Hacking basado en ataques a TCP/IP.

Carina Aqueveque Legajo84054 cariaquev@yahoo.com.ar
Natalia Huenchuman Legajo84478 natalia.huenchuman@gmail.com

Resumen

Hacking es la búsqueda permanente de conocimientos sobre los sistemas informáticos, sus mecanismos de seguridad, vulnerabilidades, la forma de aprovecharlas y compartirlas con otros. Estos hackers son los que realizan los ataques para producir daño a los sistemas informáticos. Los distintos tipos de ataques explotan las variadas vulnerabilidades que se pueden encontrar en una red basada en TCP/IP.

La mayoría de estos ataques están basados en las debilidades del protocolo TCP/IP, el cual no posee todas las propiedades deseables actualmente para mantener una "comunicación segura" entre las partes.

En este informe se describen algunos ejemplos de los ataques típicos al protocolo TCP/IP con el fin de que el lector comprenda el funcionamiento e impacto en las organización atacadas.

ÍNDICE

Introducción …… 3

1. El Modelo de Referencia TCP/IP …… 4
1.1 Concepto ……... 4
1.2 Vulnerabilidades de TCP/IP ……... 4

2. Ejemplos de Ataques …… 6
2.1 Ataque de DOS y DDOS …… 6
2.1.1 Concepto ……... 6
2.1.2 Ataque DOS a Yahoo! …… 7
2.1.3 Ataque DDOS a CNN ……..…… 8
2.2 Ataque de Phishing y Pharming ……..... 9
2.2.1 Conceptos ……..…… 9
2.2.2 Ataque a Mountain America ……..……..… 9
2.2.3 Ataque a eBay ……. 10
2.3 Ataque a servidores de correo: Spamming …….. 10
2.4 Ataque web spoofing……... 13

3. Otros ataques…….14

4. Conclusiones …….. 15

5. Referencias …… 16

INTRODUCCIÓN

Hoy en día, el uso de TCP/IP se ha extendido prácticamente a la totalidad de las redes de comunicaciones de datos, potenciado fundamentalmente por la expansión de Internet así como de las redes corporativas y de cooperación asociadas a esta tecnología: Intranets y Extranets.

Es importante destacar que dicho protocolo de comunicaciones es abierto y totalmente documentado; y en la versión 4 (IPv4) que es la más ampliamente usada, no incluye la seguridad como parte de su construcción. Fue diseñado para su empleo en una comunidad abierta y confiada, y en busca de ciertas características, como la funcionalidad y la eficiencia, solamente sin contemplar otros aspectos.

Durante los primeros años esta falencia no se había convertido todavía en un problema, ya que los ataques a sistemas informáticos involucraban poca sofisticación técnica y se realizaban de dos formas: por un lado, aquellos realizados desde el interior de la red se basaban en la alteración de permisos para modificar la información del sistema. Por otro lado, los ataques externos se producían gracias al conocimiento de las contraseñas necesarias para acceder a los equipos de la red.

Con el paso de los años se fueron desarrollando nuevos ataques cada vez más sofisticados para explotar vulnerabilidades tanto en el diseño de las redes TCP/IP como en la configuración y operación de los sistemas informáticos que conforman las redes conectadas a internet. Estos nuevos métodos de ataque se han ido automatizando, por lo que en muchos casos sólo se necesita un conocimiento técnico muy básico para realizarlos. Cualquier usuario con una conexión a internet, tiene acceso hoy en día a numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos.

La búsqueda de dichas vulnerabilidades no sólo la llevan adelante individuos en busca de diversión, retos o por un momento de fama, sino que también es llevada a cabo por profesionales (que incluso trabajan en equipo), impulsados por diferentes motivos, ya sean económicos o políticos. Dichos ataques pueden tener como fin conseguir una base de datos, bloquear las transacciones de un sitio web, robar identidades para cometer fraudes y estafas o realizar espionaje industrial.

Existen una gran cantidad de ataques perpetrados principalmente por hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, y usando diferentes protocolos. Pueden ser clasificados de diferentes formas dependiendo del autor. Una buena clasificación, a nuestro parecer, es aquella que separa en ataques de *monitorización*, *autenticación*, *DOS* y *DDOS*, y de *modificación*. Dentro de cada uno, se encuentran una gran variedad de ataques, se podría decir, una sub-clasificación, para los que existe una gran cantidad de herramientas para realizarlos.

A continuación se detallarán cuatro ejemplos de hacking en TCP/IP seleccionados como los más significativos por las técnicas utilizadas.

- *Ataque DOS*: se expondrá el caso de Yahoo! y en el *ataque DDOS*, se expondrá, el realizado a CNN.
- *Ataque de Phishing:* los casos seleccionados fueron los de Mountain America, eBay y Movistar.
- *Ataque a servidores de correo: Spamming*. Existen numerosas organizaciones que han sufrido estos ataques de este tipo, por esto se describirá esta clase de atauqe en general, citando algunas organizaciones que han sido afectadas
- *Ataque Web Spoofing:* en Argentina y más precisamente en nuestra región, se han perpetrados estos ataques a diversos sitos, llevado a cabo por grupo de otros países.

