

Organización Mexicana de Hackers Éticos

Sniffers







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.





Protocolos suceptibles para sniffing

El software para snifear trabaja capturando paquetes no destinados por el sistema hacia una direccion mac especifica, pero tambien a un host en especifico.

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 suceptible a ser sniffeado. Protocolos tal como HTTP, POP3, SNMP (Simple Network Management Protocol) y FTP son los más comunes para ser capturados.





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





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.







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.





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

- Cuando un host usa TCP/IP en una LAN, se trata de conectar a otro host y necesita la direccion MAC de su similar. Para realizar la conexión se realiza lo siguiente:
- I. Revisa la cache ARP para verificar si tiene la direccion 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 peticion, responde con su propia direccion MAC
- 4. La conversación empieza usando TCP/IP





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.







El hacker puede tambien "inundar" (flood) un switch con mucho tráfico para que pare su operacion 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.







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 peticion de un sitio WEB, la direccion es encontrada por el servidor DNS, asi 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.





Para el ataque DNS, el atacante explota una defecto en el software del servidor, tal que puede aceptar datos incorrectos. Asi 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.





Técnicas DNS spoofing

- Intranet spofing. Actuan como un dispositivo en una red interna.
- Internet spoofing. Actuan 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.





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





Medidas para evitar el sniffing

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

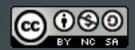
Para prevenir el ARP spoofing, se debe añadir permanentemente la dirección MAC en el gateway a la cache ARP del sistema.

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





Preguntas?? GRACIAS



Javier--demos fj@omhe.org

