



OMHE

Organización Mexicana de Hackers Éticos

Organización Mexicana de Hackers Éticos

Sniffers



OMHE

Organización Mexicana de Hackers Éticos

Definición

Un sniffer es una herramienta que captura paquetes o frames.

Este intercepta tráfico en la red y muestra por línea de comandos o GUI la información. Algunos Sniffer son tan sofisticados que interpreta los paquetes y puede unir el stream de paquetes en sus datos originales, tal como un correo o un documento.

Se puede usar para descubrir nombres de usuario, passwords y otra información confidencial transmitida en la red.



OMHE

Organización Mexicana de Hackers Éticos

Protocolos susceptibles para sniffing

El software para snifear trabaja capturando paquetes no destinados por el sistema hacia una dirección mac específica, pero también a un host en específico.

En el modo promiscuo el sistema lee todo el tráfico y lo manda al sniffer para su procesamiento.

Cualquier protocolo que no este encriptado es susceptible a ser sniffado. Protocolos tal como HTTP, POP3, SNMP (Simple Network Management Protocol) y FTP son los más comunes para ser capturados.



OMHE

Organización Mexicana de Hackers Éticos

Herramientas

- Ethereal ahora llamado WireShark
- Snort
- WinDump
- EtherPeek
- WinSniffer
- Iris



OMHE

Organización Mexicana de Hackers Éticos

Sniffing Activo y Pasivo

Pasivo: consiste en escuchar y capturar tráfico, es usual en una red conectada por hubs.

Activo: se basa en usar un ARP (Address Resolution Protocol) spoofing o ataque flooding.

El sniffing activo se puede detectar, pero el pasivo no.



OMHE

Organización Mexicana de Hackers Éticos

Hubs

En redes que usan hubs o en wireless, todos los host de la red pueden ver todo el tráfico.

El switch mira como se mandan los paquetes y trata de enviar los paquetes a los puertos basados en la mac address.

El switch mantiene una tabla MAC de todos los sistemas y el número de puerto en el cual esta conectado.

Esto habilita al switch para segmentar el tráfico y mandarlo solo al correcto destinatario según su dirección MAC.



OMHE

Organización Mexicana de Hackers Éticos

ARP

ARP permite a la red traducir la dirección IP a dirección MAC.

Cuando un host usa TCP/IP en una LAN, se trata de conectar a otro host y necesita la dirección MAC de su similar. Para realizar la conexión se realiza lo siguiente:

1. Revisa la cache ARP para verificar si tiene la dirección MAC
2. Si no la tiene genera broadcast preguntando ¿ Quien tiene la IP tal...la quiero contactar?.
3. Si el host que tiene a IP descrita escucha la petición, responde con su propia dirección MAC
4. La conversación empieza usando TCP/IP



OMHE

Organización Mexicana de Hackers Éticos

ARP Poisoning

Es una técnica que se usa para el ataque en una red ethernet y permite un ataque en una red con switchs o parar el trafico tambien.

Este utiliza ARP spoofing donde el proposito es mandar falsos mensajes ARP a la red LAN. Estos frames contienen falsas MAC que producen confusion en los dispositivos tal como los switchs.

Como resultado, los frames intentan con una y otra maquina (que es en donde se pueden snifear) o provocando un DoS.



OMHE

Organización Mexicana de Hackers Éticos

MAC Flooding

El hacker puede también "inundar" (flood) un switch con mucho tráfico para que pare su operación y para que el switch empiece a operar como un hub, mandando tráfico a todos los puertos del switch.

Este ataque activo de sniffer permite al sistema con el sniffer capturar todo los paquetes en la red.



OMHE

Organización Mexicana de Hackers Éticos

DNS spoofing

También llamado DNS poisoning es una técnica que engaña a un servidor DNS para que crea que a recibido información autentica cuando en realidad no lo es.

Cuando el usuario manda una petición de un sitio WEB, la dirección es encontrada por el servidor DNS, así como su correspondiente IP.

En el DNS que ha sido comprometido, el usuario es redireccionado a otro sitio web que el requerido, tal como un sitio falso.



OMHE

Organización Mexicana de Hackers Éticos

DNS spoofing

Para el ataque DNS, el atacante explota un defecto en el software del servidor, tal que puede aceptar datos incorrectos. Así se carga la información incorrecta en la cache del servidor.

Esta técnica puede ser usada para reemplazar contenido arbitrariamente para desplegar información que el hacker haya escogido.



OMHE

Organización Mexicana de Hackers Éticos

Técnicas DNS spoofing

- Intranet spoofing. Actúan como un dispositivo en una red interna.
- Internet spoofing. Actúan como un dispositivo de internet.
- Proxy server DNS poisoning. modifican las entradas de DNS en los servers proxis, redireccionando a los usuarios a diferentes host.
- DNS cache poisoning. modifican las entradas DNS en cualquier sistema.



OMHE

Organización Mexicana de Hackers Éticos

Herramientas

- EtherFlood
- Dsniff
- Sshmitm
- Arpspoof
- Cain&Abel



OMHE

Organización Mexicana de Hackers Éticos

Medidas para evitar el sniffing

La mejor medida es la encriptación. Ya que el atacante no puede interpretar los paquetes recibidos.

Para prevenir el ARP spoofing ,se debe añadir permanentemente la dirección MAC en el gateway a la cache ARP del sistema.

En un sistema de networking, solo se debe permitir a un solo puerto del switch una MAC address.



OMHE

Organización Mexicana de Hackers Éticos

Final

Preguntas??

GRACIAS



**Javier--demos
fj@omhe.org**