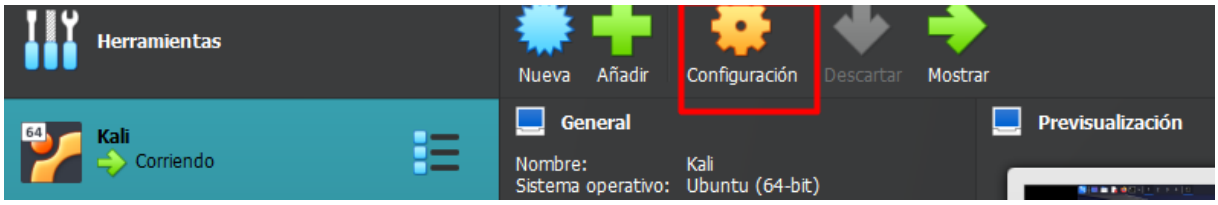
EJERCICIO FINAL - ATAQUES A INFRAESTRUCTURAS DE SISTEMAS Y REDES

Definición de alcance y requisitos

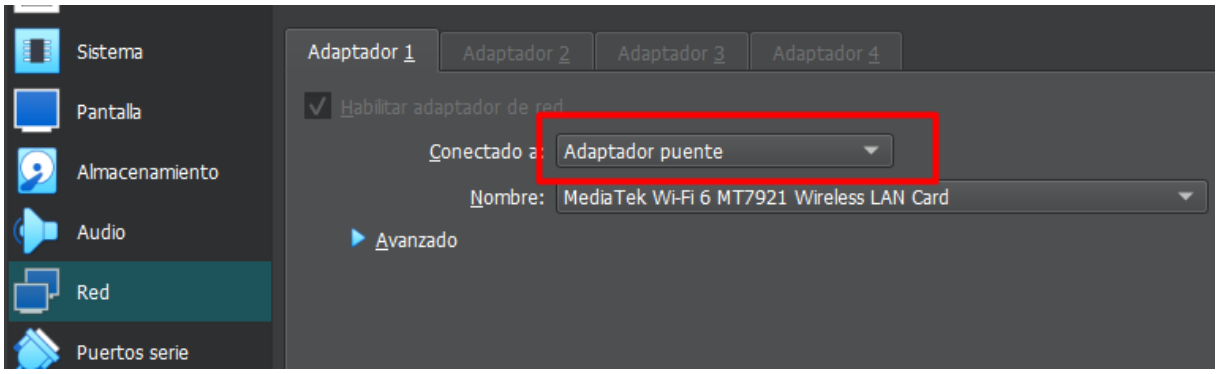
Suponed que tenemos un cliente (vosotros) y queréis conocer el estado de vuestra red.
Vais a realizar vuestra primera "incursión" en entorno real, sin usar máquinas virtuales preparadas, y generaros un informe para vosotros mismos sobre lo que habéis hecho.
Para realizar este ejercicio hay que tener en cuenta que los ataques y análisis van a realizarse en la propia red personal de cada uno, por lo que es necesario antes de nada, "pedir permiso" e "informar" al resto de usuarios de la red de los objetivos, horario para poder hacerlo, si el router está accesible para reiniciarlo... etc.
DISCLAIMER - ¡¡¡Hacedlo con responsabilidad y cabeza!!!

1. Configuración

Configurar el tipo de red de Kali Linux como "Bridge" o "Adaptador puente". De esta manera estará configurado como si fuera un equipo más de la propia red.
Comprobar que la IP asignada a Kali Linux está en el rango de red del resto de equipos de la misma.



Escogemos Adaptador puente y reiniciamos la maquina.




```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.150  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe9d:3f2  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9d:03:f2  txqueuelen 1000  (Ethernet)
        RX packets 101  bytes 29244 (28.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 104  bytes 12734 (12.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Se observa que la información se modifica debido al cambio de red

2. Selección de objetivo

Realizar una identificación de equipos de toda la red.

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.1.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-13 11:32 CEST
Nmap scan report for csp1.zte.com.cn (192.168.1.1)
Host is up (0.044s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
52869/tcp open  unknown
MAC Address: 34:DA:B7:D5:4B:21 (zte)

Nmap scan report for 192.168.1.128 (192.168.1.128)
Host is up (0.024s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: 62:80:6A:21:DC:AF (Unknown)

Nmap scan report for 192.168.1.130
Host is up (0.021s latency).
Not shown: 957 filtered tcp ports (no-response), 40 closed tcp ports (reset)
PORT     STATE SERVICE
1080/tcp open  socks
6543/tcp open  mythtv
8888/tcp open  sun-answerbook
MAC Address: 90:F8:2E:C3:41:8F (Amazon Technologies)

Nmap scan report for 192.168.1.134
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.1.134 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 48:E7:DA:54:D4:91 (AzureWave Technology)

Nmap scan report for mitv (192.168.1.139)
Host is up (0.095s latency).
All 1000 scanned ports on mitv (192.168.1.139) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 10:38:1F:5B:3D:61 (Sichuan AI-Link Technology)
```

```
Nmap scan report for kali (192.168.1.150)
Host is up (0.0000060s latency).
All 1000 scanned ports on kali (192.168.1.150) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (6 hosts up) scanned in 17.68 seconds
```

Identificar equipos por la MAC Address (recordad que podemos sacar basándonos en la MAC el fabricante y por lo tanto acotar que equipos son).
Elegir un equipo como objetivo.

Nota: Contad con que haya en la red, al menos, 4 equipos:
Equipo 1) Kali Linux en modo "Bridge" o "Adaptador puente".

```
Nmap scan report for kali (192.168.1.150)
Host is up (0.000057s latency).
All 1000 scanned ports on kali (192.168.1.150) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

Equipo 2) Vuestra máquina Host.

