Técnicas Básicas de Sniffing y MITM

marzo 29, 2011 adastra Deja un comentario Go to comments

En esta entrada, intentaremos explicar de forma clara y simple el uso algunas de las herramientas mas utilizadas para realizar ataques de MITM (Men/Monkey In The Middle) y Sniffing en una red de ordenadores determinada, el fin de esta entrada es introducir al lector sobre las técnicas empleadas con las herramientas a continuación indicadas, de esta forma, se podrán realizar posteriores entradas sobre tópicos mas avanzados con relación al hacking en redes y conceptos avanzados de networking.

DRIFTNET Y WIRESHARK

Herramientas muy útiles para capturar y analizar los paquetes que viajan por la red, usando driftnet desde linea de comandos debemos indicar la interfaz de red que deseamos utilizar para la captura activa de paquetes. En el caso de Wireshark, tenemos una herramienta mucho más completa que nos permite la selección de una interfaz de red para la captura activa de paquetes, filtros por protocolo y un pequeño lenguaje de expresiones que permite afinar los filtros establecidos, análisis de frames, etc.

NETCAT Y SOCAT

Netcat es una utilidad que permite iniciar un servicio de escucha en un puerto determinado, dicho puerto se encontrará abierto a nuevas conexiones y posteriormente es posible manipular los comandos o las teclas ingresadas en dicha conexión, como por ejemplo enviar todo a un fichero de log:

nc -lp 22 > /home/fichero

posteriormente cada una de las conexiones que se realicen sobre el puerto 22 serán dirigidas al fichero */home/fichero*

telnet MAQUINA 22

ETTERCAP:

Esta herramienta permite capturar y analizar los paquetes que viajan por la red y algunas otras operaciones como envenenamiento de paquetes ARP. Por ejemplo, para realizar un envenenamiento de ARP en una intranet, podemos seguir los siguientes pasos:

sudo ettercap -C

+ Menu Sniff/Unified sniffing…

– Se solicita el nombre de la interfaz de red.

+ Menu Hosts/Scan for Hosts

– Se buscan todos los ordenadores que se encuentran conectados en la red.

+ Hosts/Host List

– Seleccionamos el host que nos interesa y pulsamos 1 y luego seleccionamos el gateway y pulsamos 2.

+ Menu Mitm/Arp Poisoning

– Se solicitar el filtro, escribimos “remote”

+ Menu Start/Start Sniffing

+ Menu View/View Connections

DSNIFF

Se trata de una suite de herramientas para medir la seguridad en un segmento de red donde podemos incluir ataques como envenenamiento de ARP o sniffing de paquetes que viajan por la red, un uso clásico de dsniff consiste en un ataque ARP donde podemos engañar al gateway que somos el cliente y por otro lado, al cliente que somos el gateway, con esto todos los paquetes intercambiados en las peticiones entre gateway y cliente pasaran primero por nuestra máquina y posteriormente serán reenviados a su destino, con lo cual, tanto para el cliente como para el gateway la comunicación será transparente y enviaran peticiones/respuestas sin saber que están siendo capturadas por una entidad intermedia.

arpspoof -i wlan0 -t 192.168.1.35 192.168.1.1

(arpspoof -i -t)

arpspoof -i wlan0 -t 192.168.1.1 192.168.1.35

(arpspoof -i -t)

En el fichero */etc/sysctl.conf* se debe establecer:

net.ipv4.conf.forwarding=1

O ejecutar:

echo “1” > /proc/sys/net/ipv4/ip_forward

Posteriormente se puede comenzar a “olfatear”

ngrep host 192.168.1.35 | less

o

dsniff | less

DSNIFF es una suite de herramientas que abarcan mucho más que el envenenamiento de ARP, también nos permite realizar una auditoria completa de los datos que viajan en nuestra red por medio de algunos comandos bastante simples y útiles, a continuación se listan algunos de los comandos incluidos la suite:
filesnarf:

Te permite visualizar los ficheros que viajan por la red. Para su uso solamente basta con indicar la interfaz de red.

filesnarf -i wlan0

mailsnarf:

Te permite visualizar los correos que viajan por la red. Para su uso solamente basta con indicar la interfaz de red.

mailsnarf -i wlan0

msgsnarf:

Te permite visualizar los mensajes de clientes de mensajería instantánea que viajan por la red. Para su uso solamente basta con indicar la interfaz de red.

msgsnarf -i wlan0

sshow:

Te permite analizar el trafico sobre SSH que viaja por la red

sshow -i wlan0

urlsnarf:

Te permite visualizar las rutas de las páginas que viajan por la red. Para su uso solamente basta con indicar la interfaz de red.

urlsnarf -i wlan0

SSLSTRIP

Con sslstrip es posible ejecutar un ataque de hombre en medio sobre SSL (tipicamente por medio de HTTPS), SSLStrip intentará cambiar la ruta de navegación de la víctima por HTTP, de este modo se ejecuta un típico ataque MITM, así que la máquina que este ejecutando el comando sslstrip tendrá la capacidad de recibir los paquetes, cambiarlos al usuario final por HTTP y convertirlos nuevamente en una petición HTTPS al servidor, de esta forma tanto servidor como cliente pasan inadvertidos de lo que ocurre.

Obtener el código fuente desde:

http://www.thoughtcrime.org/software/sslstrip/

Posteriormente ejecutar

echo “1” > /proc/sys/net/ipv4/ip_forward

se debe configurar iptables para redirigir el trafico HTTP hacia sslstrip

iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 4444

En este caso se debería establecer el puerto *4444* en la ejecución de sslstrip como parámetro, para aceptar las conexiones y filtrar los paquetes que viajen por el puerto 80, (aplicaciones web).

Es posible instalar SSLStrip directamente en el sistema como un comando definido en el classpath o usarlo desde el directorio de descarga. Para instalarlo basta con ejecutar:

sudo python ./setup.py install

posteriormente ejecutar:

sslstrip -l 4444 -w fichero_capturas

con esto el programa quedará a la espera de nuevas peticiones entrantes por el puerto 4444, sin embargo para que esto tenga sentido es necesario engañar a un cliente de que somos los responsables del enrutamiento de la petición, para hacer esto es necesario realizar un ataque MITM donde el cliente pensará que nosotros somos el router y el router a su vez pensará que nosotros somos el cliente final, de este modo todo el trafico pasará por medio de nuestra máquina. Dado que anteriormente hemos definido que todos los paquetes que pasen por el puerto 80 serán redireccionados al puerto 4444, todas las peticiones web serán tratadas por sslstrip. El ataque MITM puede ser ejecutado con ettercap o con arpspoof (suite dnsniff)

TCPDUMP

Es bastante útil para capturar todos los paquetes que viajan por una interfaz de red, permite almacenar los paquetes capturados en un fichero dump muy completo con toda la información de paquetes y protocolos empleados, inclusive captura ficheros que viajan por la red, tales como documentos y/o imágenes. El uso más sencillo que se le puede dar es:

tcpdump -i wlan0 -s 0 -w /home/adastra/file.dump

Sin embargo cuenta con mas opciones para definir salidas al fichero de dump mas elaboradas y/o con mas información

Posteriormente es posible desempaquetar los contenidos del fichero dump por medio de la utilidad chaosreader

chaosreader /home/adastra/file.dump

La cual generará una estructura de directorios y páginas HTML donde se vincula toda la información capturada por el comando tcpdump.