Por último se comentarán algunos ataques que son conocidos pero de los no hay detalles como han sido realizados.

Antes de pasar a hablar detalladamente de cada uno de los ejemplos de ataque presentados, se explicarán algunas vulnerabilidades de los protocolo TCP/IP, que servirán de base para entender cómo se realizaron los distintos ataques.

1 El modelo de referencia TCP/IP

1.1 Concepto

Denominado de esta forma por las iniciales de sus protocolos primarios, es el modelo más ampliamente utilizado por su independencia del Sistema Operativo y hardware.

En dicho modelo se diferencian cuatro capas en las que se agrupan los diferentes protocolos:

- *Capa de aplicación:* es responsable de soportar las aplicaciones de redes (HTTP, FTP, SMTP, Telnet, DNS)
- *Capa de transporte*: proporciona el servicio de transporte de mensajes de la capa de aplicación entre los lados del cliente y el servidor de una aplicación (TCP, UDP)
- *Capa de red*: es responsable de rutar los datagramas de una máquina a otra. Tiene un protocolo que define los campos del datagrama IP y cómo actúan los sistemas terminales y routers sobre esos campos. Dicho protocolo se denomina IP. Lo más importante es el ruteo de los paquetes y también evitar la congestión.
- *Capa de interfaz de red*: correspondiente al nivel de Enlace y Físico de la pila OSI. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada host, como puede ser una línea punto a punto o una red Ethernet.

  La capa inferior, que podemos nombrar como Física, contiene varios estándares (conocidos con el nombre del IEEE 802.X) que establecen las reglas para enviar datos por cable coaxial delgado, cable coaxial grueso, par trenzado, fibra óptica y su propio método de acceso.

1.2 Vulnerabilides de TCP/IP

Como ya se ha comentado, en cada una de las capas en cada capa del modelo TCP/IP pueden existir distintas vulnerabilidades y un atacante puede explotar los protocolos asociados a cada una de ellas.

Cada día se descubren nuevas deficiencias, la mayoría de las cuales se hacen públicas por organismos internacionales, tratando de documentar, si es posible, la forma de solucionar y contrarrestar los problemas.

A continuación se presentan las vulnerabilidades mencionadas:

a) ***Vulnerabilidades de la capa de aplicación***. Debido al gran número de protocolos definidos en esta capa, la cantidad de deficiencias presentes también será superior al resto de capas. Algunos ejemplos de deficiencias de seguridad a este nivel podrían ser los siguientes:

- *Servicio de nombres de dominio***.** Normalmente, cuando un sistema solicita conexión a un servicio, pide la dirección IP de un nombre de dominio y envía un paquete UDP a un servidor DNS; entonces, este responde con la dirección IP del dominio solicitado o una referencia que apunta a otro DNS que pueda suministrar la dirección IP solicitada.

Un servidor DNS debe entregar la dirección IP correcta pero, además, también puede entregar un nombre de dominio, dada una dirección IP u otro tipo de información.

En el fondo, un servidor de DNS es una base de datos accesible desde internet. Por lo tanto, un atacante puede modificar la información que suministra esta base de datos o acceder a información sensible almacenada en la base de datos por error, pudiendo obtener información relativa a la topología de la red de una organización concreta

Estos ataques de suplantación de DNS se conocen con el nombre de *spoofing* de DNS.

- *Telnet***:** este servicio autentica al usuario mediante la solicitud del identificador de usuario y su contraseña, que se transmiten en claro por la red.

Así, al igual que el resto de servicios de internet que no protegen los datos mediante algún mecanismo, el protocolo de aplicación Telnet hace posible la captura de información sensible mediante el uso de técnicas de *sniffing*.

- *File Transfer Protocol***.** Al igual que Telnet, FTP es un protocolo que envía la información en texto claro (tanto por el canal de datos como por el canal de control). Así pues, al enviar el identificador de usuario y la contraseña en claro por una red potencialmente hostil, presenta las mismas deficiencias de seguridad que el protocolo Telnet.

- *Hypertext Transfer Protocol.* Una de sus vulnerabilidades más conocidas procede de la posibilidad de entrega de información por parte de los usuarios del servicio. Esta entrega de información desde el cliente de HTTP es posible mediante la ejecución remota de código en la parte del servidor.

La ejecución de este código por parte del servidor suele utilizarse para dar el formato adecuado tanto a la información entregada por el usuario como a los resultados devueltos (para que el navegador del cliente la pueda visualizar correctamente). Si este código que se ejecuta presenta deficiencias de programación, la seguridad del equipo en el que esté funcionando el servidor se podrá poner en peligro.

b) ***Vulnerabilidades de la capa de transporte.*** La capa de transporte transmite información TCP o UDP sobre datagramas IP. En esta capa podemos encontrar problemas de autenticación, de integridad y de confidencialidad. Algunos de los ataques más conocidos en esta capa son las *denegaciones de servicio* referidas a protocolos de transporte.