```
Nmap scan report for 192.168.1.134
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.1.134 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 48:E7:DA:54:D4:91 (AzureWave Technology)
```

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::a8dd:f690:1115:5370%7
   Dirección IPv4. . . . . . . . . . . . : 192.168.1.134
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

En el cmd de Windows aparece esto

Equipo 3) Un teléfono móvil.

```
Nmap scan report for 192.168.1.128 (192.168.1.128)
Host is up (0.024s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: 62:80:6A:21:DC:AF (Unknown)
```

Equipo 4) Router.

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-13 11:24 CEST
Nmap scan report for csp1.zte.com.cn (192.168.1.1)
Host is up (0.0098s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
52869/tcp open  unknown
MAC Address: 34:DA:B7:D5:4B:21 (zte)
```

El resto serán otros equipos conectados, aparte de éstos, que haya en la red.

Equipo 5: ONT Nokia

```
Nmap scan report for 192.168.1.130
Host is up (0.021s latency).
Not shown: 957 filtered tcp ports (no-response), 40 closed tcp ports (reset)
PORT     STATE SERVICE
1080/tcp open  socks
6543/tcp open  mythtv
8888/tcp open  sun-answerbook
MAC Address: 90:F8:2E:C3:41:8F (Amazon Technologies)
```

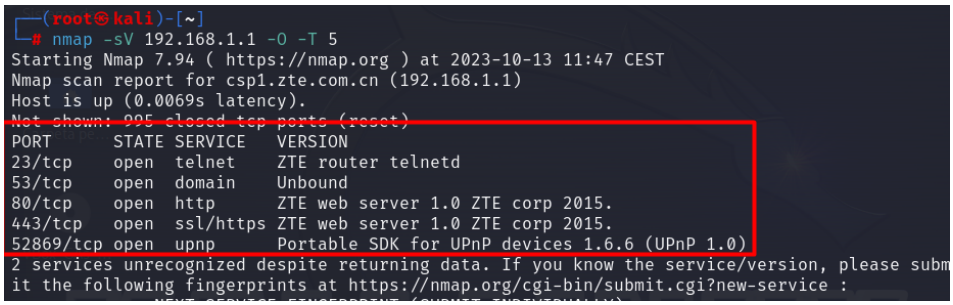
Equipo 6: Televisor Xiaomi

```
Nmap scan report for mitv (192.168.1.139)
Host is up (0.095s latency).
All 1000 scanned ports on mitv (192.168.1.139) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 10:38:1F:5B:3D:61 (Sichuan AI-Link Technology)
```

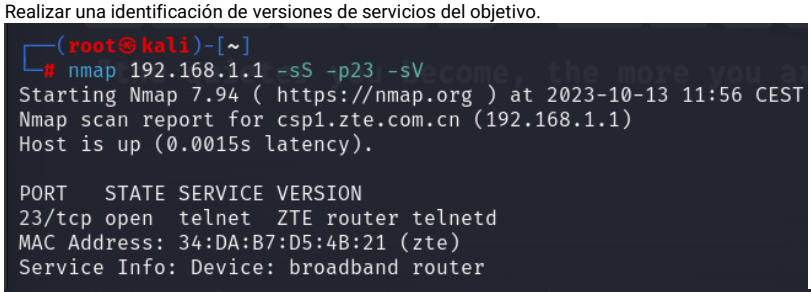
3. Análisis de vulnerabilidades - Exploración

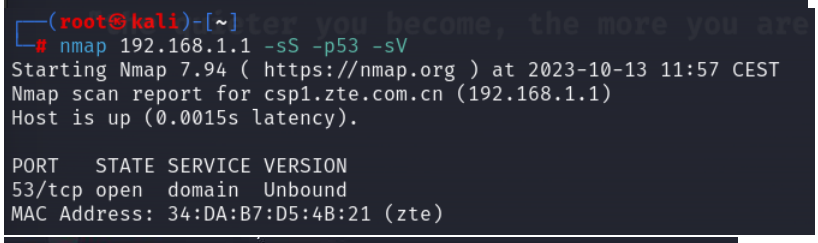
Realizar una identificación de sistema operativo de un equipo objetivo. (También es importante para validar el punto anterior y ver que equipos son).

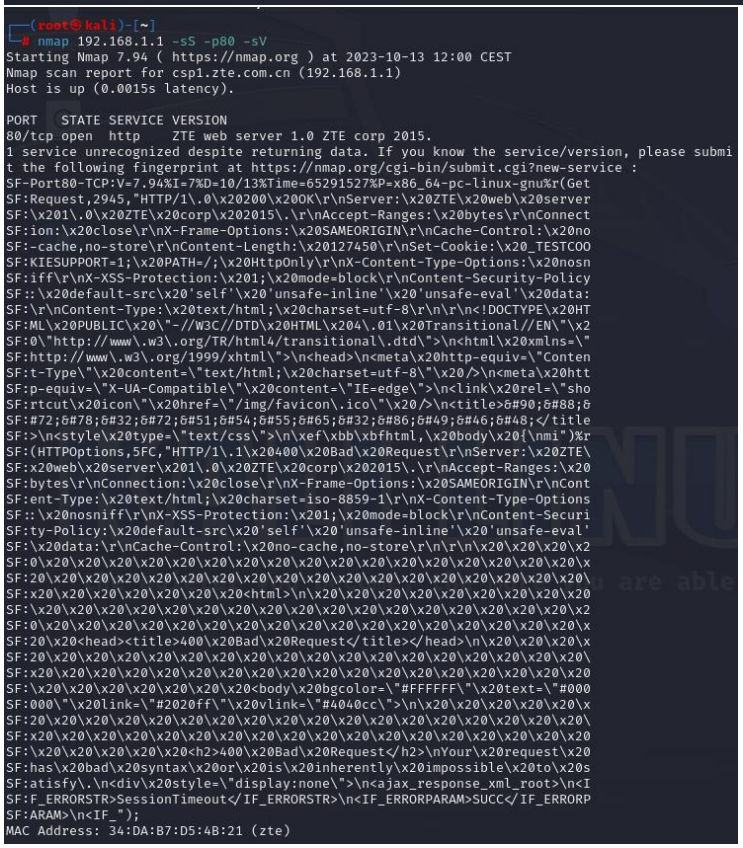
Realizar una identificación de servicios y puertos abiertos del objetivo.



