Sniffers. Escáneres. Ataques de denegación de servicio

Métodos de ataque [3]

Un ataque de "Denegación de servicio" impide el uso legítimo de los usuarios al usar un servicio de red. El ataque se puede dar de muchas formas. Pero todas tienen algo en común: utilizan la familia de protocolos TCP/IP para conseguir su propósito.

Un ataque DoS puede ser perpetrado de varias formas. Aunque básicamente consisten en:

- Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.
- Alteración de información de configuración, tales como información de rutas de encaminamiento.
- Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset).
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.
- Inundación SYN (SYN Flood)

Principios de TCP/IP

Cuando una máquina se comunica mediante TCP/IP con otra, envía una serie de datos junto a la petición real. Estos datos forman la cabecera de la solicitud. Dentro de la cabecera se encuentran unas señalizaciones llamadas Flags (banderas). Estas señalizaciones (banderas) permiten iniciar una conexión, cerrarla, indicar que una solicitud es urgente, reiniciar una conexión, etc. Las banderas se incluyen tanto en la solicitud (cliente), como en la respuesta (servidor).

Para aclararlo, veamos cómo es un intercambio estándar TCP/IP:

1.- Establecer Conexión: El cliente envía una Flag SYN, si el servidor acepta la conexión, éste, debería responderle con un SYN/ACK luego el cliente debería responder con una Flag ACK.

Inundación SYN (SYN Flood)

- 1-Cliente --------SYN-----> 2 Servidor
- 4-Cliente <-----SYN/ACK---- 3 Servidor
- 5-Cliente --------ACK-----> 6 Servidor

2.- Resetear Conexión: Al haber algún error o pérdidas de paquetes de envío se establece envío de Flags RST:

- 1-Cliente -------Reset-----> 2-servidor
- 4-Cliente <----Reset/ACK---- 3-Servidor
- 5-Cliente --------ACK------> 6-Servidor

La inundación SYN envía un flujo de paquetes TCP/SYN (varias peticiones con Flags SYN en la cabecera), muchas veces con la dirección de origen falsificada. Cada uno de los paquetes recibidos es tratado por el destino como una petición de conexión, causando que el servidor intente establecer una conexión al responder con un paquete TCP/SYN-ACK y esperando el paquete de respuesta TCP/ACK (Parte del proceso de establecimiento de conexión TCP de 3 vías). Sin embargo, debido a que la dirección de origen es falsa o la dirección IP real no ha solicitado la conexión, nunca llega la respuesta.

Estos intentos de conexión consumen recursos en el servidor y copan el número de conexiones que se pueden establecer, reduciendo la disponibilidad del servidor para responder peticiones legítimas de conexión.

SYN cookies provee un mecanismo de protección contra Inundación SYN, eliminando la reserva de recursos en el host destino, para una conexión en momento de su gestión inicial.

NUKE

Es una técnica DoS que pretende agotar el ancho de banda de la víctima. Consiste en enviar de forma continuada un número elevado de paquetes ICMP Echo request (ping) de tamaño considerable a la víctima, de forma que esta ha de responder con paquetes ICMP Echo reply (pong) lo que supone una sobrecarga tanto en la red como en el sistema de la víctima.

Dependiendo de la relación entre capacidad de procesamiento de la víctima y el atacante, el grado de sobrecarga varía, es decir, si un atacante tiene una capacidad mucho mayor, la víctima no puede manejar el tráfico generado,

SMURF

Existe una variante a ICMP Flood denominado Ataque Smurf que amplifica considerablemente los efectos de un ataque ICMP.

Existen tres partes en un Ataque Smurf: El atacante, el intermediario y la víctima (comprobaremos que el intermediario también puede ser víctima).

- En el ataque Smurf, el atacante dirige paquetes ICMP tipo "echo request" (ping) a una dirección IP de broadcast, usando como dirección IP origen, la dirección de la víctima (Spoofing). Se espera que los equipos conectados respondan a la petición, usando Echo reply, a la máquina origen (víctima).

- Se dice que el efecto es amplificado, debido a que la cantidad de respuestas obtenidas, corresponde a la cantidad de equipos en la red que puedan responder. Todas estas respuestas son dirigidas a la víctima intentando colapsar sus recursos de red.
- Como se dijo anteriormente, los intermediarios también sufren los mismos problemas que las propias víctimas.

Básicamente este ataque consiste en generar grandes cantidades de paquetes UDP contra la víctima elegida. Debido a la naturaleza sin conexión del protocolo UDP, este tipo de ataques suele venir acompañado de IP spoofing.

