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

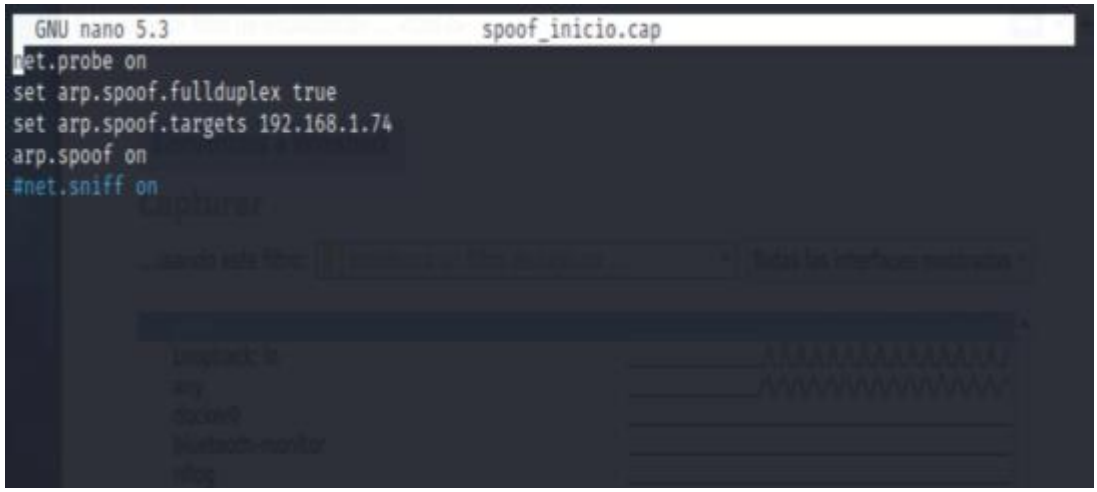
ACTIVIDADES

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/.

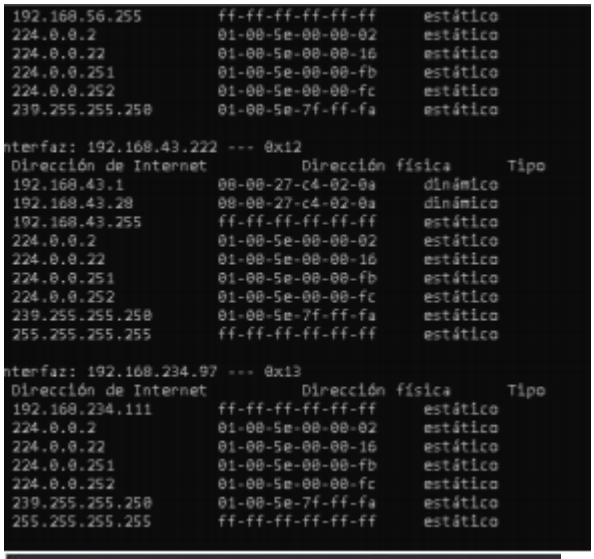
Rellena los siguientes puntos:

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

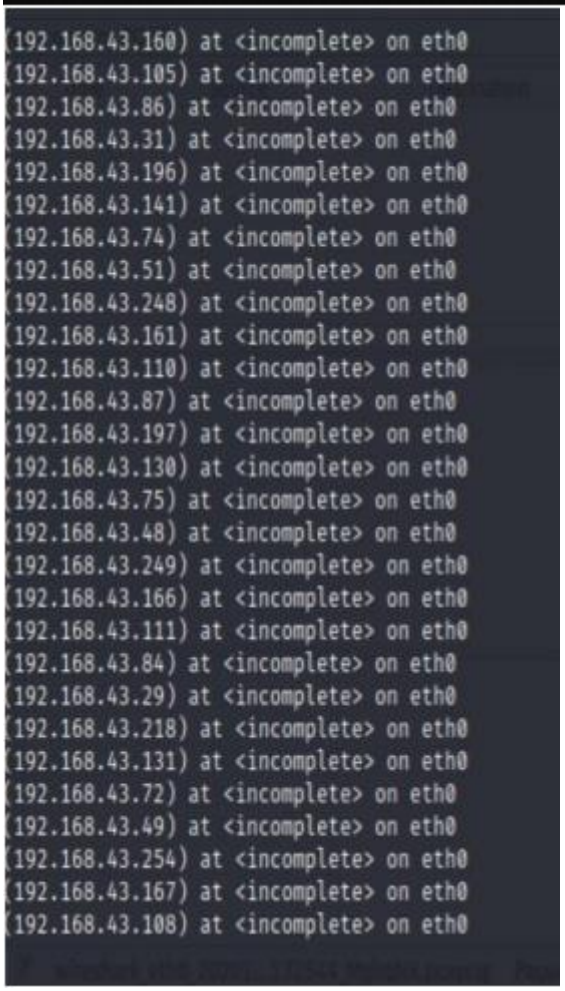


NOTA: En el script el sniffer no debe estar activado

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.

