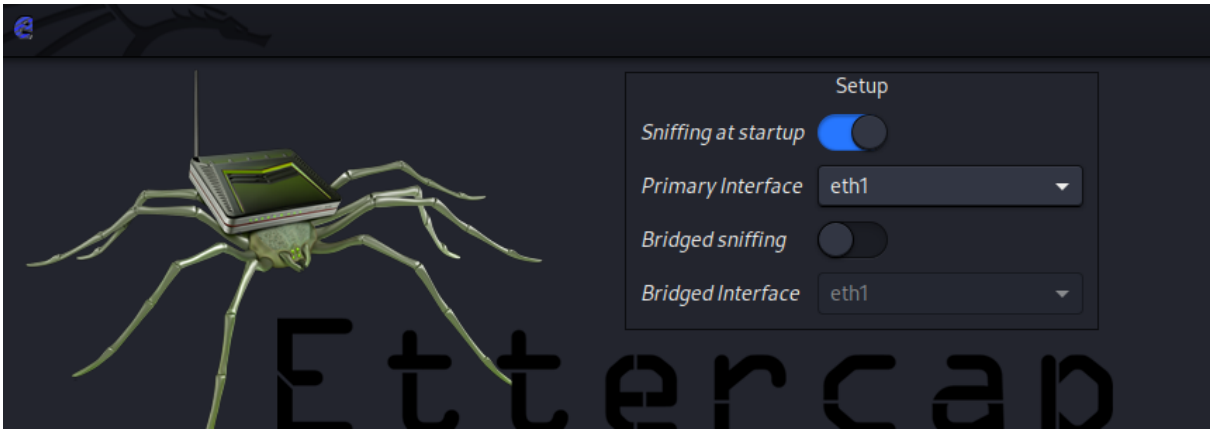
Man in The Middle

Una vez iniciada cada maquina comienzo iniciando ettercap y wireshark en mi kali linux.

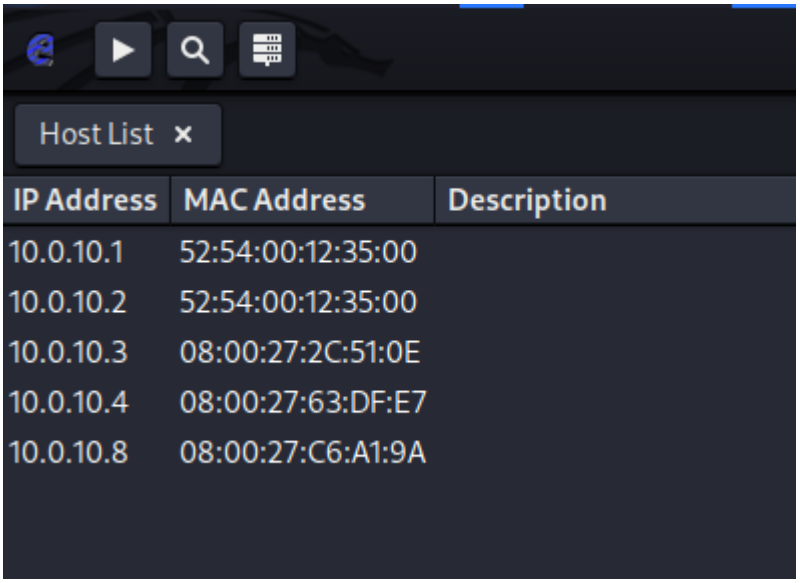
```
sudo ettercap -G
```

Seleccionamos la interfaz en la que se encuentran nuestras maquinas.



Hago clic en el check superior derecha para aceptar la configuración

Después hago clic en la lupa para buscar los dispositivos en la red y listo los hosts encontrados.



