empresa de tal magnitud fue el peor año en lo que ha su seguridad de servicios en línea se refiere y desencadeno una serie de ataques causando pérdidas millonarias para la compañía. La mayor repercusión fue en unos de sus servicios online llamado PlayStation Network hasta el punto de dejarla deshabilitada, así también obteniendo millones de cuantas de usuarios en donde se tenía información personal e inclusive tan crítica como el número de tarjetas de crédito.

Del 17 al 19 de abril del 2011 el servicio de Play Station Network había sido comprometido, el hecho no fue anunciado todavía por la compañía pero lo hizo más adelante en un blog oficial.

El 20 de abril del mismo año Sony procedió al cierre de su servicio sin anunciar que había sido hackeado pero una declaración en la que decía: "Somos conscientes de ciertas funciones de PlayStation Network están deshabilitadas. Informaremos aquí tan pronto como nos sea posible con

más información. Gracias por su comprensión"[16] así entrando en modo de mantenimiento.

El 21 de abril la compañía insistió que todo eso se debía un apagón de luz antes de que todo vuelva a la normalidad, pero un blog de Sony en Europa desato la polémica al decir que se trata de un ataque hacker pero poco después viéndose obligados a retirar el anuncio.

Pero ya el 22 de abril del 2011 se confirma que es un ataque en un anuncio en su blog diciendo "Una intrusión externa en nuestro sistema ha afectado nuestros servicios de PlayStation Network y Qriocity. Con el fin de llevar a cabo una investigación a fondo y verificar el buen funcionamiento y seguridad de nuestros servicios de red en el futuro, apagamos los servicios PlayStation Network y Qriocity en la tarde del miércoles 20 de abril. La prestación de servicios de entretenimiento de calidad a nuestros clientes y socios es nuestra máxima prioridad. Estamos haciendo todo lo posible para resolver esta situación rápidamente, y que una vez más le agradecemos por su paciencia. Vamos a seguir para modificar rápidamente ya que tenemos más información que compartir."[17]

Imagen 15 Ilustración Ataque PlayStation Network
http://siliconangle.com/files/2012/08/anonymous-psn-nohack.png

[16]SONY. «Play Station Blog.» 20 de 04 de 2011. *Play Station Blog.* 21 de 09 de 2014. <http://blog.us.playstation.com/2011/04/20/update-on-psn-service-outages-2/>.

[17] —. «Play Station Blog.» 26 de 04 de 2011. *Play Station Blog.* 22 de 09 de 2014. <http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity>.

Después del ataque Sony anuncio la reconstrucción de la red, todo esto un día después del anuncio del sus ataques pero con el servicio todavía deshabilitado. Ya el 24 de abril del 2011 comenzaron a dar actualizaciones de seguridad y hacen el llamado a una empresa especialista en seguridad informática para que determine lo sucedido, un día después un portavoz de la compañía en la cede de Tokio que está realizando una investigación exhaustiva y que números de tarjeta de crédito y números personales de los usuarios habían sido comprometido, la empresa contratada por Sony para el análisis luego de todo lo sucedido concluyo que se generó efectivamente la violación de la seguridad comprometiendo la información de los usuarios fue por un ataque hacker.

El 26 de abril del 2011 Sony confirma la información robada en su blog diciendo "Gracias por su paciencia mientras trabajamos para resolver la interrupción actual de los servicios de PlayStation Network y Qriocity. Actualmente estamos trabajando para enviar un mensaje similar a la de abajo a través de correo electrónico a todos nuestros titulares de cuentas registradas con respecto a un compromiso de la información personal, como resultado de una intrusión ilegal en nuestros sistemas. Estas acciones maliciosas también han tenido un impacto en su capacidad para disfrutar de los servicios prestados por PlayStation Network y Qriocity incluyendo juegos en línea y el acceso en línea a música, películas, deportes y programas de televisión. Tenemos un camino claro para tener sistemas de PlayStation Network y Qriocity de nuevo en línea, y esperan restablecer algunos servicios en una semana."[18]

Este suceso conllevo al robo de 77 millones de cuentas de usuarios aproximadamente, que fueron extraídas desde los servidores de Sony Network siendo el robo informático de información más grande de la historia hasta esa fecha.

[18] —. «Play Station Blog .» 22 de 04 de 2011. *Play Station Blog*. 22 de 09 de 2014. <http://blog.us.playstation.com/2011/04/22/update-on-playstation-network-qriocity-services/>.

4.3 Metodología del Ataque.

4.3.1 Identificación de Vulnerabilidades

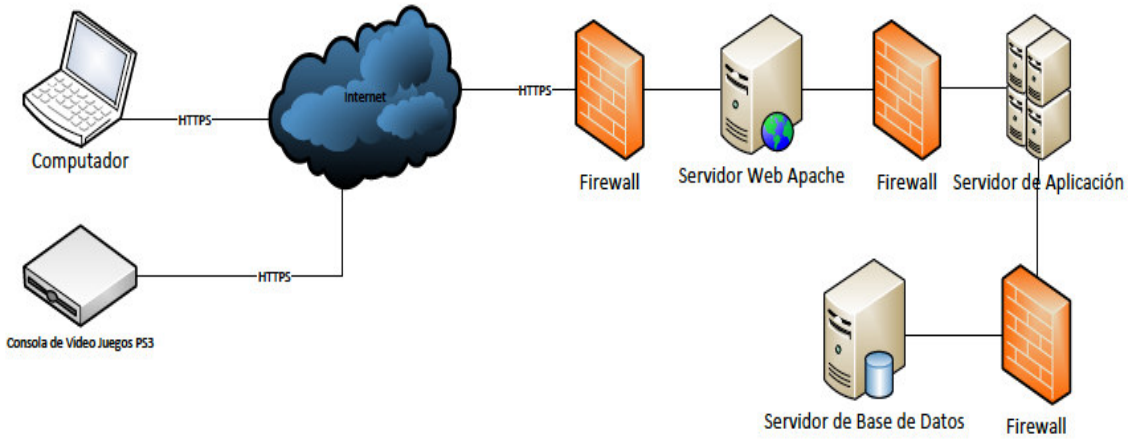


Imagen 16 Infraestructura Sony Network

Para determinar las primeras fases de exploración y reconocimiento de la anatomía del ataque a Sony Network se realizara un análisis de la infraestructura de Red comprendiendo el funcionamiento del servicio online.

Sony Network o también conocido como PSN(PlayStation Network) desde el 2006 es un servicio online ofertado por Sony que tiene como objetivo la venta de contenidos digitales tales como juegos online, películas, música, para su consolas de video juegos en este caso PlayStation 3 que fue creada para este propósito. También puede ser accedido por un computador mediante internet en la página de www.playstation.com.

Su infraestructura de red como se puede apreciar en la gráfica anterior, que su medio de conexión es por el internet y hace uso del protocolo HTTPS [19] para el transporte de datos, siendo esta desde una computadora o desde una consola de videojuegos PS3 (PlayStation 3), para acceder a todos los servicios ofertados como por ejemplo la compra de un juego.

[19] HTTPS.- Hypertext Transfer Protocol Secure (ó HTTPS) es una combinación del protocolo HTTP y protocolos criptográficos.

La utilización de servicios web es el medio de comunicación entre el usuario que se conecta por el PS3 o por un computador a los servidores de Sony Network. Un servicio web es un software que utiliza un conjunto de protocolos y estándares para intercambiar datos entre aplicaciones sin importar el lenguaje en el que estén programadas.

El protocolo HTTPS siempre va a requerir un servidor web en el caso de Sony Network un Servidor Apache con un firewall que se lo antepone para su seguridad.

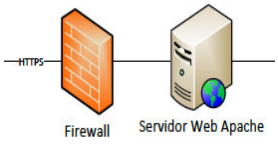


Imagen 17 Servidor Web y Firewall

Sony Network es una red interna que tiene una arquitectura de 3 capas en donde se separa la capa de aplicación, de negocio o lógica del negocio y de datos.

La capa de aplicación está conformada por el software que interactúa con el usuario en un PS3 o un computador y se comunica con la siguiente capa negociación o lógica. Aquí se incluye el servidor web que ejecuta los *web services*.

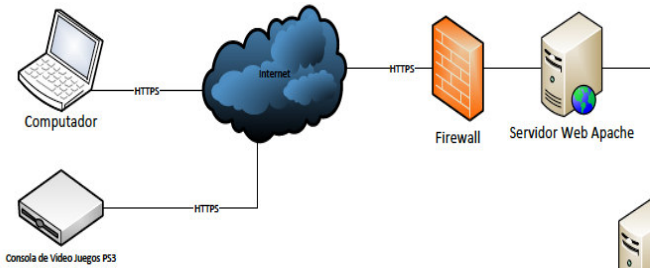


Imagen 18 Capa de Aplicación

La capa de negocio es donde se procesan las solicitudes de la capa de aplicación y está a su vez se conecta con la capa de datos donde solicita la información necesaria.

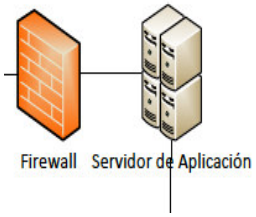


Imagen 19 Capa Lógica

Y por último esta la capa de datos que no es más que el servidor de base de datos, siendo independiente a las demás es en donde se guarda y busca la información.

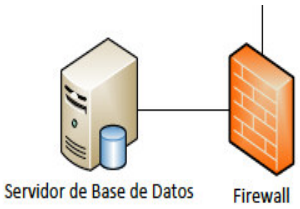


Imagen 20 Capa de Datos

En la red que mantenía PSN posee un firewall entre cada capa controlando el acceso entre las mismas, pero no fue suficiente para evitar ser atacado.

El proceso de autentificación entre las consolas de video juegos PS3 y la red de PSN es:

1. La consola de Video Juegos PS3 por medio de una conexión segura (SSL) vía internet se conecta al servidor de autentificación que sería la capa de aplicación quedando así la consola conectada con el servidor.
2. Ya establecida la conexión, la consola envía un passphrase[20] que es una contraseña con un gran número de caracteres como puede ser una frase, esto es una forma de autentificación.
3. Además de la passphrase también la consola pasa como parámetro la versión del firmware.
4. Luego se envía los parámetros de acceso para los usuarios; el nombre de usuario y la contraseña.

[20] Passphrase.- Una palabra de paso es una secuencia de palabras o de otro tipo de texto que se utilizan para controlar el acceso a un sistema, programa o datos informáticos.

5. Una vez validados todos los parámetros enviados por la consola se establece la conexión y el usuario puede realizar cualquier transacción como por ejemplo la compra de un juego o cualquier contenido digital.

El proceso de identificación y autentificación entre la red de PSN con un computador es un poco similar a la anterior con la diferencia que no se envía passphrase sino directamente se ingresa las credenciales de acceso del usuario; nombre de usuario y contraseña.

El PS3 contaba con una vulnerabilidad que permitía instalar firmware ilegal y que dejaba controlar la consola, permitiendo a los atacantes explorar sin ningún problema la red de Sony Network, en donde lograron capturar los datos que van desde la consola hacia la red, encontrando vulnerabilidades y sobre todo obteniendo parámetros que les servirían para ingresar a la red sin ser detectados por los firewall, dando como resultado el tipo de hardware de los servidores, software utilizado, la arquitectura de red, lenguajes de programación, bibliotecas, código, etc. Información que será aprovechada para la fase de explotación.

Además el análisis del tráfico entre la consola y Sony Network sirvió para comprender como funciona el protocolo de comunicación, pero dicho tráfico estaba cifrado por SSL (Secure Sockets Layer) que no son más que capa de conexiones seguras. Pero gracias a las modificaciones que podían ser instaladas en las consolas lo pudieron realizar.

Además se logró determinar que la consola enviaba la versión del Firmware y que también enviaba un passphrase como un método de autenticación, que el servidor web utilizado por Sony es WEB APACHE. Los parámetros obtenidos en esta exploración fueron esenciales para poder ingresar sin ser detenidos por los firewalls y al ser un reconocimiento activo teniendo interacción directa con la red de PlayStation Network ayudados con herramientas como por ejemplo NMAP, determinando la obsolescencia y fallo de seguridad en los servidores permitió crear una estrategia de ataque.

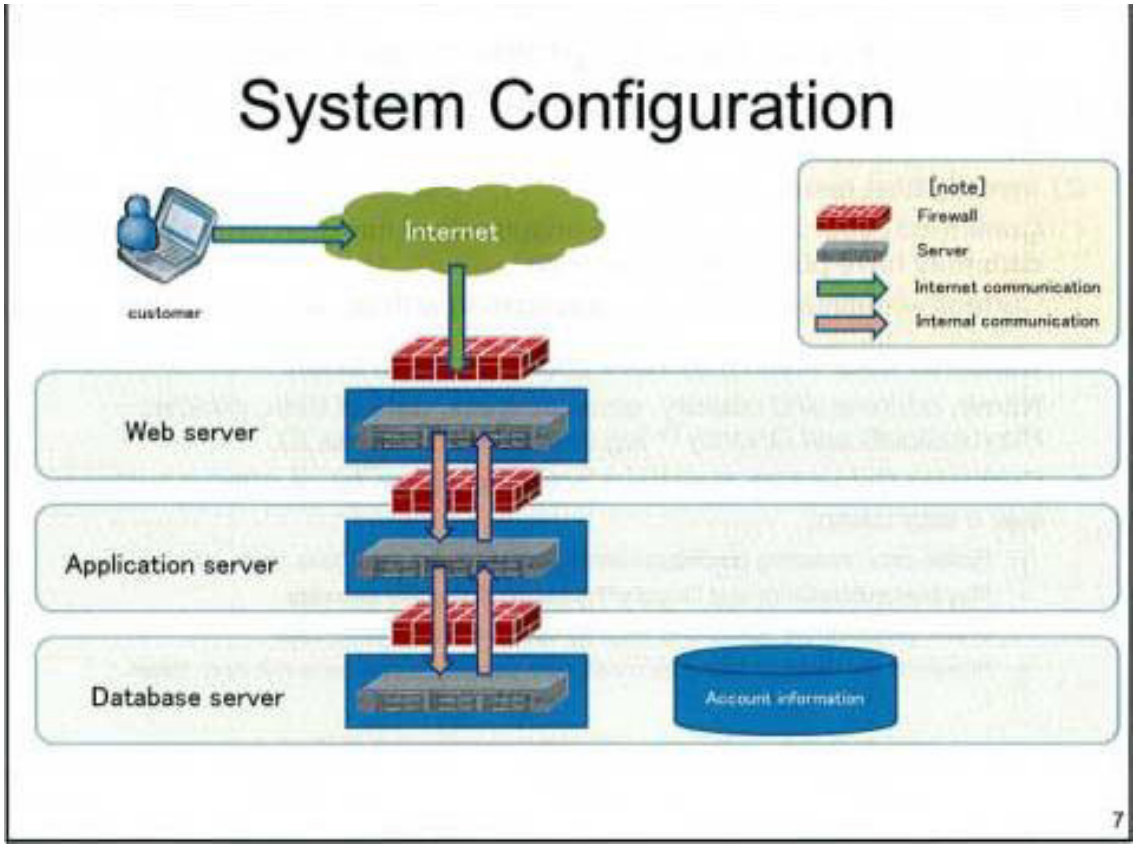


Imagen 21 Diagrama de Red según SONY

4.3.2 Obteniendo Acceso

Una vez que los atacantes han logrado comprender el funcionamiento de PlayStation Network y establecida la estrategia de ataque pueden determinar la amplitud del mismo, logrando ser indetectables hasta el momento por cualquier tipo de seguridad.

El comienzo de esta fase inicia cuando al usar un proxy anónimo obteniendo acceso sin ser detectado para interactuar directamente con los servidores como se explica a continuación.

1. Para realizarlo crearon un Certificate Authority (CA) que emita un certificado SSL con el nombre de dominio de auth.np.ac.playstatio.net que apunta al servidor de autentificación de PSN.

2. Una vez emitido el certificado SSL instalaron un servidor Proxy entre la consola y el internet configurándolo con el certificado antes creado.
3. Luego se modifica la configuración del PS3 que en vez de resolver el dominio auth.np.ac.playstatio.net se dirigía a la dirección IP del servidor proxy de los atacantes. Copiando el certificado CA creado al PS3, para que tome como valido el certificado SSL.

Todo esto implica que el PS3 resuelva la dirección auth.np.ac.playstatio.net con la proxy de los atacantes estableciendo una conexión SSL con el mismo, como el Certificado firmado por el CA creado y este dirigido al dominio auth.np.ac.playstatio.net, la consola crea una conexión autentica con el servidor de Sony. El proxy estable una conexión verdadera con el servidor Sony reenviando todo el tráfico de red al mismo. Hasta este punto los atacantes han logrado ingresar al sistema sin ser detectados.

