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

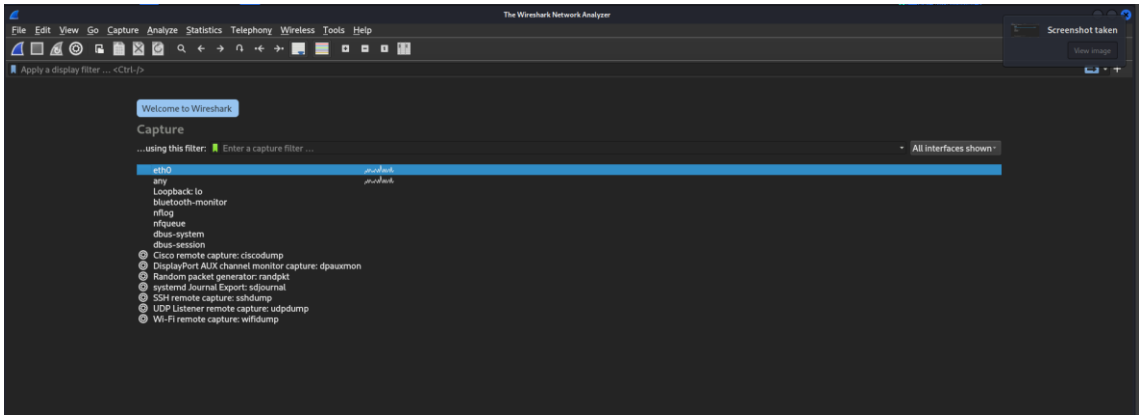
sudo: Executa o comando com privilégios de superutilizador.
arpspoof: Ferramenta para realizar o ataque de ARP spoofing.
-i eth0: Especifica a interface de rede através da qual o ataque será realizado (eth0).
-t 192.168.1.94: Define o alvo do ataque de spoofing.
192.168.1.254: O endereço IP do gateway. Este é o endereço que será usado para enganar o alvo, fazendo-o pensar que este é o seu gateway de rede.

```
┌──(kali㉿kali)-[~]
└─$ sudo arpspoof -i eth0 -t 192.168.1.94 192.168.1.254
8:0:27:1e:36:4a 8:0:27:b3:e:65 0806 42: arp reply 192.168.1.254 is-at 8:0:27:1e:36:4a
8:0:27:1e:36:4a 8:0:27:b3:e:65 0806 42: arp reply 192.168.1.254 is-at 8:0:27:1e:36:4a
8:0:27:1e:36:4a 8:0:27:b3:e:65 0806 42: arp reply 192.168.1.254 is-at 8:0:27:1e:36:4a
8:0:27:1e:36:4a 8:0:27:b3:e:65 0806 42: arp reply 192.168.1.254 is-at 8:0:27:1e:36:4a
8:0:27:1e:36:4a 8:0:27:b3:e:65 0806 42: arp reply 192.168.1.254 is-at 8:0:27:1e:36:4a
8:0:27:1e:36:4a 8:0:27:b3:e:65 0806 42: arp reply 192.168.1.254 is-at 8:0:27:1e:36:4a
8:0:27:1e:36:4a 8:0:27:b3:e:65 0806 42: arp reply 192.168.1.254 is-at 8:0:27:1e:36:4a
8:0:27:1e:36:4a 8:0:27:b3:e:65 0806 42: arp reply 192.168.1.254 is-at 8:0:27:1e:36:4a
8:0:27:1e:36:4a 8:0:27:b3:e:65 0806 42: arp reply 192.168.1.254 is-at 8:0:27:1e:36:4a
8:0:27:1e:36:4a 8:0:27:b3:e:65 0806 42: arp reply 192.168.1.254 is-at 8:0:27:1e:36:4a
```

O próximo passo é monitorar e analisar esse tráfego.

