

# **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.

**arp spoof**: 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.

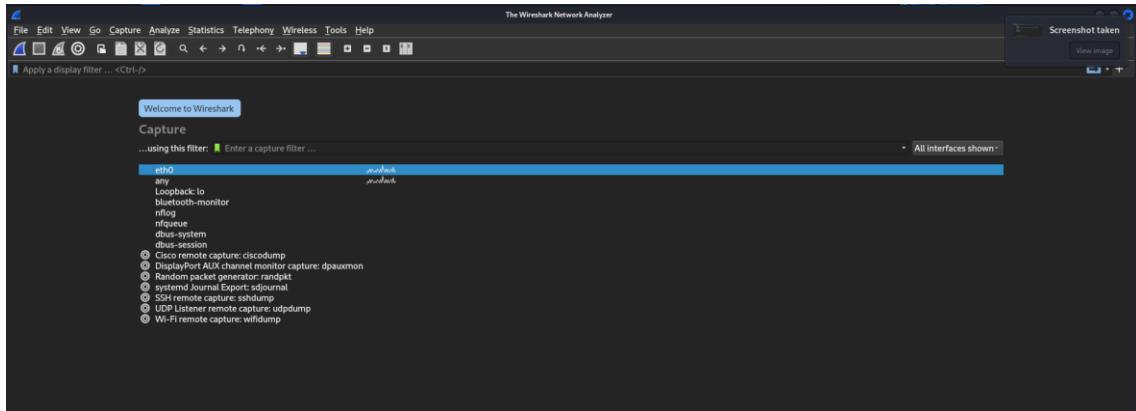
**192.168.1.254:** O endereço IP do gateway. Este é o endereço que será usado para enganar o alvo, fazendo-o pensar que este é o seu gateway de rede.

O próximo passo é monitorar e analisar esse tráfego.