Realizar una identificación de versiones de servicios del objetivo.





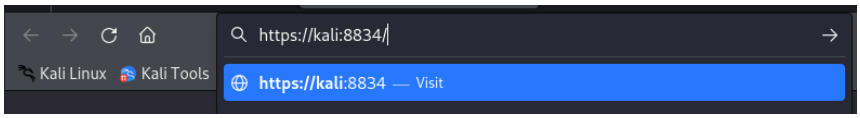


```
┌──(root㉿kali)-[~]
└─# nmap 192.168.1.1 -sS -p443 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-13 12:01 CEST
Nmap scan report for csp1.zte.com.cn (192.168.1.1)
Host is up (0.0047s latency).

PORT    STATE SERVICE   VERSION
443/tcp open  ssl/https ZTE web server 1.0 ZTE corp 2015.
1 service unrecognized despite returning data. If you know the service/version, p
rint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.94%T=SSL%I=7%D=10/13%Time=6529158A%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,41AD,"HTTP/1\.0\x20200\x20OK\r\nServer:\x20ZTE\x20web\x2
SF:0server\x201\.0\x20ZTE\x20corp\x202015\.\r\nAccept-Ranges:\x20bytes\r\n
SF:Connection:\x20close\r\nX-Frame-Options:\x20SAMEORIGIN\r\nCache-Control
SF::\x20no-cache,no-store\r\nContent-Length:\x20127450\r\nSet-Cookie:\x20_
SF:TESTCOOKIESUPPORT=1;\x20PATH=/;\x20HttpOnly\r\nX-Content-Type-Options:\
SF:x20nosniff\r\nX-XSS-Protection:\x201;\x20mode=block\r\nContent-Security
SF:-Policy:\x20default-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval'\x
SF:20data:\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\n\r\n<!DOCTYP
SF:E\x20HTML\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x204\.01\x20Transitional//
SF:EN\"\x20\"http://www\.w3\.org/TR/html4/transitional\.dtd\">\n<html\x20x
SF:mlns=\"http://www\.w3\.org/1999/xhtml\">\n<head>\n<meta\x20http-equiv=\
SF:"Content-Type\"\x20content=\"text/html;\x20charset=utf-8\"\x20/>\n<meta
SF:\x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=edge\">\n<link\x20re
SF:l=\"shortcut\x20icon\"\x20href=\"/img/favicon\.ico\"\x20/>\n<title>&#90
SF:;&#88;&#72;&#78;&#32;&#72;&#51;&#54;&#55;&#65;&#32;&#86;&#49;&#46;&#48;
SF:</title>\n<style\x20type=\"text/css\">\n\xef\xbb\xbfhtml,\x20body\x20{\
SF:nmi")%r(FourOhFourRequest,5EF,"HTTP/1\.0\x20404\x20Not\x20Found\r\nServ
SF:er:\x20ZTE\x20web\x20server\x201\.0\x20ZTE\x20corp\x202015\.\r\nAccept-
SF:Ranges:\x20bytes\r\nConnection:\x20close\r\nX-Frame-Options:\x20SAMEORI
SF:GIN\r\nContent-Type:\x20text/html;\x20charset=iso-8859-1\r\nX-Content-T
SF:ype-Options:\x20nosniff\r\nX-XSS-Protection:\x201;\x20mode=block\r\nCon
SF:tent-Security-Policy:\x20default-src\x20'self'\x20'unsafe-inline'\x20'u
SF:nsafe-eval'\x20data:\r\nCache-Control:\x20no-cache,no-store\r\n\r\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20<html>\n\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20<head><title>404\x20Not\x20Found</title></head>\n\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20<body\x20bgcolor=\"#FFFFFF\"\x20te
SF:xt=\"#000000\"\x20link=\"#2020ff\"\x20vlink=\"#4040cc\">\n\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20<h2>404\x20Not\x20Found</h2>\n<span>The\x2
SF:0requested\x20URL\x20was\x20not\x20found\x20on\x20this\x20server\.</spa
SF:n>\n<div\x20style=\"display:none\">\n<ajax_response_xml_root>\n<IF_ERRO
SF:RSTR>SessionTimeout</IF_ERRORSTR>\n<IF_ERRORPARAM>SUCC</IF_ERRORPARAM>\
SF:n<IF_ERRORTYPE>SUC");
MAC Address: 34:DA:B7:D5:4B:21 (zte)
```