Es usual dirigir este ataque contra máquinas que ejecutan el servicio Echo, de forma que se generan mensajes Echo de un elevado tamaño.

Packet Analyzer [4]

Un analizador de paquetes (también conocido como un analizador de red, analizador de protocolos, o sniffer, o para determinados tipos de redes, un sniffer o sniffer inalámbrico Ethernet) es un programa de computadora o un pedazo de hardware que se pueden interceptar y registrar tráfico que pasa por un digital de la red o parte de una red. Como los flujos de datos fluyen a través de la red, el sniffer captura cada paquete y, si es necesario, decodifica los datos en bruto de los paquetes, que muestra los valores de varios campos en el paquete, y analiza su contenido de acuerdo a la correspondiente RFC u otras especificaciones.

Capacidades

El cable de transmisión LAN, dependiendo de la estructura de la red (hub o conmutador), se puede capturar el tráfico en todas o sólo algunas partes de la red desde una sola máquina en la red, sin embargo, hay algunos métodos para evitar la reducción del tráfico por los interruptores para ganar el acceso al tráfico de otros sistemas en la red (por ejemplo, ARP spoofing). Por supervisión de red propósitos, sino que también puede ser deseable para controlar todos los paquetes de datos en una LAN mediante un conmutador de red con una salida de control de llamada, cuyo propósito es reflejar todos los paquetes pasan a través de todos los puertos del conmutador cuando los sistemas de ordenadores están conectados a un puerto de conmutación. Para utilizar un grifo de la red es una solución mucho más confiable que utilizar un puerto de supervisión, ya que los grifos son menos propensos a abandonar los paquetes durante las cargas de alto tráfico.

En las redes LAN inalámbricas, se puede capturar el tráfico en un canal en particular, o en varios canales al utilizar varios adaptadores.

En emisión redes LAN y WLAN, para capturar el tráfico que no sea unicast tráfico enviado a la máquina que ejecuta el software de rastreo, multicast tráfico enviado a un grupo multicast a los que la máquina está a la escucha, y de difusión de tráfico, el adaptador de red que se utiliza para capturar el tráfico se debe poner en modo promiscuo, algunos rastreadores de apoyar esto, otros no lo hacen. En las redes LAN inalámbricas, incluso si el adaptador está en modo promiscuo, los paquetes no para el conjunto de servicios para los cuales se configura el adaptador por lo general se ignoran. Para ver los paquetes, el adaptador debe estar en modo monitor.

La información capturada se decodifica de forma digital en bruto en un legible formato que permite a los usuarios del analizador de protocolos para revisar fácilmente la información intercambiada. Analizadores de protocolo varían en su capacidad para mostrar los datos en múltiples puntos de vista, de forma automática detectar errores, determinar las causas profundas de los errores, generar diagramas de tiempo, la reconstrucción de TCP y UDP flujos de datos, etc.

Algunos analizadores de protocolo también puede generar tráfico y por lo tanto actuar como dispositivo de referencia, los cuales pueden actuar como evaluadores de protocolo. Estos probadores de generar el protocolo correcto para el tráfico de las pruebas funcionales, y también pueden tener la capacidad de introducir errores deliberadamente para probar la capacidad del DUT para hacer frente a las condiciones de error.

Analizadores de protocolo también puede ser basado en hardware, ya sea en formato de sonda o, como ocurre cada vez más común, combinado con un conjunto de discos. Estos dispositivos de los paquetes de registro (o una rebanada del paquete) a un conjunto de discos.

Usos

La versatilidad de la captura de paquetes significa que se puede utilizar para:

- Analizar los problemas de red
- Detectar la red de intrusos intentos
- Detectar uso indebido de la red por los usuarios internos y externos
- La documentación de cumplimiento de la normativa por la tala todo el tráfico perimetral y el punto final
- Obtener información para efectuar una intrusión en la red
- Aislar los sistemas de explotación
- Monitor de ancho de banda WAN de utilización
- Monitor de uso de la red (incluyendo a los usuarios internos y externos y sistemas)
- Monitor de los datos en movimiento
- Monitor de la WAN y el estado de seguridad de punto final
- Recopilar y reportar estadísticas de la red
- Filtro de contenido sospechoso de tráfico de la red
- Servir como fuente de datos primarios para la supervisión de la red día a día y de gestión

- Espiar a otros usuarios de la red y recoger información sensible como contraseñas (en función de cualquier contenido cifrado de los métodos que pueden estar en uso)

- Ingeniería inversa con protocolos propietarios utilizados por la red

- Depurar cliente / servidor de comunicaciones

- Depurar las implementaciones de protocolos de red

- Verifique que añade, se mueve y cambia

- Verificar la eficacia del sistema interno de control (servidores de seguridad, control de acceso, filtrado web, filtro de spam de proxy)

Sniffers [5]

El modo más sencillo de comprender su funcionamiento, es examinándola forma en que funciona un sniffer en una **red Ethernet**. Se aplican los mismos principios para otras arquitecturas de red.

