EJERCICIO ATAQUE MAN IN THE MIDDLE

Prerrequisitos

Kali Linux
Damn Vulnerable Linux 1.5
Metasploitable2

Ejercicio 1

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

https://keepcoding.io/blog/como-instalar-dvwa-en-kali-linux/

```
┌──(root㉿kali)-[/home/ginner]
└─# nmap -sV 10.0.2.0/24 -T5 -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-16 17:54 CEST
```

Una vez hayan aparecido las IP's la manera de conocer cual pertenece a la máquina correspondiente será debido a que *metasploitable* tiene muchos puertos abiertos mientras que *DVL* no tantos. Por tanto

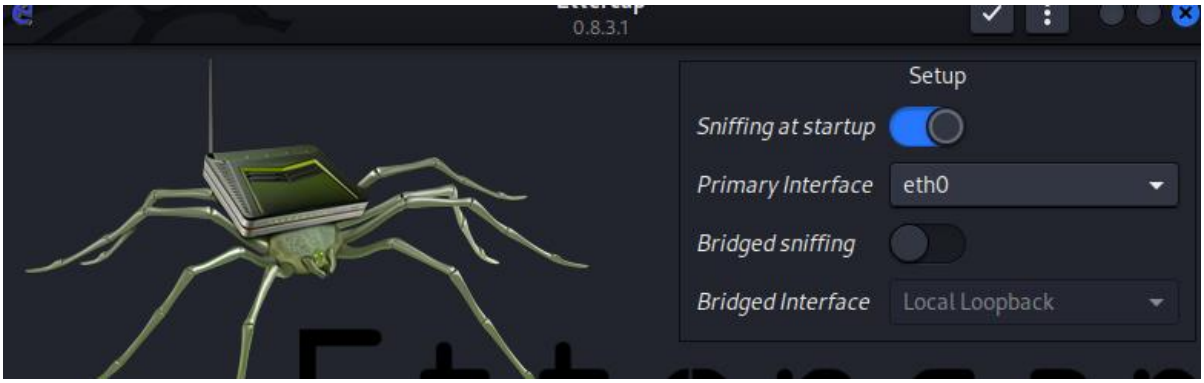
- Metasploitable

```
Nmap scan report for 10.0.2.7
Host is up (0.021s 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?
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:FF:D7:A9 (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: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kerne
```

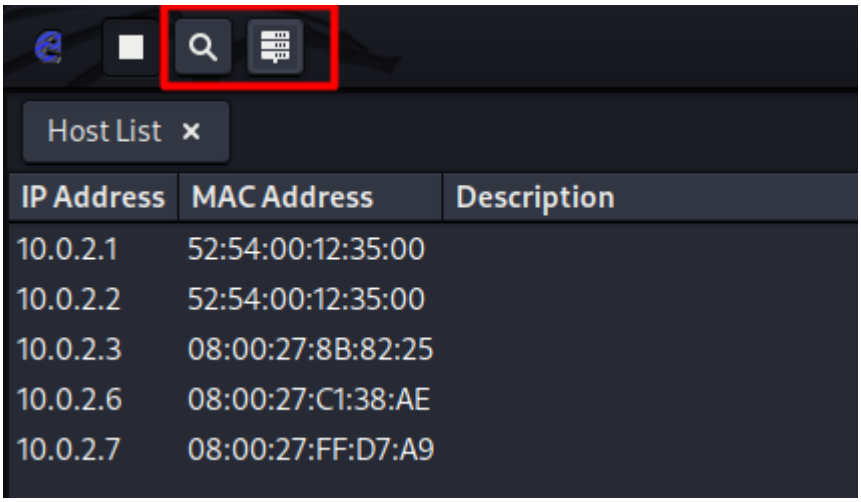
- DVL

```
Nmap scan report for 10.0.2.6
Host is up (0.0014s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
631/tcp  open  ipp     CUPS 1.1
3306/tcp open  mysql   MySQL (unauthorized)
6000/tcp open  X11     (access denied)
MAC Address: 08:00:27:C1:38:AE (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: OS: Unix
```