Imagen 22 Homebrew Firmware
http://www.dpad.cl/el-desarrollo-de-juegos-homebrew-para-sony-ps3/

Pese a los varios intentos de Sony por bloquear el acceso a la red de PlayStation Network de las consolas que tenían el firmware[21] pirata o ilegal con claves de autentificación en este caso los passphrase, dejando una gran brecha de seguridad. De esta manera incapacitando totalmente contrarrestarlo, por el hecho que tendría que cambiar los root keys de las consolas dejando a un lado el funcionamiento de juegos y aplicaciones creado hasta esa fecha.

Sony en su última conferencia de prense en ese año no dio muchos detalles sobre el ataque sin embargo demostraron en imágenes como sucedió el ataque.

[21] Firmware.- Es un bloque de instrucciones de máquina para propósitos específicos, grabado en un chip, normalmente de lectura/escritura.

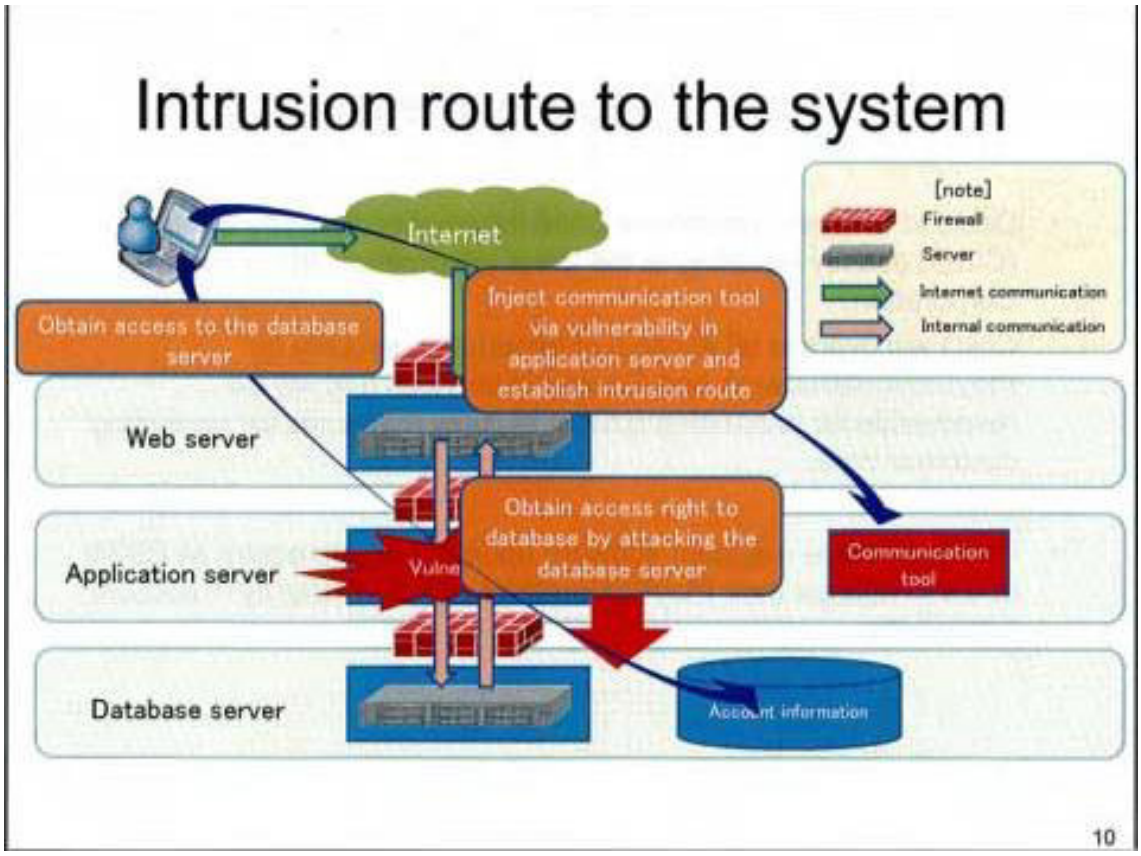


Imagen 23 Acceso PlayStation Network

Para explicar mejor el ataque y la fase de explotación se desglosara analizando el grafico que se muestra anteriormente.

1. Enviaron una transacción valida al Web Server Apache por ejemplo la compra de un juego o un video.
2. Al ser una transacción válida para el firewall deja pasar la misma comprometiendo la capa lógica dejando inservibles los mismos.
3. Envían la transacción con un código que contenía un software de comunicación que luego sería usado.
4. Se instala el software de comunicación en el servidor de aplicación
5. Comprometida el servidor de aplicación se realiza la técnica de inyección SQL suministrando sintaxis SQL dando forma a un error que devuelva la capa de datos, obteniendo resultados y posiblemente automatizando los ataques de inyección comprometiendo toda la información.

4.3.3 Manteniendo Acceso

Sin duda la fase que ayudo a los atacantes a obtener el robo de información fue esta. Por parte de Sony nunca existió una confirmación de que se mantuvo el acceso, sin embargo el análisis nos permite determinar que la herramienta de comunicación instalada fue un backdoor[22] para mantener dicho acceso, en este caso para los atacantes es importante, porque necesitan ingresar varias veces para repetir vector de ataque por la puerta trasera (Backdoor).

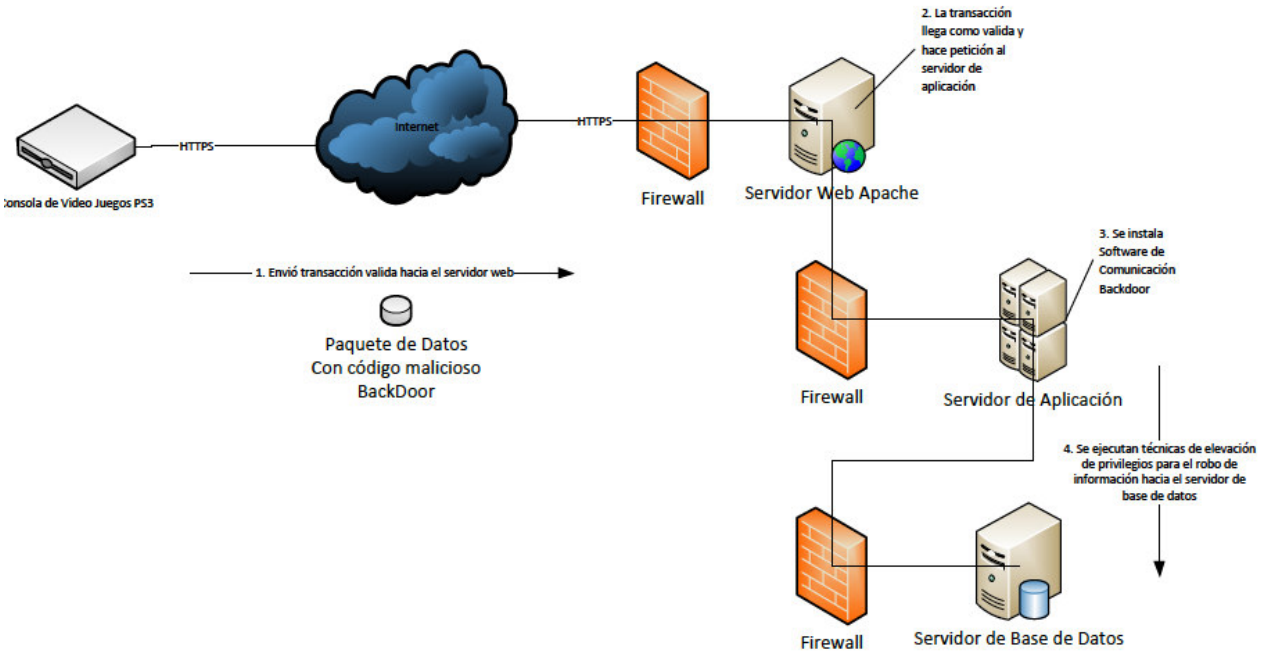


Imagen 24 Backdoor

Como se observa en el grafico el Backdoor juega un papel importante no solo al ataque, sino al robo de información como consecuencia del mismo. Esto por el hecho de que debieron probar repetidas veces ataques de inyección SQL hasta encontrar el punto débil para obtener datos.

4.3.4 Borrando Huellas

[22] Backdoor.- puerta trasera (o en inglés backdoor), en un sistema informático es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema.

Desde la primera fase los atacantes cubrieron sus huellas para no ser detectados. Esto gracias al uso de un proxy anónimo que permite interactuar con el PlayStation Network haciendo difícil detectar de donde viene el ataque.

Para los administradores de la Sony Network fue difícil identificar y bloquear por el hecho de usar el proxy anónimo, si este es bloqueado o identificado, lo único que el atacante hace es volver conectarse usando uno diferente y nuevamente obtiene el acceso.

4.4 Consecuencias

Sin duda la consecuencia más significativa para la empresa es en este caso es el robo de información sensible como lo es del número de tarjeta de crédito de los usuarios, que además también incluía la siguiente información:

- Nombre Completo
- Dirección Completa
- Email
- Fecha de Nacimiento
- Usuario Sony Network
- Contraseña Sony Network

Para la empresa el hecho de que se haya robado información de aproximadamente 77 millones de cuentas será una secuela que dejara en la historia en su imagen y credibilidad, también dejando en claro que nadie está exento de algún tipo de ataque.

En el aspecto monetario Sony por la violación a su base de datos tendrá que reponer alrededor de 1.500 millones en perdida aproximadamente esto quiere decir 20 dólares por casa uno de los usuarios.

El impacto mundial que este ataque ha generado es inevitable, esto porque algunos países analizan la posibilidad de tomar acciones legales y

consecuencia también establecer leyes de protección contra datos personales.

Países como Estados Unidos, Gran Bretaña y España con casi 30 millones de usuarios han entablado un proceso investigativo en donde determinaran si es o no culpable y por ende pagar una multa e indemnizar a los usuarios.

Además de todo esto Sony tiene que asumir los rubros investigativos contratando a empresas que se encargaran de todo este proceso y determinar el origen del ataque.

Después de todo este proceso sin duda tendrá que mejorar tanto su infraestructura como su seguridad en su red, esto generando otro gasto más para la empresa, pero necesario de acuerdo a los hechos ocurridos responsabilizándose con los datos que los usuarios confían a la empresa.

Sony Network estuvo casi un mes sin servicio generando desconfianza por parte de los usuarios y pérdida con los que decidieron cancelar su suscripción.

4.5 Contramedidas

Encriptación

Al hablar de encriptación nos referimos a cifrar la información para que esta resulte ilegible a menos que se conozca los datos necesarios para ser interpretada. Entonces la primera contramedida a establecer es mejorar dicha encriptación con la que se trasmite los datos desde la consola hasta los servidores de la compañía, ya que se contaba con un nivel de encriptación débil que los atacantes pudieron capturar datos importantes, que luego serían claves para proceder al ataque.

Esto lo podemos realizar gracias a las técnicas de encriptación que existen, con el afán de proteger como al principio de este trabajo se trata; la confiabilidad y la integridad parte de los pilares de la seguridad de la información, debido a que en este caso se maneja información sensible como números de tarjetas de crédito.

La primera técnica es el uso de **algoritmos Hash**, método que genera llaves en base de un algoritmo matemático, obteniendo como resultado un contenido ilegible y cifrado. Los más Utilizados son MD5, SHA-1 y SHA-2.

- MD5 algoritmo hash de 128 bits básico no muy recomendado.
- SHA-1 trabaja en 160 bits, es más complejo y por ende más lento al tener una mayor longitud.
- SHA-2 tiene como una salida máxima de 512 bits y combina varios algoritmos hash. Este siendo el más recomendado para este caso de análisis, sin embargo cada empresa acorde a que tan sensible es la información que se maneja se podría hacer uso de cualquiera de ellos, considerando que mientras más seguro es más lento el procesamiento y por ese motivo hay que encontrar el equilibrio entre la seguridad y la velocidad.

En sistemas operativos como Linux existen software preinstalados como md5sum y sha1sum, también en Windows el más usado Snap MD5 que permite realizar SHA-1 y MD5, dando la posibilidad de encriptar información haciendo uso de un software.

Existen también **algoritmos simétricos** que utilizan la misma clave para encriptar y desencriptar, además **algoritmos asimétricos** que combina una clave privada y pública relacionadas a una fórmula matemática compleja que es imposible de reproducir.

Otra técnica para encriptar información es el uso de una **VPN (Virtual Private Network),** que encapsula un protocolo de red sobre otro creando un canal virtual de comunicación generalmente a través de internet y que cuenta con protocolos de encriptación y seguridad, manteniendo la confidencialidad y autenticidad de la información.

El funcionamiento de una VPN se basa en un denominado protocolo túnel donde cifra los datos transmitidos desde un lado de la VPN a otro es decir al cliente.

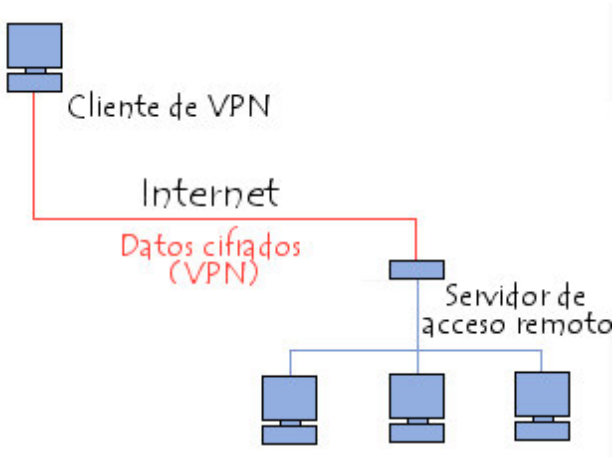


Imagen 25 Ejemplo VPN
http://static.commentcamarche.net/es.kioskea.net/pictures/initiation-images-vpnet.gif

Los protocolos más comunes de una VPN son:

- PPTP protocolo de túnel punto a punto, capa dos (Capa de enlace de datos).
- L2TP protocolo de túnel de capa dos, capa dos y contiene características de PPTP.
- Ipsec es un protocolo capa tres (capa de red) y que permite enviar datos cifrados para redes IP.

PPT cuenta con una encriptación básica de 128 bits pero trabaja a mayor velocidad, Ipsec y L2TP cuentan con una encriptación de 256 bits que comprueba la integridad de los datos y encapsula los mismos dos veces, como consecuencia es más lento pero una buena opción si la seguridad es una prioridad máxima.

Seguridad de la Información y Gestión de Eventos (SIEM)

Sin duda el ataque a Sony fue sofisticado y en la actualidad lo son aún más que dispositivos como un IDS (Sistema de detección de Intrusos) convencional no es de mucha utilidad. En este caso de análisis hubo el ingreso no autorizado y actividad maliciosa pasando desapercibida que como consecuencia lograron robar información.

En base a todo esto una contramedida a tomar en consideración es establecer un **SIEM** que ayudaría a detectar y seguir el rastro de posibles

ataques combinando la gestión de eventos (SEM) y la gestión de la seguridad de la información (SIM).

SEM nos permite observar en tiempo real y gestionar eventos de TI (Tecnologías de la Información), con la capacidad de recolectar, comparar y realizan informes con los datos de registro de actividades (logs) de los dispositivos de red; switch, routers, etc. También ayudan en el caso de un incidente a resolverlos de una manera organizada siguiendo procedimientos en el menor tiempo posible.

SIM realiza un análisis histórico presentando informes con datos de eventos de seguridad, es decir recopila, compara y realiza informes pero no en tiempo real de un repositorio de registro de actividades (logs).

Existen muchas soluciones SIEM actualmente que cuentan con SIM y SEM antes mencionados. Algunos productos ofrecen estas dos opciones, sin embargo existen otros que están más orientados a SIM que ha SEM o viceversa, por esta razón es necesario evaluar las necesidades antes de implementar una solución definitiva. A continuación algunas soluciones presentes en el mercado

- Alert Logic - Log Manager
- AlienVault - OSSIM
- ArcSight - ArcSight Enterprise Security Manager
- Cisco - Security MARS
- Enterasys - DSCC
- IBM - Tivoli Security Information and Event Manager
- NetIQ - Security Manager
- NitroView - ESM
- Q1 Labs - QRadar SIEM
- RSA Security - RSA enVision Platform
- Tenable - Tenable's Security Center 3.4 con Log Correlation Engine 3.2
- TriGeo Network Security - TriGeo SIM

Cualquiera de estas opciones u otras que sea acogida como una solución ayudara a identificar y responder a ataques que pueden pasar desapercibidos por otros sistemas, además administrar y guardar logs que generaran informes claves para la seguridad de la información.

