EJERCICIO ATAQUE MAN IN THE MIDDLE

- Kali linux
- DVL 1.5
- Metasploitable2

- Realizar un ataque MiTM entre el cliente DVL y Metasploitable2 en el acceso al servicio web DVWA y capturar el usuario y contraseña.

1- Paso 1: se procede a realizar un nmap a la IP 10.0.2.0-255 de manera que nos diga cuales son las IPs que se encuentran en la red.

Nmap -sn 10.0.2.0/25

Kali linux IP: 10.0.2.15

Dvl 1.5 IP: 10.0.2.6

Metasploitable2 IP: 10.0.2.8

```
┌──(root㉿kali)-[~]
└─# nmap -sn 10.0.2.0-255
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-16 03:09 CET
Nmap scan report for 10.0.2.1
Host is up (0.00012s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00011s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00011s latency).
MAC Address: 08:00:27:D4:13:88 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.6
Host is up (0.00019s latency).
MAC Address: 08:00:27:74:E3:C3 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.8
Host is up (0.00064s latency).
MAC Address: 08:00:27:7B:5D:38 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.06 seconds
```

2- Paso 2: a continuación, para capturar más información procedemos a revisar el sistema operativo de las posibles victimas

```
┌──(root㉿kali)-[~]
└─# nmap -sV -O 10.0.2.0-255 -T 5
```

Información de la maquina DVL

```
Nmap scan report for 10.0.2.6
Host is up (0.00085s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Apache httpd 1.3.37
631/tcp  open  ipp        CUPS 1.1
3306/tcp open  mysql      MySQL (unauthorized)
5801/tcp open  http-proxy sslstrip
5901/tcp open  vnc        VNC (protocol 3.7)
6000/tcp open  X11        (access denied)
6001/tcp open  X11        (access denied)
MAC Address: 08:00:27:74:E3:C3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop
Service Info: Host: bt.example.net; OS: Unix
```

