TIPOS DE ATAQUES: CÓMO ACTÚAN LOS PIRATAS INFORMÁTICOS

Servidores Web de Altas Prestaciones, UGR Ingeniería Informática

Realizado por : Juan Manuel López Castro
Ignacio Pineda Mochon

Tecnologías de la información

1- Definición de ataque informático:

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

2-Tipos de ataques informáticos:

2.1 Cartoneo

Podría considerarse como el ataque más sencillo de todos. De hecho, cualquiera con conocimientos minimos de informatica podria llevarlo a cabo. Se produce cuando un usuario decide apuntar su login y contraseña en un papel y posteriormente lo tira a la basura. Basta con rebuscar en la basura de la víctima para obtener dichos datos y suplantar su identidad.

2.2 DoS

Un ataque de denegación de servicio, también llamado ataque 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 provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.
Los ataques DoS se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando su servicio, es decir, hace que el servidor no pueda atender a la cantidad enorme de solicitudes. Esta técnica es usada por los piratas informáticos para dejar fuera de servicio al servidor en cuestión.

Una mejora del ataque DoS , es el ataque de denegación de servicio distribuido (DDoS), el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo destino. Esta herramienta ha sido utilizada para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y afectar a los servicios que ofrece.
Los síntomas de estar sufriendo un ataque DoS con los siguientes:

- Rendimiento de la red inusualmente lento (abrir archivos o acceder a sitios web)
- Indisponibilidad de un sitio web en particular
- Incapacidad para acceder a cualquier sitio web

-Ping de la Muerte:

Consiste en el envío de paquetes IP (fragmento ICMP) de un tamaño mayor a 64 bytes. Ante la imposibilidad de enviar un paquete de dicho tamaño con los protocolos de establecimiento de red, se procede a fragmentar el paquete en porciones que se envían a la víctima. Una vez en destino, la computadora víctima procede a montar el paquete saturando el buffer, lo que conlleva en la mayoría de los casos a un fallo en el sistema. Este tipo de ataques dejó de ser útil a finales del siglo XX, pues la gran mayoría de sistemas operativos han corregido la vulnerabilidad que daba lugar a dichos ataques.

-Ping Flooding:

Al igual que en el anterior, este tipo de ataques se llevan a cabo mediante el empleo de la herramienta ‘ping’. En este tipo de ataque DoS, se envían múltiples paquetes ICMP a la víctima, que tendrá que hacer frente a una gran cantidad de peticiones y posiblemente verá mermada su disponibilidad, llegando incluso a caer. Es fundamental en éste tipo de ataques que el ancho de banda del atacante sea mayor que el de la víctima, de esta forma se colapsará el receptor “antes” que el atacante. No obstante, lo ideal es delegar el ataque en máquinas que actúen como bots y realicen las peticiones. El receptor de los paquetes

ICMP los procesará y enviará de vuelta al origen. De ésta forma se colapsará el sistema, pero también podría llegar a afectar a la máquina desde la que se realizan las peticiones. Si el ataque se hace a un router, podría llegar a caer la red que conforman los ordenadores conectados a la(s) interfaz(es) del router.

2.3 ARP Spoofing

-Inundación MAC:

En un ataque típico de inundación MAC, un switch se inunda con paquetes, cada uno con diferentes direcciones MAC de origen. La intención es consumir la memoria limitada reservada en el switch para almacenar la tabla de traducción de puerto a físico de MAC. El resultado de este ataque hace que el switch ingrese a un estado llamado modo de apertura fallida, en el cual todos los paquetes entrantes se emiten en todos los puertos (como con un concentrador), en lugar de simplemente hacia abajo del puerto correcto según la operación normal. Un usuario malintencionado podría utilizar un analizador de paquetes (como Wireshark) ejecutándose en modo promiscuo para capturar datos confidenciales de otras computadoras (como contraseñas no encriptadas, correo electrónico y conversaciones de mensajería instantánea), que no serían accesibles si el interruptor funcionará con normalidad.

-Envenenamiento de caché DNS:

Consiste en el envío de datos a un servidor de nombres de almacenamiento en caché que no se originó en fuentes autorizadas del Sistema de nombres de dominio (DNS). Esto puede suceder a través del diseño incorrecto del software, la mala configuración de los servidores de nombres y los escenarios diseñados maliciosamente que explotan la arquitectura tradicionalmente abierta del sistema DNS. Una vez que un servidor DNS ha recibido datos no auténticos y los almacena en caché para aumentar el rendimiento en el futuro, se considera

envenenado, proporcionando los datos no auténticos a los clientes del servidor.