Zona Desmilitarizada (DMZ)

La tercera contramedida a establecer es una red perimetral también conocida como zona desmilitarizada (DMZ) que se ubica entre la red interna de la empresa y la extranet en este caso el internet. Esta tiene como objetivos

Que los servidores con algún servicio público no se puedan comunicar con otros servidores o computadores que están en la red interna, con el afán de no comprometer servidores por ejemplo donde se almacene la base de datos de la empresa.

Además de la DMZ un firewall es de vital importancia cuando se implementa garantizando y ejecutando las políticas de seguridad para aislar la red interna mientras los usuarios están ingresando a la DMZ.

Los servicios más comunes que se colocan en un DMZ son:

- Servidores Web.
- Servidores de Correo.
- Servidores FTP.
- Servidores VoIP

Existen diferentes maneras de diseñar la arquitectura que compone una DMZ, pero las más comunes son con un solo Firewall y otra haciendo uso de un Firewall Doble.

Con un solo firewall se maneja al menos 3 interfaces para componer la arquitectura DMZ, en donde el primer interfaz se compone por el firewall, la red interna la segunda y la tercera la DMZ.

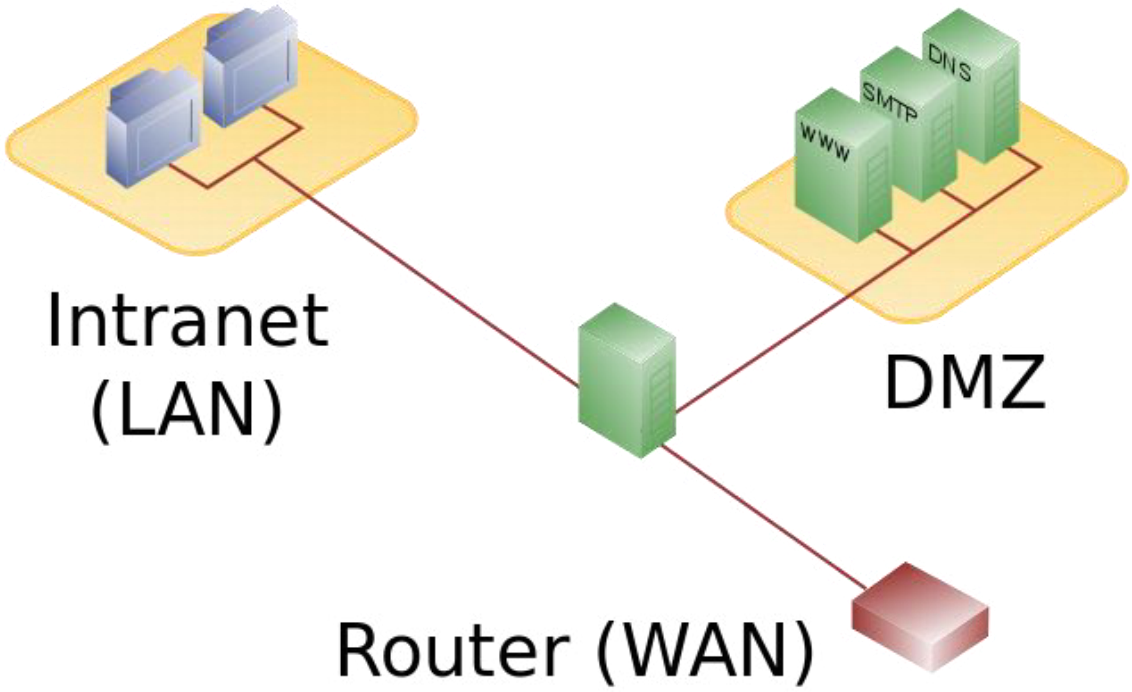


Imagen 26 DMZ Firewall Único
http://upload.wikimedia.org/wikipedia/commons/thumb/6/6f/DMZ_network_diagram_1_firewall.svg/640px-DMZ_network_diagram_1_firewall.svg.png

La segunda arquitectura es haciendo uso de firewall doble en donde el primero de ellos también conocido como "front-end" o perímetro para destinar el trafico entrante solo a la zona que requiera y el segundo de ellos llamado "back-end" o firewall interno proteja el tráfico que va de la DMZ a la red interna como lo podemos apreciar en la imagen a continuación.

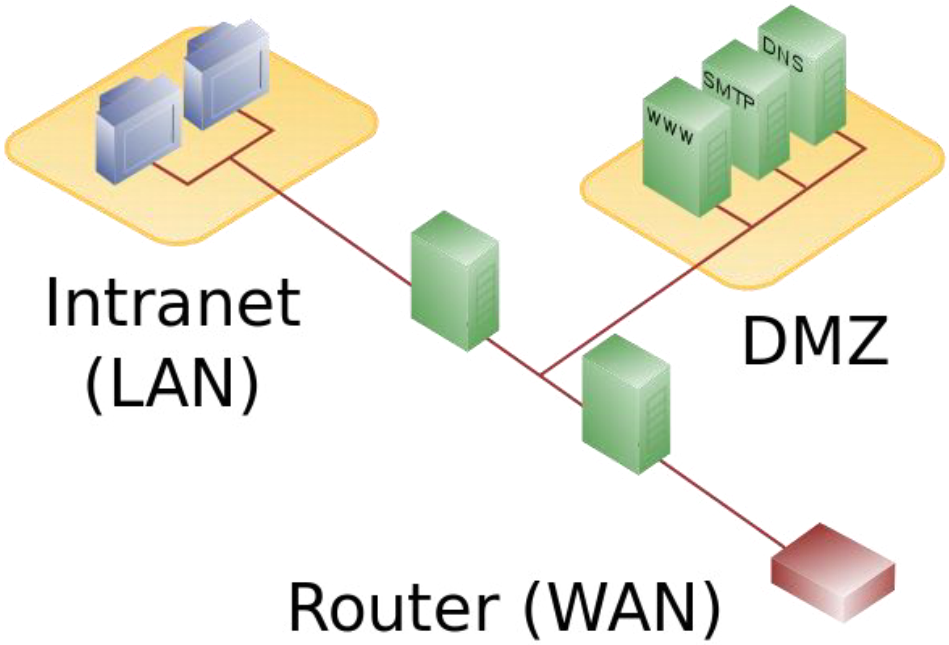


Imagen 27 DMZ Firewall Double
http://upload.wikimedia.org/wikipedia/commons/thumb/6/60/DMZ_network_diagram_2_firewall.svg/640px-DMZ_network_diagram_2_firewall.svg.png

CAPITULO 5

VIRUS INFORMÁTICO

5.1 Introducción

A través de los años los virus informáticos han evolucionado tornándose más letales en un mundo en que la tecnología se ha vuelto parte de la vida diaria. También son conocidos como malware, que no son más que programas teniendo como propósito causar algún tipo de daño en un sistema informático, su accionar va desde una simple molestia para el sistema hasta la pérdida de información valiosa.

Este capítulo tratara sobre definición historia y clasificación de los virus informáticos introducción conocimientos básicos sobre los mismos.

5.2 Historia

La historia de los virus informáticos se puede decir que su origen es desde el nacimiento mismo de las computadoras, eso gracias a John Von Neumann describiendo en su libro "Teoría y organización de autómatas" programas que se reproducían así mismo.

Años después la computación era una tecnología para un cierto grupo de organizaciones como gubernamentales, científicas o militares. En donde a pesar de existir la presencia de virus en sus sistemas no hacían públicos los mismos por no demostrar vulnerabilidad en sus sistemas de seguridad. Pero no solo las organizaciones públicas sufrían este problema, ya que las privadas como bancos no podían sacar a la luz porque simplemente perdían el prestigio y la confianza de sus clientes o accionistas.

Los virus informáticos ya conocidos con esa palabra se remonta gracias a los programadores de AT&T en 1959 donde se desarrolló un juego llamado "Core War" por Robert Thomas Morris, Douglas McIlroy y Victor Vysottsky, el cual trataba básicamente en consumir la memoria RAM del contrincante en el menor tiempo posible. Conjuntamente se desarrolló el primer antivirus llamado "Reeper" que destruía las copias hechas por el juego.

Con el nacimiento del micro computación empresas como Apple sacaron la computadora Apple II que en el año de 1982 sufrió de un ataque de un virus que se llamaba "Cloner" que se presentaba en forma de poema.

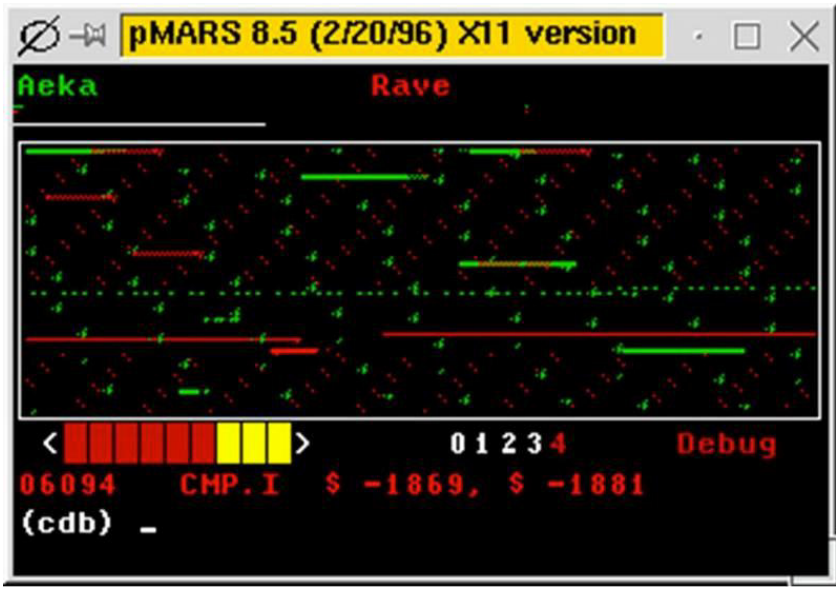


Imagen 28 CoreWars
http://bgsrms.typepad.com/photos/uncategorized/2008/08/20/dans_blog_3.jpg

No es hasta el año de 1986 que se identifica el primer virus destructivo y dañino conocido como "Brain", este tuvo la distribución por sus creadores en cd de software pirata que la gente adquiriera y ponían en sus computadoras llegando a ser infectado. El código de este virus fue modificado de tal manera que dio origen a muchos virus, cada versión siendo más nociva que la original.

En esa época las computadoras ni los sistemas estaban listos, ya que no eran tomados en serios los virus dando como consecuencia que se volviera peligroso para cualquier organización, empresa o persona con una computadora.

5.3 Definición

"Un virus informático es un programa que tiene la capacidad de causar daño y su característica más relevante es que pueda replicarse a sí mismo y propagarse a otros sistemas informáticos. Actúa sobre cualquier archivo o

sector de las unidades de almacenamiento que contenga códigos de instrucción que el microprocesador vaya a ejecutar, incluyéndose dentro de ellos y modificando su comportamiento. "[23]

Es un programa informático que se instala en un sistema computacional sin permiso y que de acuerdo a su objetivo de creación puede infectar, alterar o eliminar datos, reproduciéndose a sí mismo en algunos casos y en otros propagándose lo más que les sea posible. Teniendo un potencial daño de acuerdo a la información que logro infectar, no dependiendo de su complejidad sino del entorno donde actúa.

Las características más comunes de los virus son capaces de reproducirse a sí mismo y propagarse, puede tener un tamaño muy pequeño sin ser notado, se auto ejecuta o potencialmente ejecutable, logra tomar el control del objetivo infectado modificando otros programas a su conveniencia y logra convertir otros objetivos clones víricos.

5.4 ¿Cómo Funcionan?

Los virus informáticos cumplen un ciclo de vida el cual está desde su creación hasta la erradicación total del mismo.

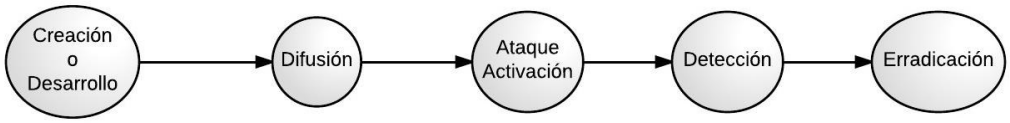


Imagen 29 Ciclo de Vida Virus Informático

El contagio es el punto de partida de un virus informático, es por donde empieza a causar daño al sistema. Se encuentra en memoria para su ejecución y las vías pueden ser desde una memoria USB o redes de datos, etc.

Su funcionamiento está determinado de acuerdo al objetivo con que el programador lo creo. Al ser pequeños en tamaño almacenado en el disco

[23] Miranda, Carlos Valdivia. *Sistemas Informáticos y redes Locales*. Madrid: Parainfo, 2014.

sin embargo tienen la necesidad de encontrar un lugar donde pueda reproducirse en donde ya fue infectado y así continuar su ciclo de vida.

Ase mucho solo lograban infectarse archivos con extensiones .exe, .com, .bat, .sys, pero ahora también se infectan a nivel de macros es decir están programados para archivos del paquete Microsoft Office.

Luego de ser contagiado el virus pasa a estar activo tomando el control del sistema y empieza se ejecuta de acuerdo con su objetivo, haciendo que el computador no tenga un funcionamiento normal esto pudiendo generar daño en los datos. El virus espera ciertas condiciones donde espera atacar o replicarse.

Su objetivo además de hacer daño es no ser detectado tanto por el usuario o por el antivirus, creciendo la amenaza. Como consecuencia puede ser molestos anuncios o mensajes, disminución considerable de velocidad de procesamiento en el computador y pérdida total de información.

Y por último paso se realiza el ataque en la cual espera la condición que el programador puso para su accionar tratándose de ocultar de los antivirus y del usuario.

5.5 Clasificación Malware (Software Malicioso)

Se dice Malware a todo programa malintencionado que ingrese a un sistema sin autorización y cause cualquier tipo de daño al mismo. A continuación se definen los más comunes.

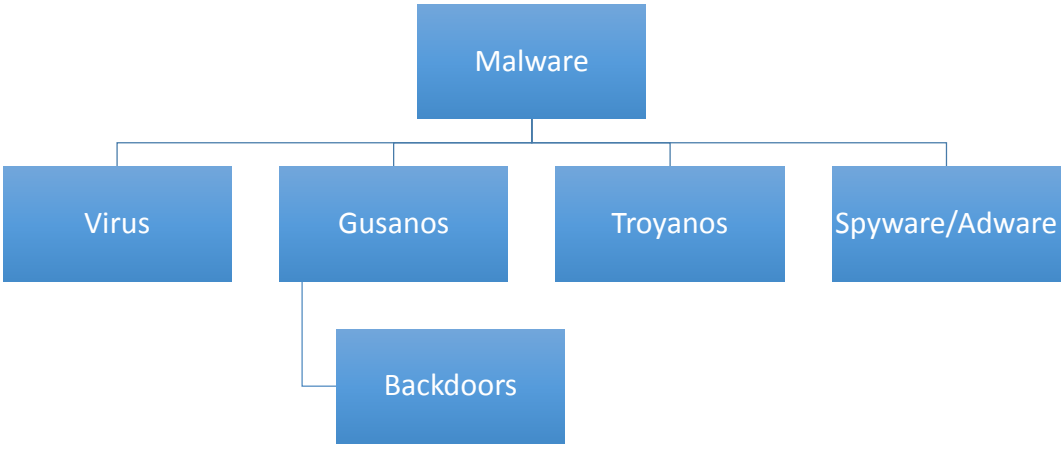


Imagen 30 Clasificación de Malware

5.5.1 Virus

El virus informático, como tal es un programa malicioso que modifica el comportamiento de un computador sin el consentimiento del usuario.

Su forma de propagarse es adjuntándose en archivo o un programa generando infección en los ordenadores mientras se transporta por cualquier medio de un computador a otro y dañando a su paso hardware, software o archivos.

En la gran parte estos están ligados en un archivo ejecutable, este no siendo infeccioso hasta que se lo ejecute. Pero en muchos de los casos el propio usuario es el causante de esa infección al ejecutarlo. La propagación muchas de las veces el usuario es el causante ya que él envía archivos infectados por ejemplo vía mail, o transportando en una memoria USB.

La principal característica de un virus a comparación de otro tipo de malware, es de auto reproducción y sobre todo sobre cargar los recursos del sistema por ejemplo memoria RAM.