Para isso inicie o wireshark

**sudo wireshark**

Seleciono a interface de rede que é o eth0

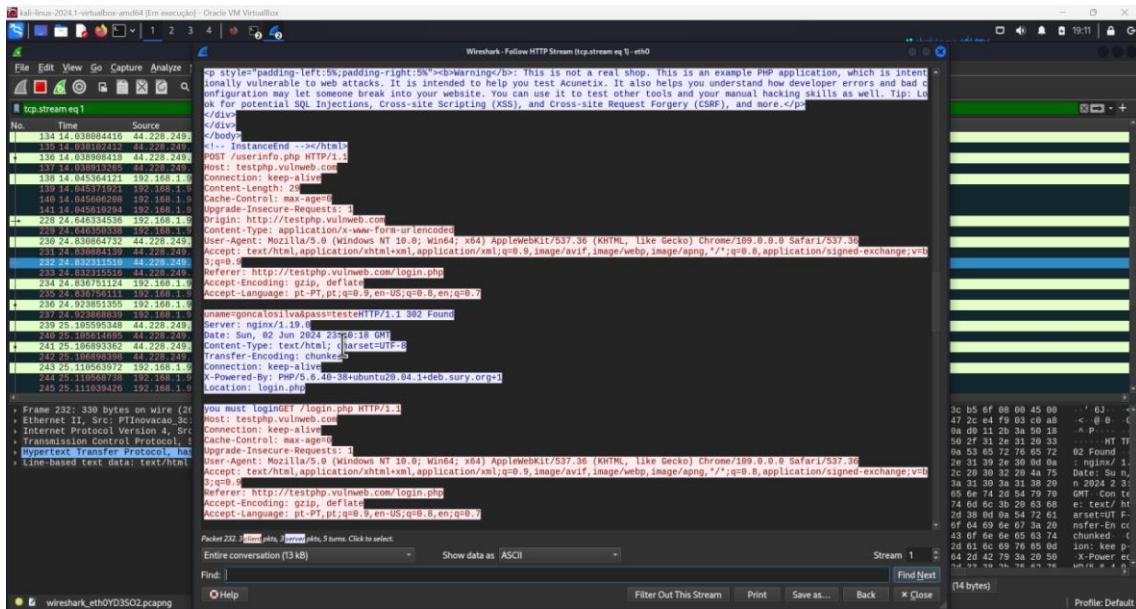


Filtro o tráfego usando o filtro **http**

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

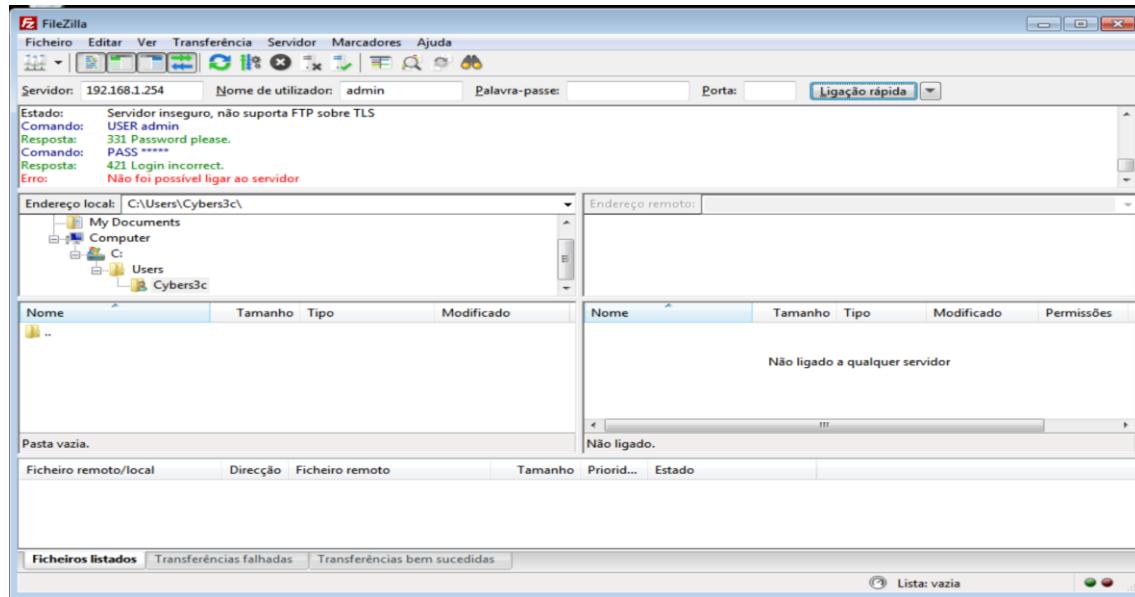
A screenshot of a web browser displaying a login page. The address bar shows "Inseguro | testphp.vulnweb.com/login.php". The page has a header with the "acunetix acuart" logo. Below the header, it says "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". There is a navigation menu with links: home, categories, artists, disclaimer, your cart, guestbook, and AJAX Demo. On the left, there is a sidebar with links: search art, browse categories, browse artists, your cart, Signup, Your profile, Our guestbook, and AJAX Demo. The main content area contains a login form with fields for "Username" and "Password", and a "login" button. Below the form, it says "You can also signup here. Signup disabled. Please use the username test and the password test." At the bottom, there are links for About Us, Privacy Policy, and Contact Us, along with a copyright notice: "©2019 Acunetix Ltd".

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

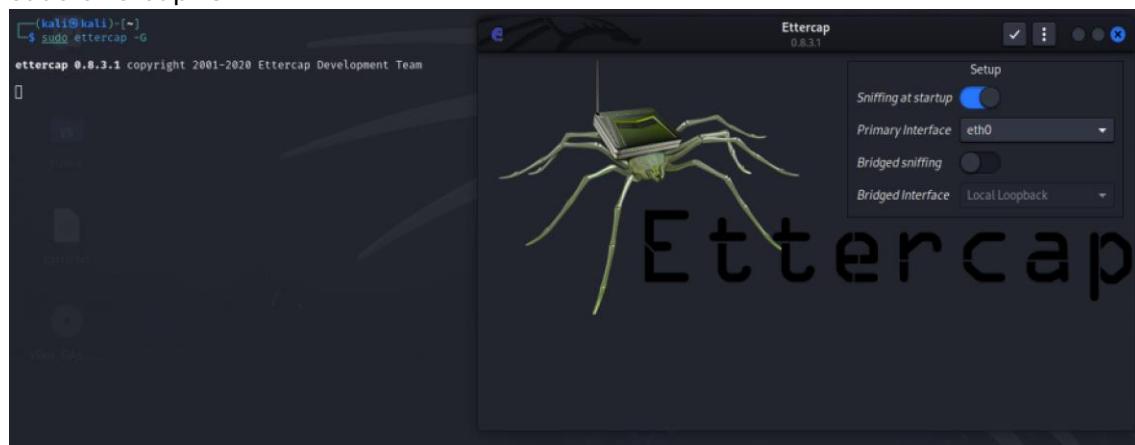


Pedido 2. (5 valores) Capture as credenciais de acessos de um serviço FTP com recurso à ferramenta Ethercap, demonstrando todos os passos, comandos e com recurso a screenshots.