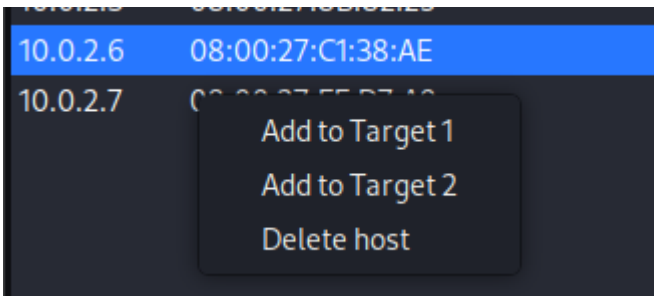
Una vez identificadas las maquinas procedemos a abrir *ettercap*



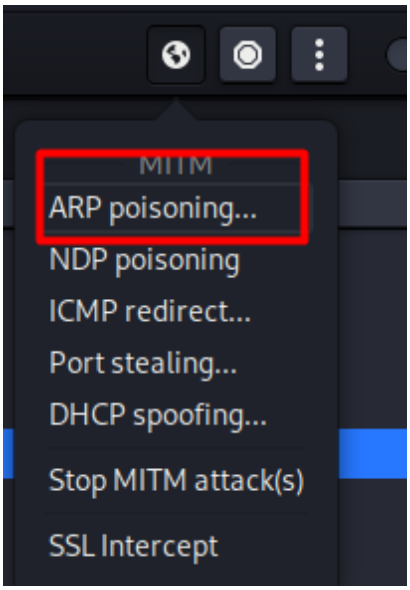
Tras esto iniciaremos una búsqueda de IP's através de la herramienta pulsando el botón de la lupa y tras haber realizado la búsqueda listaremos lo encontrado.



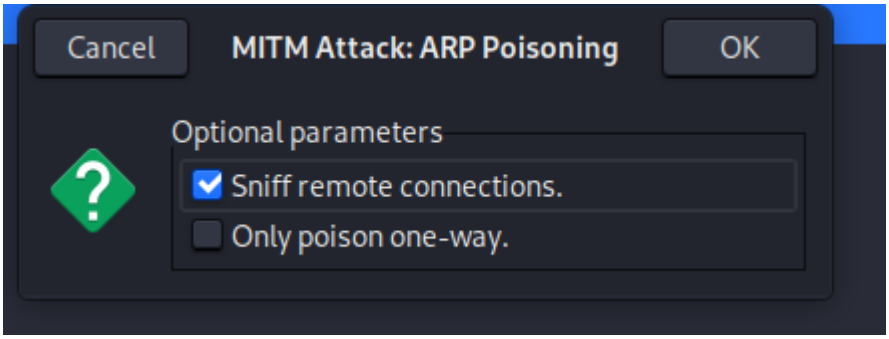
Tras esto estableceremos el *Target* 1 y el 2 a las IP's vistas anteriormente

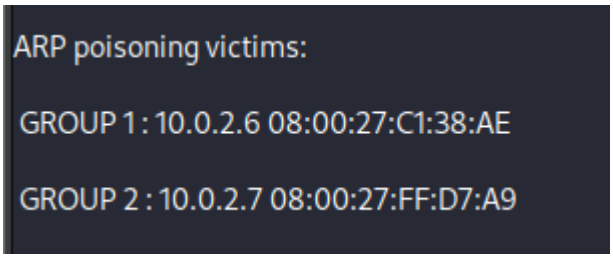


Posteriormente pincharemos el botón del mundo y nos aparecerán varias opciones, de estas escogeremos *ARP poisning*