Con el auge del internet en la actualidad son más comunes los gusanos que los virus por sus características. Esto llevando a los medios de protección como los antivirus expandan para cubrir gusanos, troyanos o spyware.

5.5.2 Gusanos

Los gusanos o worm en el idioma inglés son una subclase de los virus, siendo el medio de propagación el internet o una intranet con una replicación e instalación semiautomática ya que el usuario a veces tienen participación.

Los medios de propagación más comunes son:

- Archivos adjunto de un mail
- Enlace a un recurso web
- Enlace enviado desde un sistema de mensajería instantánea
- Archivos P2P(entre pares)
- Paquetes de datos en redes.

Una vez que el gusano se encuentra dentro de su objetivo de una manera activa su replicación se vuelva automática, esto a una gran escala. Teniendo más índice de propagación de los virus tradicionales por su velocidad de propagación es debido al internet con el que contamos actualmente y la capacidad de transmitir paquetes de datos rápidamente, también esto implica factores como los mecanismos de propagación la infraestructura de red y como está programada para saber cuál es su objetivo potencial. El problema que esto genera que los antivirus están basados en firmas no logren detectarlo ya que todavía no constan en la misma.

Además de su característica principal de replicación tiene como característica secundaria no tener un host o un fichero para reproducirse.

5.5.2.1 Backdoors

Es un programa que se introduce en un sistema sin representar amenaza alguna en el momento aparentando ser inofensivo, generalmente es una parte del código existente en un troyano

Su objetivo como dice su nombre es establecer una puerta trasera que luego será utilizada por el atacante permitiéndole en muchos de los casos comprometer información confidencial de los usuarios del sistema atacado. El accionar de un backdoor es mucho más nocivo que un troyano ya que

nos permiten abrir puertos de comunicación, además capturan datos y los envían a una dirección externa establecida.

Loas Backdoors están siempre a la escucha de instrucciones en donde el atacante puede realizar acciones particulares como por ejemplo instalar otra aplicación sin ser detectado o que necesite permiso alguno por parte del usuario.

5.5.3 Troyanos

Son programas que aparenta ser legítimos y de cierto modo útil para el usuario. Pero en realidad son maliciosos e incapaz de reproducirse a sí mismo como los casos anteriores. El objetivo de un troyano no es ser un huésped destructivo sino brindar un acceso remoto al atacante donde pueda ejecutar botnet, instalar un programa que puede ser malicioso, robar información, ejecutar procesos, etc.

Se dice troyano porque su funcionamiento se homologa al caballo de Troya que se menciona en la novela de Homero "La Odisea".

Diseñados para creer una puerta trasera permitiendo un acceso remoto, dando como consecuencia que el atacante realice tareas en donde no necesite un permiso. En la actualidad y con el auge de la movilidad son estos dispositivos móviles los más afectados, ya que no tienen ningún control cuando se bajan aplicaciones fraudulentas de las tiendas de los fabricantes y que tienen el mismo objetivo y efecto que en una computadora.

La arquitectura en la que se basa un troyano es cliente- servidor, ya que el computador infectado será un cliente que este a la escucha de una petición del servidor en este caso el atacante y a su vez este pueda ejecutar un proceso o función en específico. Para tener ese tipo de arquitectura el troyano consta de un programa que administra a otro programa que recibe la orden y hasta puede devolver un resultado.

5.5.4 Spyware

También llamado un programa espía cuyo objetivo es ser instalado en un computador para recopilar la información de su víctima como los datos de los usuarios y esta llega manos de empresas pero sin consentimiento de su dueño. Esto se utiliza con fines publicitarios o beneficios económicos.

El medio de transmisión es la internet esto hace que el consumo de ancho de banda sea mayor, afectando no solo al rendimiento de red de ese computador sino de toda la infraestructura. Su vía de infección puede ser por un troyano, un virus, visitar páginas web que explotan un código por una determinada acción del usuario, etc.

Los datos más comunes que recopilan son mensajes, contactos de correo electrónico, dirección IP, DNS, teléfonos, claves privadas como por ejemplo de email, entre otros. Pero su uso no se limita por empresas que lucran de esta información sino también de organismos gubernamentales que sacan partida para detener a cualquier tipo de delincuente.

Además de robar información pueden ser los causantes de disminuir Memoria RAM, utilizar espacio en el disco duro, disminuir rendimiento del procesador, afectar otros programas, mostrar anuncios emergentes en navegadores.

5.5.5 Adware

Un Adware es básicamente un programa creado para mostrar publicidad, cuya diferencia con un spyware es que el usuario autoriza su instalación. Esto se debe a que este tipo de malware viene incluido en programas tipo Shareware que no son más que versiones de evaluación de software con algún tipo de limitación que el pagado y que al aceptar los términos de legales cuando se está instalando dan pasó a un Adware.

Estos programas llegan no solo a ser un malware sino con su publicidad llega a ser una molestia poder trabajar en ese software. Por la publicidad que estos muestran en software, pero ahora también se instalan en los navegadores de internet tornándose peligrosos, ya que abre ventanas emergentes direccionando al usuario a sitios no deseados en donde se pueden encontrar un virus, troyano o un gusano.

CAPITULO 6

CASO DE ANALISIS MYDOOM

6.1 Introducción

En el capítulo a continuación se realiza un análisis del gusano MYDOOM identificando las fases de su accionar, cuál era su objetivo, las consecuencias que dejo a su paso y por ultimo plantear contramedidas a este malware clasificado como de tipo gusano.

6.2 Antecedentes

MyDoom.A tuvo nacimiento en el 2004 e identificado por primera vez el 26 de enero del mismo año, considerado hasta esa fecha como gusano con más rápida propagación en la historia de la informática, que tenía un principal foco de infección hacia computadoras con Sistema Operativo Microsoft Windows.

El 26 de Enero del 2004 cuando se identifica por primera vez el gusano MyDoom.A denominado así por su objetivo y su accionar, después vendrían versiones diferentes del mismo. En esa misma fecha se localiza su origen en Rusia pero no a su creador, su propagación es por email utilizando los contactos que se tiene almacenados en el computador infectado y con un propósito adicional el cual era realizar un ataque de Denegación de Servicio Distribuido a la página de la compañía **SCO Group**[24]

Ya el 27 de febrero del 2004 gracias a la ingeniería inversa aplicada en el virus determinan el código de programación y las funciones que contiene, una vez con esta información se procede con algún tipo de vacuna que lo mitigue y otra lo desinfecte. La compañía ese mismo día SCO Group ofrece un recompensa para quien determine el creador y se dé información del mismo, así también organizaciones gubernamentales como FBI y CIA ponen en marcha una investigación con el mismo propósito.

[24] **SCO Group** .- The TSG Group, previamente conocido como SCO Group y antes como Caldera Systems y Caldera International, es una corporación que asociada en sus orígenes a Linux y el movimiento software libre, desarrollaba distribuciones Linux para servidores y estaciones de trabajo.

Dos días después de que apareciera el gusano el 28 de febrero del mismo año se descubre una nueva versión denominado MyDoom.B teniendo el mismo método de propagación y todo exactamente igual al primero hasta su origen ruso, pero con la diferencia que el ataque de denegación de servicio distribuida está enfocado a la página web www.microsoft.com. A demás esta versión viene con un extra que es bloquear el acceso a páginas de empresas de seguridad informática, bloquear anuncios de tipo pop-up en los navegadores.

El 29,30 y 31 de Enero del 2004 MyDoom.A mantienen un elevado nivel de propagación pero su segunda versión empieza a declinar por errores de programación y Microsoft ofrece una recompensa por el creador de MyDoom.B.

El ataque de denegación de servicio distribuido de MyDoom.A fue programado para el 1 de febrero del 2004 hacia la compañía SCO Group, esto siendo posible gracias a todos los computadores infectados con el gusano y que sirven como zombis para realizarlo, no se hace ninguna declaración por parte de la compañía perjudicada sin embargo su dominio deja de funcionar dejando sin acceso a los usuarios.

El 3 de febrero del 2004 comienza el ataque programado por MyDoom.B hacia la página web www.microsoft.com pero con un mínimo impacto ya que su nivel de propagación no fue el mismo que la primera versión, también hay que destacar la seguridad y la preparación por parte de Microsoft para soportar un elevada carga a sus servidores.

Para el 12 de febrero del 2004 el gusano MyDoom.A está programado para detener su propagación, el motivo es desconocido pero dejando una secuela y daños a su paso irreversible. Uno de ellos es el puerto trasero al habilitar un puerto en los computadores infectados generando una vulnerabilidad y pudiendo ser usado por algún otro software malicioso.

El 1 de marzo del 2004 la segunda versión del gusano MyDoom.B detiene su propagación tal como fue programada, dejando el mismo puerto abierto que su antecesor.

Estas primeras versiones fueron el inicio para que luego aparecieran otras más, por ejemplo el 26 de julio del mismo año su variante ataca buscadores como Google, AltaVista y Lycos realizando un ataque de denegación de servicio distribuido deteniendo su funcionamiento. Inclusive aparecen muchas versiones más generando una preocupación de una versión más catastrófica.

Luego de unos años exactamente en el 2009 vuelve a aparecer el gusano pero esta vez sus ataques son contra Corea del Sur y Estados Unidos, esta fue la última vez que genero algún tipo de problema pero su larga trayectoria dejo mucho daño.

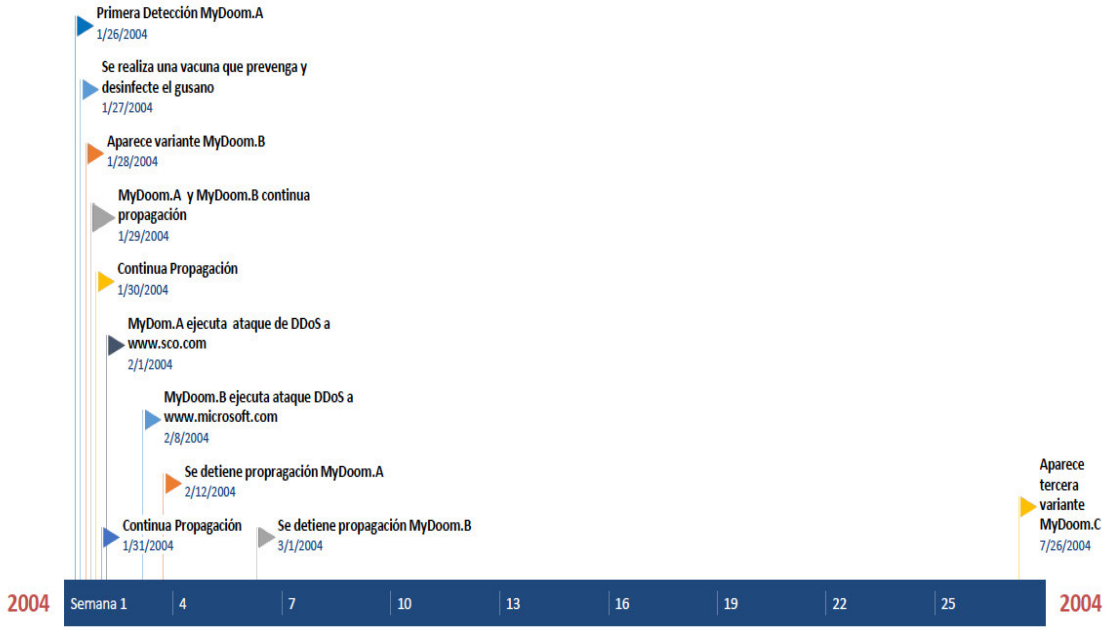


Imagen 31 Cronología Gusano MyDoom.A y sus variantes en el 2004

6.3 Análisis de Gusano MyDoom.A

6.3.1 Análisis Estático

Un análisis estático de un malware es realizado sin ejecutar el código malicioso dentro de él, tratando de determinar si un archivo es o no maligno, proporcionando información sobre su contenido.

Sabiendo esto se realizara un análisis estático básico del gusano MyDoom.A, en primer lugar hay que considerar que el gusano se expandirá solo si se

cumplen dos condiciones; cundo el usuario abre un archivo infectado y que no posea una base de actualizada en su antivirus.

6.3.1.1 Protocolos / Servicios / Aplicaciones

El gusano MyDoom.A tiene como medio de propagación vía mail o el software de intercambio P2P[25] Kazaa. Una vez instalado en el sistema instalara su propio SMTP, DNS y Backdoor en los puertos que comprenden entre 3178 al 3198 TCP, además genera un ataque DoS contra www.sco.com del 1 de febrero del 2004 al 12 de febrero del 2004.

El medio de propagación vía email se envía desde la computadora infectada es usando SMTP[26] que es el puerto 25 TCP.

Al contrario el otro medio de propagación es Kazaa un servicio de intercambio de archivos P2P disponible para cualquier usuario, que comparte grandes cantidades de información con cero costo. Trabaja con protocolos de red TCP/UDP en el puerto 1214 inicialmente, caso que no estuviere disponible ese puerto utiliza cual quiera que comprendiera desde 1000 al 4000.

El gusano solo afecta a sistemas operativos Windows a continuación una lista de las versiones que se ven afectadas, hay que considerar que el gusano se propaga por autorización del usuario y al faltar los parches de seguridad en el sistema se verán afectados.

Sistema Operativo
Microsoft Windows 9x
Microsoft Windows ME
Microsoft Windows NT
Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows Server 2003

Tabla 3 Sistemas Operativos infectados MyDoom.A

[25] P2P.- Peer to peer red que permite a todo usuario actuar esencialmente como cliente y servidor.
[26] SMTP.- Protocolo para transferencia de email entre servidores de correo electrónico.

6.3.1.2 Análisis VirusTotal

Para realizar el análisis estático el gusano será subido el archivo para ser analizado por la página web www.virustotal.com, un servicio gratuito para determinar si es malicioso o no.

El primer resultado que nos muestra al analizar el archivo es el siguiente.

Imagen 32 Análisis VirusTotal MyDoom.A

SHA256 es una función hash que viene a ser como una firma única para un texto especifico. También nos indica que de 57 antivirus 52 lo detectan y la fecha del último análisis que se realizó sobre el archivo.

Como información adicional obtenemos la siguiente información en donde nos indica que el tipo win32 EXE del archivo, el tamaño del fichero, como la información más importante a ser considerada y las tres primeras filas de la gráfica son las firmas digitales del malware.

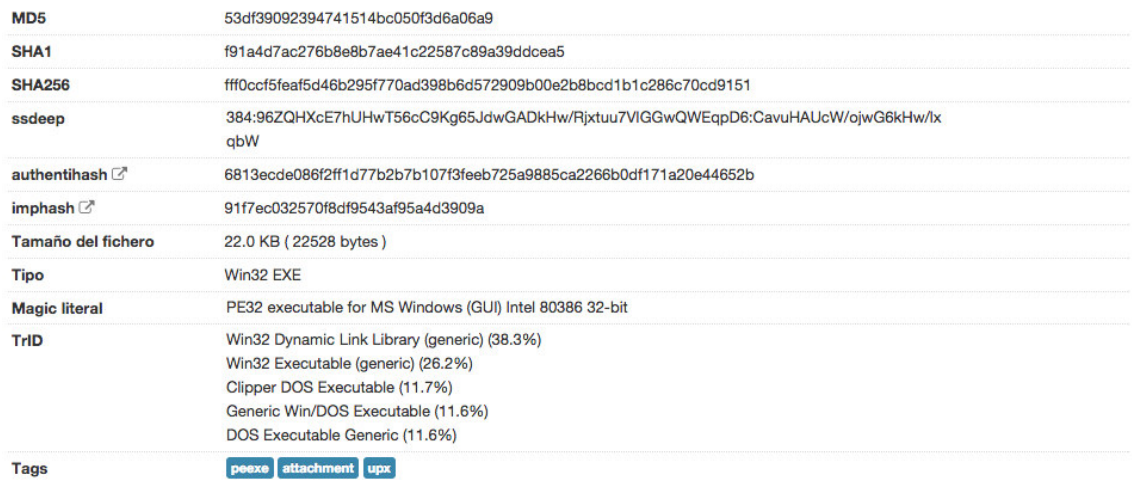


Imagen 33 Análisis VirusTotal MyDoom.A

En la tabla a continuación indica los antivirus que detectan este malware.

