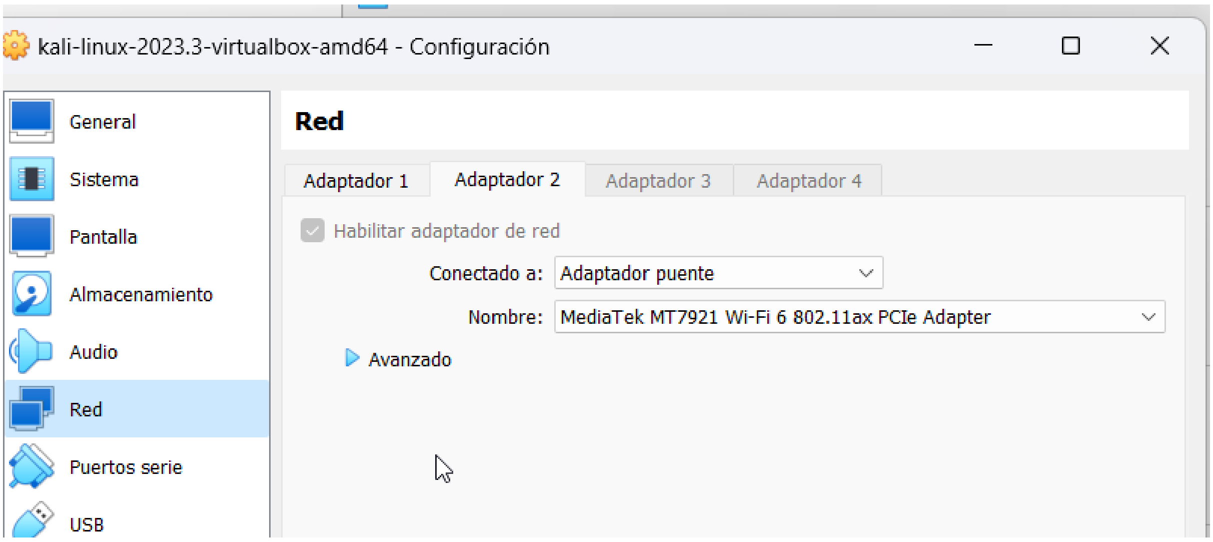
CTF Final

Configuracion

Configuramos la tarjeta de red a brigde



kali-linux-2023.3-virtualbox-amd64 - Configuración

Red

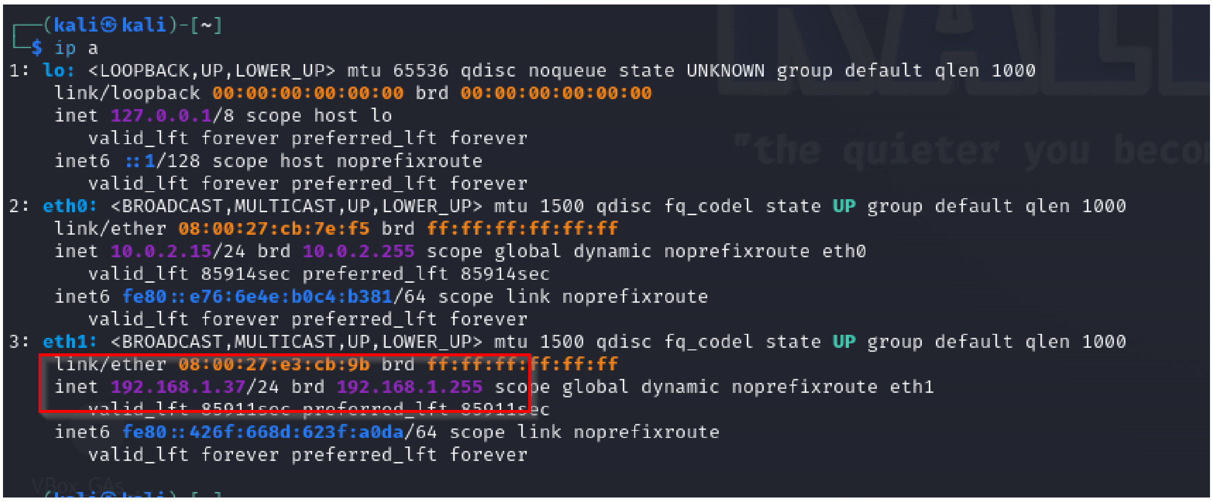
Adaptador 2

☑ Habilitar adaptador de red

Conectado a: Adaptador puente

Nombre: MediaTek MT7921 Wi-Fi 6 802.11ax PCIe Adapter

Vemos nuestra nueva IP

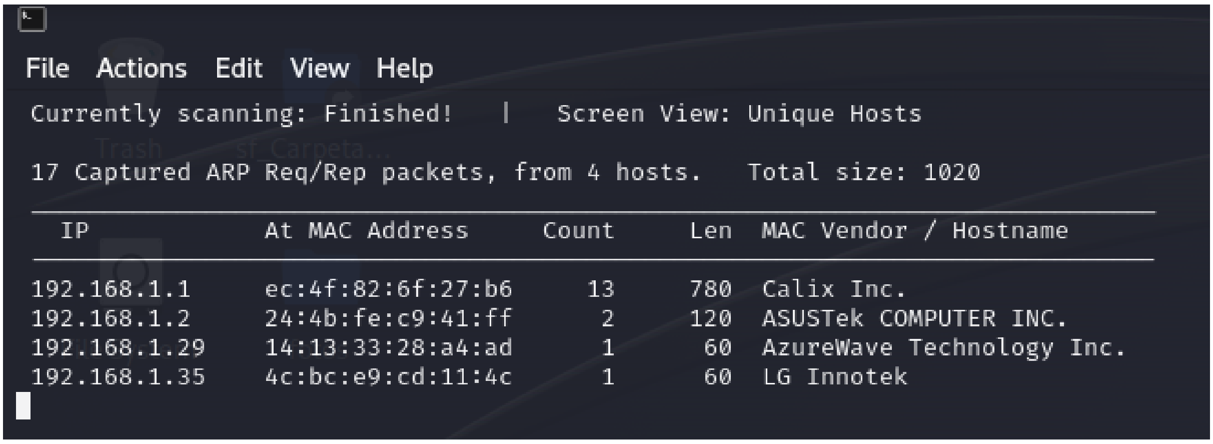


```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:7e:f5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85914sec preferred_lft 85914sec
    inet6 fe80::e76:6e4e:b0c4:b381/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e3:cb:9b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.37/24 brd 192.168.1.255 scope global dynamic noprefixroute eth1
       valid_lft 85911sec preferred_lft 85911sec
    inet6 fe80::426f:668d:623f:a0da/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Selección de objetivo

Para localizar equipos conectados a la red hago uso del comando arp-scan además de la ip obtengo su MAC

```
sudo netdiscover -i eth1 -r 192.168.1.0/24
```



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 17 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 1020
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     ec:4f:82:6f:27:b6     13     780  Calix Inc.
 192.168.1.2     24:4b:fe:c9:41:ff      2     120  ASUSTek COMPUTER INC.
 192.168.1.29    14:13:33:28:a4:ad      1      60  AzureWave Technology Inc.
 192.168.1.35    4c:bc:e9:cd:11:4c      1      60  LG Innotek
```

192.168.1.1 → router

192.168.1.2 → Equipo windows de sobremesa(objetivo)