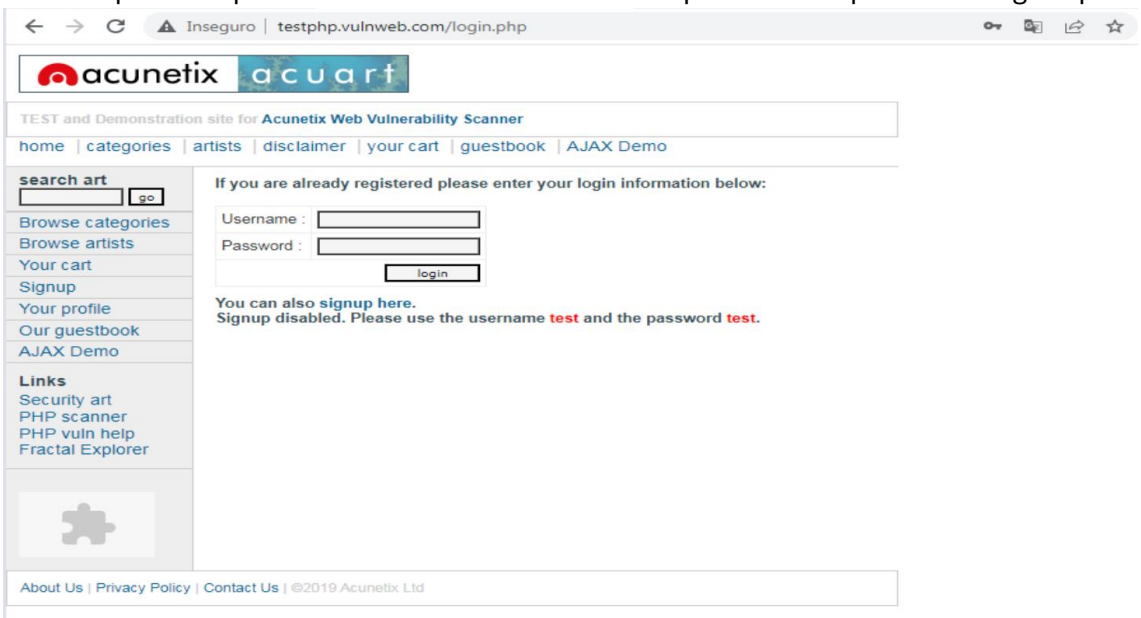
Para isso início o wireshark
sudo wireshark

