Anexos

A

Glosario

ARP Spoofing. Técnica utilizada para infiltrase en una red. El principio del ARP Spoofing es enviar mensajes ARP falsos (falsificados, o spoofed) a la Ethernet. Normalmente la finalidad es asociar la dirección MAC del atacante con la dirección IP de otro nodo (el nodo atacado), como por ejemplo la puerta de enlace predeterminada (gateway). Cualquier tráfico dirigido a la dirección IP de ese nodo, será erróneamente enviado al atacante, en lugar de a su destino real

Background. Técnica utilizada en el monitoreo de red, se refiere a realizar un análisis detallado, generalmente al realizar un análisis mediante backgrund se llegan a tener estadísticas muy detalladas de los archivos analizados.

Bases de Datos. Es un "almacén" que nos permite guardar grandes cantidades de información de forma organizada para que luego sea posible acceder y utilizar esta información fácilmente

Crakear. Término utilizado cuando se aplican parches orientados a software propietario, que tienen el objetivo de alterar el funcionamiento del software original. Generalmente un software "crakeado" ocasiona que el software propietario al que ha sido aplicado el parche sea utilizado sin tener que pagar por su uso.

Debian. Es una comunidad conformada por desarrolladores y usuarios, que mantiene un S.O. GNU basado en software libre. Este sistema se encuentra precompilado, empaquetado y en un formato "deb". Debian nació como una apuesta por separar en sus versiones el software libre del software no libre. Por este motivo no vende directamente su software, lo pone a disposición de cualquiera en Internet, aunque sí permite a personas o empresas distribuirlo comercialmente mientras se respete su licencia.

Dirección IP. Se llama Dirección IP al número único asignado a un "host" en la red. Dichonúmero consta de 32 bits dividido en cuatro campos de 8 bits.Cada campo de 8 bits, es representado por un número decimal entre 0 y255, separado por periodos.

Cada dirección IPv4 identifica una red y un host único en cada red. Elvalor del primer campo determina cual porción de la dirección IP es elnúmero de la red y cual porción es el número del host. Los números dered están divididos en cuatro clases:

- Clase A (0.0.0.0 a 127.255.255.255)
- Clase B (128.0.0.0 a 191.255.255.255)
- Clase C (192.0.0.0 a 223.255.255.255)
- Clase D Multicast (224.0.0.0 a 239.255.255.255)

EITF (Internet Engineering Task Force). Es una organización internacional abierta de normalización, creada en Estados Unidos en 1986, que se encarga de regular las propuestas y los estándares de Internet, conocidos como RFC.

IP flooding. Ataque que se basa en la inundación masiva de la red mediante datagramas IP. Estos ataques se pueden utilizar para degradar el rendimiento de la red a la cual está conectado el perpetrador, generando paquetes con origen y destino aleatorio.

Además del degradado de la red, también pueden colapsar un equipo, con un ataque dirigido contra una víctima.

IP Spoofing. Ataque que tiene el objetivo de sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UDP o TCP. Hay que tener en cuenta que las respuestas del host que reciba los paquetes alterados irán dirigidas a la IP falsificada.

Estadísticas TOPN: Técnica utilizada en el monitoreo de red, que permite observar a los host o subredes que consumen el mayor BW.

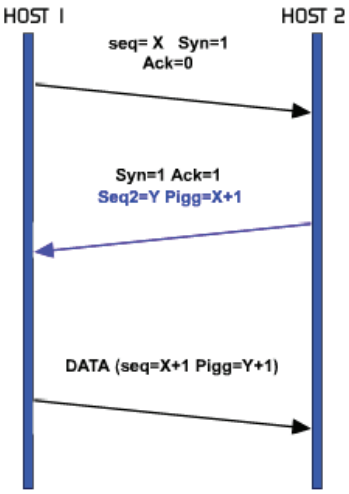
Estenografía. Rama perteneciente a la criptografía que permite ocultar información de distintas formas, como puede ser en imágenes, archivos, música, etc.