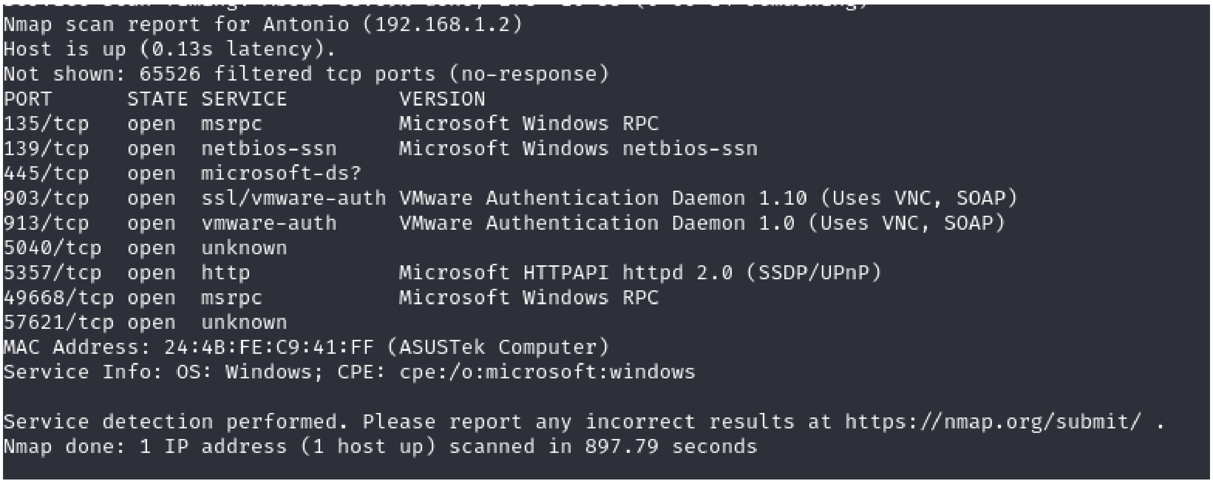
192.168.1.29 →Equipo host de kali

192.168.1.35 → tele LG

Análisis de vulnerabilidades

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.

```
sudo nmap -sS  -p- -sV -Pn 192.168.1.2 -oN target
```

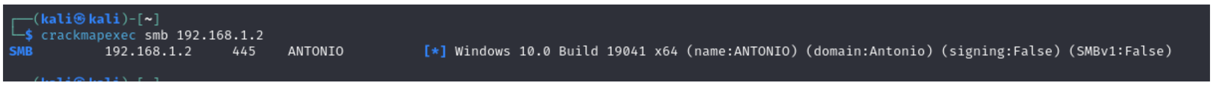


```
Nmap scan report for Antonio (192.168.1.2)
Host is up (0.13s latency).
Not shown: 65526 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
903/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
913/tcp   open  vmware-auth      VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5040/tcp  open  unknown
5357/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49668/tcp open  msrpc            Microsoft Windows RPC
57621/tcp open  unknown
MAC Address: 24:4B:FE:C9:41:FF (ASUSTek Computer)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 897.79 seconds
```

observo los `puertos abiertos, servicios y versiones.

Al estar el smb abierto compruebo a traves de crackmapexec que tipo de windows es

```
cracmapexec smb 192.168.1.2
```