Seleciono a interface de rede que é o eth0

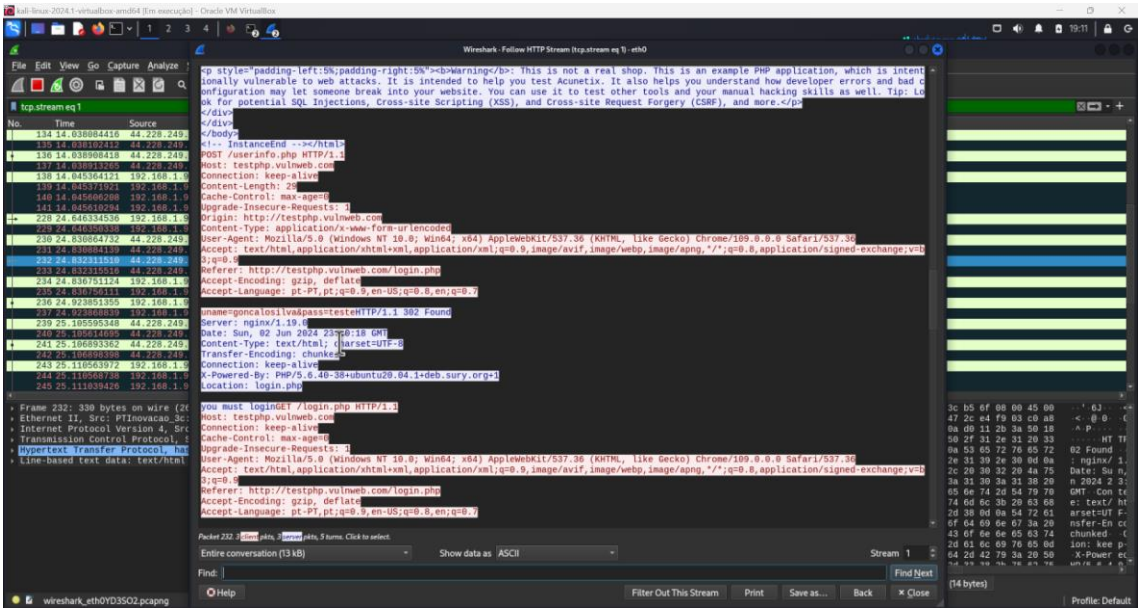


Filtro o tráfego usando o filtro **http**

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

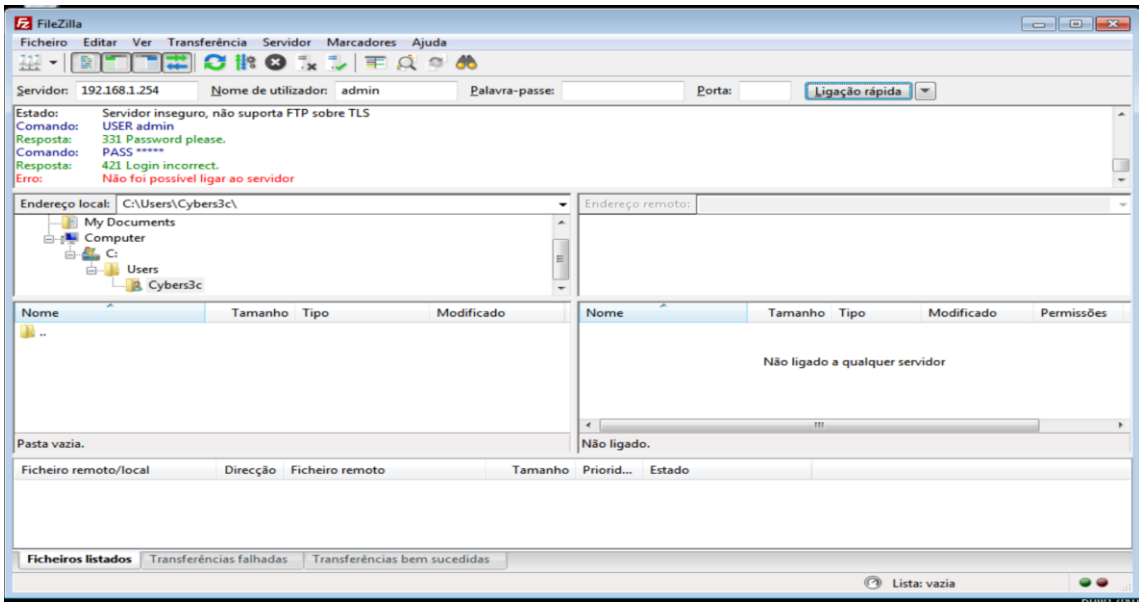


Através do wireshark verifico quando faço follow http Stream o login e pass usado :