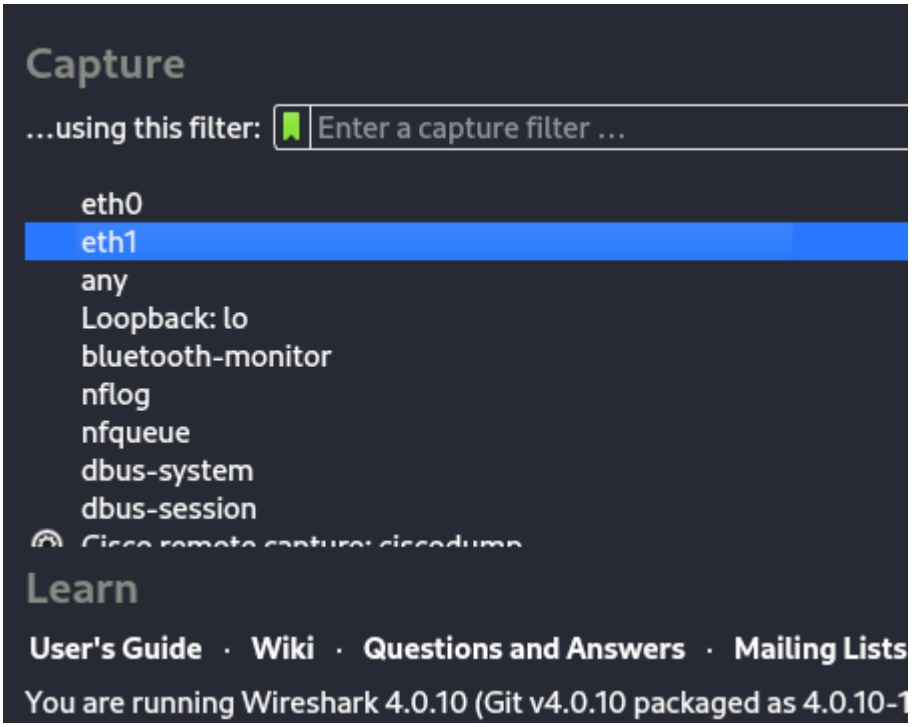
Después de comprobar las ips en cada equipo para identificarles se que la 10.0.10.8 es la DVL y la 10.0.10.4 la metasploitable.

añado la DVL a target 1 y la metasploitable a target 2.