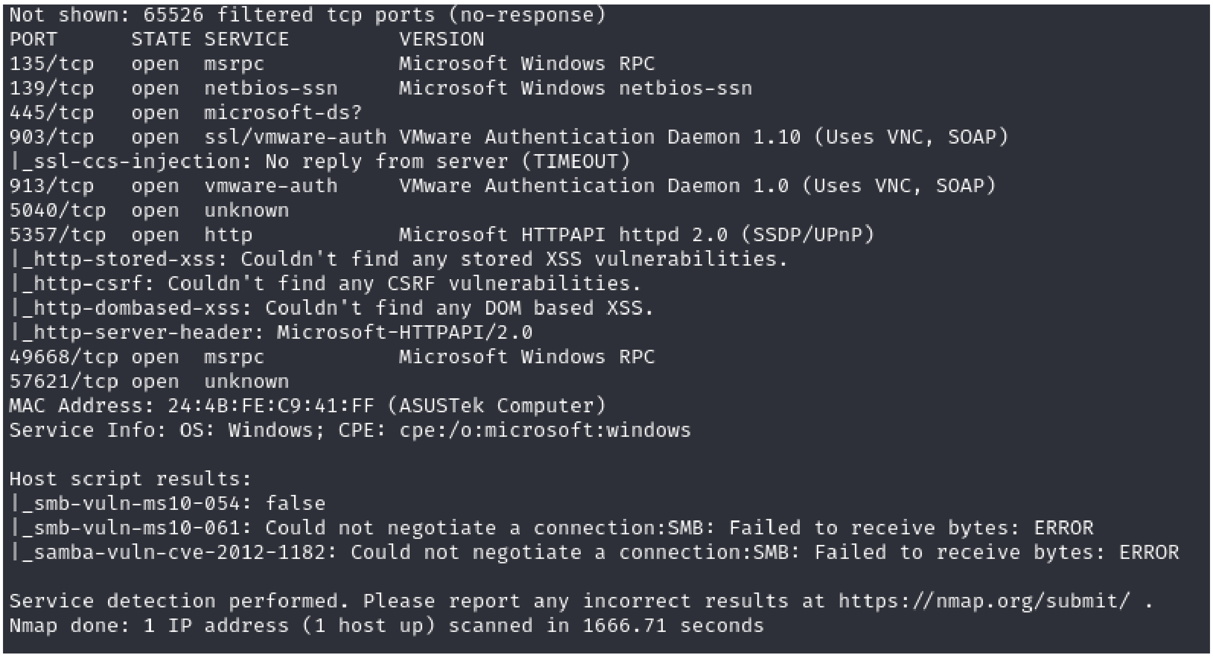
```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.1.2
SMB         192.168.1.2     445    ANTONIO          [*] Windows 10.0 Build 19041 x64 (name:ANTONIO) (domain:Antonio) (signing:False) (SMBv1:False)
```

veo que se trata de Windows 10 de 64 bits

Evaluación

Lanzo el script vuln de escaneo de vulnerabilidades con nmap

```
nmap -sV -p- --script "vuln" 192.168.1.2
```

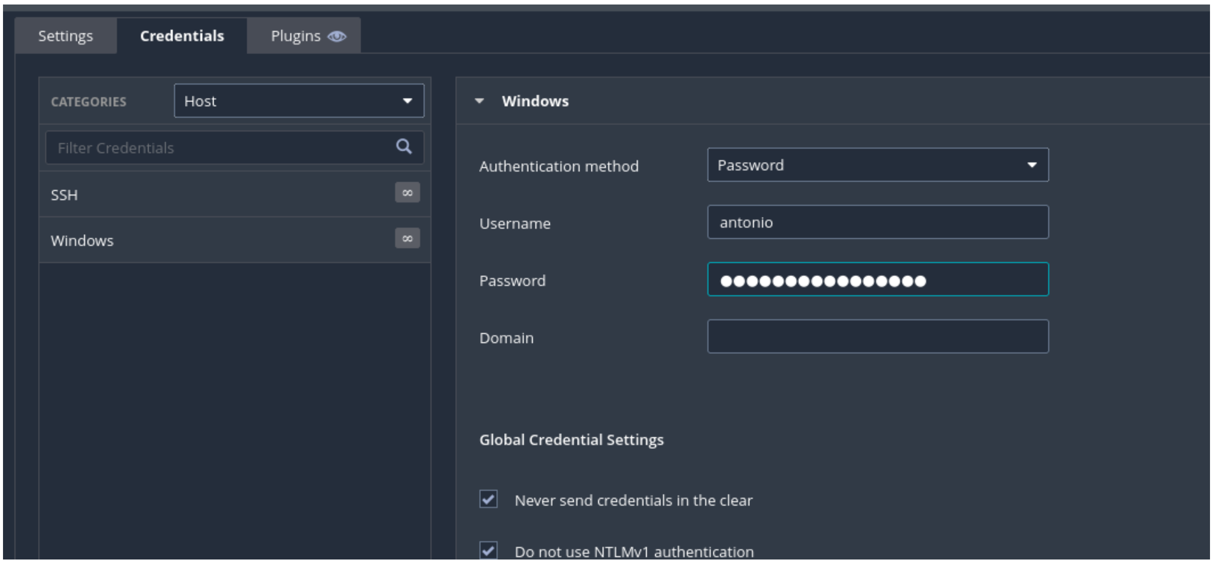


```
Not shown: 65526 filtered tcp ports (no-response)
PORT      STATE SERVICE         VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
903/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
913/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5040/tcp  open  unknown
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-HTTPAPI/2.0
49668/tcp open  msrpc           Microsoft Windows RPC
57621/tcp open  unknown
MAC Address: 24:4B:FE:C9:41:FF (ASUSTek Computer)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1666.71 seconds
```