En cuanto a los mecanismos de seguridad incorporados en el diseño del protocolo de TCP (como las negociaciones involucradas en el establecimiento de una sesión TCP), existe una serie de ataques que aprovechan ciertas deficiencias en su diseño. Una de las vulnerabilidades más graves contra estos mecanismos de control, se debe a la posibilidad de interceptar sesiones TCP establecidas, con el objetivo de secuestrarlas y dirigirlas a otros equipos con fines deshonestos, o bien realizar un monitoreo de ellas.

Estos ataques de secuestro se aprovechan de la poca exigencia en el protocolo de intercambio de TCP, respecto a la autenticación de los equipos involucrados en una sesión. Así, si un usuario hostil puede observar los intercambios de información utilizados durante el inicio de la sesión y es capaz de interceptar con éxito una conexión en marcha con todos los parámetros de autenticación configurados adecuadamente, podrá secuestrar la sesión.

Es importante también destacar una técnica para realizar los *ataques de monitorización*, en esta capar que el *scanning*, con sus diferentes variantes (TCP Connect Scanning, TCP SYN Scanning, TCP FIN Scanning, Fragmentation Scannig).

c) ***Vulnerabilidades de la capa de red.*** En esta capa se puede realizar cualquier ataque que afecte un datagrama IP. Se incluyen como ataques contra esta capa las técnicas de *sniffing*, la suplantación de mensajes, la modificación de datos, los retrasos de mensajes y la denegación de mensajes.

Cualquier atacante puede suplantar un paquete si indica que proviene de otro sistema. La suplantación de un mensaje se puede realizar, por ejemplo, dando una respuesta a otro mensaje antes de que lo haga el suplantado.
En esta capa, la autenticación de los paquetes se realiza a nivel de máquina (por dirección IP)
IP) y no a nivel de usuario. Si un sistema suministra una dirección de máquina errónea, el receptor no detectará la suplantación. Estos ataques se denominan de autenticación, y una de las técnicas más utilizadas es el *spoofing*.

Para conseguir su objetivo, este tipo de ataques suele utilizar otras técnicas, como la predicción de números de secuencia TCP, el envenenamiento de tablas caché, etc.

Por otro lado, los paquetes se pueden manipular si se modifican sus datos y se reconstruyen de forma adecuada los controles de las cabeceras. Si esto es posible, el receptor será incapaz de detectar el cambio.

c) ***Vulnerabilidades de la interfaz de red.*** Las vulnerabilidades de la capa de red están estrechamente ligadas al medio sobre el que se realiza la conexión. Esta capa presenta problemas de control de acceso y de confidencialidad.

Son ejemplos de vulnerabilidades a este nivel los ataques a las líneas punto a punto: desvío de los cables de conexión hacia otros sistemas, interceptación intrusiva de las comunicaciones (pinchar la línea), escuchas no intrusivas en medios de transmisión sin cables, etc. Se necesita acceso físico para realizar el ataque.

2. Ejemplos de Ataques

2.1 Ataque de DOS y DDOS

2.1.1 Concepto

Antes de comenzar a explicar los ejemplos puntuales. Se definirá los ataques DOS y DDOS.

Como sugiere el nombre, un ataque DOS hace que una red, un host u otro elemento de la infraestructura de red sean inutilizables por parte de sus legítimos usuarios. Típicamente, un ataque DOS consiste en incrementar mucho la carga de trabajo de la infraestructura atacada, de modo que no pueda realizar las tareas legítimas. En el ataque denominado de *inundación de SYN*, el atacante inunda un servidor con paquetes TCP SYN, cada uno con una dirección IP falsificada. El servidor al ser incapaz de diferenciar un SYN legítimo de otro falso, completa el segundo paso del acuerdo TCP para un SYN falso, reservando el estado y las estructuras de datos correspondientes (recordar el acuerdo de tres vías, que se realizaba en TCP).

El tercer paso nunca es completado por el atacante dejando un número de conexiones parcialmente abiertas. La carga asociada al procesamiento de los paquetes SYN y la escasez de memoria libre hace que el servidor colapse. Una forma de ataque similar consiste en enviar fragmentos IP a un host pero nunca los suficientes como para completar el datagrama. El host atacado continua acumulando fragmentos, esperando en vano los que completarían el datagrama, consumiendo cada vez más cantidad mayor de espacio de memoria. Un ataque *smurf* funciona haciendo que un gran número de host inocentes respondan a los paquetes ICMP de solicitud de *eco* con una dirección IP de origen falsa. Esto produce un gran número de paquetes ICMP de respuesta al *eco* enviado al host cuya dirección IP fue tomada *prestada*.
En el ataque de *Denegación de Servicio Distribuida (DDoS)*, el atacante, en primer lugar, consigue acceso a cuentas de usuario en numerosos host de Internet (por ejemplo, capturando contraseñas, husmeando paquetes o utilizando cualquier otro sistema para irrumpir en las cuentas de los