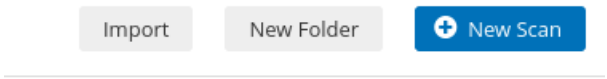
```
┌──(root㉿kali)-[~]
└─# nmap 192.168.1.1 -sS -p52869 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-13 12:02 CEST
Nmap scan report for csp1.zte.com.cn (192.168.1.1)
Host is up (0.0034s latency).

PORT      STATE SERVICE VERSION
52869/tcp open  upnp    Portable SDK for UPnP devices 1.6.6 (UPnP 1.0)
MAC Address: 34:DA:B7:D5:4B:21 (zte)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.69 seconds
```

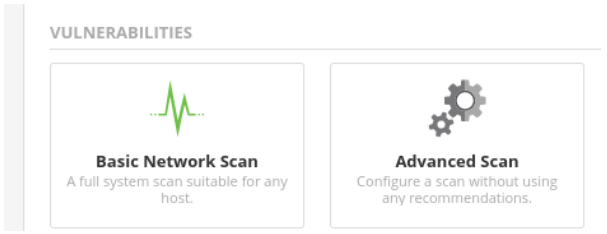
4. Análisis de vulnerabilidades - Evaluación

Realizar un análisis de vulnerabilidades con las herramientas automáticas vistas en este módulo sobre el objetivo.

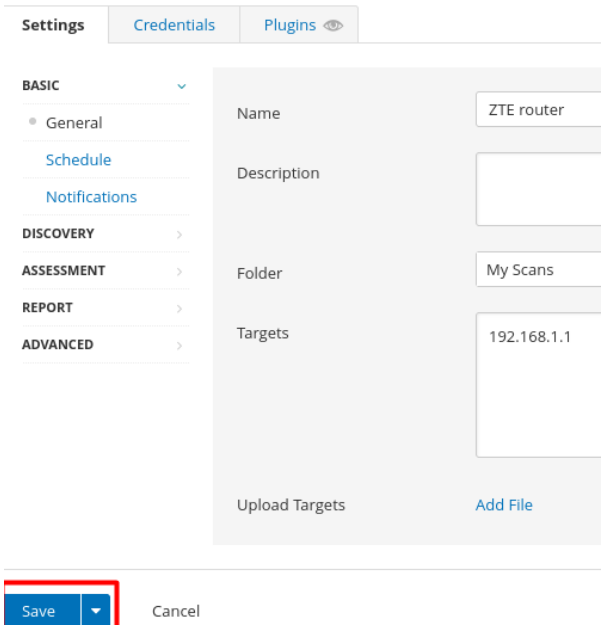


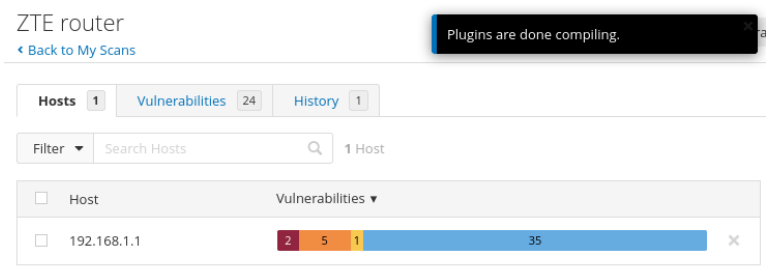
Una vez abrimos el enlace nos logeamos y continuamos con ello





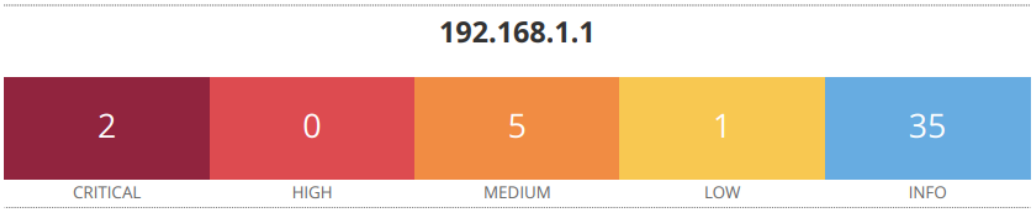
Realizamos un escaneo básico después de rellenar la información correspondiente





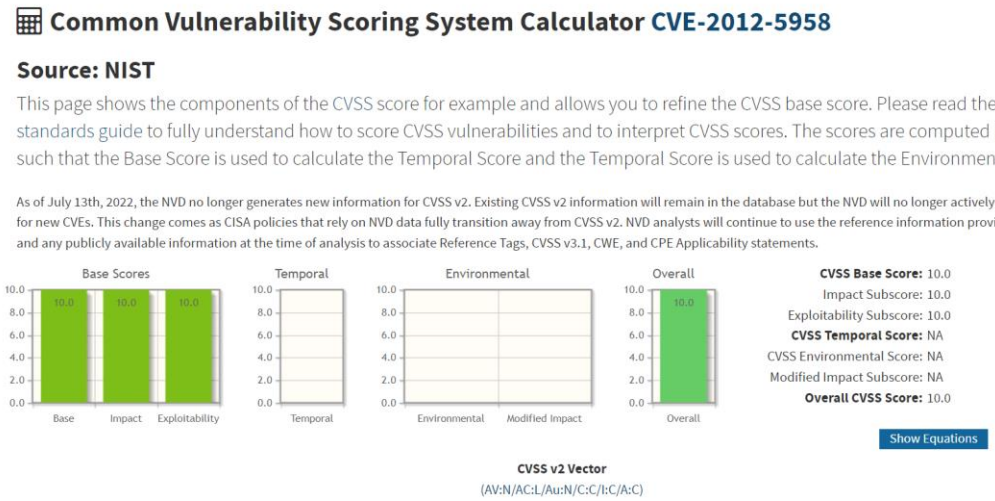
Una vez completado lo descargamos en pdf y observamos las distintas vulnerabilidades encontradas

Realizar triaje y comprobar si hay alguna vulnerabilidad crítica (CVSS alto) sobre el objetivo.