No obtengo resultados de ninguna vulnerabilidad

Nessus

hago un escaneo autenticado



CATEGORIES: Host

Authentication method: Password

Username: antonio

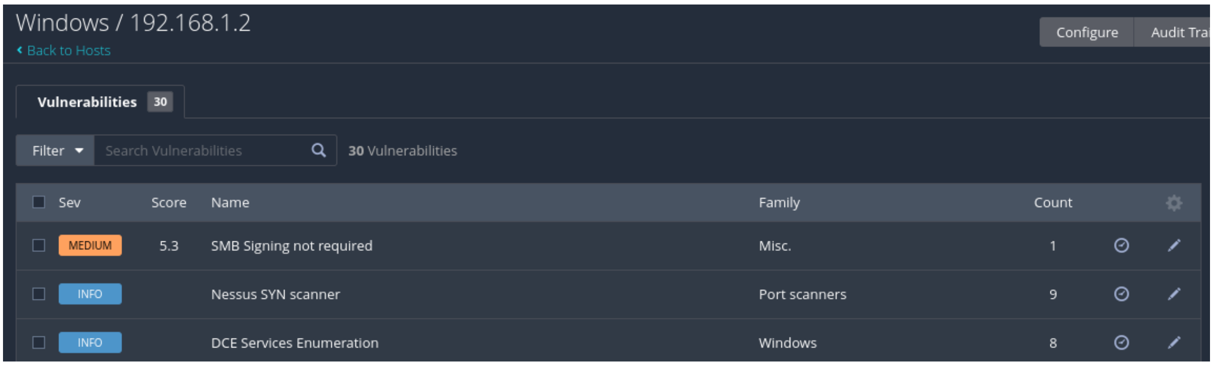
Password: ●●●●●●●●●●●●●●●●●

Domain:

Global Credential Settings

☑ Never send credentials in the clear

☑ Do not use NTLMv1 authentication


Windows / 192.168.1.2

‹ Back to Hosts

30 Vulnerabilities

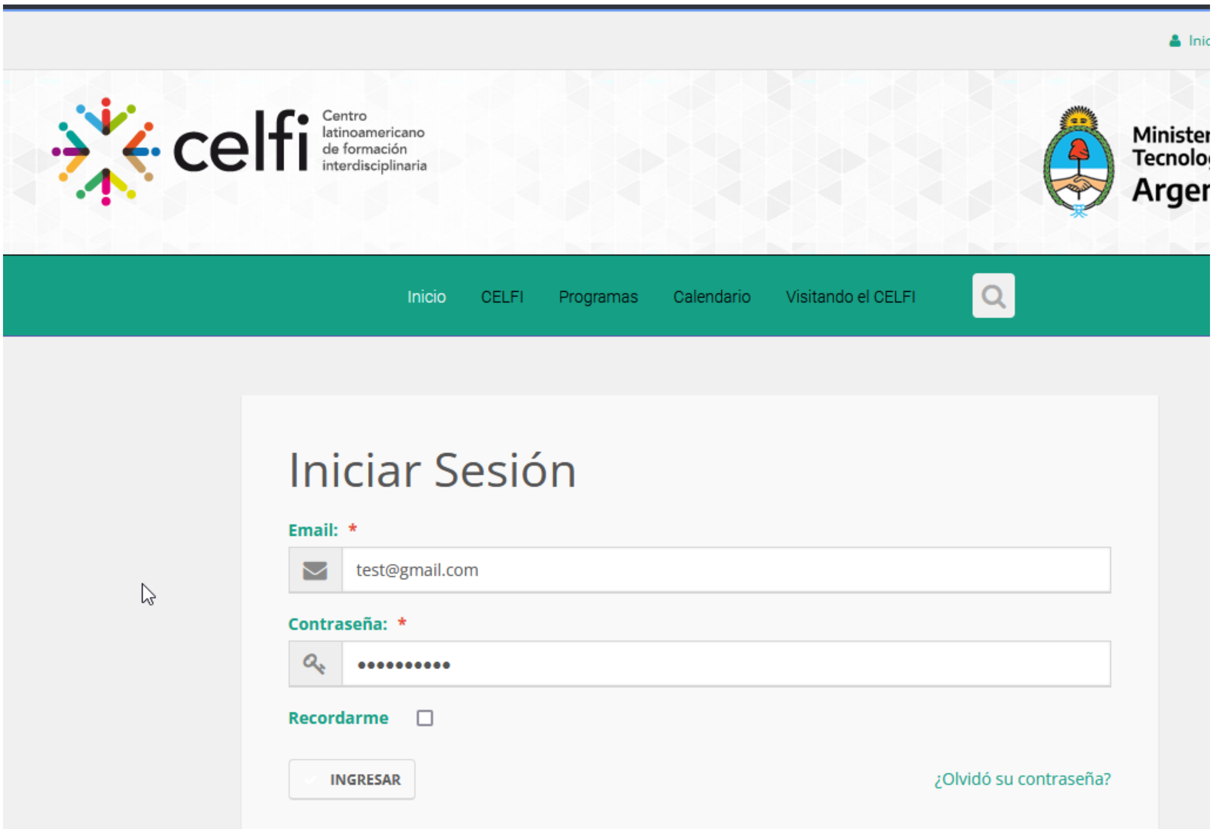
Sev	Score	Name	Family	Count
MEDIUM	5.3	SMB Signing not required	Misc.	1
INFO		Nessus SYN scanner	Port scanners	9
INFO		DCE Services Enumeration	Windows	8

no obtengo ninguna vulnerabilidad alta, solo que la firma de autenticacion via smb esta deshabilitada.