Información de la maquina Metasploitable2

```
Nmap scan report for 10.0.2.8
Host is up (0.00072s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7B:5D:38 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

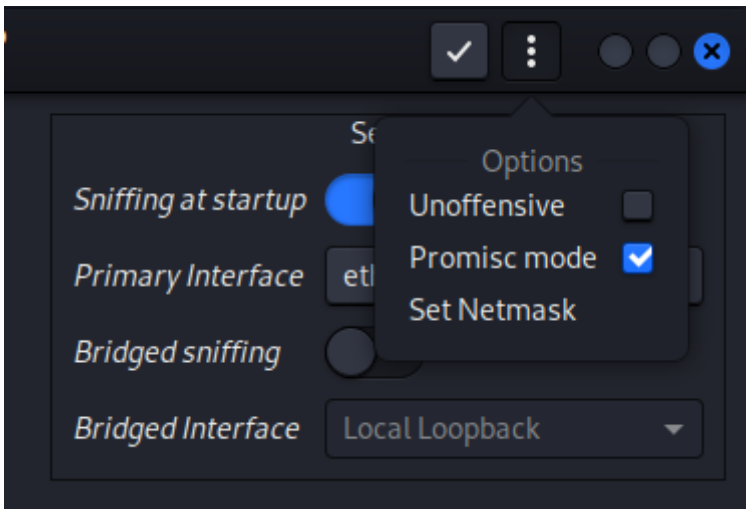
3- Paso 3: procedemos a abrir ettercap

Ettercap -G

Configuramos ettercap para iniciar la intercepción,

Primary interface: eth0

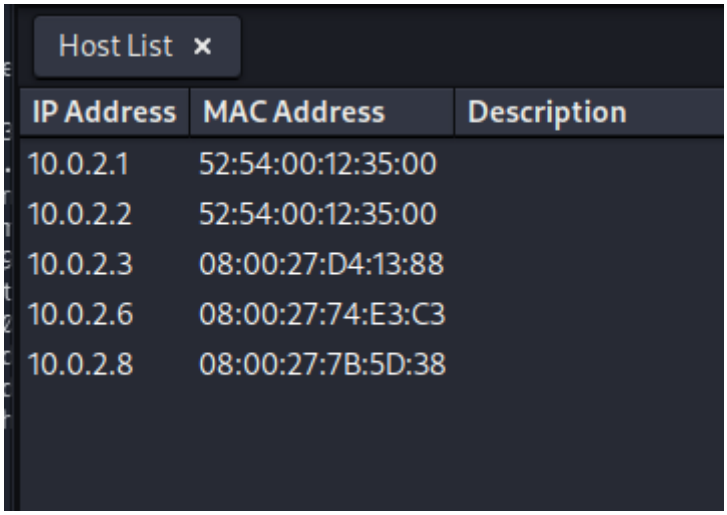
Modo promiscuo



4- Paso 4: escogemos los objetivos

En este son: Victima 1: DVL Y victima 2: Metasploitable2

Buscamos host y sus respectivos MAC Y escogemos las victimas como arriba.



Escogemos el método ARP que significa suplantar un dispositivo enviando mensajes falsos al router para que nos de acceso.

5- Paso 5: vamos a la victima 1 DVL y vemos si se logro la suplantación de Kali con un dispositivo.

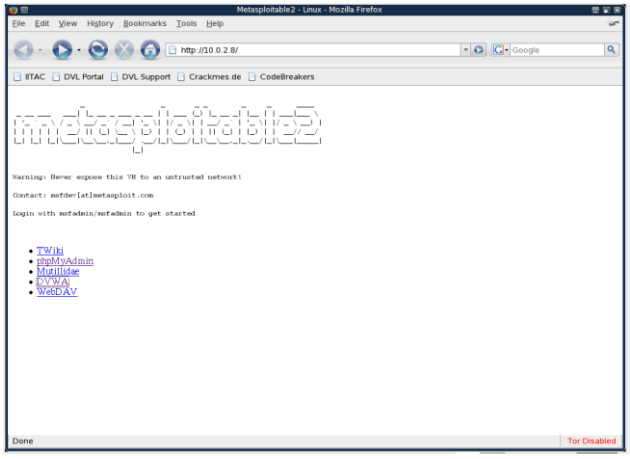
Con arp -a y ping comprobamos la suplantación de Kali a metaspolitable2

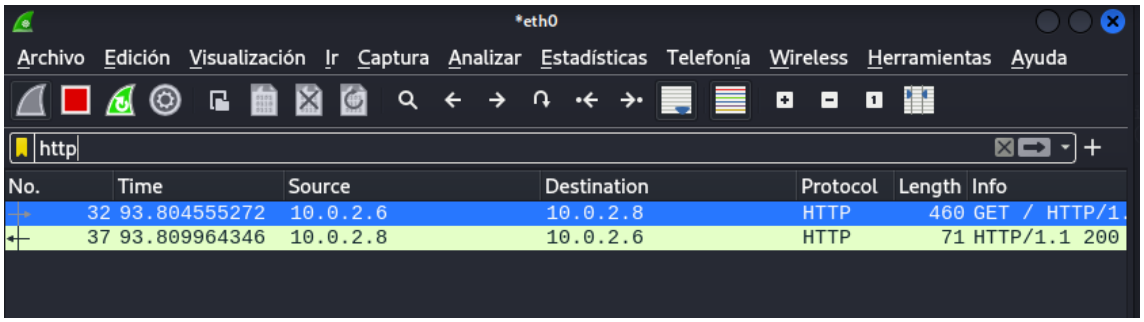
```
bt ~ # arp -a
? (10.0.2.8) at 08:00:27:4B:1F:9F [ether] on eth0
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
bt ~ # ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=3.81 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=2.52 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.403 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=1.31 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=1.44 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.582 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=1.96 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=1.42 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=1.01 ms