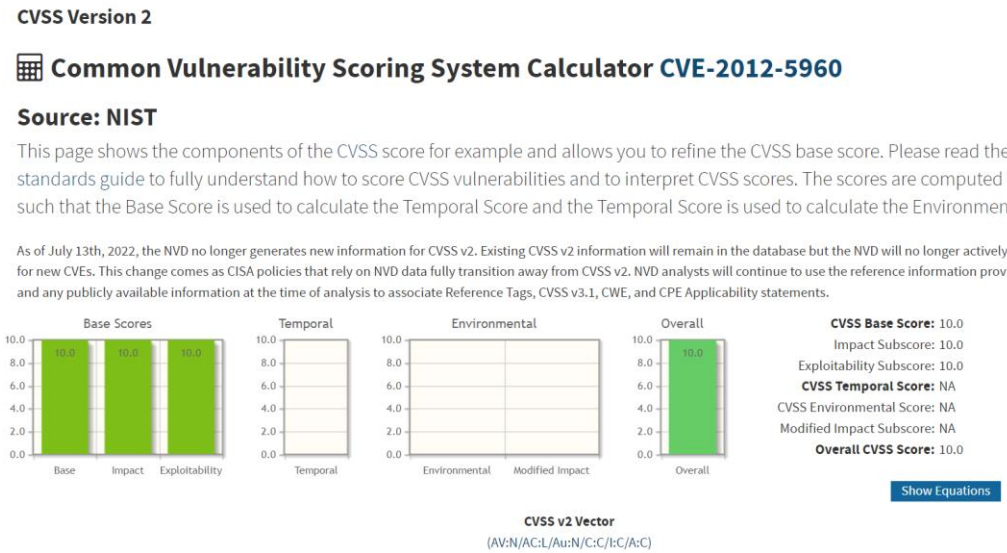
En el análisis detallado se encontraron dos vulnerabilidades críticas.

- (CVE-2012-5958)
- Descripción: Desbordamiento de búfer basado en la pila en la función unique_service_name en ssdp/ssdp_server.c en el validador SSDP del SDK para dispositivos UPnP (también conocido como libupnp, anteriormente el SDK Intel para dispositivos UPnP) v1.6.18 que permite a atacantes remotos ejecutar código arbitrario a través de un paquete UDP con una cadena modificada que no es manejada adecuadamente después de la resta de un determinado puntero.
- Impacto:



- Recomendaciones: actualizar el sistema con las recomendaciones encontradas en https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2012-5958; restringir el acceso mediante reglas del firewall; deshabilitar UPnP si no es necesario. Para más información consultar el siguiente enlace https://www.kb.cert.org/vuls/id/922681

- (CVE-2012-5960)
- Descripción: Desbordamiento de búfer basado en pila en la función de unique_service_name en ssdp/ssdp_server.c en el analizador SSDP en el SDK portátil para dispositivos UPnP (alias libupnp, anteriormente el SDK Intel para dispositivos UPnP) antes de v1.6.18 que permite a atacantes remotos ejecutar código arbitrario a través de un campo long UDN (también conocido como UPnP: rootdevice) en un paquete UDP.
- Impacto:



- Recomendaciones: Actualizar el sistema con las recomendaciones encontradas en https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2012-5960; restringir el acceso mediante reglas del firewall; deshabilitar UPnP si no es necesario. Para conocer más información acceder a este enlace https://www.kb.cert.org/vuls/id/922681

5. Ataque MITM y captura/sniffing de tráfico

Realizar un ataque MITM entre un equipo de la red y el router para capturar tráfico entre ellos, e intentar averiguar a qué servicios, IPs o webs se está accediendo.
En caso que se utilice algún protocolo inseguro, como el que se genera en el protocolo ftp, telnet o http, es posible analizar la información más en detalle utilizando filtros en Wireshark, y así, extraer información sensible como usuarios y contraseñas.
Demostrar mediante capturas de pantalla que obtienes información "sensible" de alguno de los protocolos anteriormente nombrados.

```
┌──(root㉿kali)-[~]
└─# nmap -sV 10.0.2.0/24 -T5 -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 12:33 EDT
Nmap scan report for 10.0.2.1 (10.0.2.1)
Host is up (0.0071s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
```

La información de la maquina DVL

```
Nmap scan report for 10.0.2.6 (10.0.2.6)
Host is up (0.00055s 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
```