MITM

inicio wireshark y selecciono la interfaz eth1

en el ordenador victima busco un web con un login en http



Iniciar Sesión

Email: * test@gmail.com

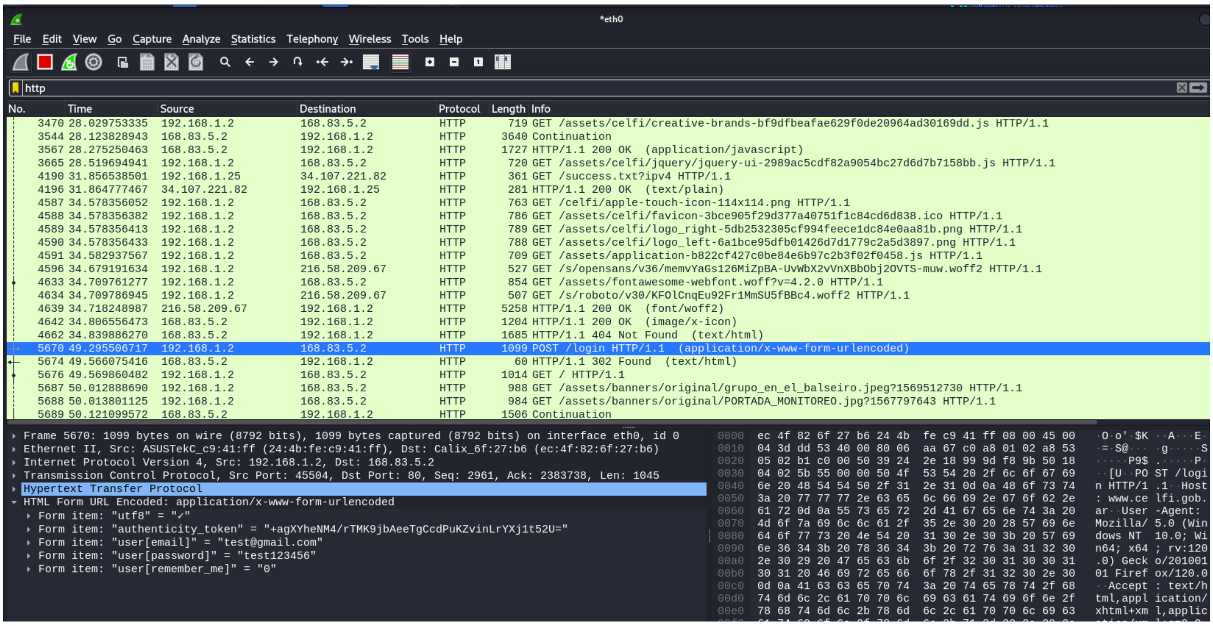
Contraseña: * ••••••••••

Recordarme □

Introduzco unas credenciales

Filtro en wireshark por el protocolo http

busco la peticion POST

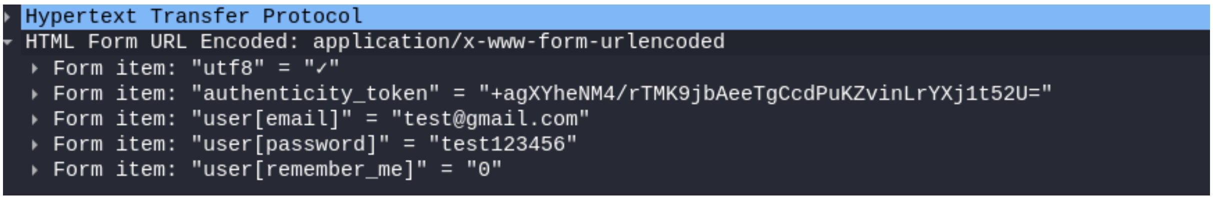

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time           Source          Destination     Protocol Length Info
3470 28.029753335   192.168.1.2     168.83.5.2      HTTP      719 GET /assets/celfi/creative-brands-bf9dfbeafae629f0de20964ad30169dd.js HTTP/1.1
3544 28.123828943   168.83.5.2      192.168.1.2     HTTP     3640 Continuation
3567 28.275250463   168.83.5.2      192.168.1.2     HTTP     1727 HTTP/1.1 200 OK  (application/javascript)
3665 28.519694941   192.168.1.2     168.83.5.2      HTTP      720 GET /assets/celfi/jquery/jquery-ui-2989ac5cdf82a9054bc27d6d7b7158bb.js HTTP/1.1
4190 31.856538501   192.168.1.25    34.107.221.82   HTTP      361 GET /success.txt?ipv4 HTTP/1.1
4196 31.864777467   34.107.221.82   192.168.1.25    HTTP      281 HTTP/1.1 200 OK  (text/plain)
4587 34.578356052   192.168.1.2     168.83.5.2      HTTP      763 GET /celfi/apple-touch-icon-114x114.png HTTP/1.1
4588 34.578356382   192.168.1.2     168.83.5.2      HTTP      786 GET /assets/celfi/favicon-3bce905f29d377a40751f1c84cd6d838.ico HTTP/1.1
4589 34.578356413   192.168.1.2     168.83.5.2      HTTP      789 GET /assets/celfi/logo_right-5db2532305cf994feece1dc84e0aa81b.png HTTP/1.1
