Laboratorio 20

Herramientas de seguridad

Misión: Usar herramientas de seguridad para hacer exploración de instalaciones Asterisk

Requisitos:

Sistema con Asterisk instalado

Conexión a internet desde el sistema.

Acceso root

Pasos:

1. Conectarse a su maquina via ssh usando un cliente como mobaXterm (192.168.39.140 debe ser cambiado por su propia maquina).

Ssh 192.168.39.140

1. Probar si se tiene instalado netcat

$ nc

1. En caso contrario, instalarlo

$ sudo yum install –y nc

1. Probar de Nuevo

$ nc

1. Usarlo como scanner de puertos. Qué puertos tenemos abiertos? Como hacemos para un scan UDP?

$ nc –v –z localhost 1-10000 2>&1 | grep succeeded

1. Usemos el flag “-u” para hacer el scan por UDP

$ nc –v –z –u localhost 1-10000 2>&1 | grep succeeded

1. Podemos “escuchar”(eavesdropping) lo que está haciendo SIP? Encontremos el dispositivo que usa la ip de asterisk. En este caso es “enp0s8”

$ ifconfig

----------------------------

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.39.150 netmask 255.255.255.0 broadcast 192.168.39.255

inet6 fe80::54e9:dfa9:109d:9b4e prefixlen 64 scopeid 0x20<link>

ether 08:00:27:54:81:fb txqueuelen 1000 (Ethernet)

RX packets 108772 bytes 68411859 (68.4 MB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 77481 bytes 8982715 (8.9 MB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

1. Escuchemos a SIP

$ tcpdump -v -i enp0s8 port 5060

1. Ahora hagamos una llamada de la 5001 a la 5002. Observemos que sucede. Si todo salió bien, ya podemos escuchar a asterisk!
2. Ahora escuchemos a AMI. Cómo lo hacemos?

$ tcpdump -v -i enp0s8 port 5038

1. Ahora ejecutemos nuestro programa en php

$ php /root/modulos/conectarse.php

1. Qué sucedió? Por qué interfaz está funcionando el AMI?

$ sudo cat /etc/asterisk/manager.conf

1. Intentemoslo de nuevo con la interfaz apropiada

$ tcpdump -v -i lo port 5038

1. Ejecutemos el programa

$ php /root/modulos/conectarse.php

1. Observemos ahora que sucede
2. Y listo, estamos haciendo eavesdropping a AMI y a SIP en Asterisk!