--- 10.0.2.15 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8011ms
rtt min/avg/max/mdev = 0.403/1.609/3.817/0.992 ms
bt ~ # arp -a
? (10.0.2.8) at 08:00:27:4B:1F:9F [ether] on eth0
? (10.0.2.15) at 08:00:27:4B:1F:9F [ether] on eth0
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
bt ~ #
```

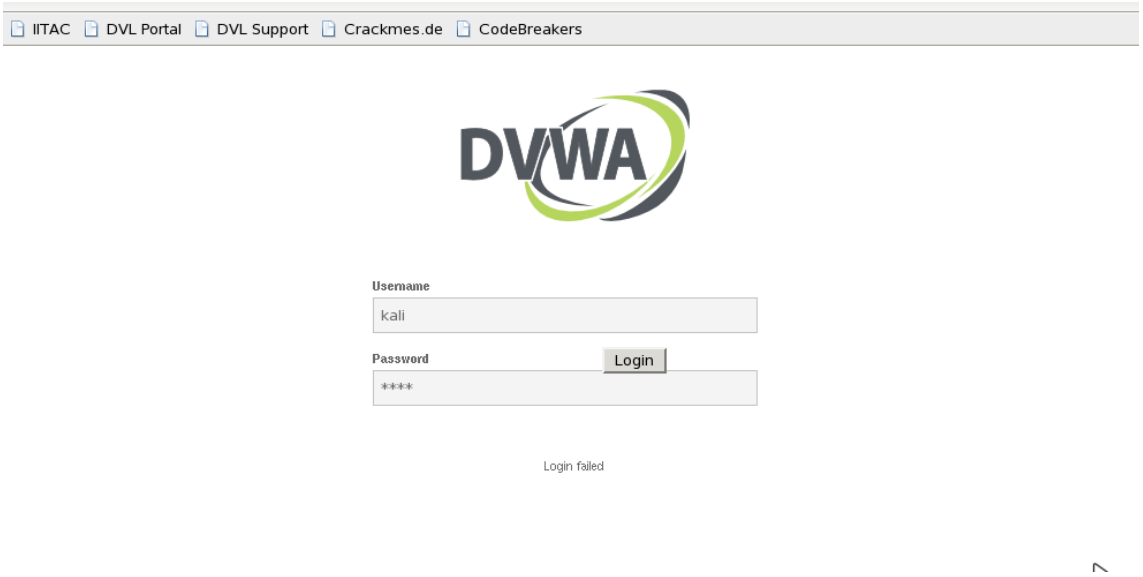
6- Paso 6: Veamos que información podemos sacar con esta suplantación

Procedemos a usar wireshark para capturar trafico y ver que información interesante se encuentra.





Para probar introducimos un usuario y contraseña para ingresar a DVWA y vemos si fue capturado en wireshark

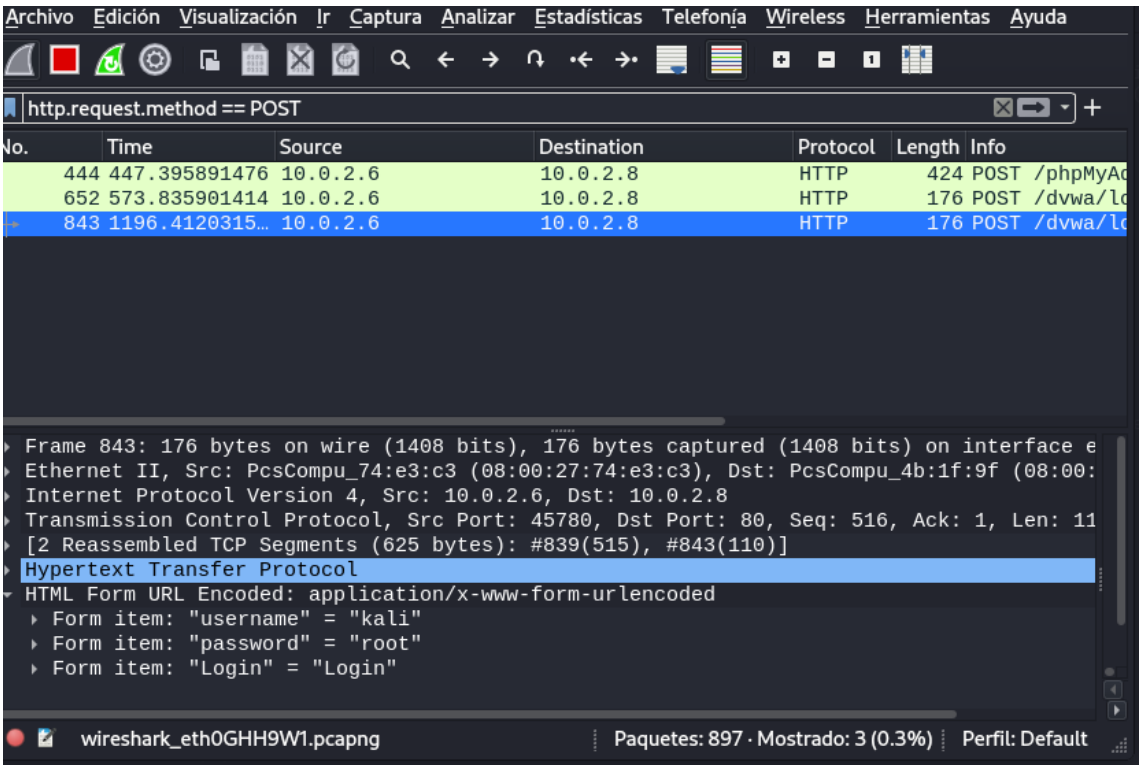


En el grafico de abajo podemos ver que se capturo tanto contraseña como user de DVWA

User:Kali

Password: root

Se usa http.request.method == POST para buscar en todas las capturas lo que necesitamos.



Con esto comprobamos que pudimos interceptar la comunicación entre estos dos dispositivos y extraer información interesante.