usuarios). Tras ellos, el atacante instala y ejecuta programas esclavos en cada sitio comprometido, las cuales esperan en silencio las órdenes recibidas desde el programa maestro. Con un gran número de estos programas esclavos en ejecución, el programa maestro puede contactar con todos ellos e indicarles que dirijan sus ataques de denegación de servicio hacia el mismo host objetivo. El resultado de este ataque coordinado es particularmente devastador, ya que proviene de muchos host atacantes al mismo tiempo.
Los ataques de denegación de servicio ocuparon los titulares en febrero de 2000, cuando eBay, Yahoo, CNN y otros grandes sitios web fueron atacados. Resulta difícil protegerse de los DoS, y más difíciles aún los de DDoS. El filtrado de paquetes es inútil, porque es difícil distinguir los datagramas "buenos" de los "malos". Con la utilización de la falsificación de IP, resulta difícil localizar el\los verdadero(s) origen(es) de los ataques. Varios recientes esfuerzos en investigación han intentado distintas técnicas para marcar las cabeceras IP según pasan a través de un router para poder rastrear el flujo de los datagramas DoS hacia su origen. Una vez que el host comprometido ha sido identificado, puede ser puesto en cuarentena, aunque este proceso es lento, al requerir intervención humana. Un ataque DDoS es incluso difícil y largo de resolver.

2.1.2 Ataque DOS a Yahoo!

El buscador más popular del mundo, Yahoo!, sufrió de un ataque de Denegación de Servicio el lunes 7 de Febrero del 2000 por la tarde, que lo dejó inutilizado durante tres horas.

El ataque fue llevado a cabo por un grupo de hackers que desde distintas ciudades del mundo lograron saturar los sistemas informáticos que mantienen en pie la compañía, realizando millones de peticiones utilizando el método de ataque *Smurfing*.

El *funcionamiento del ataque* consistió en "bombardear" coordinadamente, desde las 2:20 pm, con peticiones ficticias de información al motor de búsqueda, al directorio y a otras secciones del portal, con el objetivo de bloquear sus conexiones electrónicas.

El buscador recibió unas peticiones de información equivalentes a un gigabyte por segundo, una demanda extraordinaria que es desconocida en el mundo del comercio electrónico y que suele producirse no en un día sino en todo un año, este alto número de peticiones llevó al bloqueo de sus servicios.

Este ataque, es conocido como *Flooding* y S*murfing* demuestra la vulnerabilidad de los grandes portales, incluso algunos tan seguros y que dedican tantos recursos a prevenir las acciones de los hackers como es Yahoo!.

Flooding es el tipo de ataques que desactiva o satura los recursos del sistema. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando *Spoofing* y *Looping*. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Smurfing es una variante del ataque *ICMP Flooding*. Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones BroadCast para, a continuación, mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen (máquina víctima).

Este paquete maliciosamente manipulado, será repetido en difusión (Broadcast), y cientos ó miles de hosts mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP. Desgraciadamente la víctima no puede hacer nada para evitarlo

El ataque al portal, en que se utilizaron estas dos técnicas, fue caratulado como múltiple y letal, porque bloqueó las rutas electrónicas de Yahoo! durante más de tres horas. Los usuarios del buscador no pudieron acceder a sus servicios, especialmente a las cuentas de correo electrónico,

mientras que los intrusos informáticos enviaban mensajes falsos que recargaban los sistemas electrónicos e impedían el acceso.

Yahoo! tiene unas 465 millones de páginas web a las que ofrece servicios, lo que le convierte en el mayor operador en la Red. Es el portal más visitado de Internet en Estados Unidos, con una distribución total de 465 millones de páginas, muchas de las cuales contienen propaganda u otro tipo de publicidad.

Sin embargo, el ataque no tuvo por objetivo robar información confidencial de los clientes, sino dejarlo inoperativo a través de una denegación de todos sus servicios.

Al percatarse del ataque, Yahoo! intentó reconducir sus enlaces a sus centros en la costa este, pero sucedió tan rápido y fue tan masivo que no se pudieron transferir los servicios a tiempo a otros lugares.

Los atacantes no dejaron huellas, ni firmas y no colocaron mensaje alguno. Su único objetivo fue demostrar que podían sabotear el portal más famoso de Internet y "secuestrar" sus operaciones.

La *solución a estos tipos* de ataque está en manos de los administradores de red, los cuales deben configurar adecuadamente sus Routers, para filtrar los paquetes ICMP de petición indeseados (Broadcast); o bien configurar sus máquinas para que no respondan a dichos paquetes. Es decir, que lo que se parchea son las máquinas/redes que puedan actuar de intermediarias (inocentes) en el ataque y no la máquina víctima.

También se podría evitar el ataque si el Router/Firewall de salida del atacante estuviera convenientemente configurado para evitar Spoofing. Esto se haría filtrando todos los paquetes de salida que tuvieran una dirección de origen que no perteneciera a la red interna.

2.1.2 Ataque DDOS a CNN

La web de noticias, la CNN, sufrió un ataque distribuido de denegación de servicio (DDoS), el 19 de abril de 2008, que hizo que sus servidores no estuviesen disponibles durante unas horas.

El ataque consistió en inundar el sitio Web de CNN, con tráfico de internet para dejarla fuera de línea.