Falso Positivo. Son supuestos ataques generados por actividades legítimas. Generalmente son actividades normales clasificadas como anomalías. Ejemplo: El antivirus detecta un programa "casero" que genera múltiples conexiones como un gusano.

Falso Negativo. Son ataques reales considerados como actividades legítimas. Generalmente son anomalías clasificadas como actividades normales. Ejemplo: Múltiples conexiones de una misma IP hacia un servidor Web.

Handshake. Técnica utiliza en el protocolo TCP para conectar dos equipos electrónicos mediante los siguientes pasos:

- El servidor se mantiene a la espera de una conexión ejecutando las primitivas LISTEN y ACCEPT.
- El host que desea iniciar la conexión ejecuta una primitiva CONNECT especificando la dirección IP y el puerto con el que se desea conectar, el tamaño máximo del segmento que está dispuesto a aceptar. Entonces la primitiva CONNECT hace una apertura activa, enviando al otro host un paquete que tiene el bit SYN activado, indicándole también el número de secuencia inicial "x" que usará para enviar sus mensajes.



- El host receptor recibe el segmento revisa si hay algún proceso activo que haya ejecutado un LISTEN en el puerto solicitado. Si lo hay, el proceso a la escucha recibe el segmento TCP entrante, registra el número de secuencia "x" y, si desea abrir la conexión, responde con un acuse de recibo "x + 1" con el bit SYN activado e incluye su propio número de secuencia inicial "y", dejando entonces abierta la conexión por su extremo. El número de acuse de recibo "x + 1" significa que el host ha recibido todos los octetos hasta e incluyendo "x", y espera "x + 1" a continuación. Si no desea establecer la conexión, envía una contestación con el bit RST activado, para que el host en el otro extremo lo sepa.
- El primer host recibe el segmento y envía su confirmación, momento a partir del cual puede enviar datos al otro extremo, abriendo entonces la conexión por su extremo.

- La máquina receptora recibe la confirmación y entiende que el otro extremo ha abierto ya su conexión, por lo que a partir de ese momento también puede ella enviar datos. Con esto, la conexión ha quedado abierta en ambos sentidos.

ICMP (Internet Control Message Protocol). Protocolo estandarizado (RFC 792), que se utiliza como un medio de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta ping y traceroute, que envían mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa.

IDS (Intrusion Detection System). Mecanismo de seguridad encargado de detectas anomalías o actividad fuera de lo normal, que posiblemente se trate de un ataque o un falso.

Es importante mencionar que los IDS son mecanismos de detección no de prevención y son complementarios a mecanismos de seguridad existentes (Firewall, routers, etc.).

IPS (Intrusion Prevention System). Mecanismo de seguridad que monitorea la actividad en busca de anomalías, ataques o intrusiones y puede reaccionar de forma preventiva (bloquear) en tiempo real.

LAN (Local Area Network). Son redes de propiedad privada, de hasta unos cuantos kilómetros de extensión. Por ejemplo una oficina o un centro educativo.

Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.

Están restringidas en tamaño, lo cual significa que el tiempo de transmisión, en el peor de los casos, se conoce, lo que permite cierto tipo de diseños (deterministas) que de otro modo podrían resultar ineficientes. Además, simplifica la administración de la red.

Suelen emplear tecnología de difusión mediante un cable sencillo al que están conectadas todas las máquinas.

- Operan a velocidades entre 10 y 100 Mbps.
- Tienen bajo retardo y experimentan pocos errores.

Live CD. Es un sistema operativo (normalmente acompañado de un conjunto de aplicaciones) almacenado en un medio extraíble, tradicionalmente un CD o un DVD, que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de archivos.

Algunos Live CD incluyen una herramienta que permite instalarlos en el disco duro. Otra característica es que por lo general no se efectúan cambios en la computadora utilizada, aunque algunos pueden almacenar preferencias si así se desea.