-IP Spoofing:

También existe la posibilidad de crear paquetes IP con una IP origen falsa, con el propósito de ocultar la identidad del remitente o hacerse pasar por otro sistema informático. De esta forma se puede acceder a un sistema sin estar autorizado a ello.

2.4 Escaneo de puertos

Es una de las técnicas de reconocimiento más populares que utilizan los piratas informáticos para descubrir los servicios expuestos a posibles ataques. Todas la máquinas conectadas a una red ejecutan muchos servicios que escuchan puertos. Un escaneo de puertos ayuda al atacante a encontrar los puertos que están disponibles.
Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos. Es usado por administradores de sistemas para analizar posibles problemas de seguridad, pero también es utilizado por usuarios malintencionados que intentan comprometer la seguridad de la máquina o la red.
Existen varios programas para escanear puertos por la red. Uno de los más conocidos es *Nmap*, disponible tanto para Linux como Windows.
El escaneo de puertos sería algo como el típico ladrón caminando por un grupo de automóviles y probando las puertas de los automóviles para ver qué puertas del automóvil están abiertas.

2.4.1 Formas de limitar la información dada en los puertos

- Una forma de limitar la información obtenida de escaneos de puertos es cerrar los servicios innecesarios en los sistemas de destino, es decir, si está ejecutando un servidor web, http debe ser el único servicio ofrecido. En los sistemas UNIX, la manera más fácil de limitar la información proporcionada a los escáneres de puertos es editar el /etc/inetd.conf y comentar cualquier servicio innecesario.
- Otra forma de limitar la cantidad de información dada a los escaneos de puertos es utilizar productos como PortSentry ofrecido por Psionic. PortSentry detecta las solicitudes de conexión en una serie de puertos seleccionados. PortSentry es personalizable y se puede configurar para ignorar una cierta cantidad de intentos. El administrador puede seleccionar qué puertos escuchará PortSentry para las solicitudes de conexión y la cantidad de solicitudes no válidas.

2.5 Ataque Man-In-The-Middle

Los ataques Man In The Middle son bien conocidos por gran parte de la comunidad informática. A pesar de que actualmente la seguridad ha aumentado, sigue siendo posible su realización; ya sea por el uso de software no actualizado por parte de algunos usuarios, o por el empleo de técnicas sofisticadas.

-LAN

En un primer lugar, nos centraremos en los MITM a nivel de red privada, para posteriormente explicar cómo se puede llevar a cabo un MITM a través de toda la red de internet. El procedimiento es sencillo. Basta con llevar a cabo un envenenamiento de la tabla ARP para hacer creer a la víctima que envía paquetes, por ejemplo, a otro host dentro de la LAN o incluso a su default Gateway real, cuando verdaderamente los está enviando al atacante (e igual para los paquetes que llegan a la víctima, por ejemplo, desde el Gateway). Existen en el mercado múltiples programas para llevar a cabo dicho procedimiento, que básicamente suplanta las IPs y las MACs. Una vez hecho ésto, se pueden analizar y leer los paquetes que envía y recibe la víctima, o incluso inyectar algún script malicioso. En el caso de que la conexión sea cifrada el proceso se dificulta.

En este caso, existe la posibilidad de utilizar determinados software para saltarse la protección que aporta https a los usuarios. Por ejemplo, SSLStrip es una herramienta que permite al atacante, una vez situado *en medio*, cambiar las peticiones HTTPS por HTTP (entre la víctima y el atacante) y que sea dicho atacante el que realice la peticion HTTPS al servidor. A pesar de que muchos navegadores ya implementan HTST (no aceptan peticiones HTTP para servidores que aceptan HTTPS), hay muchos usuarios que no han actualizado sus navegadores; incluso existe una versión de SSLStrip (2) para engañar al navegador que implementa HTST.

Otra opción para robar información con un MITM es a través de un troyano que se instala como una extensión en el navegador de la víctima. Dicho troyano, invisible, capturará información y la enviará a la máquina atacante. De esta forma se puede incluso modificar información de transacciones bancarias de maner transparente a la víctima.

Por último, mencionar la opción de montar un punto de acceso WiFi falso haciendo creer a las víctimas que se conectan a una red pública, cuando realmente se están conectando al atacante, que hace de intermediario entre la red real y la víctima.