Fue llevado a cabo por un grupo de hacker pro-chino que se autodenomina “Revenge of the Flame”, que tomaron esta iniciativa después de que la red de noticias CNN hizo una cobertura del Tíbet, que en su opinión hubo demasiada crítica a China.

CNN informó que había sido atacado ya desde el jueves 18, causando que su página web se pusiera más lenta. Pero fue capaz de protegerse con bastante facilidad contra los ataques, reduciendo el número de visitas que aceptó de Asia, haciendo que su sitio fuese de difícil acceso desde este continente.

El efecto real del ataque fue "imperceptible". Por eso los atacantes decidieron llevar a cabo uno más masivo, pero fue cancelado debido a que la cadena CNN y los proveedores de Internet, se estaban preparando para contrarrestar el ataque.

2.2 Ataque de Phishing y Pharming

2.2.1 Conceptos

Uno de los fraudes más extendidos es el phishing, consiste en engañar a los usuarios para que efectúen operaciones bancarias en servidores web con el mismo diseño de un banco on-line.

Otra técnica similar y que cabe destacar es el pharming. Consiste en la manipulación de la resolución de nombres en internet, llevada a cabo por un código malicioso que se introdujo en el equipo. En los servidores DNS, se almacenan tablas con las direcciones IP de cada nombre de dominio. A una escala menor, en cada ordenador conectado a internet hay un fichero en el que se almacena una pequeña tabla con nombres de servidores y direcciones IP, de manera que no haga falta acceder a los DNS para determinados nombres de servidor.

El pharming consiste en modificar este sistema de resolución de nombres, de manera que cuando el usuario crea que está accediendo a su banco, realmente está accediendo a la IP de una página web falsa.

El phishing debe su éxito a la ingeniería social, aunque no todos los usuarios caen en estos trucos y su éxito está limitado. La diferencia está que el pharming no se lleva a cabo en un momento concreto, como lo hace el phishing mediante sus envíos, ya que la modificación de DNS queda en un ordenador, a la espera que el usuario acceda a su servicio bancario.

A través del "pharming", cuando el usuario teclea en su navegador la dirección de la página a la que quiere acceder, en realidad puede ser enviado a otra creada por el hacker, que **tiene el mismo aspecto que la original**. Así, introducirá sus datos confidenciales sin ningún temor, sin saber que los está remitiendo a un delincuente.

2.2.2 Ataque a Mountain America

El caso de Mountain America sin duda es de los que llama la atención, por la sofisticación del ataque. Los phishers montaron el sitio falso en https://www.mountain-america.net. La verdadera URL de esta entidad es https://www.mtnamerica.org/.

El primer punto a favor de los atacantes, se debió a la elección de un nombre de dominio que contiene el nombre de la entidad y nada más. Y segundo punto a favor, el ataque lo montaron sobre protocolo seguro https.

Pero se diferenció de otros ataques porque ese protocolo seguro https también permitía, como es lógico, pinchar en el candadito, y mostrar la información de los certificados. Y además había un certificado perfectamente válido.

Este certificado aparecía firmado por Equifax Secure Inc, y con un cifrado AES-256 de 256 bit. Un navegador Firefox ofrecería el mensaje "High-Grade Encryption" y los detalles del certificado, eran perfectamente claros y visibles.

El usuario que todavía dudase, y que tuviera algunas nociones, podía ver en el certificado SSL referencias a Checkpoint, una compañía con base en Salt Lake City, en Utah, EEUU, cuyos datos aparecían en el "Organizational Unit" del certificado SSL. La sede central de Mountain America está en Salt Lake City.

El usuario, una vez ha hecho todas esas comprobaciones, se dirigía al índice de la web falsa e introducía los datos que le eran requeridos, todo ello bajo una presunta actualización del programa Visa de la entidad.

El sitio web les deja el siguiente mensaje a los usuarios:

"Trust Your Instincts

If something in a communication from Mountain America Credit Union does not seem "right," go with your gut feeling. Do not respond to any suspicious communication. Immediately contact your nearest branch or our service center at 1-800-748-4302. "

Este mensaje quiere decir *"Confía en tus instintos. Tú eres el eslabón más débil de la cadena de seguridad"*

2.2.3 Ataque a eBay

No solo las entidades bancarias han sido víctimas del temible phishing, la empresa Ebay (sitio web, destinado a la subasta de productos a través de internet) también fue víctima de estos ataques.

El procedimiento fue la recepción de un correo electrónico, en el mismo se comunicaba que se habían realizado cinco intentos fallidos de usar clave y usuario de Ebay, y por motivos de seguridad se debían comprobar el usuario antes de 24 horas, para comprobarlo se debía usar el link del correo electrónico. El link los enviaba a una web falsa. Una vez ingresados los datos, se realizaba confirmaban que habían sido actualizados.