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

Após configurar o meu servidor com o filezilla



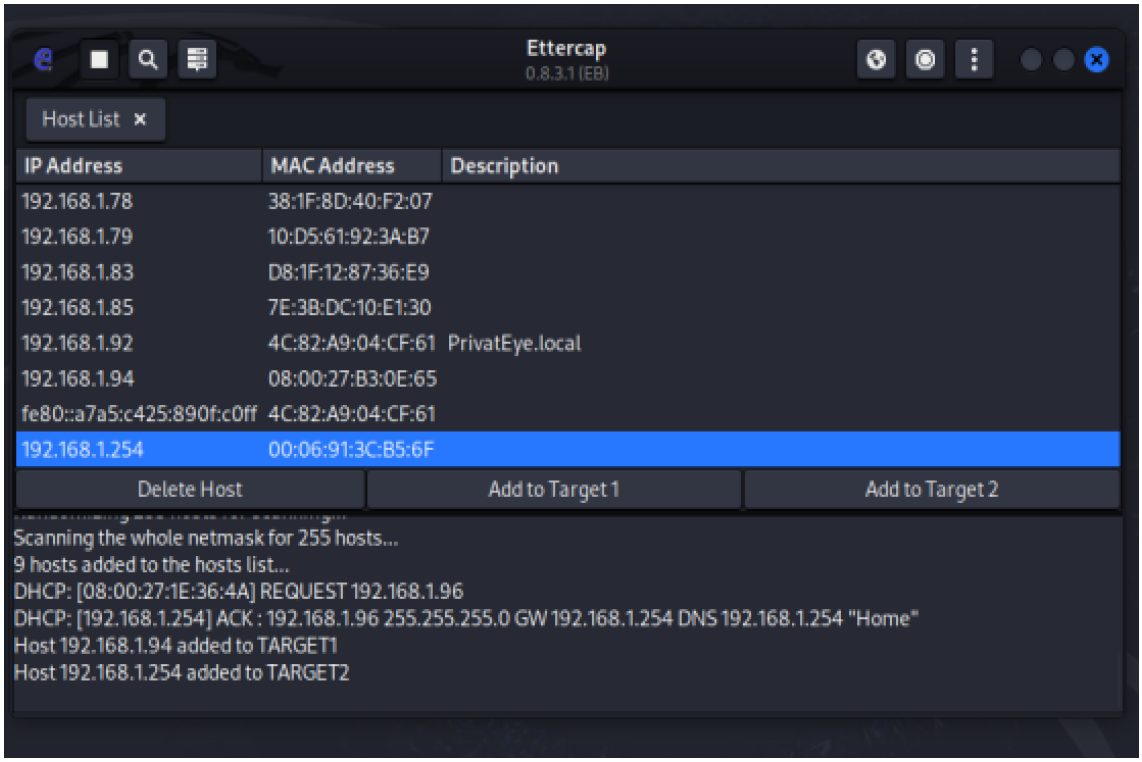
Abro a ferramenta através do comando:
sudo ettercap -G

Faço scan for hosts e abro a Hosts list

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

Faço add to target1 o IP da máquina sobre escuta

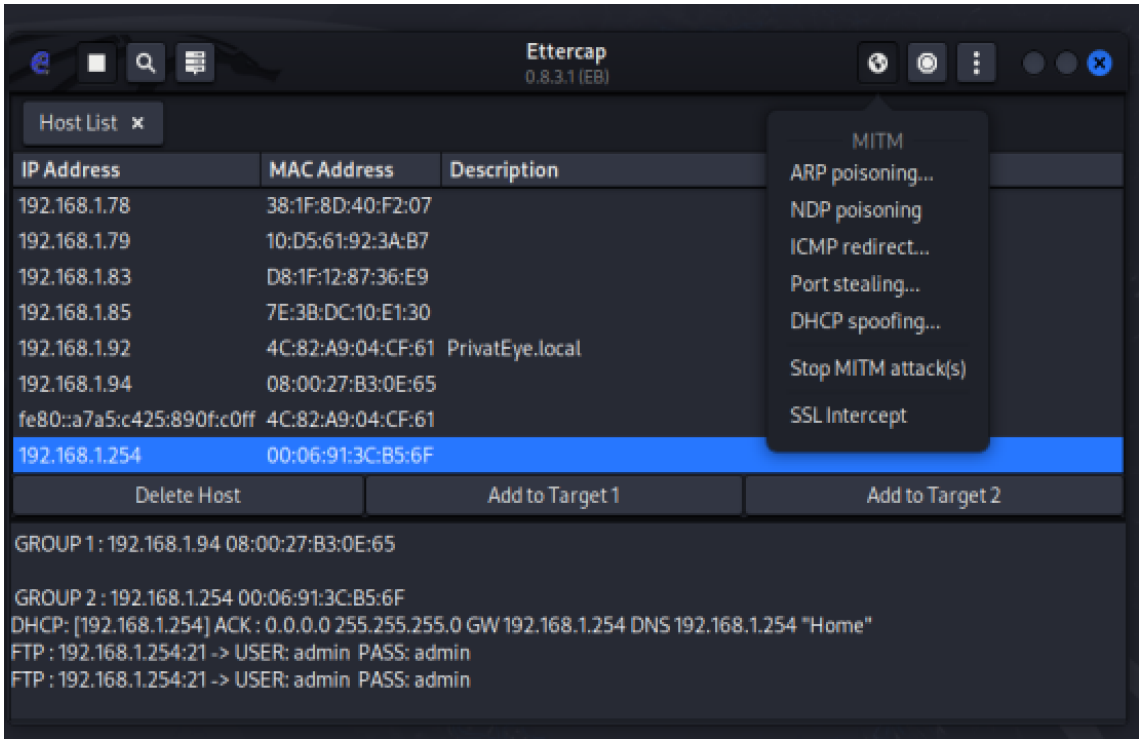
IP do servidor FTP (192.168.1.254) como Target 2