Antivirus	Resultado	Actualización

ALYac	Worm.Mydoom	20150223
AVG	I-Worm/Mydoom.A	20150223
AVware	Trojan.Win32.Generic!BT	20150223
Ad-Aware	Trojan.Waledac.EN	20150223
Agnitum	I-Worm.Mydoom.A	20150222
AhnLab-V3	Worm/Win32.MyDoom	20150222
Antiy-AVL	Worm[Email]/Win32.Mydoom	20150223
Avast	Win32:Mydoom-CA [Wrm]	20150223
Avira	Worm/Mydoom.A.3	20150223
Baidu-International	Worm.Win32.Mydoom.a	20150222
BitDefender	Trojan.Waledac.EN	20150223
Bkav	W32.MyDoom.Worm	20150213
CAT-QuickHeal	W32.Mydoom	20150223
CMC	Generic.Win32.53df390923!MD	20150223
Comodo	Worm.Win32.Mydoom.A	20150223
Cyren	W32/Mydoom.YNRP-3556	20150223
DrWeb	Win32.HLLM.MyDoom	20150223
ESET-NOD32	Win32/Mydoom.A	20150223
Emsisoft	Trojan.Waledac.EN (B)	20150223

F-Prot	W32/Mydoom.A@mm	20150223
F-Secure	Trojan.Waledac.EN	20150222
Fortinet	W32/MyDoom.GA!dam	20150223
GData	Trojan.Waledac.EN	20150223
Ikarus	Worm.Win32.Mydoom	20150223
Jiangmin	Worm/Mydoom.cw	20150222
K7AntiVirus	EmailWorm (000043061)	20150222
K7GW	EmailWorm (000043061)	20150223
Kaspersky	Email-Worm.Win32.Mydoom.a	20150223
Kingsoft	Worm.MyDoom.a.(kcloud)	20150223
McAfee	W32/Mydoom.a@MM	20150223
McAfee-GW-Edition	BehavesLike.Win32.Mydoom.mc	20150222
MicroWorld-eScan	Trojan.Waledac.EN	20150223
Microsoft	Worm:Win32/Mydoom.A@mm	20150223
NANO-Antivirus	Trojan.Win32.MyDoom.bjbv	20150223
Norman	MyDoom.A	20150222
Panda	W32/Mydoom.A.worm	20150222
Qihoo-360	Win32/Worm.Email-Worm.e7b	20150223
Rising	PE:Trojan.Win32.Generic.1396D242!328651330	20150222

SUPERAntiSpyware	Trojan.Agent/Gen-Cryptic	20150222
Sophos	W32/MyDoom-A	20150223
Symantec	W32.Mydoom.A@mm	20150223
Tencent	Win32.Worm-email.Mydoom.Swvf	20150223
TheHacker	W32/Mydoom@MM	20150222
TotalDefense	Win32/Mydoom.A	20150223
TrendMicro	WORM_MYDOOM.BU	20150223
TrendMicro-HouseCall	WORM_MYDOOM.BU	20150223
VBA32	Win32.Backdoor.Novarg.A	20150220
VIPRE	Trojan.Win32.Generic!BT	20150223
ViRobot	Trojan.Win32.Mydoom.22528[h]	20150223
Zillya	Worm.Mydoom.Win32.4	20150222
Zoner	I-Worm.Mydoom.A	20150220
nProtect	Worm/W32.Mydoom.22528	20150218
AegisLab	No detecta	20150223
Alibaba	No detecta	20150223
ByteHero	No detecta	20150223
ClamAV	No detecta	20150223
Malwarebytes	No detecta	20150223

Tabla 4 Antivirus que detectan MyDoom.A
https://www.virustotal.com/es/file/fff0ccf5feaf5d46b295f770ad398b6d572909b00e2b8bcd1b1c286c70cd9151/analysis/

PE header basic information	
Target machine	Intel 386 or later processors and compatible processors
Link date	1:00 AM 1/1/1970
Entry Point	0x0000BE60
Number of sections	3

Imagen 34 Cabecera PE

Este resultado nos demuestra que el archivo es de tipo ejecutable portátil, es decir un archivo de Windows .EXE para sistemas operativos de 32 bits del subsistema Windows GUI.

Los PE imports son las funciones de un software realizando llamados a otros archivos esto por lo general en un malware utiliza varias DLL que proporcionan funcionalidad para el sistema operativo Windows.

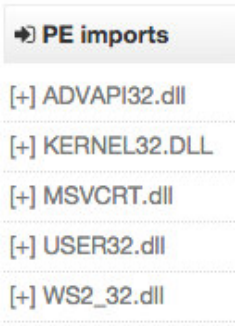


Imagen 35 PE Imports

Como se puede apreciar en la gráfica anterior son las DLL a los que ataca el gusano MyDoom.A. El KERNEL32.DLL es el más relevante de todos, puesto que la mayor parte de funciones de las ventanas del sistema operativo se conecta a esta DLL. Además de ser un archivo ejecutable lee y modifica los valores del registro, también crea y modifica las claves del registro.

6.3.1 Análisis Dinámico

El análisis dinámico es básicamente el comportamiento del malware, es decir su actividad en el sistema objetivo. Por lo general se realiza el análisis en un sistema controlado en una máquina virtual bloqueando el acceso de red para posible infección por ese medio, en este caso se realizara en una máquina virtual con sistema operativo Windows XP service pack 1, sin antivirus o protección que nos permita hacer el análisis.

Lo primero que hace el gusano es mostrar una ventana con caracteres sin sentido cuando se realiza doble clic sobre el archivo.

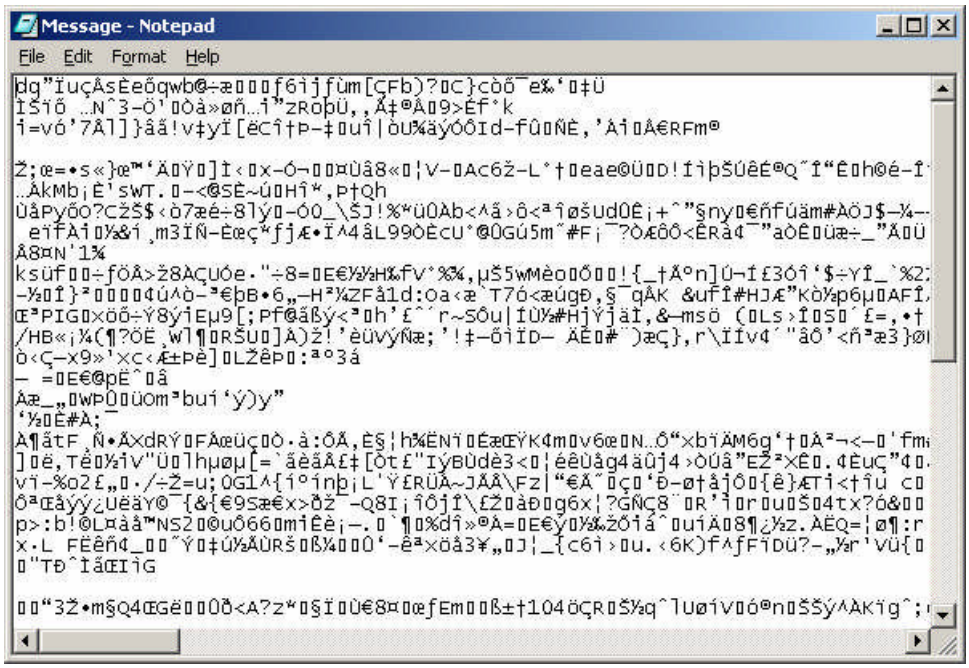


Imagen 36 Ventana de Caracteres MyDoom.A

Una vez ejecutado dicho archivo el accionar normal de un usuario es cerrar la ventana, pero el gusano deja una puerta trasera, es decir el puerto abierto que es 3127 para un posible ataque futuro. Para determinar esto se ejecuta en el CMD del sistema operativo el comando netstat -an que nos indica que puertos están a la escucha es decir abiertos.

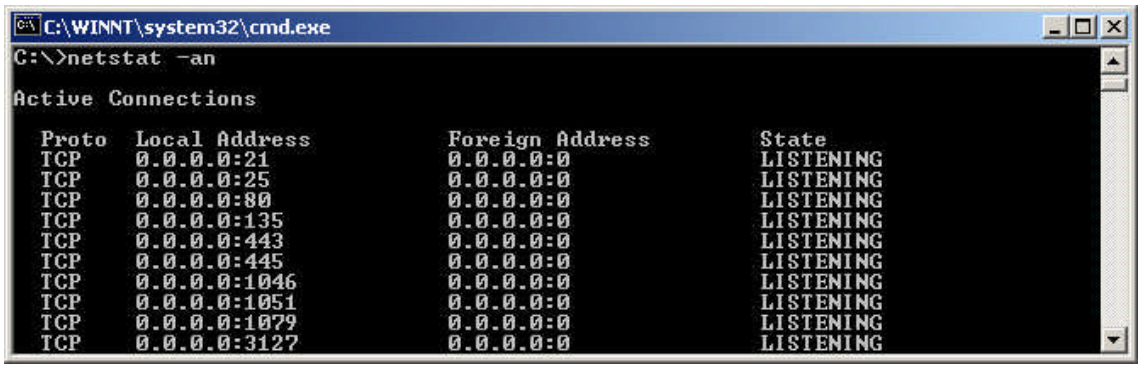


Imagen 37 Ejecución Comando netstat-an

Además de realizar esta acción el gusano crea llamado a la librería SHIMGAPI.DLL. Es añadido el archivo por sí mismo a la siguiente dirección C:\Windows\System32 y crea la llave de registro en el sistema HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32

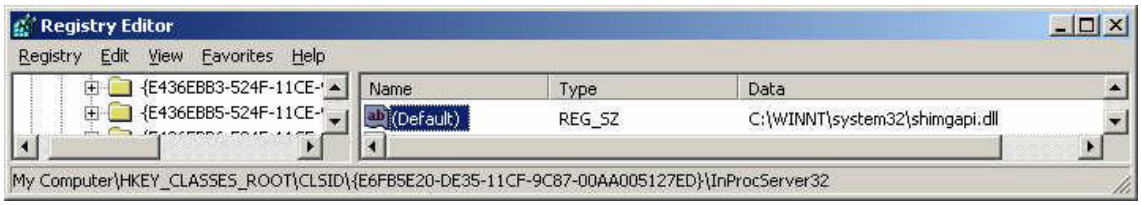


Imagen 38 Comportamiento de Gusano Registro del Sistema

Además cuando se ejecuta el gusano se copia así mismo como taskmon.exe en la siguiente dirección C:\Windows\System32 y se añade las llaves de registro de este archivo en las siguientes ubicaciones HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run y HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run como podemos apreciar en los gráficos.

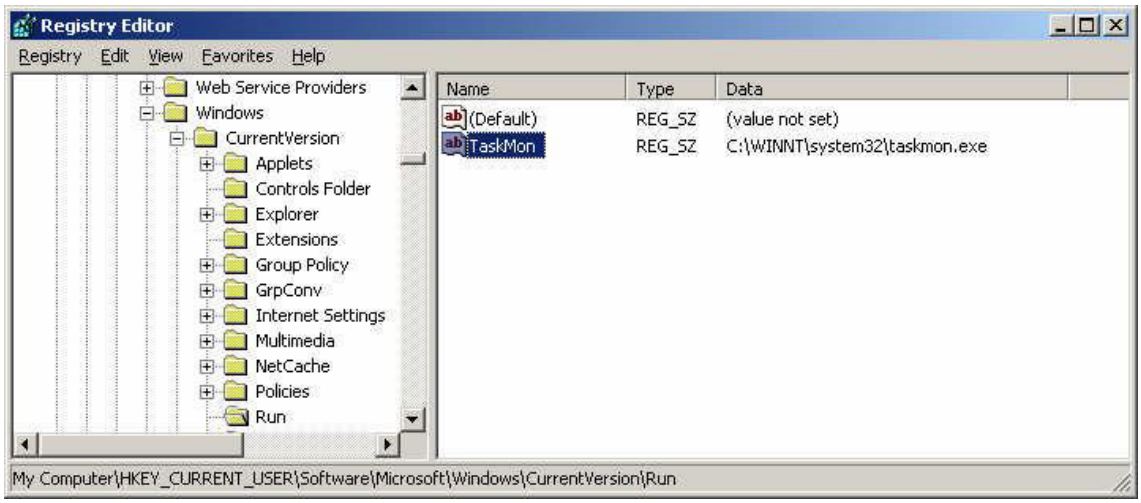


Imagen 39 Registro del Sistema TaskMon

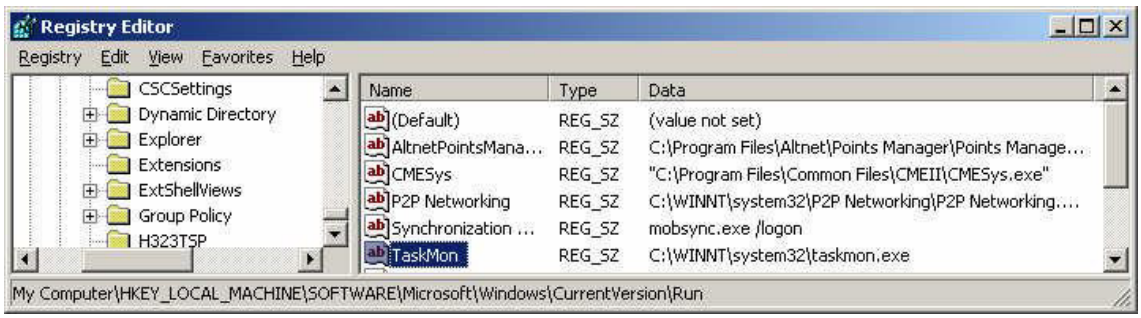


Imagen 40 Registro del Sistema TaskMon Modificado

Lo esencial de una infección con el gusano MyDoom.A es la creación de llaves en el registro del sistema. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\

Explorer\ComDlg32\Version y HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version.

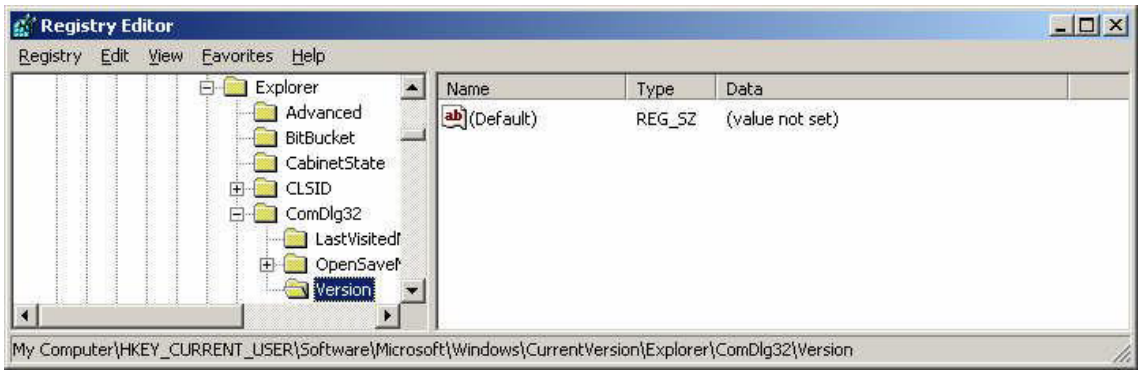


Imagen 41 Registro del Sistema ComDlg32

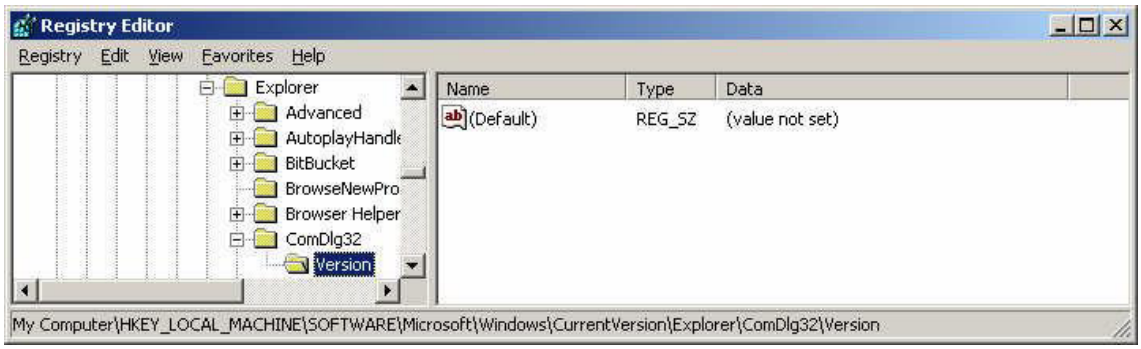


Imagen 42 Registro del Sistema ComDlg32 Modificado

Ya una vez que el gusano añade sus archivos crea y modifica llaves del registro, hace uso de la puerta trasera previamente instalada para su propagación.

MyDoom.A busca direcciones de correo electrónico con muchas extensiones con el afán de que utilizando su propio SMTP se propague. Este correo electrónico puede contener diferentes asuntos, contenidos y archivos adjuntos que servirán para la infección si son ejecutados.