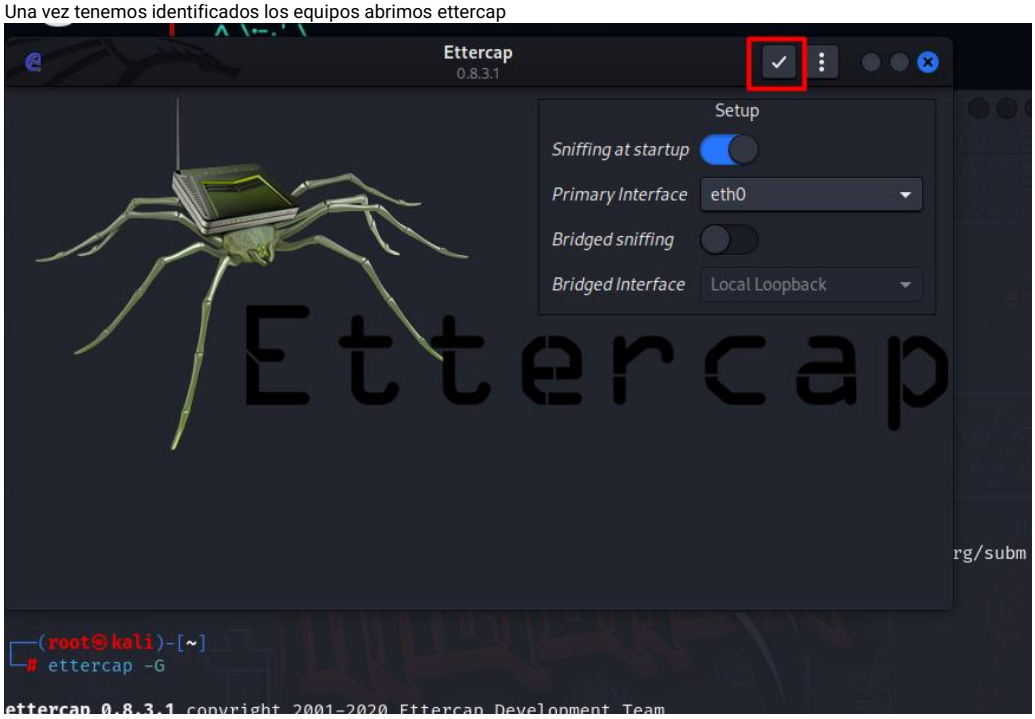
El router

```
Nmap scan report for 10.0.2.1 (10.0.2.1)
Host is up (0.0071s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Device type: VoIP phone|specialized|webcam|general purpose
Running (JUST GUESSING): Grandstream embedded (99%), 2N embedded (96%), Garmin embedded (94%), P
hilips embedded (93%), lwIP 1.4.X (93%), Espressif embedded (92%), NodeMCU embedded (92%), Enlog
ic embedded (92%)
```