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**



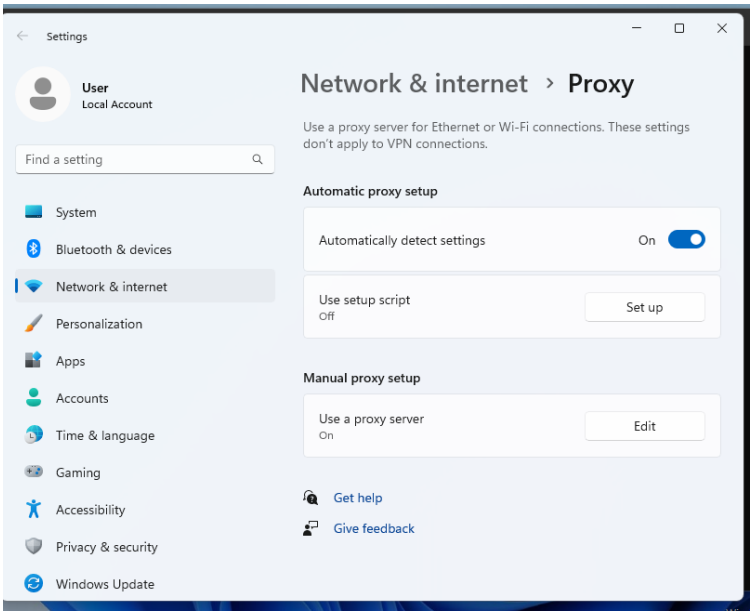
Pedido 3. (5 valores) Capture as credenciais de acessos de um serviço HTTPS com recurso à ferramenta mitmproxy, demonstrando todos os passos, comandos e com recurso a screenshots.