Aparecerá un recuadro y daremos al botón de OK

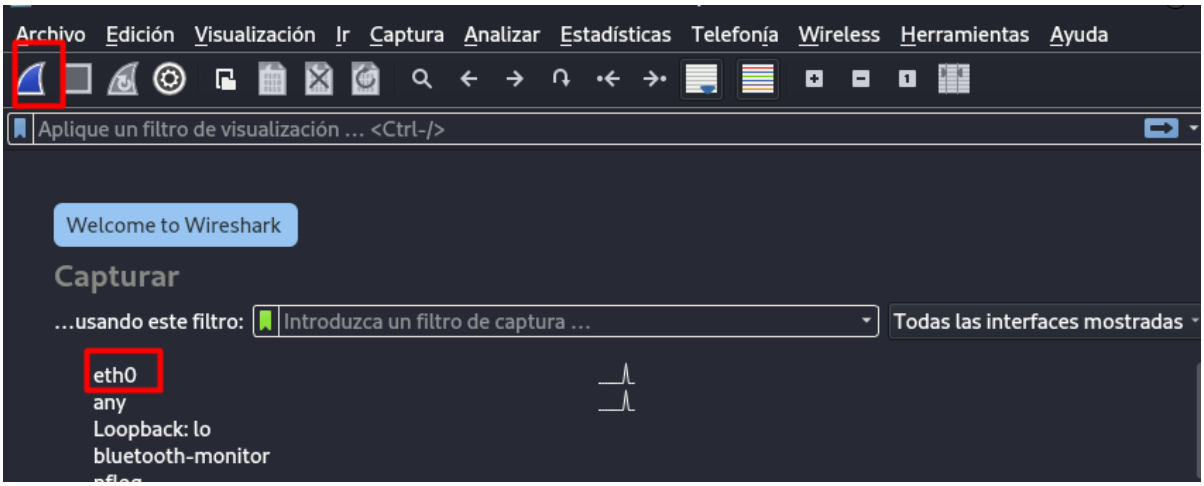


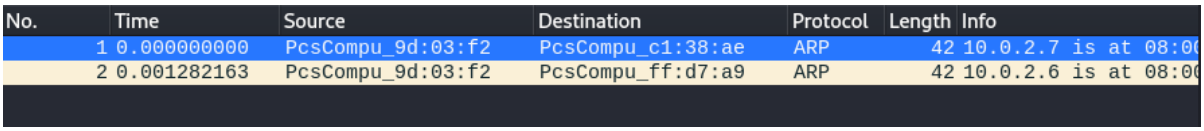


Con esto confirmamos los *targets* establecidos

Una vez realizado todo esto abrimos el *wireshark* desde otra terminal para poder continuar con la actividad.

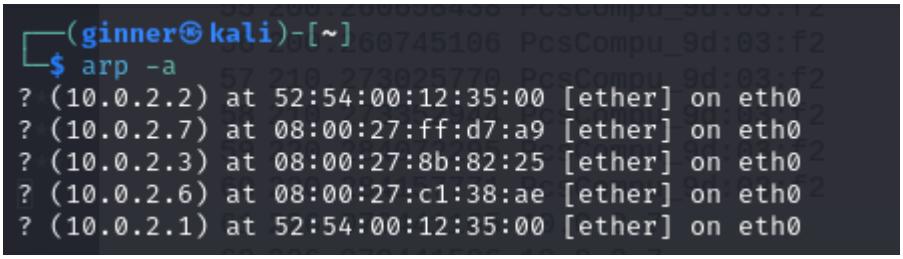
Seleccionamos eth0 e iniciamos la busqueda