El contenido del mensaje puede contener lo siguiente.

Asunto: También está hecho de tal manera que confunda al usuario poniendo como asuntos:

- test
- hi
- hello
- Mail Delivery System
- Mail Transaction Failed
- Server Report
- Status
- Error

Contenido: Según el encabezado y el asunto hace que se complemente con el contenido para crear un mejor engaño al usuario poniendo unos de estos mensajes:

- Mail Transaction Failed. Partial message is available.
- The message contains Unicode characters and has been sent as a binary attachment.

- The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

Archivo Adjunto: Tanto el nombre del archivo como su extensión que el gusano genera son de una manera aleatoria estos pudiendo ser:

Nombres Posibles: DOCUMENT, README, DOC, TEXT, FILE, DATA, TEST, MESSAGE, BODY

Extensiones Posibles: PIF, SCR, EXE, CMD, BAT, ZIP, HTM, TXT o DOC.

Imagen 43 Ejemplo archivo adjunto MyDoom.A
http://www.vsantivirus.com/mydoom.gif

6.4 Metodología del Ataque

6.4.1 Identificación Vulnerabilidades.

El análisis del gusano MyDoom.A parte desde la identificación de vulnerabilidades es decir de la primera fase de la anatomía de un ataque (Reconocimiento), ya que el origen del mismo no forma parte de este análisis ni a sus variantes.

Se puede decir que no hay fase de reconocimiento ejecutado por los guanos MyDoom.A sabiendo que el gusano es un programa de auto-propagación, aunque extrae las direcciones de correo electrónico en la máquina del usuario infectada sin consentimiento del mismo. MyDoom.A busca en los directorios de posibles libretas de direcciones de correo electrónico. Una vez que un archivo apuntado se encuentra, las direcciones de correo electrónico serán utilizadas para el envío posterior del gusano y para encontrar posibles servidores de correo a las que enviarse y continuar con su propagación.

Parte de la identificación de vulnerabilidades es la fase de **exploración** en esta versión del gusano MyDoom.A no existe dicha exploración sin embargo en su variante Mydoom.C está programado para escanear direcciones IP al azar utilizando los puertos TCP desde 3127-3198, este rango de direcciones abierto por las primeras versiones del gusano.

Una vez que una dirección se encuentra con un puerto TCP abierto, Mydoom.C se enviará una copia de sí mismo a través del puerto abierto y tratar de instalar en la máquina víctima. La instalación del gusano MyDoom.A es necesario para que el Mydoom.C pueda tener un puerto de acceso abierto. Detección de la exploración ejecutados por el gusano Mydoom.C puede ser posible por ver tráfico en el puerto 3127.

6.4.2 Obteniendo Acceso

El gusano MyDoom.A tiene dos tipos de explotación un local cuando infecta el computador y otra externa que es el ataque de denegación de servicio para la cual fue programada.

Antes que el gusano sea explotado por el computador la composición del mensaje de correo electrónico es la siguiente:

Remitente: Este es falsificado para confundir al usuario por ejemplo puede estar como Mail Administrador.

Gracias al contenido del mensaje hace que el usuario y la ingeniería social detrás del gusano MyDoom.A deja por demostrado lo fácil de explotar un sistema sin necesidad de conocerlo profundamente y obtener información como este caso las dirección es de correo electrónico.

Luego de recibir el mensaje el gusano una vez en el computador comienza con la ejecución del archivo que se encuentra disfrazado por otro que es ejecutable, una vez que este es ejecutado lo valores en el registro de sistema operativo Microsoft Windows son modificados. A continuación los registros modificados:

1. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
2. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Estas entradas de registro permiten que programas o aplicaciones se inicialicen conjuntamente con Windows y estos cambios se producen de manera encubierta para que el gusano no sea detectado en el computador y poder mantener el acceso, haciendo más fácil el ataque de denegación de servicio y la infección a otros computadores atreves del puerto que deja abierto.

Como segundo paso de explotación tenemos la creación de una llave en el registro del sistema la cual se encuentra en la siguiente ubicación HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ que hará que el virus se ejecute una vez que el computador es reiniciado.

Ya realizada la fase de explotación a nivel local del gusano, continua con dicha explotación a nivel externo es decir que una vez instalado u ejecutado está programado para enviar peticiones a la dirección IP de la página web de la Organización SCO.

Estas peticiones generadas por el gusano hacen que el sistema operativo se torne relativamente lento al dar mucha carga de trabajo al procesador.

Para realizar el ataque de denegación de servicio a la página web objetiva el gusano envía peticiones SYN a través del puerto 80. Haciendo una inundación SYN que es un tipo de ataque de denegación de servicio.

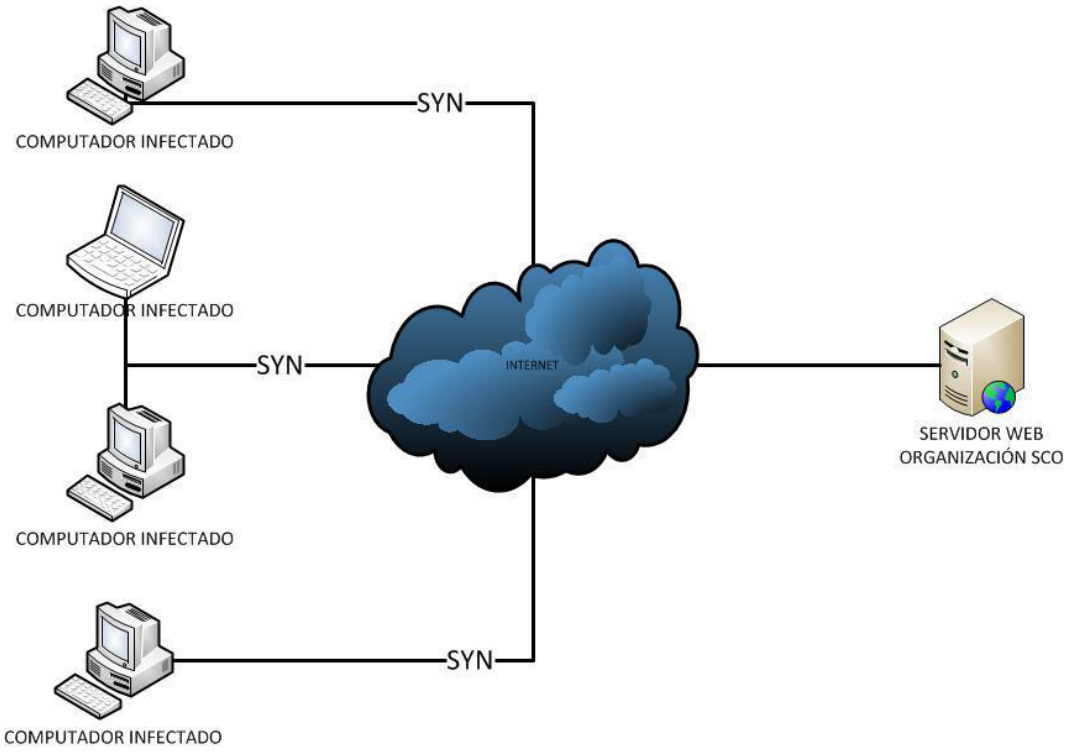


Imagen 44 Ataque SYN a página web de Organización SCO

El ataque se realiza de una manera distribuida, como se puede observar en el gráfico anterior existen varias computadoras infectadas con el gusano MyDoom.A convirtiéndose en zombis que simplemente ejecutaran una orden remotamente, pero como el gusano está programado para ejecutar el ataque desde el equipo local sin depender de que alguien remotamente lo ejecute.

El protocolo TCP se basa en una conexión de tres pasos, si el último paso no se llegara a realizarse esta pasa a un estado "semiabierto". Es decir que si se realiza muchas peticiones y están son inconclusas, el servidor permanecerá a la espera inactiva ocasionando lentitud en los demás servicios hasta tal punto de dejarlo totalmente deshabilitado.

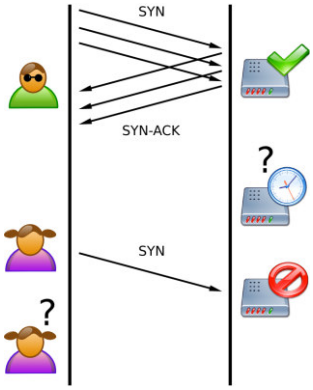


Imagen 45 Ataque Syn Flood
http://upload.wikimedia.org/wikipedia/commons/9/94/Tcp_synflood.png

En el caso del gusano envía una serie de paquetes TCP con el Bit SYN activo desde una dirección IP falsa para que no se pueda completar los tres pasos de conexión, generando que el servidor intente terminar dicha conexión dejando al equipo sin respuesta. MyDoom.A fue programado para realizar todo esto en una fecha establecida está comprendida desde su aparición hasta el 12 de febrero del 2014 sin saber el motivo por que fue hecho así, pero sin embargo dejando deshabilitada totalmente la página web y jamás vuelta a reabrir por la organización.

6.4.3 Manteniendo Acceso

El gusano MyDoom.A al momento de infectar un computador deja abierto un puerto que va en esta en el intervalo de 3127 hasta 3198 TCP, dejando acceso a cualquier usuario que tenga conocimiento sobre dicho puerto. El puerto que está abierto es una **puerta trasera (Backdoor)** en el sistema dejando a que usuarios malintencionados puedan ejecutar Exploits o infectar con otro Malware e ingresar de una manera desautorizada.

Para mantener acceso el gusano MyDoom.A altera los valores en el registros del sistema operativo Microsoft Windows, puesto que el puerto en el intervalo preestablecido se abrirá tras la carga del sistema operativo es decir cuando este encienda.

La puerta trasera que el gusano deja abierta deja a las variantes que más adelante fueran creadas acceso al sistema infectado como el caso de Mydoom.C.

El rango especificado de puertos tiene como propósito el tornar difícil bloquear un rango de puertos que uno solo en el sistema, además al conocer el rango para el atacante que pretenda acceder al sistema es mucho más sencillo comprobar la vulnerabilidad realizando un escaneo de puertos.

6.4.4 Borrando Huellas

El gusano MyDoom.A borra sus huellas desde que es instalado haciendo uso de nombres de archivos comunes en el sistema operativo. Uno de los nombres utilizados es Taskmoon.exe, el cual se coloca en un directorio diferente al original.

Sin embargo existe una diferencia al archivo original donde se camufla el gusano, el cual es el icono de bloc de notas que se encuentra dentro del sistema infectado.

Este archivo se ejecuta en segundo plano en el sistema con el afán de que el usuario cuando inspeccione los procesos activos no se percata de que el gusano se está ejecutando. Y que al intentar finalizar el proceso lanzara un error que no es posible finalizar el mismo, dejando imposibilitada esta opción.

El gusano como tal puede ser terminado su proceso pero la eliminación por completo del mismo es mucho más compleja dando paso a que un software especializado lo haga como es el caso de un antivirus.

6.5 Consecuencias

El gusano MyDoom.A fue el causante de la peor epidemia viral en la historia informática con mayor propagación puesto que uno de cada cinco correos electrónicos que estuvieron en circulación a inicios del 2004 estuvieron infectados, esto dando un 77% correo electrónico global, además desacelero el tráfico del internet en todo el mundo.

También otra de las consecuencias es que cerca de un millón de computadoras estuvo expuestas a la entrada de otros malware gracias a la puerta trasera (Backdoor) que dejo el gusano.

Uno de sus principales objetivos fue deshabilitar el dominio ww.sco.com de SCO Group generando un ataque de denegación de servicio distribuido y el cual lo lograría dejándolo totalmente fuera de servicio. Esto como consecuencia no solo es que la página dejara de funcionar sino que la empresa perdió dinero, llegando así a ofrecer una recompensa de $250.000 a quien dé con el origen o creador del gusano.

Las consecuencias del gusano a lo largo de su tiempo de vida no solo fueron a corto plazo sino que desencadeno secuelas que a largo plazo que afectaría como es el caso de las puertas traseras que dejo, pero lo más relevante es que todo sistema es vulnerable y más aún si es aprovechado el factor más débil de la cadena de seguridad que es el humano generando consecuencias como estas.

6.5 Contramedidas

Malware

El primer factor a considerar para establecer una contramedida es la infección de malware, al ser MyDoom.A uno de tipo gusano.

Sin duda para este caso es una contramedida básica la instalación de un software **Anti-Virus**, que tiene como función identificar y eliminar todo tipo de malware. Para tener la certeza de que este funcione y que tenga la capacidad de identificar uno de los últimos software malicioso que aparecen día a día hay que actualizarlo con frecuencia.

Existen hoy en día muchos antivirus cada una con diferentes versiones comerciales pero tienen la misma metodología. Últimamente existe anti-virus que elevan su funcionalidad e implementan sistemas de prevención de intrusiones de host, comprobando que no se produzcan singularidades en el funcionamiento de los programas en un computador.

Desde el año que salió el gusano MyDoom.A hasta el día de hoy el acceso a internet es más sencillo y por ende se es más expuesta a una infección de malware, lo que genera una necesidad de no solo poner un antivirus sino sistemas más sofisticados. Uno de ellos es **NIDS (Sistemas de detección de intrusos de red)** con un funcionamiento similar a un anti-virus con la diferencia que monitorea el tráfico de red, es de mucha utilidad porque a

un administrador de la red puede alertar al usuario o detener el tráfico que pretende infectar el malware.

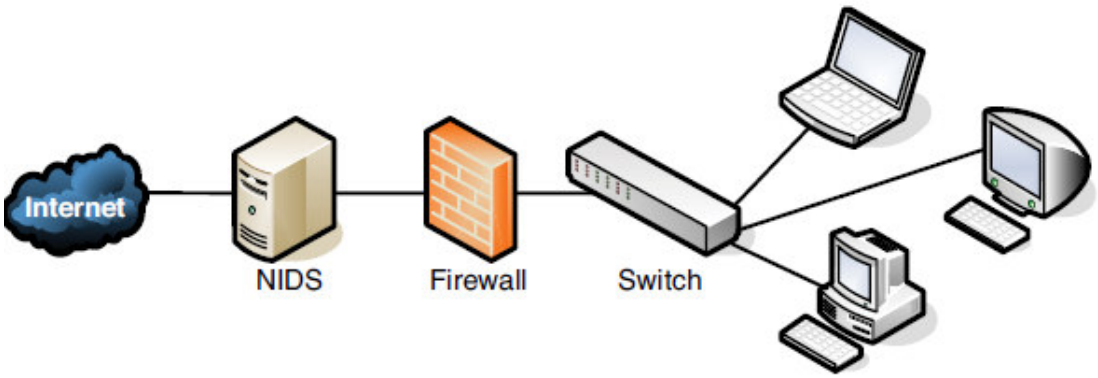


Imagen 46 Ejemplo de NIDS
http://2.bp.blogspot.com/-Mx-i1b1XcKo/U9uU99F5GrI/AAAAAAAAALw/Yyq9qkLJsAk/s1600/NIDS.png

Una opción mucho más rigurosa seria implementar un **HIDS (Sistemas de detección de intrusión host)** que son capaces de detectar cambios sobre cualquier archivo en un servidor mediante el control de sus características como el tamaño, fecha de creación o modificación, controlar la integridad detectando inmediatamente si es que ocurriera algo. Esta es una alternativa opcional ya que para un usuario normal no tendrá la misma necesidad ni magnitud de información de un servidor.

Ataques SYN-Flood

El segundo factor a contrarrestar según el caso de análisis es el ataque de Denegación de Servicio Distribuido (DDoS) de tipo Syn-Flood que es un objetivo secundario del gusano MyDoom.A.

Este tipo de ataques se da cuando se inicia la comunicación TCP, con el proceso llamado tres vías que utiliza este protocolo. Esta conexión al no ser establecida en su totalidad se toma con una conexión potencial sin embargo el protocolo asigna pocos recursos, pero los asigna, con esto es fácil provocar esto tipos de ataques.

Hoy en día existen tanto software como hardware para mitigar este tipo de ataques en el mercado, que los administradores de una red deben de tener en cuenta para establecer una contramedida.

La primera contramedida sin duda para una empresa media o grande es la Implementación MIXTA de un **firewall**, **balanceo de carga** y un **proxy inverso**. El firewall bloqueara el acceso no autorizado y que ingresen únicamente los que tengan autorización, el balanceo de carga que permitirá distribuir todo el tráfico que llega a la web dividiendo la cantidad de trabajo entres dos o más servidores teniendo una capacidad de procesamiento superior en el mismo periodo de tiempo, y por último el proxy inverso que actúa como intermediario entre los servidores y el cliente, además de distribuir la carga de peticiones a varios servidores y disminuyendo la carga gracias al almacenamiento en cache de contenido estático .