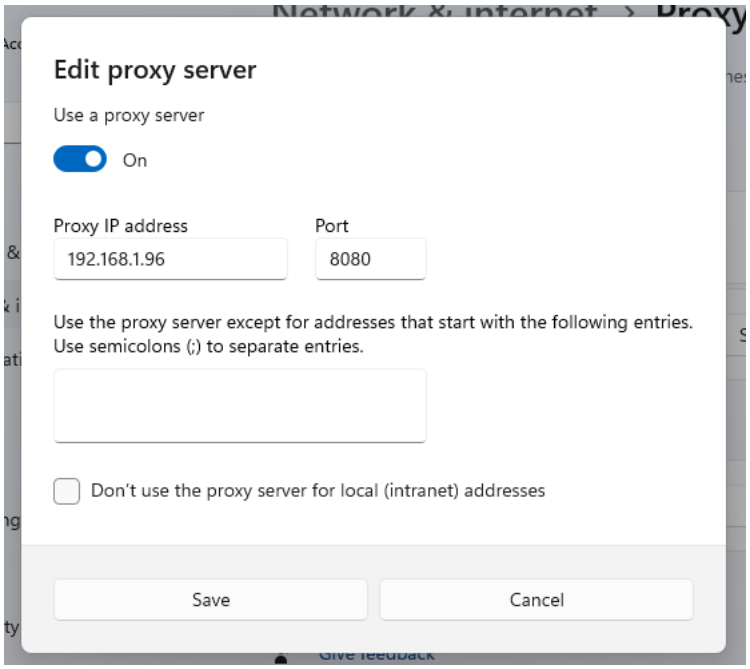
Instalo e executo o mitmproxy

sudo apt-get install mitmproxy

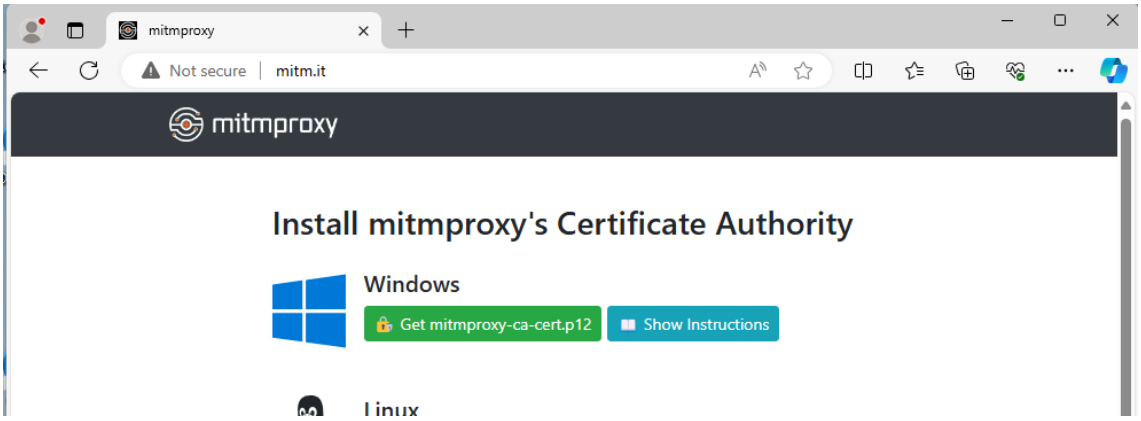
mitmproxy

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.