Após configurar o meu servidor com o filezilla



Abro a ferramenta através do comando:  
sudo ettercap -G



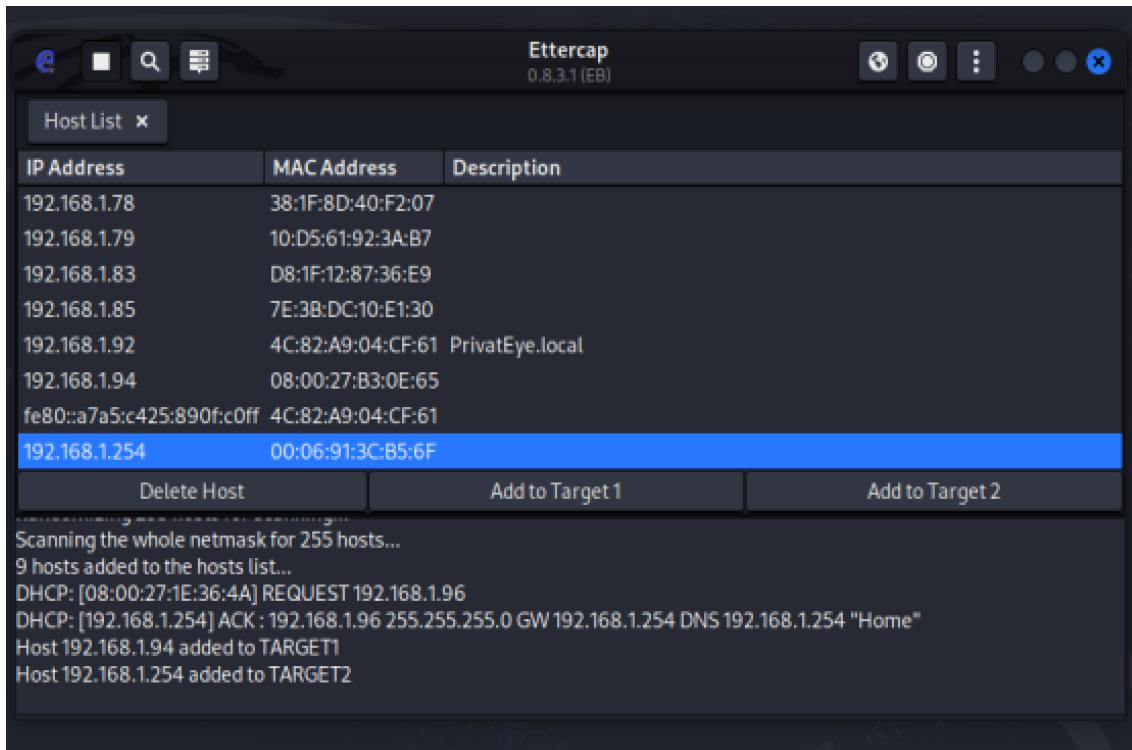
Faço scan for hosts e abro a Hosts list



No IP da 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**

The screenshot shows the Ettercap interface version 0.8.3.1 (EB). The main window displays a 'Host List' table with the following data:

IP Address	MAC Address	Description
192.168.1.78	38:1F:8D:40:F2:07	
192.168.1.79	10:D5:61:92:3A:B7	
192.168.1.83	D8:1F:12:87:36:E9	
192.168.1.85	7E:3B:DC:10:E1:30	
192.168.1.92	4C:82:A9:04:CF:61	PrivatEye.local
192.168.1.94	08:00:27:B3:0E:65	
fe80::a7a5:c425:890f:c0ff	4C:82:A9:04:CF:61	
192.168.1.254	00:06:91:3C:B5:6F	

A context menu is open over the row for host 192.168.1.254, listing options: MITM, ARP poisoning..., NDP poisoning, ICMP redirect..., Port stealing..., DHCP spoofing..., Stop MITM attack(s), and SSL Intercept.