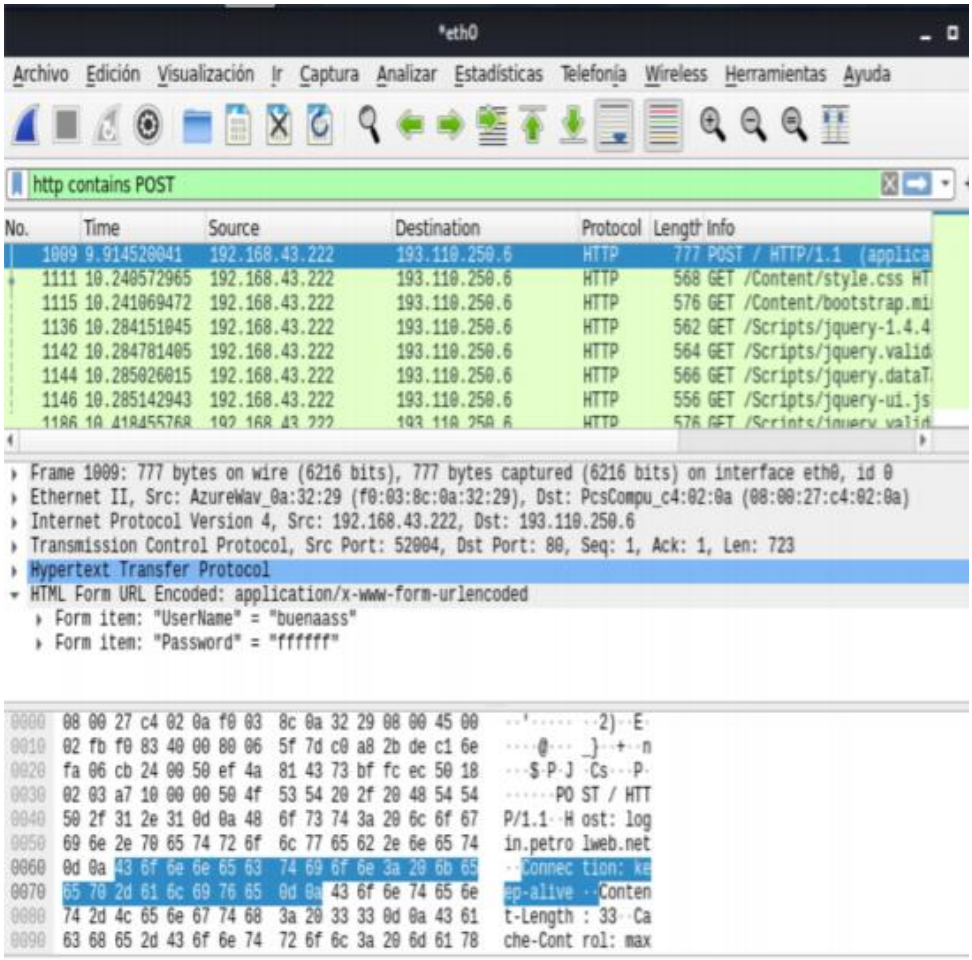


```
192.168.56.255        ff-ff-ff-ff-ff-ff     estático
224.0.0.2             01-00-5e-00-00-02     estático
224.0.0.22            01-00-5e-00-00-16     estático
224.0.0.251           01-00-5e-00-00-fb     estático
224.0.0.252           01-00-5e-00-00-fc     estático
239.255.255.250       01-00-5e-7f-ff-fa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

nterfaz: 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

nterfaz: 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.



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:

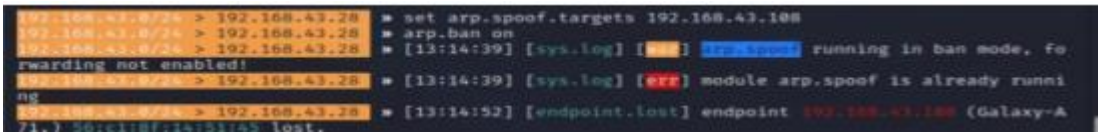
a. Clonar una web de un servicio de streaming como por ejemplo Netflix, HBO o Amazon (probar alguna herramienta que haga esto de forma automática)

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.



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.