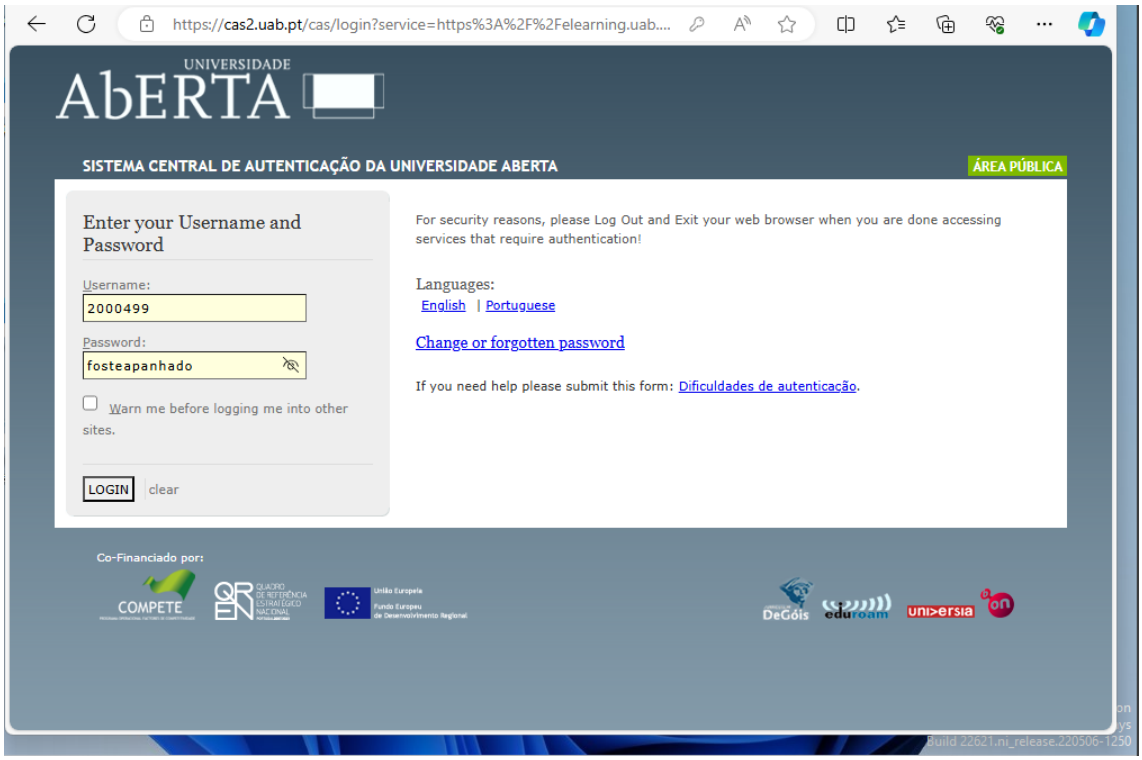




De seguida acedo ao site http://mitm.it e instalo o certificado o que irá garantir que o sistema confie plenamente no certificado do mitmproxy.