-*WAN*

Existe también la posibilidad de llevar a cabo un MITM desde fuera haciendo uso del ICMP redirect. Los routers utilizan esto para ofrecer rutas alternativas y más rápidas para llegar a un destino. El atacante puede aprovecharse de ésto para alterar las tablas de ruta en los router y redirigir, por ejemplo, las peticiones DNS a su máquina. De ésta forma, podrá redirigir al atacante a las WEBs que él desee que podrán estar en un servidor propio. De esta forma, puede ofrecer a la víctima páginas falsas con las que robar sus datos, y posteriormente redirigir a la víctima a la WEB real a la que deseaba acceder para no levantar sospechas. Ésto también se puede llevar a cabo a nivel de LAN. Se han registrado ataques de éste tipo, denominados como MITM DoubleDirect.

También existe la posibilidad de montar un proxy en un país con una legislación *dudosa* para aprovecharse de aquellos usuarios que buscan el anonimato en la red (incluso otros hackers). De esta forma, cuando se conecten al proxy para llevar a cabo sus ataques, se les podría robar información o incluso inyectar scripts maliciosos cuando el usuario realiza una petición de un javascript, pudiendo así inyectar troyanos a las víctimas. De ésta forma se pueden incluso llegar a infectar los navegadores con *extensiones* que envíen al atacante los datos de un formulario de inicio de sesión, por ejemplo.

2.6 Ataque de secuencia TCP

Un ataque de predicción de secuencia TCP es un intento de predecir el número de secuencia utilizado para identificar los paquetes en una conexión TCP, que se puede usar para duplicar paquetes que conducen al secuestro de la sesión.
En un escenario típico de ataque de predicción de secuencia TCP, un atacante pasará cierto tiempo monitorizando el flujo de datos entre dos hosts. El atacante cortaría el sistema que no le interesa(que es confiable para el objetivo) de la comunicación, tal vez a través de un ataque de denegación de servicio (DoS), dejándolos a sí mismos para tomar el lugar de ese sistema confiable, a los ojos de su objetivo .
Habiendo predicho el número de secuencia del siguiente paquete que el objetivo espera de su host de confianza, el atacante prepara un paquete con la dirección IP de origen del sistema de confianza y el número de secuencia esperado. Es seguro que este paquete llegará a su destino antes que cualquier información legítima del host confiable (que tiene un ataque DoS para mantenerlo ocupado). El paquete del atacante se puede usar como una vía para obtener acceso al sistema de destino, terminar a la fuerza una comunicación o entregar una carga maliciosa.

2.6.1 Cómo prevenir los ataques de secuencia TCP

Teóricamente, información como diferencias de tiempo o información de capas bajas de protocolos, pueden permitir al host de destino distinguir paquetes auténticos de TCP del host de confianza y paquetes falsos, esto, con el número secuencial correcto enviado por el atacante. Si esa información está disponible para el host de destino, si el atacante no es capaz de falsificar esa información y el host de destino junta y usa esa

información correctamente, entonces el host de destino puede ser “inmune” a ataques de secuencia tipo TCP. Usualmente, este no es caso, así que el número secuencial es el primer medio de protección de tráfico TCP contra este tipo de ataque.
Otra solución a este ataque es configurar un router o un firewall para no permitir que entren paquetes de una fuente externa, pero con una dirección IP interna. Aunque esto no soluciona el ataque, va a prevenir que los potenciales ataques no lleguen a su destino.

3. Casos Reales

Zimperium Mobile Security Labs

Se trata de un blog de seguridad que realizó una investigación sobre los ataques Man In The Middle utilizando la técnica del DoubleDirect. Se descubrió que había más de 31 países afectados, entre los que estaban España, Italia y Alemania.

Ataque DDoS a Dyn

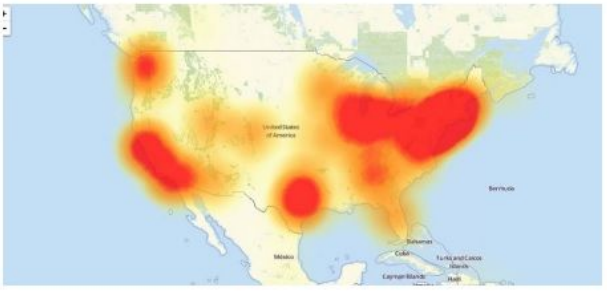
El ataque DDoS más grande registrado que afectó a sitios como Twitter, Spotify, Netflix, GitHub y Amazon

in noticias by claudia morales 24 octubre, 2016 0 comments

El 21 de octubre, la compañía DYN de gestión de rendimiento de Internet con sede en New Hampshire sufrió el ataque DDoS más grande registrado hasta el momento.