Below the table, there are buttons for 'Delete Host', 'Add to Target 1', and 'Add to Target 2'. The text area at the bottom shows network traffic analysis results:

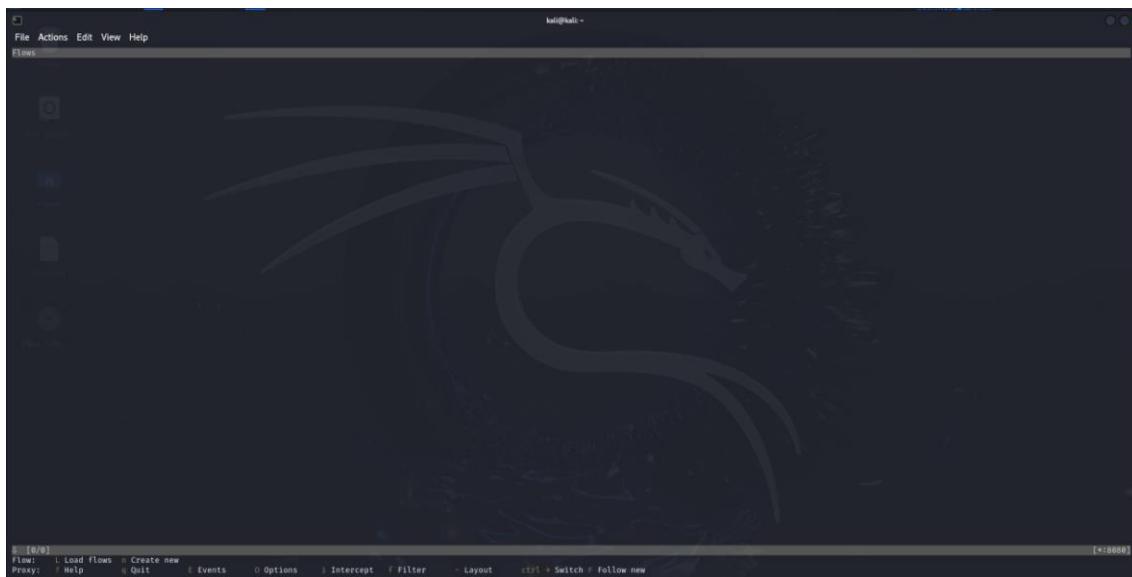
```
GROUP1:192.168.1.94 08:00:27:B3:0E:65
GROUP 2 :192.168.1.254 00:06:91:3C:B5:6F
DHCP: [192.168.1.254] ACK : 0.0.0.0 255.255.255.0 GW 192.168.1.254 DNS 192.168.1.254 "Home"
FTP : 192.168.1.254:21 -> USER: admin PASS: admin
FTP : 192.168.1.254:21 -> USER: admin PASS: admin
```

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.

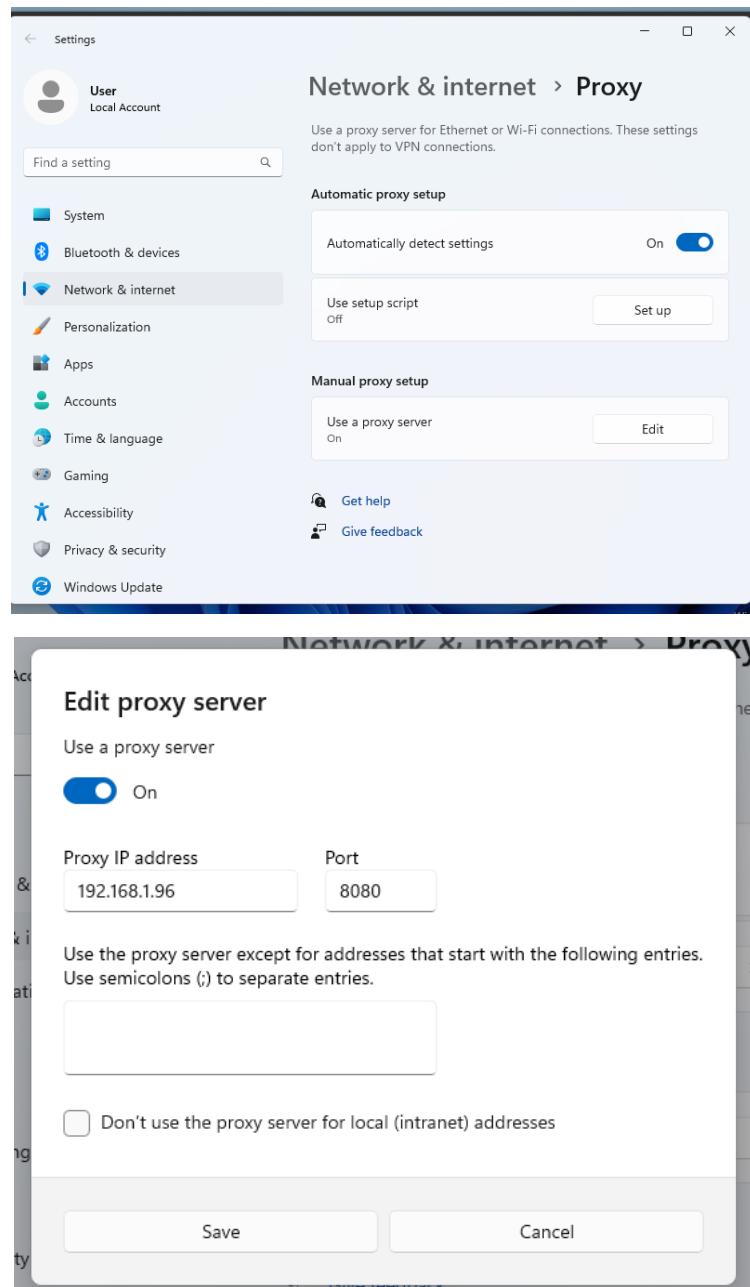
Instalo e executo o mitmproxy

```
sudo apt-get install mitmproxy
```