MAC (Media Access Control). Una dirección MAC es una dirección física de 48 bits que identifica a una computadora de forma única en una trama Ethernet o alguna otra tecnología utilizada en la capa 2 del modelo OSI. Generalmente una MAC se divide en los primeros 24 bits que indican la dirección del fabricante y los últimos 24 bits indican el número de serie de nuestra computadora.

La dirección MAC es utilizada por los switch para identificar a una computadora en un segmento de red.

Memoria caché: Memoria en la que se almacenas una serie de datos para su rápido acceso.

Memoria Volátil. Es aquella memoria cuya información se pierde al interrumpirse el flujo de corriente eléctrica.

Modelo OSI El modelo OSI fue creado en 1984, surgió como un método para estandarizar todas las redes. Antes de su aparición las redes presentes tenían problemas para comunicarse entre sí; debido a que no se contaban con una serie de normas que debieran de cumplir dichas redes por lo cual las empresas podían crear sus redes de cualquier forma y esto causaba problemas en la comunicación de unas redes con otras redes pertenecientes a otras empresas.

Objetivo del modelo OSI: Una o más computadoras y el software asociado, periféricos, operadores, procesos físicos y significado de las transferencias que forman algo autónomo, el cual es capaz de procesar y/o transferir información.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. Estas capas son:

1. **Capa física.** Provee la transmisión binaria:
    a. Cables, conectores, voltajes, velocidades de transmisión de datos.
2. **Capa de enlace de datos.** Provee un control directo de enlaces, acceso a medios:
    a. Provee la transferencia confiable de los datos a través de los medios
    b. Conectividad y selección de ruta entre sistemas.
    c. Direccionamiento lógico.
    d. Entrega de mejor esfuerzo.
3. **Capa de red.** Provee dirección de red y determinación de la mejor ruta.
    a. Provee transferencia confiable de los datos a través de los medios.
    b. Conectividad y selección de ruta entre los sistemas.
4. **Capa de transporte.** Provee la conexión extremo a extremo.
    a. Se ocupa de aspectos de transporte entre host.
    b. Contabilidad de transporte de datos.
    c. Establecer, mantener y terminar circuitos virtuales.
    d. Detección de fallas y control de flujo de la información.
5. **Capa de sesión.** Provee la comunicación entre host.
    a. Establece, mantiene y termina sesiones entre aplicaciones
6. **Capa de presentación:** Provee la presentación de los datos.
    a. Garantizar que los datos sean legibles para el sistema receptor.
    b. Formato de datos.

c. Estructuras de datos.
d. Negocia la sintaxis de transferencia de datos para la capa de aplicación.

7. **Capa de aplicación:** Provee procesos de red a aplicaciones
    a. Suministra procesos de red a los procesos de aplicaciones (como por ejemplo: correo electrónico, transferencia de archivos y emulación de terminales).

Password: También conocido como contraseña, es una clave utilizada para impedir que cualquier usuario pueda tener acceso a la información propietaria. Es recomendable utilizar contraseñas con un mínimo de 6 dígitos, incluyendo mayúsculas, minúsculas, números, símbolos y caracteres especiales para evitar el fácil robo de la contraseña por un perpetrador.

Perl. Lenguaje de programación diseñado por Larry Wall en 1987. Este lenguaje toma características del lenguaje C, del lenguaje interpretado shell (sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

Estructuralmente, Perl está basado en un estilo de bloques como los del C o AWK, y fue ampliamente adoptado por su destreza en el procesador de texto y no tener ninguna de las limitaciones de los otros lenguajes de script.

Ping of Death. Ataque que consiste en mandar numerosos paquetes ICMP muy pesados (mayores a 65.535 bytes) con el fin de colapsar el sistema atacado.

Perpetradores. También conocidos como atacantes, piratas informáticos o entidades maliciosas, son personas que poseen conocimientos de seguridad informática y orientan sus habilidades en la obtención ilegal de información, bienes o activos mediante el uso de diverso malware creado por el (ellos) o por terceras personas.