selecciono el ataque a arp spoofing

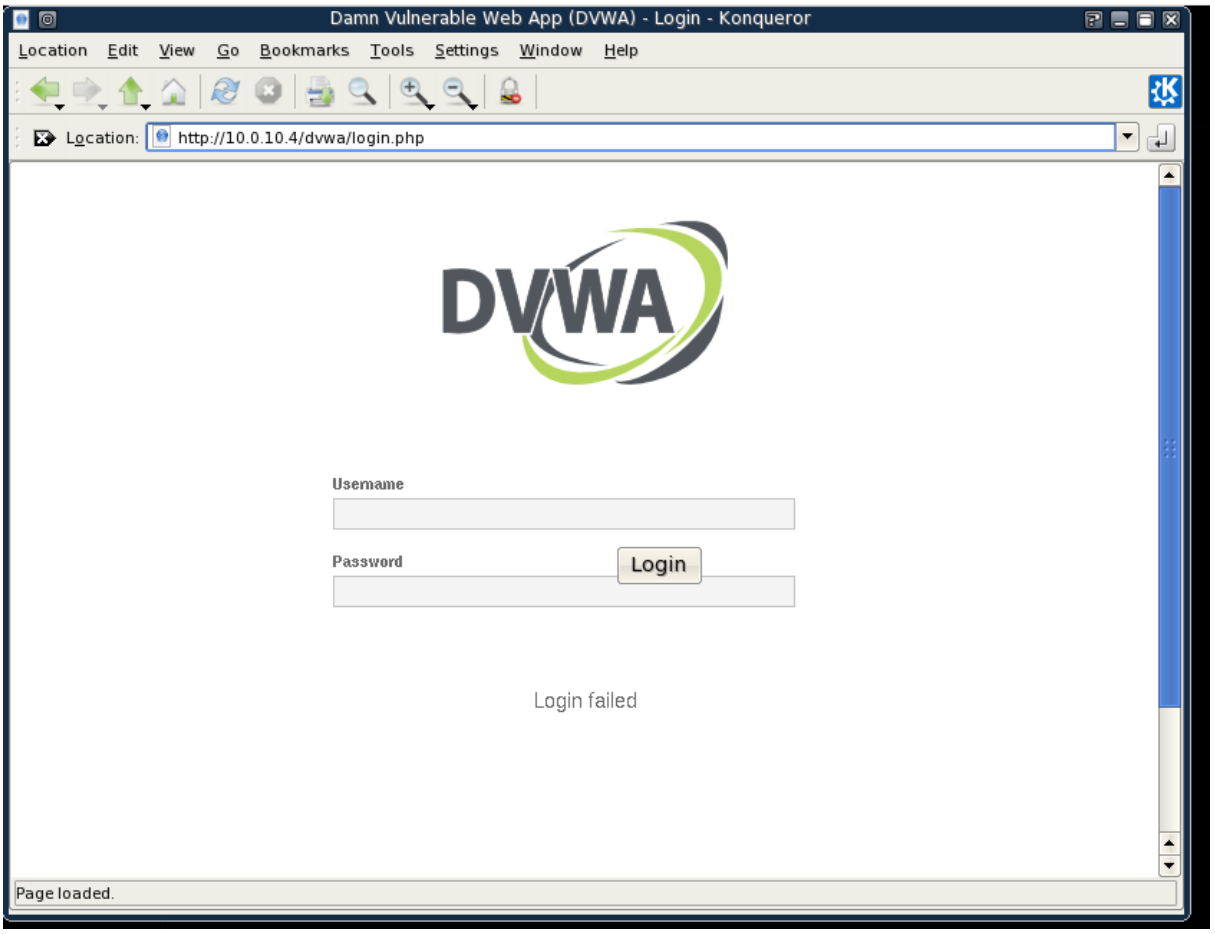
Doy a botón del play para que empiece a sniffar la red.

Después inicio el wireshark y selecciono la interfaz correcta.



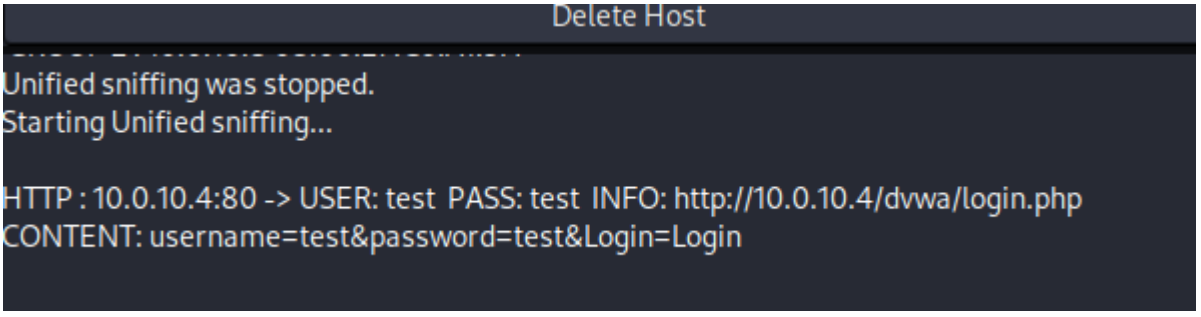
Una vez capturando la red voy a la maquina DVL y abro el buscador.

Busco la ip de metasploitable y entro en DVWA.