Para fazer o teste acedo ao site https://cas2.uab.pt

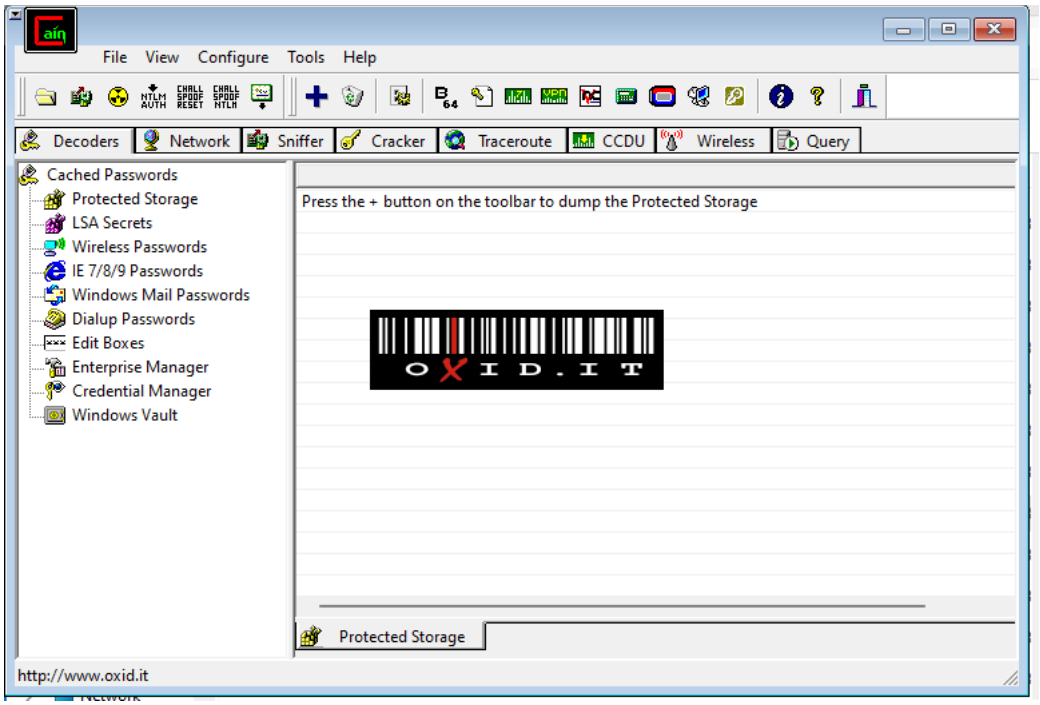


Podemos verificar através do mitm no Linux as ligações efetuados a uab

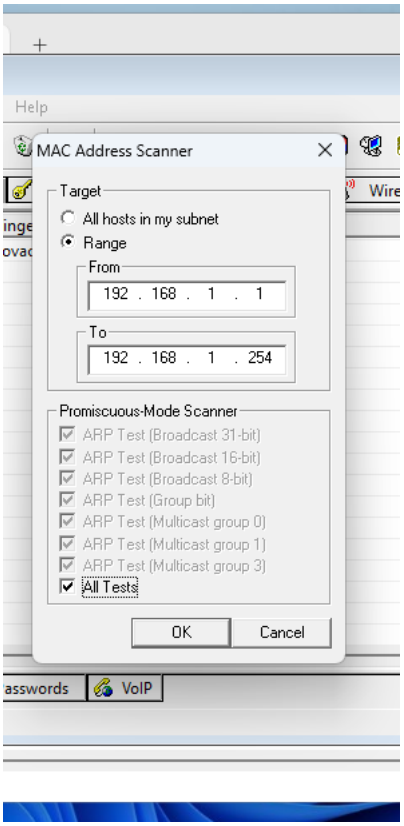
Procurando no https Post verifiquei o Login do utilizador e a password de forma muito clara!!!

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.

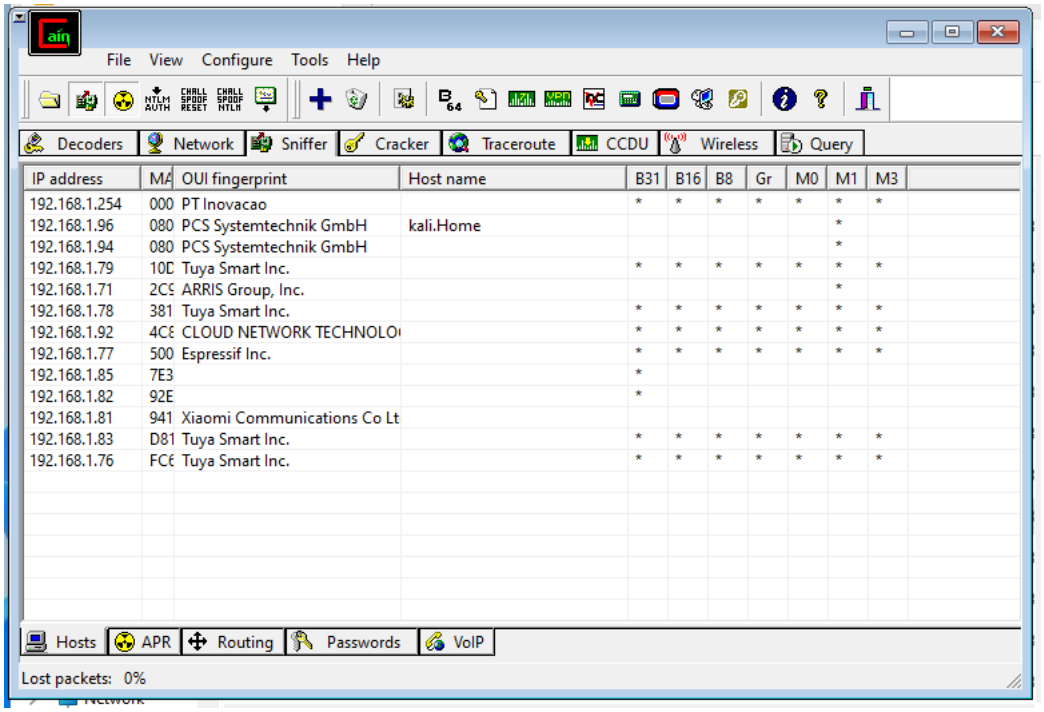
Fiz download e executo a ferramenta Cain&Abel tendo desativado a Proteção de antivírus e firewall do Windows 10 e instalado um pacote auxiliar (**WinPcap).**



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 selecionar a rede toda e selecionar 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.