La clasificación de los distintos tipos de perpetradores es muy amplia, sin embargo, los que más destacan son: crackers, hackers, phreakers, entre otros.

PHP. Lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas. Es usado principalmente en interpretación del lado del servidor (server-side scripting) pero actualmente puede ser utilizado desde una interfaz de línea de comandos o en la creación de otros tipos de programas incluyendo aplicaciones con interfaz gráfica usando las bibliotecas Qt o GTK+.

Polimorfismo. Técnica utilizada por diversos malware (como virus informáticos y gusanos) para modificar partes de su código dificultando su detección.

Programa: Conjunto de instrucciones ordenadas correctamente que permiten realizar una tarea o trabajo especifico.

Protocolo. Es un conjunto de reglas específicas, relacionadas al formato y tiempo de los datos transmitidos entre dos dispositivos.

Router. Dispositivos activos que operan en la tercera capa del modelo OSI. Su función es la de conectar dos o más LAN y proveer una transmisión fiables de los paquetes enviados.

Los routers son capaces de proveer conectividad para mezclar ambientes MAC y poder trabajar con un protocolo en la capa superior. Esto permite la conexión de diferentes segmentos de red.

Sin embargo, los routers no son capaces de traducir protocolos utilizados en capas superiores, por lo que un router debe ser equipado con software apropiado para poder soportar dichos protocolos.

El rol del router es dirigir paquetes a lo largo de manera eficiente, utilizando algoritmos de enrutamiento para obtener la ruta más corta o económica.

Sistema Operativo: Conjunto de programas relacionados entre sí que permiten administrar y controlar los recursos de la computadora de manera segura y eficaz, de tal manera que permite conectarse al usuario con la máquina.

Switch. Dispositivo activo que opera en la capa dos del modelo OSI, su función es evitar tener colisiones en la red y asignar a cada puerto un nodo específico, logrando con esto una separación entre la red y una mejor transmisión de la información. También nos sirve para interconectar dos o más segmentos en la red, pasando de un segmento a otro de acuerdo a las MAC que tienen los dispositivos conectados a los switch.

TCP (Transmision Control Protocol). Protocolo estandarizado (RFC 793) que opera en la capa de transporte del modelo OSI. El protocolo TCP permite establecer una conexión entre dos equipos, garantizando la entrega de datos sin errores y en el mismo orden en que se transmitieron. Algunos protocolos de aplicación que operan sobre TCP son; HTTP, SMTP, FTP, SSH, entre otros.

UDP (User Datagram Protocol). Protocolo estandarizado (RFC 768) que opera en la capa de transporte del modelo OSI. El protocolo UDP está orientado a enviar mensajes sin establecer una conexión mediante datagramas, además este protocolo no garantiza la entrega secuencial de los paquetes enviados ni que todos los paquetes se reciban.

Red Hat. Es la compañía responsable de la creación y mantenimiento S.O. Red Hat Enterprise Linux, Fedora y Centos entre otros. Red Hat es famoso en todo el mundo por los diferentes esfuerzos orientados a apoyar el movimiento del software libre. No sólo trabajan en el desarrollo de una de las distribuciones más populares de Linux, sino también en la comercialización de diferentes productos y servicios basados en software de código abierto. Algunas de las contribuciones más notables han sido la creación de un sistema de empaquetación de software (RPM), y varias utilidades para la administración y configuración de equipos, como sndconfig o mouseconfig.

TopN. Técnica implementada en cualquier software de monitoreo de red que muestra los host o subredes que han consumido el mayor tráfico en un lapso de tiempo específico.

VPN (Virtual Private Network). Tecnología que permite la conexión virtual segura entre puntos remotos cuya localización geográfica impide que la red local sea física. Generalmente la información que viaja a través de este túnel, viaja encapsulada y a través de un túnel cifrado.