2.3 Ataque a servidores de correo: Spamming

Este tipo de ataque también se encuentra dentro de los ataques de Denegación de Servicios.
El SPAM es difícil de detectar, principalmente porque es adaptativo. Esto significa que los administradores estudian el SPAM para encontrar la manera de evitarlo, pero las personas que envían el SPAM también estudian los métodos de los administradores para poder pasar por encima de ellos, y hacer llegar sus mensajes.
El problema del correo no deseado se tiene que afrontar con mucho cuidado, porque un filtro demasiado permisivo no parará el spam, pero un filtro demasiado restrictivo hará que existan los 'falsos positivos', correos legítimos que no han llegado a su destino porque se han confundido con spam.

Estos ataques son los más extendidos, y los más realizados, y han sido propiciados por los *relay*.

Este es un gran problema de los sistemas de correo SMTP, del que se ha tomado conciencia los últimos años. Se llama relay a un servidor de correo, que permite el envío de correo sin ninguna restricción.

Si un servidor permite el *relay* se está favoreciendo el SPAM en la red, el envío de *e-mail* no deseado con fines casi siempre publicitarios.

Además, el *relay* causa una negación de servicio contra los usuarios legítimos, tanto desde un punto de vista estrictamente teórico – ya que alguien consume los recursos de forma no autorizada, degradando así el servicio ofrecido a los usuarios legítimos - como en la práctica: cuando un robot encuentra un servidor SMTP en el que se permite el *relay,* y lo utiliza masivamente mientras puede, cargando enormemente la máquina y entorpeciendo el funcionamiento normal de los sistemas.

Pero además, si se incluye a la organización en alguna `lista negra' de servidores que facilitan el SPAM se causa un importante daño a la imagen, e incluso ciertos dominios pueden llegar a negar todo el correo proveniente de dichos servidores.

Sólo existe una manera de evitar el *relay*: configurando correctamente todos los servidores de correo. Por supuesto, esto es completamente dependiente de los programas utilizados, por lo que es necesario consultar en la documentación correspondiente la forma de habilitar filtros que eviten el *relay*; por Internet existen incluso filtros genéricos para los servidores más extendidos, por lo que ese trabajo no será excesivo ni complicado.

En la zona se han realizado, una gran cantidad de ataques de spam, la mayoría han sido controlados por los administradores de correo, pero ante el mínimo descuido dichos ataques se ha llegado a concretar, teniendo por resultado la denegación del servicio para los usuarios legítimos.

Para las empresas que funcionan en la zona el correo electrónico es crítico, ya que por el se envían presupuestos, se comunican con subempleados, con otras empresas, etc. Un ataque de spam que deje al servidor en lista negras provoca una gran pérdida para los usuarios, además el tiempo

para volver a levantar el servicio es de mínimo 48 horas. Durante este tiempo se pierden los correos que son enviados.

El método de listas negras consiste en mantener un listado de servidores de correo de los que se tiene constancia que envían spam, marcándolos como 'indeseables'. Muchos servidores al recibir una conexión, comprueban si el servidor remitente está en la lista negra o no. Si está, cierra la conexión y no acepta el correo. Por tanto, funciona antes de la transmisión del mensaje, ahorrándose el tráfico de los correos no deseados.

Con este método, se logró 'marginar' a los servidores RELAY, que ya no tenían sólo el problema del SPAM, sino que se les añadía el problema que el resto de servidores de correo no aceptaban sus mensajes legítimos. O sea, tenían que hacer que les sacara de las listas negras. Y para eso se tiene que cerrar el acceso indiscriminado del servidor, y notificarlo a la lista que los había listado, para que lo comprobasen, y los quitaran.

Telefónica ha estado en listas negras muchas veces, y hasta países enteros (Corea, Nigeria), evitando cualquier correo que llegara de allí. Sin embargo, ante los ataques de spam no ha tomado medidas para controlar el spam.

Actualmente el 90% de los ISP utilizan alguna medida para controlar estos ataques, en los últimos años se ha eliminado prácticamente el relay. Los ISP solo dejan pasar por sus servidores a las cuentas de las que son responsables.

A continuación se detalla un ataque de spam con direcciones falsificadas, del cual han sido víctima muchos servidores de correo.

Los elementos que intervienen en este tipo de incidentes son:

- Emisor del ataque (spammer). Envía un mismo mensaje a un gran número de direcciones destino (masa de direcciones)..
- Máquina atacada: Máquina desprotegida, sin medidas anti-relay y encargada forzosamente a procesar la entrega del correo y de emitir informes de error. En algunos casos, han sido varias máquinas atacadas de forma simultánea.
- Emisores de fallos de error. Son las maquinas que emiten el informe de error: la propia máquina atacada y cualquier otro servidor de correo que esté recibiendo correo del ataque.
- Máquina inocente atacada. Es la receptora de los informes de error producidos en el ataque y de las denuncias. Puede ser una máquina correctamente protegida contra el spam.

Procedimiento del ataque.