4590 34.578356433   192.168.1.2     168.83.5.2      HTTP      788 GET /assets/celfi/logo_left-6a1bce95dfb01426d7d1779c2a5d3897.png HTTP/1.1
4591 34.582937567   192.168.1.2     168.83.5.2      HTTP      709 GET /assets/application-b822cf427c0be84e6b97c2b3f02f0458.js HTTP/1.1
4596 34.679191634   192.168.1.2     216.58.209.67   HTTP      527 GET /s/opensans/v36/memvYaGs126MiZpBA-UvWbX2vVnXBbObj2OVTS-muw.woff2 HTTP/1.1
4633 34.709761277   192.168.1.2     168.83.5.2      HTTP      854 GET /assets/fontawesome-webfont.woff?v=4.2.0 HTTP/1.1
4634 34.709786945   192.168.1.2     216.58.209.67   HTTP      507 GET /s/roboto/v30/KFOlCnqEu92Fr1MmSU5fBBc4.woff2 HTTP/1.1
4639 34.718248987   216.58.209.67   192.168.1.2     HTTP     5258 HTTP/1.1 200 OK  (font/woff2)
4642 34.806556473   168.83.5.2      192.168.1.2     HTTP     1204 HTTP/1.1 200 OK  (image/x-icon)
4662 34.839886270   168.83.5.2      192.168.1.2     HTTP     1685 HTTP/1.1 404 Not Found  (text/html)
5670 49.295506717   192.168.1.2     168.83.5.2      HTTP     1099 POST /login HTTP/1.1  (application/x-www-form-urlencoded)
5674 49.566075416   168.83.5.2      192.168.1.2     HTTP       60 HTTP/1.1 302 Found  (text/html)
5676 49.569860482   192.168.1.2     168.83.5.2      HTTP     1014 GET / HTTP/1.1
5687 50.012888690   192.168.1.2     168.83.5.2      HTTP      988 GET /assets/banners/original/grupo_en_el_balseiro.jpeg?1569512730 HTTP/1.1
5688 50.013801125   192.168.1.2     168.83.5.2      HTTP      984 GET /assets/banners/original/PORTADA_MONITOREO.jpg?1567797643 HTTP/1.1
5689 50.121099572   168.83.5.2      192.168.1.2     HTTP     1506 Continuation
```