Además como otra medida de seguridad es **limitar conexiones permitidas** por cada IP, es decir hay que considerar un número de veces que el cliente (IP) puede generar una conexión, una vez superado límite establecido se rechazarían al no ser un comportamiento normal. De acuerdo al equipo o software que utilizamos se puede establecer parámetros como limitar número de conexiones por segundo, tiempo que cada cliente permanece conectado.

Por ejemplo en un router Mikrotik ejecutaríamos el siguiente comando en donde realiza un filtrado avanzado aplicado a los paquetes TCP, en donde 'SYN=400' el límite para paquetes SYN rechazando conexiones excesivas a ese valor.

```
/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new \
action=jump jump-target=SYN-Protect comment="SYN Flood protect" disabled=yes
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn limit=400,5 connection-state=new \
action=accept comment="" disabled=no
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn connection-state=new \
action=drop comment="" disabled=no
```

Imagen 47 Comando Mikrotik contra SYN-Flood
http://wiki.mikrotik.com/wiki/DoS_attack_protection

Otra técnica útil es el uso de **SYN cookies** implementada con el afán de resistir una inundación SYN, permitiendo a un servidor evitar conexiones que

caen cuando están en una cola SYN y esta se llena. Hay que considerar que no todos los equipos ni software cuentan con esta opción, pero retomando el ejemplo de un router Mikrotik la línea de comando seria la siguiente.

```
/ip settings set tcp-syncookies=yes
```

Imagen 48 Mikrotik Syn Cookie
http://wiki.mikrotik.com/wiki/DoS_attack_protection

Si es que la empresa posee un servidor web apache que por lo general es lo más utilizado se recomienda seguir la documentación oficial en el siguiente enlace: http://httpd.apache.org/docs/trunk/misc/security_tips.html.

CONCLUSIONES

Todo ataque informático se puede llegar a esquematizar las fases de su accionar, logrando determinar su anatomía e identificando las vulnerabilidades que los atacantes aprovecharon para causar daño al sistema.

Mientras más información se obtenga sobre el caso que se requiera analizar, se lograra establecer las fases del ataque de una mejor manera más eficaz, y como resultado nos dará una mejor comprensión.

Dos casos propuestos para el análisis fueron desarrollados satisfactoriamente y así obteniendo como resultado, su anatomía, vectores de ataque, consecuencias y contramedidas.

El desarrollo de esta tesis esta enfocado a dos casos de análisis; Caso Sony y Mydoom, sin embargo se puede utilizar de base para cualquier otro caso que se requiera analizar y así obtener la anatomía de su ataque.

Las contramedidas establecidas en la tesis se encuentran en función de los vectores de ataque de cada uno de los casos. Estas deberían ser tomadas en cuenta si cualquier sistema a sufrido o tiene una situación similar, o simplemente se requiere a seguridad la información.

Finalmente todos lo objetivos planteados en el diseño de tesis fueron cumplidos a cabalidad.

REFERENCIAS

Tori, C. (2008). *Hacking Ético.* Rosario.

ACISSI. (s.f.). *Seguridad Informática Ethical Hacking.* Barcelona: Epsilon.

Astudillo, K. (2013). *HACKING ÉTICO 101 - Cómo hackear profesionalmente en 21 días o menos!* Guayaquil.

ACISSI. *Seguridad Informática Ethical Hacking* . Barcelona: Editions ENI, 2011.

Alonso Cebrián, José María, y otros. *Ataques a BB. DD., SQL Injection*. 2014.

Auditoría, Consejo. *Seguridad informática-ethical hacking : conocer el ataque para una mejor defensa*. Barcelona: Ediciones ENI, 2013.

Bekman, George. *Introducción a la informática*. Madrid: Pearson Educación S. A. , 2005.

Buendía, Jose Fabian Roa. *Seguridad Informática*. Madrid: McGraw-Hill/Interamericana de España, S. L., 2013.

EDICIONES PARANINFO S.A. *SEGURIDAD INFORMATICA ED.11 Paraninfo*. EDICIONES PARANINFO S.A., 2011.

Evron, Randal Vaughn and Gadi. *DNS Amplification Attacks*. 2006.

Ganti, Srinivas. *Mydoom and its backdoor*. SANS Institute, 2004.

Goldencrown, Matt. *Mydoom is your doom: An Analysis of the Mydoom virus*. SANS Institute, 2004.

Gozáles Peréz, Pablo y Juan Antonio Calles García. *La biblia del Footpriting*. 2011.

Hernández, Claudio. «Hackers Los piratas del chip y la internet.» 01 de 12 de 2011. *Universidad de Carago.* 10 de 05 de 2014. <http://ucapanama.org/wp-content/uploads/2011/12/Hackers-3-Claudio-Hernandez.pdf>.

Jara, Hector y Federico G. Pacheco. *Ethical Hacking 2.0*. Creative Andina Corp., 2012.

Jelena Mirkovic, Sven Dietrich, David Dittrich, Peter Reiher. *Internet Denial of Service: Attack and Defense Mechanisms*. Pretince Hall PRT, 2014.

Miranda, Carlos Valdivia. *Sistemas Informáticos y redes Locales*. Madrid: Parainfo, 2014.

Portillo, Susana. «Prezi.» 06 de 09 de 2012. 2013 de 12 de 20. <http://prezi.com/vnbaj88nuq0p/historia-de-la-seguridad-informatica/>.

Verising. «Verising.» s.f. *Verising* . 2014 de 08 de 04. <http://www.verisigninc.com/es_ES/products-and-services/network-intelligence-availability/ddos/ddos-attack/index.xhtml>.

Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas y Telemática

DENUNCIA DE TESIS

Anatomía de un Ataque informático

ALUMNO:

Byron Guamán Sinchi

FECHA:

12/01/2013

CONTENIDO

UNIVERSIDAD DEL AZUAY

Edición autorizada de 20.000 ejemplares
Del 598.501 al 618.500
Nº 0617400

UNIVERSIDAD DEL AZUAY

1 DATOS GENERALES

1.1 DATOS ESTUDIANTE

Byron Vinicio Guamán Sinchi

Código: 50473

Celular: 09998280670

Teléfono: 2841503

Correo Electrónica: byr_666@hotmail.es

1.2 DIRECTOR SUGERIDO

Ingeniero Fabián Carvajal

Celular: 0992660270

Correo Electrónica: fabianc@uazuay.edu.ec

1.3 CODIRECTOR SUGERIDO

Ingeniero Esteban Crespo

Celular: 0996804562

Teléfono: 4092109

Correo Electrónica: ecrespo@uazuay.edu.ec

1.4 ASESOR METODOLÓGICO

1.5 TRIBUNAL DESIGNADO

Ing. Fabián Carvajal

Ing. Fernando Balarezo

Ing. Paúl Ochoa Arévalo

Edición autorizada de 20.000 ejemplares
Del 598.501 al 618.500
Nº 0617379

1.6 APROBACIÓN

UNIVERSIDAD DEL AZUAY

Junta Académica:

Consejo de Facultad:

1.7 LÍNEA DE INVESTIGACIÓN

1.7.1 Código UNESCO

Línea: 1203 Informática de Computadoras

Programa: 1203.99 Sistemas de Seguridad de la Información

1.7.2 Tipo de Trabajo

Investigación Formativa

1.8 ÁREA DE ESTUDIO

Seguridad de la Información

1.9 TÍTULO PROPUESTO

Anatomía de un ataque informático

1.10 ESTADO DEL PROYECTO

Trabajo Nuevo

2 CONTENIDO

2.1 MOTIVACIÓN DE LA INVESTIGACIÓN

Hoy en día la evolución de las tecnologías de la información ha creado un campo vulnerable en nuestros sistemas informáticos y nos hacen propensos a un ataque cibernético. En nuestro país no es de mucho conocimiento este campo por eso la justificación de la elaboración de este trabajo de titulación.

Edición autorizada de: 20.000 ejemplares
Del 598.501 al 618.500
Nº 0617380

2.2 Problemática

Cuando hablamos de "Hacker" o un ataque informático nos hacemos la idea de un delincuente que roba información no física, pero la realidad por la falta de conocimiento sobre el tema no podemos definirlo que no tratamos solo sobre delincuentes informáticossino también de personas que se encargan de asegurar un sistema.

Cualquiera puede ser objeto de un ataque, ya que son susceptibles las pc, Smartphone, etc. porque cuentan con conexión a internet , siendo este es un territorio hostil y mucho de los casos los atacantes tiene intereses económicos.

2.3 Pregunta de Investigación

¿Cómo se realiza un ataque informático?

2.4 Resumen

La Anatomía de un ataque informático está enfocada al análisis de dos casos específicos que han tenido más relevancia en estos últimos años en el campo informático, el cual contendrá: como llegaron a realizarlo, cuáles fueron los conceptos aplicados y cuál fue el beneficio u objetivo de haberlo realizado.

Los casos a ser analizados serán; Julio del 2009 ataque realizado por Mydoom y Caso Sony en el 2011.

2.5 Marco Teórico

Un ataque informático consiste en aprovechar alguna debilidad o falla en el software, e incluso en las personas, con el fin de obtener un beneficio, por lo general este puede ser económico, causando un efecto negativo en la seguridad del sistema, que luego repercutirá directamente en los activos de la organización (EcuRed).

Existen diversos tipos de ataque como pueden ser:

- Ataque de denegación de servicio.- También Llamado Dos (Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, normalmente eso produce una pérdida en la

Edición autorizada de 20.000 ejemplares
Del 598.501 al 618.500
Nº 0617381

conectividad de la red en donde el consumo de ancho de banda de la víctima se sobrecarga llevando esto al colapso de la misma (Evron, isotf, 2006).

- Man in the Middle (MitM).- Se base en que el atacante pueda ser capaz de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace de comunicación entre las mismas ha sido violado.
- Ataque día cero(Zero Day Attack).- Es un ataque contra una aplicación o sistema, que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que por lo general son desconocidas para la gente y el fabricante de producto este método de ataque generalmente utilizado por los crakers. Este tipo de exploit circula generalmente entre los potenciales atacantes que inclusive llegan a poner el código en foros abiertos para que el resto lo pueda leer. Esto es considerado uno de los mayores y más peligrosos instrumentos en una guerra informática, ya que con el uso de exploits se ingresa al sistema y con la elaboración de un malware podemos aprovechar este mismo exploit y conseguir información tan confidencial como una clave de acceso bancaria (Tony Bradley).

GNU/Linux uno de los sistemas más utilizados por los hackers al ser este gratuito y su código abierto. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquier bajo los términos de GPL (Licencia Publica General de GNU (GNU, s.f.)). Los escritorios más utilizados son GNOME, KDE SC, LXDE y xfce, en dispositivos móviles se encuentra en Android, que funciona sobre el núcleo Linux.

TCP (Protocolo de Control de transmisión) es el protocolo más utilizado por los atacantes porque es el que se utiliza fundamentalmente en el internet por su fiabilidad del nivel de transporte garantizando que los datos serán entregados en su destino sin errores y en el mismo orden que se transmite. También al proporcionar un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

Los puertos de conexión son explotados por los atacantes ya que gracias a ello el protocolo TCP sabe que aplicación están transmitiendo o recibiendo información asignándole de un número de puerto a cada una de ellas. Existen 65536 puertos estos a su vez son clasificados en tres categorías: Bien conocidos, Registrados y dinámicos/privados. Los puertos bien conocidos son asignados por la Internet Assingned Numbers Authority (IANA).

Google Hacking consiste en explotar gran capacidad de almacenamiento de información de Google, técnica utilizada por el buscador así como también sus aplicaciones encontrando

agujeros de seguridad en la configuración y el código informático que sitios web utilizan. (Long, 2008).

La anatomía de un ataque informático nos permite aprender a pensar como los atacantes y jamás subestimar su mentalidad, las fases a ser analizadas son Reconocimiento, Exploración, Obtener Acceso, Mantener el Acceso y Borrar Huellas, "Si utilizas al enemigo para derrotar al enemigo, serás poderoso en cualquier lugar a donde vayas" (James Michael Steward, 2011). La misma que genera una base de conocimiento identificando los pasos y las acciones que los ataques realizaron en muchos casos los cuales pueden servir como referencia histórica en donde las organizaciones pueden tomar acciones preventivas como medidas de seguridad. Uno de los recursos más importantes, para sobrellevar los desafíos en la seguridad de la información, es el conocimiento de las técnicas hacking que brindan una mejor comprensión al riesgo. Los pasos que los profesionales que se dedican al hacking ético son similares a los utilizados por los atacantes, claro que las intenciones no son las mismas, conocer la anatomía del ataque es muy importante para comprender y diseñar un buen esquema de seguridad frente a un ataque que podía ocurrir.

2.6 Objetivo General

- Sistematizar información conceptual sobre la anatomía de dos casos seleccionados de ataques informáticos.

2.7 Objetivos Específicos

- Definir el modelo y parámetros de análisis a usarse en el estudio de los casos seleccionados.
- Comprender cómo se realiza un ataque informático determinando su anatomía hasta que logra acceder a un sistema o logre causarle daño, tomando como referencia el caso de Sony y Mydoom.
- Analizar 2 casos de ataques informáticos: Julio del 2009 ataque realizado por Mydoom y Caso Sony en el 2011, utilizando el modelo y parámetros definidos.
- Describir la forma y las herramientas que fueron utilizadas para el ataque.
- Determinar las motivaciones de los atacantes, en base a la información pública disponible de indagaciones realizadas sobre ellos.
- Obtener contramedidas de los casos analizados para ser utilizados como referencia de seguridad.

2.8 METODOLOGÍA

UNIVERSIDAD DEL AZUAY

La metodología a utilizar ser a un tipo de investigación descriptiva ya que se llegara a conocer la forma de los ataques planteados a través de la descripción de las actividades y procesos que realizaron, a continuación definimos los pasos a seguir:

1. Etapa.
   a. Revisión Bibliográfica.
2. Etapa.
   a. Sintetizar Conceptos.
3. Etapa.
   a. Planteamiento de esquema como se realiza un ataque informático.
4. Etapa.
   a. Estudio de casos: Mydoom y Caso Sony.
5. Etapa.
   a. Estrategias de Intervención: Esquematizar los resultados obtenidos como las empresas fueron afectadas y cuáles fueron sus sistemas de respuestas ante esos ataques.
6. Etapa.
   a. Sintetizar los resultados de la investigación.
7. Etapa.
   a. Contramedidas: Una vez analizados los casos se propondrá medidas preventivas las cuales mitiguen el riesgo de sufrir las mismas consecuencias.
8. Etapa.
   a. Conclusiones: Después de toda la investigación se concluirá de manera concreta una guía de análisis, posibles riesgos y mitigaciones que podrían tomar para prevenir un ataque informático.

2.9 ALCANCES Y RESULTADOS ESPERADOS

La Anatomía de un ataque informático está enfocada al análisis de dos casos específicos que han tenido más relevancia en estos últimos años en este campo, el cual contendrá: ¿Cómo llegaron a realizarlo?, ¿Cuáles fueron sus conceptos aplicados? y ¿Cuál fue el beneficio u objetivo de haberlo realizado? Y ¿Qué contramedidas podemos tomar para no ser atacados de la misma manera?

Los casos a ser analizados serán; Julio del 2009 ataque realizado por Mydoom y Caso Sony en el 2011.

2.10 SUPUESTOS Y RIEGOS

Edición autorizada de 20.000 ejemplares
Del 598.501 al 618.500 Nº 0617384

Supuestos:

- Contar con todo el material bibliográfico propuesto para el desarrollo del trabajo de investigación o el necesario.
- Obtener artículos y estudios previamente realizados de los 3 2 casos propuestos.
- Contar con un plan de tiempo que permita desarrollar el trabajo sin contratiempos.

Riegos:

- El tiempo estimado para el desarrollo no sea el suficiente.
- No encontrar el material bibliográfico necesario para el desarrollo.
- No tener la orientación adecuada por parte del Director y no avanzar en el trabajo.
- Perder Material Digital por causas de falla del computador de trabajo.