- *Elaboración del mensaje*. El Emisor del ataque preparará un mensaje con un campo From: , a veces se añade también un campo Reply-to, ambos generalmente idénticos. Estas direcciones suelen ser falsas (podrán ser direcciones correctas e inundar el buzón del inocente propietario de la misma) escogidas al azar del estilo fd34rf@dpto.usal.es o incluso el mismo ataque puede utilizar unas direcciones similares en las que sólo cambian algunas letras.
- *Ataque a una máquina mal gestionada*. Mediante un procedimiento automático se inyecta el mensaje en un servidor desprotegido de Internet (Máquina atacada) con destino a un número elevado de direcciones de correo-e (masa de direcciones).

Es fácil que muchas de estas direcciones sean incorrectas.

- *Procesamiento de errores*. La máquina atacada además de gestionar la entrega de correo a direcciones correctas deberá procesar los errores producidos de las que son incorrectas.

Algunas de las direcciones a las que se envía el spam serán aceptadas por sus servidores de correo que las encaminarán hasta el servidor final el cual podrá rechazarlo por múltiples motivos y enviará un informe a la máquina del responsables de la dirección del campo From:.

- *Informes de error*. Estos informes irán a la dirección del campo From: y la máquina responsable de la misma, será la verdadera víctima de este tipo de ataques. Pero dado que la dirección del campo From: es incorrecta esta máquina inocente genera el clásico informe de error:
<<< 550 <j9fyx7429@gugu.usal.es>... User unknown
que, en este caso, se entregará en la cuenta local de postmaster Es decir, por cada dirección incorrecta, de las miles implicadas en el ataque, se producirá un informe de error que irá a la máquina inocente. Hay que tener en cuenta que pueden ser miles los errores y que la máquina receptora de fallos de error tendrá que emplear sus recursos en procesarlos. Además el buzón de postmaster de dicha organización se verá inundado de estos errores.

Detalles técnicos

Es práctica habitual que los emisores de correo basura (spammers) inserten direcciones de origen falsas. Las programas automáticos que utilizan incluyen una dirección falsa en el campo Mail From: de la transacción SMTP y en el campo From: (el que realmente ve el destinatario) de la cabecera del mensaje. Estos valores suelen ser idénticos y ninguno de ellos interviene en la entrega del ataque.

Esto se debe a una deficiencia del protocolo SMTP, ya que en su elaboración, no se pensó en la actual Internet sino en una red donde la confianza era regla común.

Siguiendo con los detalles técnicos, la verdadera dirección de entrega se encuentra en el valor del campo Rcpt To: de la transacción SMTP y ésta dirección puede no aparecer en el mensaje que recibe el destinatario, es decir el valor de la cabecera To: no tiene porqué encajar con la dirección de entrega. En algunos casos cuando se detecta que el valor del campo Rcpt To: y el To: de las cabeceras son diferentes añaden un cabecera adicional *Original-recipient*:.

A veces el spam entregado a miles de direcciones contiene una cabecera To: con la misma dirección del emisor o con una dirección de uno de sus dominios. Dicho campo, muchas veces lleva confusión y engaño.

Muchas veces no es una única máquina la atacada, ya que para obtener mejores rendimientos se realiza el ataque desde varias máquinas desprotegidas y mal gestionadas. Como el ataque lo realizan de forma automática, es muy importante tomar acciones rápidas cuando se ha detectado la causante del ataque.

Básicamente un servidor de correo bien gestionado sólo debe aceptar en el campo Rcpt To: direcciones de dominios de los que es responsable. Además los spammers eligen máquinas no protegidas y que además no incluyan las cabeceras de tipo Received: debido ya que esas cabeceras dejan un rastro de donde ha pasado el mensaje. Incluso pueden llegar a añadir falsas cabeceras Received: para complicar la labor de investigación o hacer que otras máquinas parezcan como culpables.

Es importante destacar que muchos de estos ataques suelen coincidir con el comienzo de fines semana o en períodos vacacionales. Se inyectan largas masas de direcciones destino a varios servidores mal configurados para que puedan trabajar mejor y el ataque no sea fácilmente detectado.

Como se ha visto todo es falsificable, el problema aumenta cuando el valor del campo Mail From: y To: contienen direcciones de dominios reales, ya que el ataque afecta a máquinas inocentes con el procesamiento de los errores. Si dicha dirección coincide casualmente o de forma malintencionada con una dirección real de un usuario, le ocasionará graves daños.

Efectos ocasionados

Estas máquina inocentes generalmente suelen estar bien gestionadas y el administrador se percatará de la existencia del problema por la cantidad de mensajes que llegan al buzón postmaster.

Según la intensidad del ataque los recursos de la máquina podrán verse mermados por las conexiones SMTP entrantes y el espacio en disco que irá ocupando el buzón del postmaster.

Habrá personas afectadas por el spam que emitirán denuncias haciendo un Reply y además lo enviará al responsable del dominio en postmaster y/o abuse o a otras direcciones que consideren relevantes para que su malestar sea atendido. Estas quejas producirán una avalancha de mensaje que aumentará el problema.

Otro efecto que se han presentado en máquinas inocente, es que se las ha incluido en filtros locales de algunos servidores de correo electrónico, como se mencionó anteriormente.