```
▸ Frame 5670: 1099 bytes on wire (8792 bits), 1099 bytes captured (8792 bits) on interface eth0, id 0
▸ Ethernet II, Src: ASUSTekC_c9:41:ff (24:4b:fe:c9:41:ff), Dst: Calix_6f:27:b6 (ec:4f:82:6f:27:b6)
▸ Internet Protocol Version 4, Src: 192.168.1.2, Dst: 168.83.5.2
▸ Transmission Control Protocol, Src Port: 45504, Dst Port: 80, Seq: 2961, Ack: 2383738, Len: 1045
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "utf8" = "✓"
  ▸ Form item: "authenticity_token" = "+agXYheNM4/rTMK9jbAeeTgCcdPuKZvinLrYXj1t52U="
  ▸ Form item: "user[email]" = "test@gmail.com"
  ▸ Form item: "user[password]" = "test123456"
  ▸ Form item: "user[remember_me]" = "0"
```

```
0000  ec 4f 82 6f 27 b6 24 4b  fe c9 41 ff 08 00 45 00   ·O·o'·$K ··A···E·
0010  04 3d dd 53 40 00 80 06  aa 67 c0 a8 01 02 a8 53   ·=·S@··· ·g·····S
0020  05 02 b1 c0 00 50 39 24  2e 18 99 9d f8 9b 50 18   ·····P9$ .·····P·
0030  04 02 5b 55 00 00 50 4f  53 54 20 2f 6c 6f 67 69   ··[U··PO ST /logi
0040  6e 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   n HTTP/1 .1··Host
0050  3a 20 77 77 77 2e 63 65  6c 66 69 2e 67 6f 62 2e   : www.ce lfi.gob.
0060  61 72 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   ar··User -Agent: 
0070  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0080  64 6f 77 73 20 4e 54 20  31 30 2e 30 3b 20 57 69   dows NT  10.0; Wi
0090  6e 36 34 3b 20 78 36 34  3b 20 72 76 3a 31 32 30   n64; x64 ; rv:120
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00b0  30 31 20 46 69 72 65 66  6f 78 2f 31 32 30 2e 30   01 Firef ox/120.0
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
```

y veo las credenciales en texto plano



```
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "utf8" = "✓"
  ▸ Form item: "authenticity_token" = "+agXYheNM4/rTMK9jbAeeTgCcdPuKZvinLrYXj1t52U="
  ▸ Form item: "user[email]" = "test@gmail.com"
  ▸ Form item: "user[password]" = "test123456"
  ▸ Form item: "user[remember_me]" = "0"
```