2.11 Presupuesto

Rubro-Denominación	Costo USD	Justificación
Útiles de Oficina	$100	- Hojas de Papel - Material de Escritorio - Copias - Empastado - Varios
Derechos Universitarios	$300	- Derecho de Tesis - Otros
Internet	$114	- Mensualidades del internet a utilizar para el desarrollo del trabajo
Imprevistos	$100	- En caso de que se presente un gasto no previsto
Material Bibliográfico	$300	- Compra de libro, revistas tanto digitales como físicos para elaborar la investigación.
Total	$914	

2.12 Financiamiento

Propio: 100%

UNIVERSIDAD DEL AZUAY

2.13 ESQUEMA TENTATIVO

Capítulo 1: Introducción y Definición

1.1 Introducción
1.2 Seguridad Informática
1.2.1 Definición
1.2.2 Importancia Seguridad Informática
1.2.2.1 Para Particulares
1.2.2.2 Para Empresas o Instituciones Educativas
1.2.2.3 Para País o una Nación
1.2.3 Tipo de Amenazas
1.2.4 Mecanismos de Seguridad
1.3 Hackers
1.3.1 Definición
1.3.2 Tipos de Hackers
1.3.2.1 Black Hact
1.3.2.2 Grey Hat
1.3.2.3 White Hat

Capítulo 2: Anatomía de un Ataque Informático

2.1 Anatomía de un ataque informático

2.2 Etapas

2.2.1 Reconocimiento

2.2.2 Exploración

2.2.3 Obtener Acceso

2.2.4 Mantener Acceso

2.2.5 Borrar Huellas

Capítulo 3: DOS(Denegación de Servicio) o DDOS(Denegación de Servicio Distribuido)

3.1 Definición

3.2 Métodos de Ataque

3.2.1 Inundación SYN (SYN Flood)

3.2.2 Inundación ICMP (ICMP Flood)

3.2.3 SMURF

3.2.4 Inundación UDP (UDP Flood)

Capítulo 4: Caso de Análisis Sony

2.14 CRONOGRAMA

UNIVERSIDAD DEL AZUAY

Objetivo Específico	Actividad	Resultado Esperado	Tiempo(Semanas)
Sistematizar información conceptual sobre anatomía de ataques informáticos.	-Realizar Levantamiento de Información en marco conceptual respecto a redes e informática. -Realizar una Breve introducción y definición sobre conceptos teóricos de redes e informática enfocados a la anatomía de un ataque informático.	-Levantar la información necesaria para poder realizar la introducción y dar definiciones.	4
Definir el modelo y parámetros de análisis a usarse en el estudio de los casos seleccionados.	-Especificar modelo de anatomía de un ataque informática en base a conceptos teóricos y modelos aplicados en otros casos. -Determinar los casos de análisis.	Realizar Modelo de una anatomía de un ataque Informático.	5
Analizar 3 casos de ataques informáticos: Julio del 2009 ataque realizado por Mydoom a Estados Unidos y Corea del Sur, ataque a la organización Spamhaus y Caso Sony en el 2011 ,utilizando el modelo y parámetros definidos.	-Especificar cuál fue la técnica de ataque utilizada.	-Análisis Caso Sony -Análisis Caso Mydoom - Análisis Caso Spamhouse	8
Describir la forma y las herramientas que fueron utilizadas para el ataque.	-Analizar según el marco teórico aplicado y el modelo de anatomía especificado los casos de análisis propuestos.	-Determinar Casos de Análisis y Técnicas Utilizadas	4

Edición autorizada de 20.000 ejemplares
Del 598.501 al 618.500
Nº 0617388

Determinar las motivaciones de los atacantes, en base a la información pública disponible de indagaciones realizadas sobre ellos.	-Explorar motivaciones y posibles beneficios que han tenido por realizar el ataque. -Determinar consecuencias que generaron estos ataques.	-Conclusiones, Observaciones y Motivaciones de los Ataques	4
Obtener contramedidas de los casos analizados para ser utilizados como referencia de seguridad.	-Examinar Herramientas de seguridad. -Examinar medidas de seguridad. -Asociar medidas y herramientas para recomendar contramedidas.	-Obtener medidas preventivas para ser aplicadas y no ser víctimas de un ataque como los casos analizados.	4

2.15 Referencias

ACISSI. (s.f.). *Seguridad Informática Ethical Hacking.* Barcelona: Epsilon.

Astudillo, K. (2013). *HACKING ÉTICO 101 - Cómo hackear profesionalmente en 21 días o menos!* Guayaquil.

EcuRed. (s.f.). *ecured.* Recuperado el 2013 de 06 de 25, de http://www.ecured.cu/index.php/Ataque_inform%C3%A1tico

Evron, R. V. (2006). *DNS Amplification Attacks.*

Evron, R. V. (17 de Marzo de 2006). *Isotf.* Recuperado el 2013 de 06 de 25, de http://www.isotf.org/news/DNS-Amplification-Attacks.pdf

GNU. (s.f.). *GNU Operation System.* Recuperado el 25 de 06 de 2013, de http://www.gnu.org/licenses/gpl-2.0.html

James Michael Steward, G. K. (2011). *Global Knowledge.* Recuperado el 2013 de 06 de 25, de http://www.globalknowledge.nl/content/files/documents/224536/Security-White-Paper-10-Ways-Hackers-Breach-Security

Long, J. (2008). *Google Hacking.* Syngress Publishing.

María del Pilar Ramos, A. G. (2011). *Seguridad Informatica.* Madrid: Paraninfo.

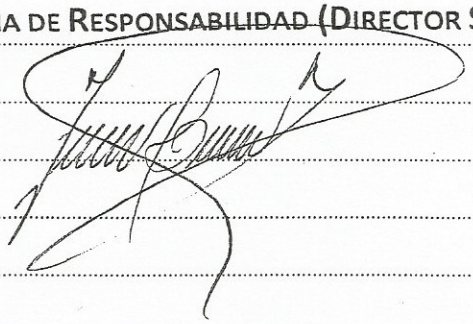
Murillo, J. C. (212). *Administración avanzada de redes.*

Tony Bradley, C.-I. (s.f.). Recuperado el 2013 de 06 de 25, de http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday.htm

UNIVERSIDAD DEL AZUAY

2.16 Firma de Responsabilidad (Estudiante)

2.17 Firma de Responsabilidad (Director Sugerido)



Edición autorizada de 20.000 ejemplares
Del 598.501 al 618.500
Nº 0617390

UNIVERSIDAD DEL AZUAY

ACTA

SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

1.1 **Nombre del estudiante:** Byron Vinicio Guamán Sinchi
1.1.1 Código 50473
1.2 **Director sugerido**: Carvajal Vargas Fabián, Ing.
1.3 **Codirector (opcional)**: Ing. Esteban Crespo
1.4 **Tribunal:** Balarezo Rodríguez Fernando, Ing / Ochoa Arévalo Paúl, Ing.
1.5 **Título propuesto: "A**natomía de un ataque informático"
1.6 **Resolución**:

1.6.1 Aceptado sin modificaciones _____

1.6.2 Aceptado con las siguientes modificaciones:

- Ajustar el objetivo general.
- Eliminar el caso Spam House del análisis
- Incluir las contra medidas en cada caso de análisis

- Responsable de dar seguimiento a las modificaciones(designado por la Junta Académica de entre los Miembros del Tribunal): Ing. Fabián Carvajal V.

1.6.3 No aceptado
- Justificación:

_____
_____
_____

Tribunal

.....	.....	.....
Ing. Fabián Carvajal V.	Ing. Fernando Balarezo R.	Ing. Paúl Ochoa Arévalo

.....
Sr. Byron Guamán Sinchi

Dra. Jenny Ríos Coello
Secretario de Facultad

Fecha de sustentación: 6 de enero de 2014

Oficio Nro. 074-2013-DIST-UDA

Cuenca, 13 de Diciembre de 2013

Señor Ingeniero
Xavier Ortega Vázquez
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMNISTRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 10 de diciembre del 2013, revisó el proyecto de tesis titulado"Anatomía de un ataque informático", presentado por la estudiante Byron Guaman Sinchi, estudiante de la Escuela de Ingeniería de Sistemas y Telemática, previo a la obtención del título de Ingeniero de Sistemas y Telemática.

La Junta considera que el diseño de trabajo de titulación cumple con los requisitos normados en la "Guía de Elaboración y Presentación de la Denuncia/Protocolo de Trabajo de Titulación", razón por la cual solicita, por su digno intermedio, notificar al tribunal designado y determinar lugar, fecha y hora de sustentación.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomienda como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior al Ing. Fabián Carvajal, y como miembros del Tribunal a la Ing. Fernando Balarezo y al Ing. Paúl Ochoa Arévalo.

Atentamente,

Ing. Marcos Orellana Cordero
Director Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay

UNIVERSIDAD DEL
AZUAY

DOCTORA JENNY RIOS COELLO, SECRETARIA DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION DE LA UNIVERSIDAD DEL AZUAY

C E R T I F I C A:

Que, el Señor **Byron Vinicio Guamán Sinchi**, registrado con el código **50473** perteneciente a la Escuela de Ingeniería de Sistemas tiene aprobado más del 80% de pensum de estudios.

Cuenca, 18 de Diciembre de 2013

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACION
SECRETARIA

Derecho 47783
vcf.-

Edición autorizada de 20.000 ejemplares
Del 578.501 al 598.500
Nº 0590062

Cuenca, 30 de enero de 2014

Ingeniero

Xavier Ortega Vázquez

DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÒN

Presente

De mi consideración:

Revisado el proyecto de tesis **"Anatomía de un ataque informático"**, debo indicar que el señor Byron Guamán Sinchi, estudiante de la Escuela de Ingeniería de Sistemas y Telemática, ha realizado los respectivo cambios que han sido sugeridos por la junta.

Razón por la cual cumple con los requisitos de modificación de tesis.

Atentamente,

Ing. Fabián Carvajal

Cuenca, diciembre 13 de 2013

Ing.

Xavier Ortega Vásquez, MBA

Decano de la Facultad de Ciencias de la Administración

Presente

De mi consideración:

Por la presente, me permito informarle que he revisado el diseño de tesis presentado por la estudiante **Byron Vinicio Guaman Sinchi** con el tema *"Anatomía de un ataque informático"* como requisito previo para la obtención del título de Ingeniero de Sistemas y Telemática.

Al respecto, el diseño de tesis presenta una estructura teórica, metodológica y técnica coherente, cuyo objetivo es comprender cómo se realiza un ataque informático determinando su anatomía hasta que logra acceder a un sistema o logre causarle daño, tomando como referencia el caso de Sony y Mydoom. Por lo expuesto, emito informe favorable y recomiendo su aprobación.

Atentamente

Ing. Fabián Carvajal

UNIVERSIDAD DEL AZUAY

ACTA
SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

1.1 **Nombre del estudiante:** Byron Vinicio Guamán Sinchi
1.1.1 Código 50473
1.2 **Director sugerido**: Carvajal Vargas Fabián, Ing.
1.3 **Codirector (opcional)**: Ing. Esteban Crespo
1.4 **Tribunal:** Balarezo Rodríguez Fernando, Ing / Ochoa Arévalo Paúl, Ing.
1.5 **Título propuesto: "A**natomía de un ataque informático"
1.6 **Resolución**:

1.6.1 Aceptado sin modificaciones _____

1.6.2 Aceptado con las siguientes modificaciones:

- Ajustar el objetivo general.
- Eliminar el caso Spam House del análisis
- Incluir las contra medidas en cada caso de análisis

- Responsable de dar seguimiento a las modificaciones(designado por la Junta Académica de entre los Miembros del Tribunal): Ing. Fabián Carvajal V.

1.6.3 No aceptado
- Justificación:

_____
_____
_____

Tribunal

.....	.....	.....
Ing. Fabián Carvajal V.	Ing. Fernando Balarezo R.	Ing. Paúl Ochoa Arévalo

.....
Sr. Byron Guamán Sinchi

Dra. Jenny Ríos Coello
Secretario de Facultad

Fecha de sustentación: 6 de enero de 2014

UNIVERSIDAD DEL AZUAY

RÚBRICA PARA LA EVALUACIÓN DEL PROTOCOLO DE TRABAJO DE TITULACIÓN

1.1 Nombre del estudiante: Sr. Byron Vinicio Guamán Sinchi

1.2 Director sugerido: Ing. Fabián Carvajal Sinchi
1.3 Codirector (opcional): apellido, nombre y título.
1.4 Título propuesto: "Anatomía de un ataque informático"
1.5 Revisores (tribunal): Ing. Fernando Balarezo Rodríguez / Ing. Paúl Ochoa Arévalo
1.6 Recomendaciones generales de la revisión:

	Cumple totalmente	Cumple parcialmente	No cumple	Observaciones (*)
Línea de investigación				
1. ¿El contenido se enmarca en la línea de investigación seleccionada?	X			
Título Propuesto				
2. ¿Es informativo?	X			
3. ¿Es conciso?	X			
Estado del arte				
4. ¿Identifica claramente el contexto histórico, científico, global y regional del tema del trabajo?				
5. ¿Describe la teoría en la que se enmarca el trabajo	X			
6. ¿Describe los trabajos relacionados más relevantes?	X			
7. ¿Utiliza citas bibliográficas?				
Problemática y/o pregunta de investigación				
8. ¿Presenta una descripción precisa y clara?	X			
9. ¿Tiene relevancia profesional y social?	X			
Hipótesis (opcional)				
10.¿Se expresa de forma clara?		X		
11.¿Es factible de verificación?	X			
Objetivo general				
12.¿Concuerda con el problema formulado?		X		Ajustar
13.¿Se encuentra redactado en tiempo verbal infinitivo?	X			
Objetivos específicos				
14.¿Concuerdan con el objetivo	X			

general?				
15.¿Son comprobables cualitativa o cuantitativamente?	X			
Metodología				
16.¿Se encuentran disponibles los datos y materiales mencionados?	X			
17.¿Las actividades se presentan siguiendo una secuencia lógica?	X			
18.¿Las actividades permitirán la consecución de los objetivos específicos planteados?	X			
19.¿Los datos, materiales y actividades mencionadas son adecuados para resolver el problema formulado?	X			
Resultados esperados				
20.¿Son relevantes para resolver o contribuir con el problema formulado?	X			
21.¿Concuerdan con los objetivos específicos?	X			
22.¿Se detalla la forma de presentación de los resultados?		X		Efectuar ajustes
23.¿Los resultados esperados son consecuencia, en todos los casos, de las actividades mencionadas?	X			
Supuestos y riesgos				
24.¿Se mencionan los supuestos y riesgos más relevantes?	X			
25.¿Es conveniente llevar a cabo el trabajo dado los supuestos y riesgos mencionados?	X			
Presupuesto				
26.¿El presupuesto es razonable?	X			
27.¿Se consideran los rubros más relevantes?				
Cronograma				
28.¿Los plazos para las actividades son realistas?	X			
Referencias				
29.¿Se siguen las recomendaciones de normas internacionales para citar?	X			Verificar
Expresión escrita				
30.¿La redacción es clara y fácilmente comprensible?	X			
31.¿El texto se encuentra libre de faltas ortográficas?	X			

(*) Breve justificación, explicación o recomendación.

- Opcional cuando cumple totalmente,

- Obligatorio cuando cumple parcialmente y NO cumple.

.....

.....

.....

CONVOCATORIA

Por disposición de la Junta Académica de Ingeniería de Sistemas, se convoca a los Miembros del Tribunal Examinador, a la sustentación del Protocolo del Trabajo de Titulación "Anatomía de un ataque informático" presentado por el estudiante Sr Byron Vinicio Guamán Sinchi, previa a la obtención del grado de Ingeniero de Sistemas y Telemática, para el día **LUNES 6 DE ENERO DE 2014 A LAS 18H30.**

Cuenca, 19 de diciembre de 2013

Dra. Jenny Ríos Coello
Secretaria de la Facultad

Ing. Fabián Carvajal Vargas .....

Ing. Fernando Balarezo Rodríguez .....

Ing. Paúl Ochoa Arévalo .....

UNIVERSIDAD DEL AZUAY

Cuenca, diciembre 13 de 2013

Ing.

Xavier Ortega Vásquez, MBA

Decano de la Facultad de Ciencias de la Administración

Presente

De mi consideración:

Por la presente, me permito informarle que he revisado el diseño de tesis presentado por la estudiante **Byron Vinicio Guaman Sinchi** con el tema *"Anatomía de un ataque informático"* como requisito previo para la obtención del título de Ingeniero de Sistemas y Telemática.

Al respecto, el diseño de tesis presenta una estructura teórica, metodológica y técnica coherente, cuyo objetivo es comprender cómo se realiza un ataque informático determinando su anatomía hasta que logra acceder a un sistema o logre causarle daño, tomando como referencia el caso de Sony y Mydoom. Por lo expuesto, emito informe favorable y recomiendo su aprobación.

Atentamente

Ing. Fabián Carvajal

Edición autorizada de 20.000 ejemplares
Del 598.501 al 618.500
Nº 0617391