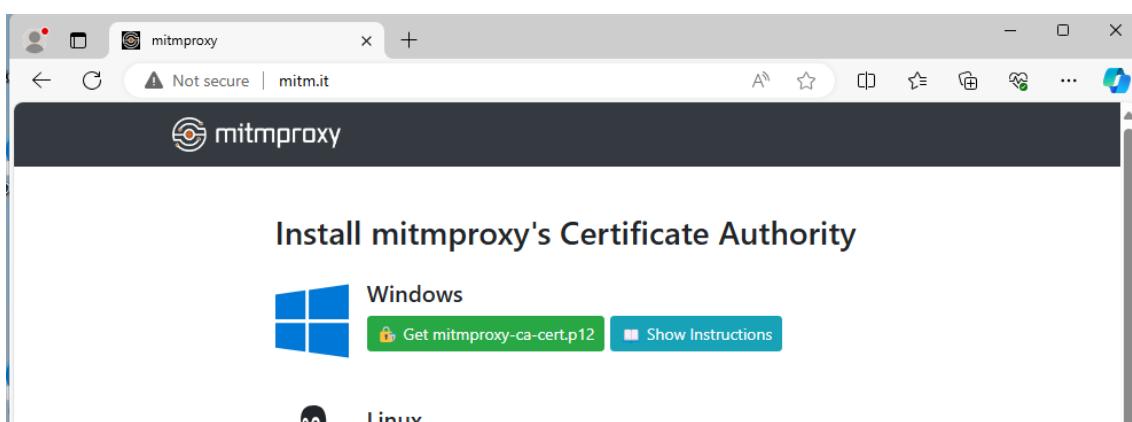
```
mitmproxy
```



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

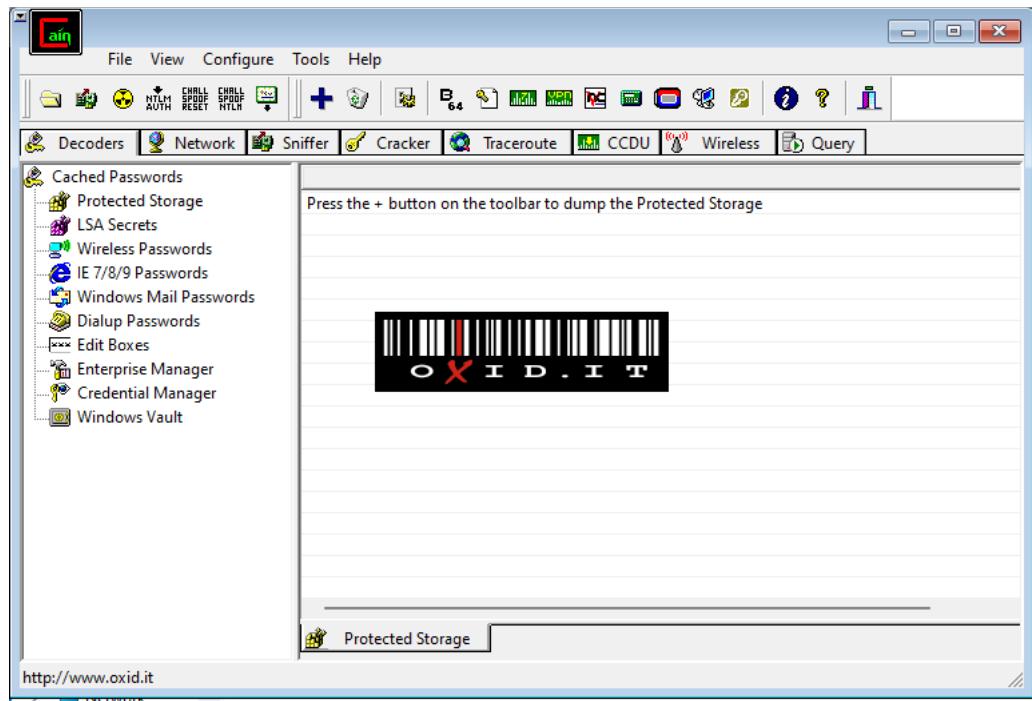


Procurando no https Post verifiquei o Login do utilizador e a password de forma muito clara!!!

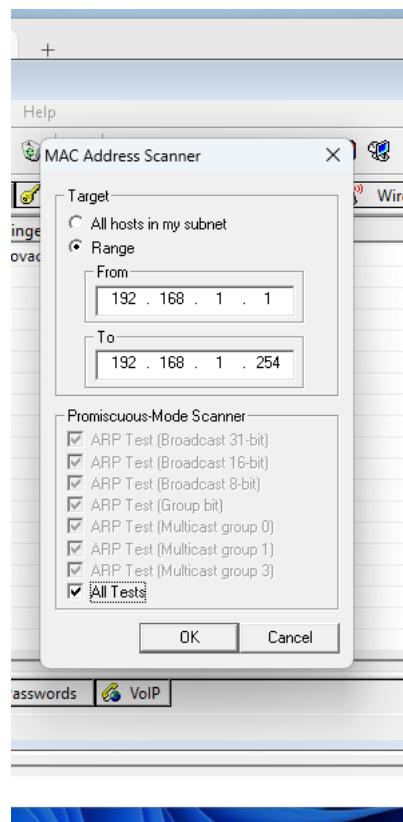


Pedido 4. (5 valores) Capture as credenciais de acessos de um serviço à sua escolha com recurso à ferramenta Cain&Abel, demonstrando todos os passos, comandos e com recurso a screenshots.

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

The screenshot shows the Cain & Abel NetworkMiner interface. The main window displays a table of discovered hosts. The columns include IP address, MAC OUI fingerprint, Host name, and various wireless interface columns (B31, B16, B8, Gr, M0, M1, M3). The table lists several devices, including PTInovacao, PCS Systemtechnik GmbH, Tuya Smart Inc., ARRIS Group, Inc., Espressif Inc., and Xiaomi Communications Co Ltd. Below the table, there are tabs for Hosts, APR, Routing, Passwords, and VoIP, along with a message about lost packets.

IP address	MAC OUI fingerprint	Host name	B31	B16	B8	Gr	M0	M1	M3
192.168.1.254	000 PTInovacao		*	*	*	*	*	*	*