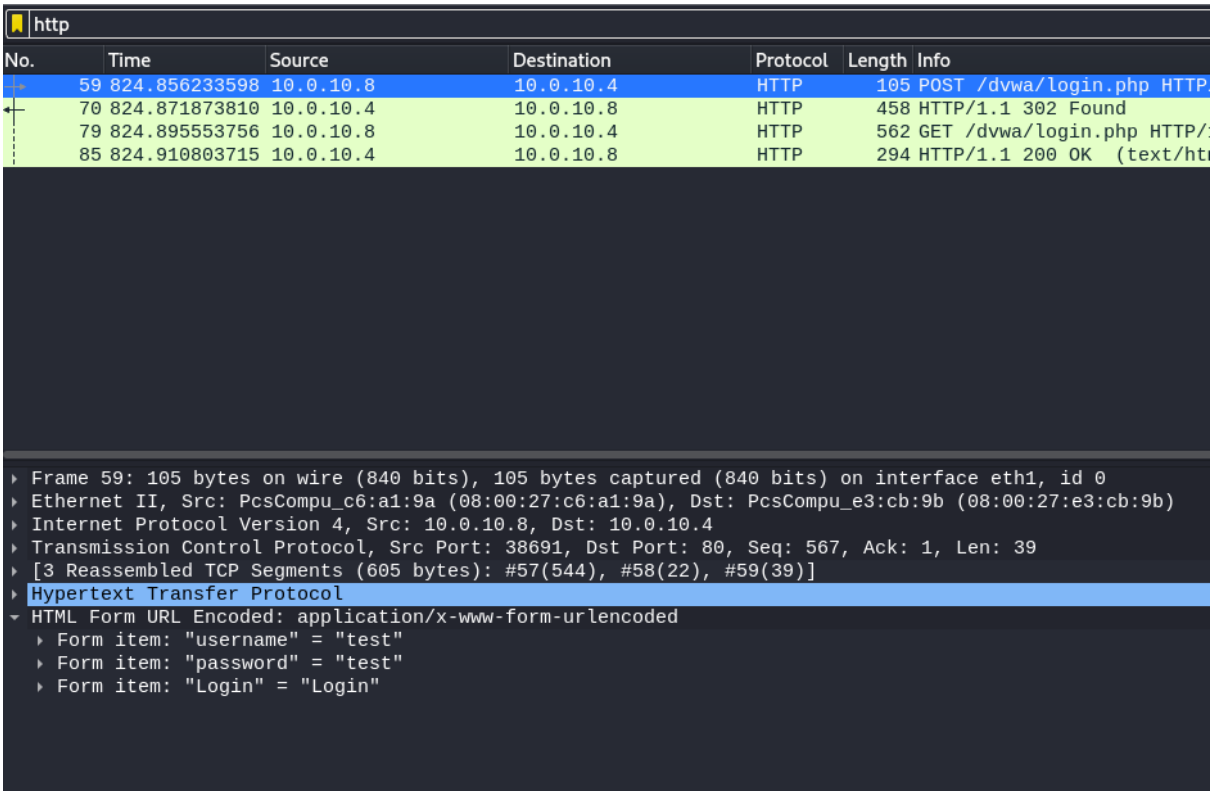


Introduzo las credenciales test:test y doy al login.

Luego compruebo ettercap y veo las credenciales que he introducido



En WireShark


http
No. Time Source Destination Protocol Length Info
59 824.856233598 10.0.10.8 10.0.10.4 HTTP 105 POST /dvwa/login.php HTTP
70 824.871873810 10.0.10.4 10.0.10.8 HTTP 458 HTTP/1.1 302 Found
79 824.895553756 10.0.10.8 10.0.10.4 HTTP 562 GET /dvwa/login.php HTTP/
85 824.910803715 10.0.10.4 10.0.10.8 HTTP 294 HTTP/1.1 200 OK (text/ht
Frame 59: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface eth1, id 0
Ethernet II, Src: PcsCompu_c6:a1:9a (08:00:27:c6:a1:9a), Dst: PcsCompu_e3:cb:9b (08:00:27:e3:cb:9b)
Internet Protocol Version 4, Src: 10.0.10.8, Dst: 10.0.10.4
Transmission Control Protocol, Src Port: 38691, Dst Port: 80, Seq: 567, Ack: 1, Len: 39
[3 Reassembled TCP Segments (605 bytes): #57(544), #58(22), #59(39)]
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "username" = "test"
Form item: "password" = "test"
Form item: "Login" = "Login"