Los ataques fueron tres, en una sucesión relativamente rápida, siendo el último mitigado fácilmente. Se orientaron a la infraestructura DNS gestionado de la compañía. Esto causó la inaccesibilidad temporal de muchos sitios web y servicios en línea como Twitter, Spotify, Netflix, Amazon, GitHub, PayPal, Etsy, entre otros.

Lo que dice Dyn acerca de los ataques



"En este momento sabemos que fue un ataque sofisticado y altamente distribuido que involucró 10s millones de direcciones IP. Estamos llevando a cabo un análisis de las causas y análisis forense, e informar lo que sabemosmane
de una ra responsable ", comentó el Jefe de Estrategia Oficial Kyle York del Dyn.

"La naturaleza y el origen del ataque está bajo investigación, pero fue un sofisticado ataque a través de múltiples vectores de ataque y lugares de Internet. Podemos afirmar, con la ayuda de análisis de Flashpoint y Akamai, que una fuente del tráfico de los ataques eran dispositivos infectados por el botnet Mirai. Hemos observado 10s millones de direcciones IP discretas asociadas a la red de bots Mirai que formaban parte del ataque".

La Fatal Mirai

De acuerdo a Flashpoint, las redes de bots Mirai que se utilizaron en el ataque contra el Dyn "fueron botnets separadas y distintas" de las que se utilizaron para ejecutar los ataques DDoS contra el blog de Brian Krebs, y el servicio francés de internet OVH.

"A principios de este mes, 'Anna_Senpai," el hacker que opera la gran botnet Mirai utilizado en el Krebs DDoS, liberó el código fuente de Mirai en línea. Desde esta versión, otros cibercriminales han utilizado el malware para crear sus propias redes de bots con el fin de lanzar ataques DDoS".

Mirai aumenta fácilmente infectando dispositivos en su mayoría routers, DVR o cámaras WebIP, servidores Linux y dispositivos IoT funcionando con Busybox. Si sus propietarios no toman medidas para protegerlos, van a terminar infectados nuevamente en cuestión de minutos.

Desafortunadamente, algunos de estos dispositivos no pueden ser protegidos como deberían por causa de contraseñas codificadas, y el hecho de que sus fabricantes no hicieron posible su actualización.

Por el momento, la solución a este problema en particular todavía no está claro, aunque algunas propuestas en boca, incluyen la opción de "hackear e vuelta" para ganar el control de los dispositivos comprometidos. A medida que el número de dispositivos del IoT comprometidos se eleva, esta opción es seriamente considerada.

https://www.widefense.com/el-ataque-ddos-mas-grande-registrado-que-afecto-a-sitios-como-twitter-spotify-netflix-github-y-amazon/

Man-in-the-middle contra carteras Ledger

Ledger es una cartera de criptomonedas en formato hardware que soporta varias divisas, entre ellas las populares Bitcoin y Ethereum. Días atrás se halló en ese dispositivo una **vulnerabilidad que abre la puerta a ataques de tipo *man-in-the-middle***, pudiendo los atacantes robar el dinero de la víctima.

La empresa reconoció la existencia del fallo de seguridad el pasado 3 febrero, del cual se publicó un documento PDF en DocDroid. Mediante su explotación, un actor malicioso podría **suministrar a los clientes direcciones de recibo falsas, desviando así el dinero enviado por la víctima** hacia las carteras de los atacantes en lugar del verdadero destinatario. El investigador que descubrió el problema no se ha identificado.

https://www.muyseguridad.net/2018/02/09/vulnerabilidad-man-in-the-middle-carteras-ledger/

4. Bibliografía

- http://martra.uadla.com/como-hacer-un-man-in-the-middle-con-sslstrip-asi-se-roban-las-contrasenas/
- https://hipertextual.com/archivo/2014/06/ataque-man-in-the-middle/
- http://www.ebankingnews.com/noticias/que-es-man-in-the-browser-el-nuevo-tipo-de-troyano-que-ataca-a-la-banca-006263
- https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/
- https://blog.zimperium.com/doubledirect-zimperium-discovers-full-duplex-icmp-redirect-attacks-in-the-wild/
- https://www.youtube.com/watch?v=wjTjzXKpCWw
- https://es.wikipedia.org/