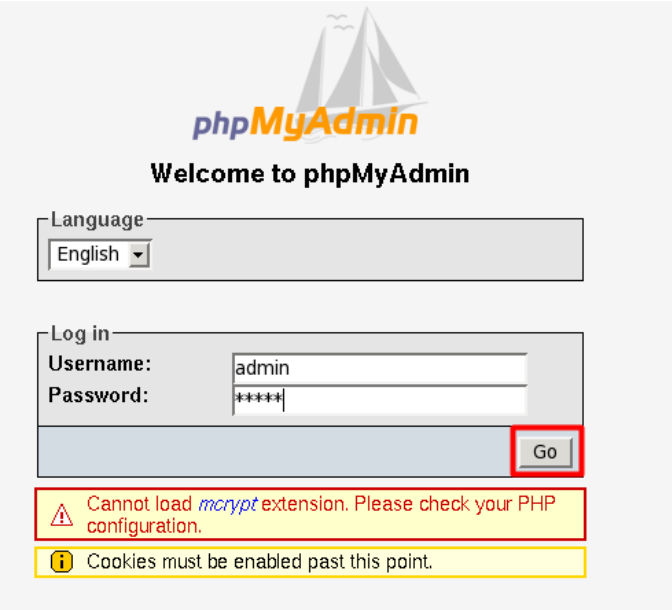
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_9d:03:f2	PcsCompu_c1:38:ae	ARP	42	10.0.2.7 is at 08:0
2	0.001282163	PcsCompu_9d:03:f2	PcsCompu_ff:d7:a9	ARP	42	10.0.2.6 is at 08:0

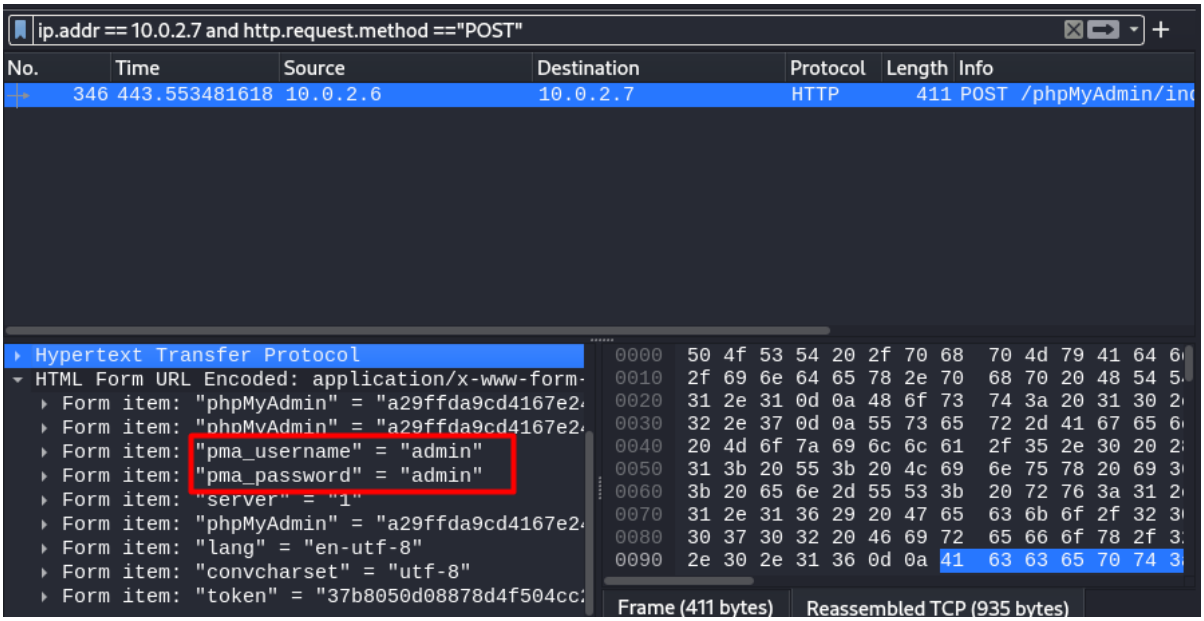
Para poder confirmar que está en funcionamiento abrimos otra terminal y realizamos lo siguiente



En DVL abrimos el navegador y solicitamos la ip de Metasploitble2

Tras esto entramos en phpAdmin y rellenamos con nuestras credenciales, tras esto abriremos wireshark y las veremos una vez hallamos aplicado los filtros correspondientes





Se observa que con el uso de los filtros correspondientes encontramos las credenciales escritas desde la DVL