192.168.1.96	080 PCS Systemtechnik GmbH	kali.Home				*			
192.168.1.94	080 PCS Systemtechnik GmbH					*			
192.168.1.79	10D Tuya Smart Inc.		*	*	*	*	*	*	*
192.168.1.71	2CE ARRIS Group, Inc.					*			
192.168.1.78	381 Tuya Smart Inc.		*	*	*	*	*	*	*
192.168.1.92	4CE CLOUD NETWORK TECHNOLOGY		*	*	*	*	*	*	*
192.168.1.77	500 Espressif Inc.		*	*	*	*	*	*	*
192.168.1.85	7E3		*						
192.168.1.82	92E		*						
192.168.1.81	941 Xiaomi Communications Co Ltd		*	*	*	*	*	*	*
192.168.1.83	D81 Tuya Smart Inc.		*	*	*	*	*	*	*
192.168.1.76	FCf Tuya Smart Inc.		*	*	*	*	*	*	*

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.

The screenshot shows the FileZilla interface. The status bar indicates "Estado: Servidor inseguro, não suporta FTP sobre TLS". The log pane shows the following sequence:  
Comando: USER Cybers3c  
Resposta: 331 Password please.  
Comando: PASS \*\*\*\*\*  
Resposta: 421 Login incorrect.  
Erro: Não foi possível ligar ao servidor.

The left panel shows the local file structure under "Endereço local: C:\Users\Cybers3c\". The right panel shows the remote file structure under "Endereço remoto: 192.168.1.254". The bottom status bar says "Não ligado".