Sin embargo, uno de los peores efectos es el daño moral que se hace a la imagen corporativa de la institución a través de su dominio en Internet. Existieron casos en que algunas instituciones, han sufrido ataques, quedando como si hubieran enviado mensajes de carácter publicitario, pornográfico o ilegal.

2.4 Ataque de Web spoofing

2.4.1 Conceptos

Este ataque se realiza suplantando una página web real. Muchas veces este concepto se confunde con phishing. Pero se diferencia porque enruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información de dicha víctima (páginas WEB vistas, información de formularios, contraseñas etc.). La página WEB falsa actúa a modo de proxy solicitando la información requerida por la víctima a cada servidor original y saltándose incluso la protección SSL. El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

El Web spoofing es difícilmente detectable, quizá la mejor medida es algún plugin del navegador que muestre en todo momento la IP del servidor visitado, si la IP nunca cambia al visitar diferentes páginas web significará que probablemente se esté sufriendo este tipo de ataque.

En Argentina se han reportados varios casos de este tipo de ataque. Hace algunos años atrás, el tema de la seguridad no era contemplado en muchos sitios web, sobre todo en la zona, que muchas organizaciones, comenzaban a usar sus primeros sistemas informáticos.

Algunas organizaciones montaban sus servidores sobre sistemas Linux, creyendo erróneamente que bastaría para no sufrir ataques, sin tener en cuenta que todo sistema posee vulnerabilidades. Además se creía que ser víctima de un ataque, que aún hoy en día todavía se piensa en esta región, era algo prácticamente imposible.

Si bien, en la zona, recién se comenzaba a difundir el uso de internet, en otros países los fraudes, ataques de todo tipo ya crecían exponencialmente.

Por estos años Argentina fue un punto de ataque para grupos de otros países, especialmente por su país vecino: Brasil. Esto se debió a que se tenía conocimiento de la poca concientización que existía acerca de la seguridad informática, y de la escasa capacitación de la personas.

Recopilando información, acerca de dichos ataques, se encontró que Brasil junto a España, es uno de los líderes en ataques, siguiendo luego de EEUU, por supuesto.

Su especialidad es el phishing, pero también realizan ataques de otros tipos.

Un ataque del tipo web spoofing, en la zona, fue llevado a cabo hace 5 años por un grupo de Brasil, que consistió en ingresar al servidor de correo electrónico, y colocar una página web falsa en la sección de webmail, donde los usuarios introducen los datos para ingresar a su casilla, a partir de ahí interceptaban toda la información a la que accedían los usuarios.

También un blog de Neuquén ha sufrido este tipo de ataque.

Los resultados de estos hechos no se conocen con exactitud, y no se han difundido, porque afecta la imagen de las organizaciones.

3 Otros casos de ataques

En esta sección se describirá como ya se ha adelantado otros ataques, de los cuales no se ha encontrado suficiente información técnica de cómo fueron realizados pero que es importante destacarlos.

Los ataques de snooping tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla.

Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron: el robo de un archivo con más de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

CONCLUSION

Se está de acuerdo con que la seguridad en las redes TCP/IP es muy importante. Debemos tener en cuenta que en los tiempos que corren las redes no son tan seguras como antes, ya que en la actualidad se cuentan con mucho conocimiento, herramientas y al alcance de todos. A tal punto que cualquier persona que descarga un simple mail desde su casilla de correo puede estar siendo atacado, sin darse cuenta.

Lo importante que debemos conocer son los distintos tipos de ataques que existen y como se originan, para así poder estar, de alguna manera, protegidos contra los ya conocidos "hackers".

Lo que se buscó con este trabajo es dar a conocer algunos casos reales de ataques. Si bien en dichos casos se exponen los conceptos teóricos de cada tipo de ataque, la idea fue combinarlos con los hechos ocurridos para una comprensión mejor de la teoría.

Una de las desventajas de nuestra investigación es que no existe demasiada documentación sobre los ataques específicos, las herramientas utilizadas, y la forma en que se realizaron, esto se debe a que dar a conocer este tipo de incidentes degrada la imagen de las organizaciones víctimas, y muchos ocultan los ataques sufridos. Además esta información aparece generalmente en forma de noticias, en la que no se describe demasiada información técnica.

Mucha información, fue encontrada a partir de indagaciones a personas que trabajan en el área informática, hace tiempo, que nos aportaron datos para realizar las distintas búsquedas.

Por último lo que también se buscó es lograr una concientización acerca de que todo sistema es vulnerable, cualquier persona puede ser víctima de un ataque y que existen muchos grupos preparados al acecho.

REFERENCIAS

- [www.segu-info.com]
- [www.wikipedia.com]
- [http://www.elmundo.es/navegante/2000/02/08/yahoo.html]
- [http://www.websecurity.es]
- [http://www.sahw.com/wp/archivos/2006/02/14/analisis-de-un-ataque-phishing-casi-perfecto]
- [www.hakin9.org]
- [http://es.kioskea.net/attaques/attaques.php3]
- Redes de Computadoras. Un Enfoque Descendente Basado en Internet. James F. Kurose – Keith W. Ross. 2º Edición 2003
- [www.rediris.es]
- Revista NEXT IT #45