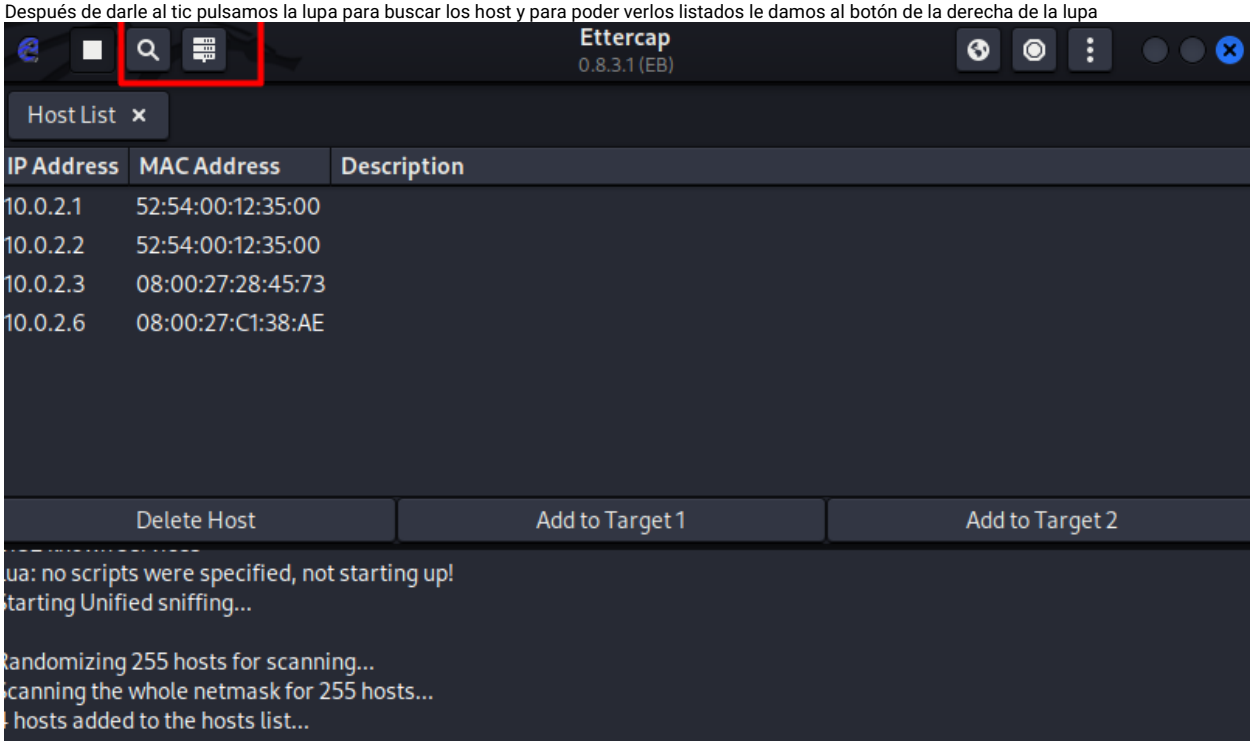
La Kali

```
Nmap scan report for 10.0.2.9 (10.0.2.9)
Host is up (0.000058s latency).
All 1000 scanned ports on 10.0.2.9 (10.0.2.9) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

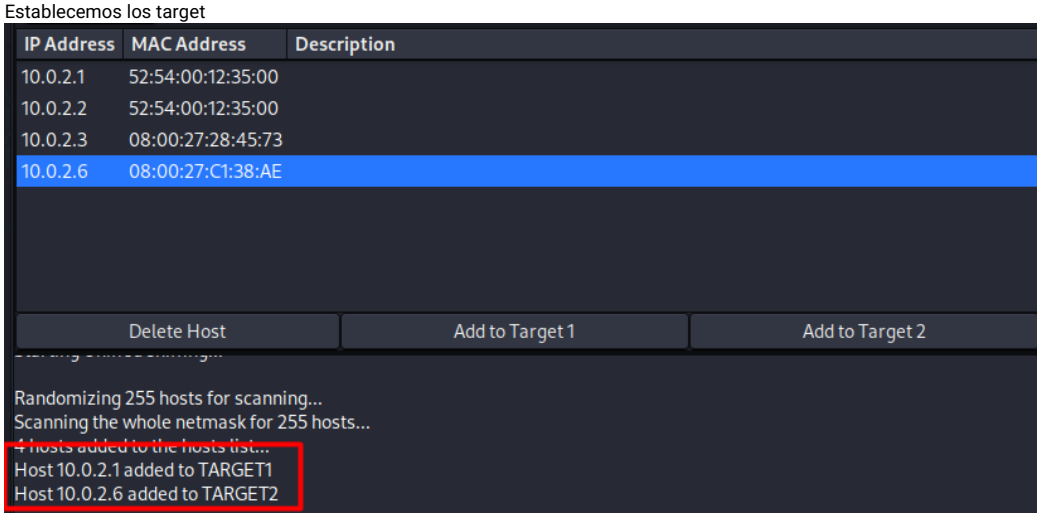
Una vez tenemos identificados los equipos abrimos ettercap



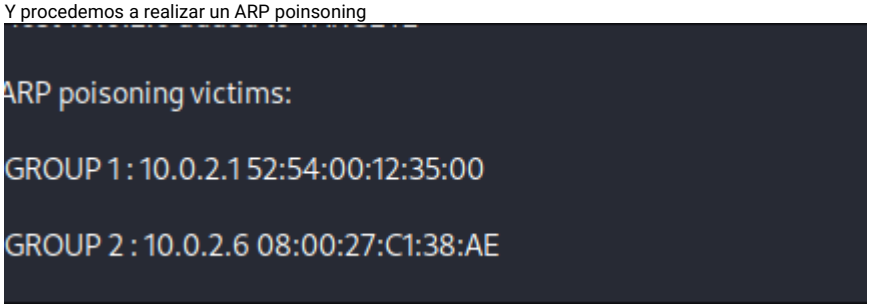
Después de darle al tic pulsamos la lupa para buscar los host y para poder verlos listados le damos al botón de la derecha de la lupa



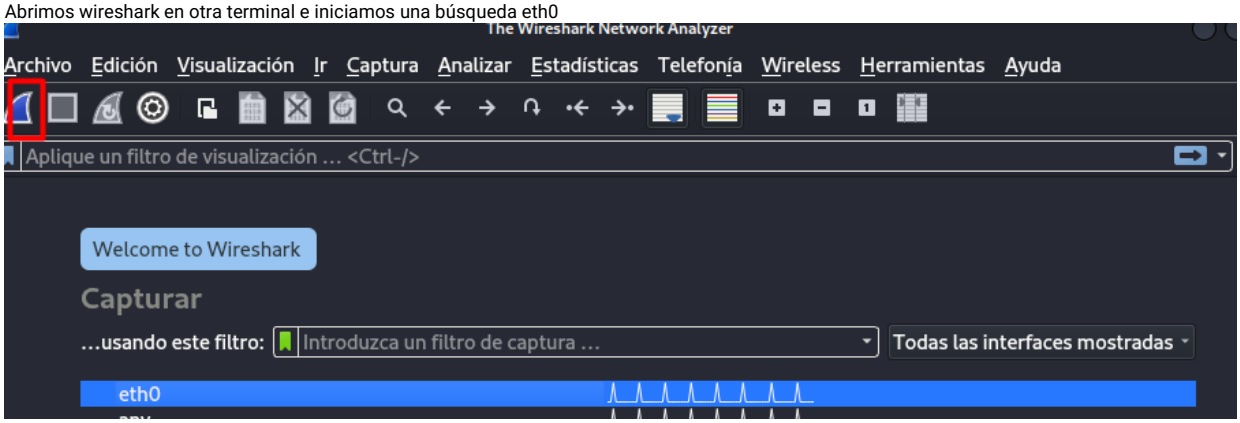
Establecemos los target