Un sniffer de Ethernet es un programa que trabaja en conjunto con la **tarjeta de interfaz de red (NIC, Network Interface Card)**, para absorber indiscriminadamente todo el tráfico que esté dentro del umbral de audición del sistema de escucha. Y no sólo el tráfico que vaya dirigido a una tarjeta de red, sino a la dirección de difusión de la red 255.255.255.255 (Para todas las partes).

Para ello, el sniffer tiene que conseguir que la tarjeta entre en modo **"promiscuo"**, en el que -como indica la propia palabra- recibirá todos los paquetes que se desplazan por la red. Así pues, lo primero que hay que hacer es colocar el hardware de la red en modo promiscuo; a continuación el software puede capturar y analizar cualquier tráfico que pase por ese segmento.

Esto limita el alcance del sniffer, pues en este caso no podrá captar el tráfico externo a la red (osea, más allá de los routers y dispositivos similares), y dependiendo de donde esté conectado en la Intranet, podrá acceder a más datos y más importantes que en otro lugar. Para absorber datos que circulan por Internet, lo que se hace es crear **servidores de correo** o de **DNS** para colocar sus sniffers en estos puntos tan estratégicos.

Programas Sniffers**:**

A) SpyNet

Es un programa shareware muy sencillo, incluye 2 programas en 1, **"CaptureNet"** y **"PeepNet"**.

El primero es el que espía el tráfico en la red, guardando los paquetes de datos en formatos de bytes hexadecimales.

Mientras que el segundo analiza los datos recopilados, reconstruyendo los paquetes, o reproduciendo los correos incluso las contraseñas de los E-mail empleados (sólo la versión de pago); además muestra las direcciones de los ordenadores que participan y el protocolo empleado (pop3, http, smtp, etc.), así como los programas empleados (navegadores, programas de ftp, de correo, etc.) incluso hasta el sistema operativo.

B) Ethereal

Muy aplaudido en el mundo Linux, y ya con una versión para Windows. Su funcionamiento es similar al anterior, pero menos gráfico, aunque informa de lo que encuentra según el uso del protocolo. Y por supuesto, cuando se trata de POP3 localiza rápidamente el usuario y la contraseña. Y para rematar es **código abierto** (open source) y además **gratuito**.

C) WinSniffer

Es un programa **especialista en contraseñas**. Busca en toda la red accesos de login (usuario) y contraseñas, mostrándolos en pantalla. En concreto en la versión de prueba muestra el usuario y en la de pago, además la contraseña.

FUENTES

[1] 20/abril/2012

http://www.alegsa.com.ar/Dic/codigo%20malicioso.php

[2] 20/abril/2012

http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node12.html

www.segu-info.com.ar/ataques/ataques.htm [2]

[3]Ataque de denegación de servicio: 18 Abril 2012

http://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

http://it.aut.uah.es/enrique/docencia/ii/seguridad/documentos/t11-0506.pdf [3]

[4] Packet_analyzer: 18 Abril 2012

http://en.wikipedia.org/wiki/Packet_analyzer

http://www.internetmania.net/int0/int93.htm [4]

[5] que es esfifer: 18 Abril 2012

http://www.iso.org/iso/catalogue_detailcsnumber=39612

[6] miércoles 25 de abril de 2012 http://ldc.usb.ve/~poc/Seguridad-viejo/c-intro.pdf

[7] viernes 20 de abril de 2012 http://revista.seguridad.unam.mx/numero-12/principios-b%C3%A1sicos-de-seguridad-en-bases-de-datos

[8] viernes 20 abril del 2012 http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/MunozTorres.pdf

INVESTIGACIÓN REALIZADA POR:

JAVIER FRANCISCO KANTUN CHABLE

ANTONIO CHI PAT

OMAR ANTONIO UC COLLI

VICTOR MANUEL HUCHIN VELA

GILBERTO IVAN CAAMAL DZUL