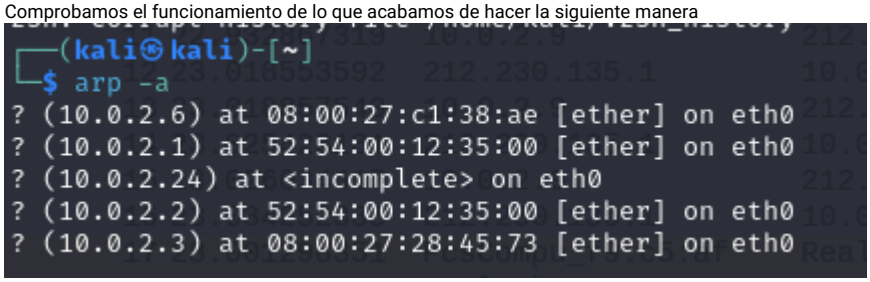
Y procedemos a realizar un ARP poinsoning



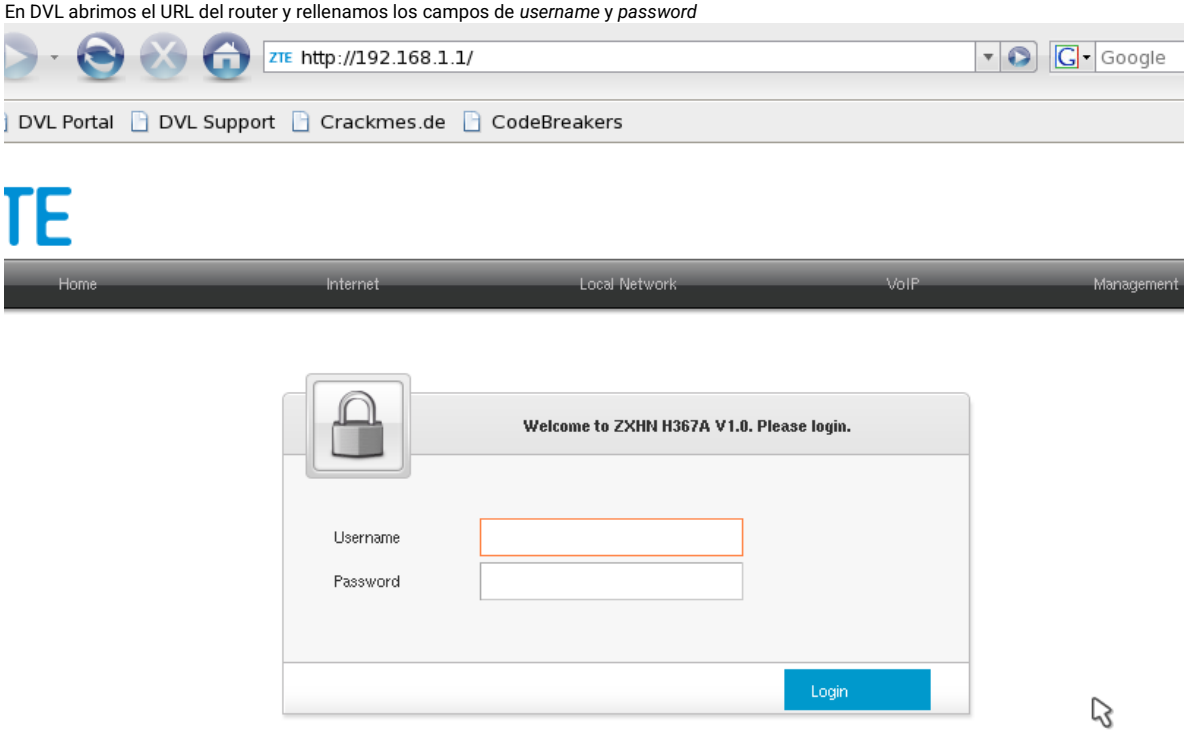
Abrimos wireshark en otra terminal e iniciamos una búsqueda eth0



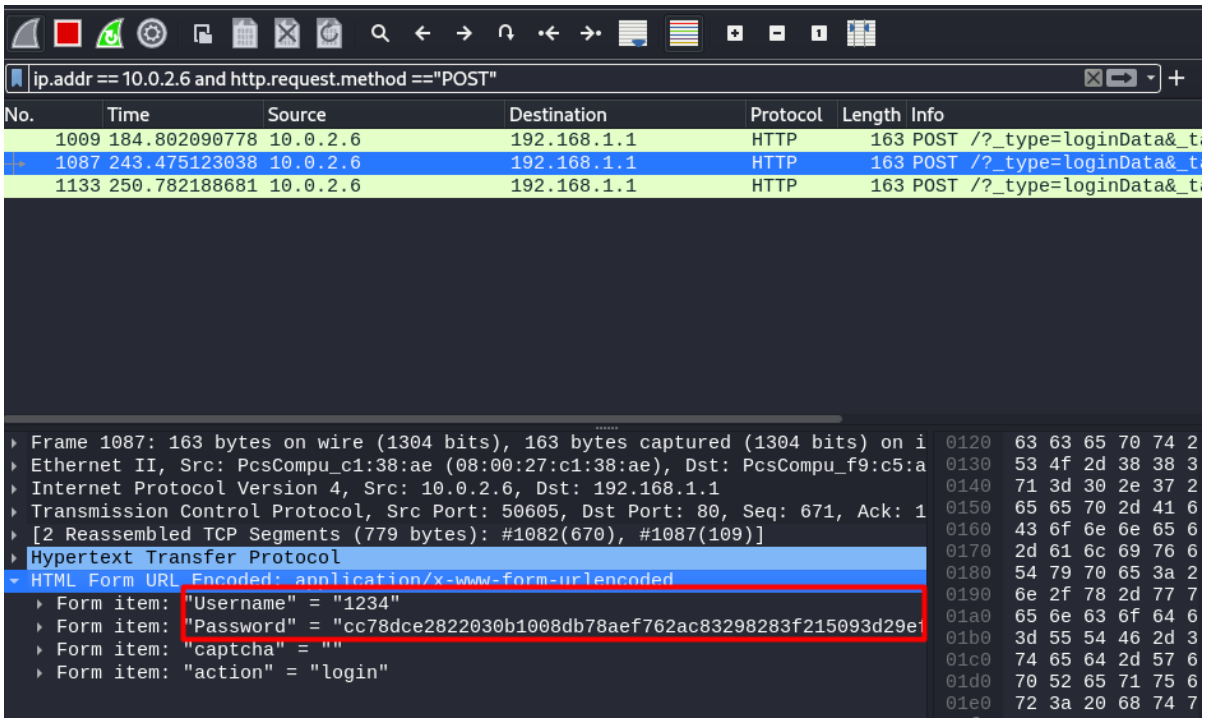
Comprobamos el funcionamiento de lo que acabamos de hacer la siguiente manera



En DVL abrimos el URL del router y rellenamos los campos de *username* y *password*



Mientras en wireshark buscamos la petición que hemos interceptado con los filtros correspondientes



Aparece el usuario pero la contraseña aparece encriptada