



Segurança

Projeto Autoproposto

2024 - 2025

Martim Ferreira de Oliveira - 2022132041

Ricardo Rodrigues Duarte - 2022137878

Ernesto Brito Cruz - 2023144672

Licenciatura em Engenharia Informática
Ramo de Redes e Administração de Sistemas
06 de junho de 2025

Conteúdo

1	Introdução	1
1.1	Como identificar dispositivos ativos na rede?	1
1.2	Como identificar o sistema operativo dos dispositivos?	1
1.3	Que serviços estão em execução nos servidores e que portas estão abertas?	2
2	Topologia	3
3	Experiências Realizadas	4
3.1	Flags de Utilização do NMap	4
3.2	Descoberta de Rede Básica	6
3.3	Descoberta de Rede Avançada	7
3.4	Descoberta dos Sistemas Operativos	8
3.5	Descoberta de rede Intensiva	9
3.6	Descoberta de Vulnerabilidades	10
3.7	Descoberta de Protocolos	11
4	Mitigação	12
4.1	Ataque	13
4.2	Mitigação do Ataque	14
5	Conclusão	18

Listas de Figuras

2.1	Topologia de Rede	3
3.1	Descoberta de Rede Básica	6
3.2	Descoberta de Rede Avançada	7
3.3	Descoberta dos Sistemas Operativos	8
3.4	Descoberta de rede Intensiva	9
3.5	Descoberta de Vulnerabilidades	10
3.6	Descoberta de Protocolos	11
4.1	Ataque sem Mitigação	13
4.2	Mitigação ACL	15
4.3	Mitigação ACL e TCP intercept	17

1. Introdução

Nmap[1] ("Network Mapper") é um software, desenvolvido por Gordon Lyon, com o objetivo de uso para descoberta de rede, muito utilizado para avaliar segurança e serviços. Nmap usa pacotes de IP, de modo a determinar quais "host's" estão disponíveis na "network". Nmap pode ser usado em diversos sistemas operativos, identificando também quais estão a ser usados na rede. Nmap é uma ferramenta que pode ser usada para descobrir serviços em sistemas conectados à internet. Como qualquer outra ferramenta do tipo, pode ser usado por black hat's, para acesso não autorizado em sistemas. Por outro lado, pode também ser usado por administradores de sistema para procurar por falhas de segurança.

1.1 Como identificar dispositivos ativos na rede?

- Sem o Nmap teríamos de efetuar *ping* manualmente para cada endereço disponível, ou seja, 254 *pings* numa rede /24.
- Com o Nmap, podemos usar um *scan* de descoberta para identificar os dispositivos ativos de forma automática.
- Podemos também utilizar o Wireshark para capturar os PDUs e analisar as respostas dos dispositivos.

1.2 Como identificar o sistema operativo dos dispositivos?

- O Nmap pode tentar identificar o sistema operativo dos dispositivos através da análise de características do protocolo TCP/IP.
- Para termos a certeza dos resultados, podemos comparar os resultados do Nmap com os obtidos por comandos internos dos dispositivos.
- Mais uma vez, podemos utilizar o Wireshark para observar os PDUs e os seus conteúdos.

1.3 Que serviços estão em execução nos servidores e que portas estão abertas?

- Através da utilização do Nmap, também conseguimos ver os serviços que estão a ser utilizados pelas máquinas na rede que queremos analisar.
- O Wireshark pode ser usado para capturar os PDUs TCP SYN e as suas respostas.

2. Topologia

A topologia de rede que iremos utilizar será realizada na aplicação, GNS3, abordada nas aulas, garantindo esta a possibilidade de serem realizados todos os testes que possam ser efetuados à rede.

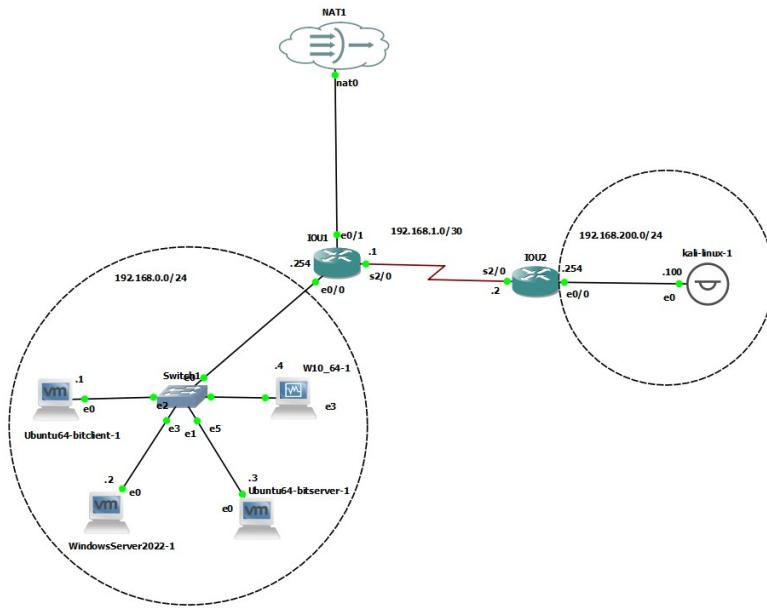


Figura 2.1: Topologia de Rede

Nesta topologia vamos utilizar:

- Quatro máquinas virtuais (Windows 10, Windows Server, Ubuntu Desktop, Ubuntu Server) e sistema Kali Linux responsáveis por realizar scans na rede com o Nmap
- Um switch (SW1) para interconectar os dispositivos nas sub-redes
- Dois routers (R1 e R2) para permitir a comunicação entre as sub-redes
- Ligação a Nat, para continuarmos a ter acesso à internet

3. Experiências Realizadas

Tal como dito anteriormente, o NMap permite realizar diversas experiências à rede. Inicialmente usamos a topologia para verificar o poder de descoberta do programa NMap, é importante salientar que serão detetadas poucas informações, como portas abertas nestes experimentos, pelo facto de serem máquinas limpas.

3.1 Flags de Utilização do NMap

Para a realização das experiências e na utilização normal do NMap são usadas várias flags para mudar o seu foco de descoberta, aqui estão as que utilizámos para as nossas experiências:

- **-sn**

Este é o scan *default* que o nmap faz, é um simples *ping sweep* que varre a rede alvo, tenta primeiro por ICMP, se não obter resposta passa para pedidos ARP, se continuar sem resposta, envia pacotes TCP com a flag 'ACK' para as portas 80 e 443.

- **-O**

Um scan deste tipo é relativamente simples mas eficaz, envia pacotes IP, quando estes são recebidos pelo alvo são tratados e há uma resposta, nessa resposta há vários campos diferentes de SO para SO, deixa assim *fingerprints* que o nmap compara com uma base de dados para descobrir o SO do alvo.

- **-sS**

Este é um dos modos de *sweeping* mais usados, é tão usado por passar por firewalls mais facilmente, são enviados pacotes TCP com a flag 'SYN' para as portas do alvo, se este responder com 'SYN ACK' a porta está aberta, se a resposta for 'RST' a porta está fechada. Ao receber 'SYN ACK' o NMap envia logo um 'RST' para não completar o *three way handshake*, não completando assim a conexão TCP.

- **-sV**

Este tende detetar os serviços que estão a correr nas portas destino, funciona de modo similar ao -O, após completar o *sweeping* da rede envia pacotes de sonda a cada porta, compara os dados de cada resposta com uma base de dados e consegue assim saber que serviços e que versão corre nas portas.

- **-A**

Este é o modo agressivo e o que faz mais coisas com uma única flag, este modo faz o *sweeping*, deteção de SO, deteção de versões, traceroute e ainda corre alguns scripts NSE (NMap Scripting Engine) que podem ser relevantes para descobrir vulnerabilidades no alvo.

- **--script vuln**

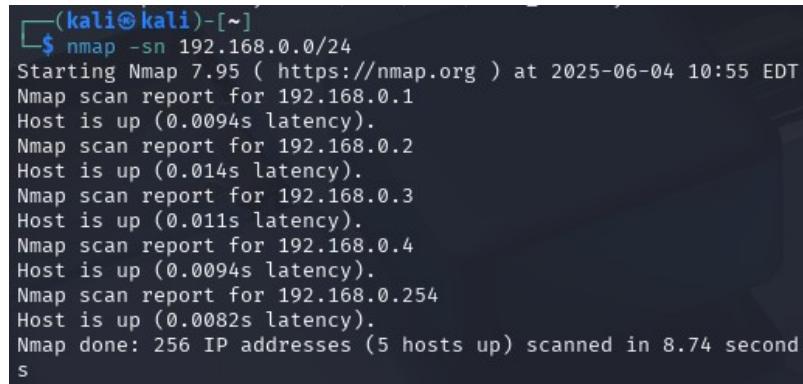
Esta opção executa a deteção de vulnerabilidades, embora corra um script diferente do que foi referido no item -A, a resposta aos pacotes é analisada e comparada com uma base de dados, podendo-se assim identificar vulnerabilidades comuns.

- **-sO**

Esta opção permite saber que protocolos estão a correr nas portas, faz isto ao enviar vários packets com diferentes números de protocolo no *header* do pacote.

3.2 Descoberta de Rede Básica

Para a realização desta descoberta foi utilizada a flag '-sn'



```
(kali㉿kali)-[~]
$ nmap -sn 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 10:55 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0094s latency).
Nmap scan report for 192.168.0.2
Host is up (0.014s latency).
Nmap scan report for 192.168.0.3
Host is up (0.011s latency).
Nmap scan report for 192.168.0.4
Host is up (0.0094s latency).
Nmap scan report for 192.168.0.254
Host is up (0.0082s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 8.74 seconds
```

Figura 3.1: Descoberta de Rede Básica

Após a realização do ataque, podemos concluir que temos 5 IP's com estado up, estes correspondem às nossas máquinas virtuais e ao router da rede a ser atacada.

3.3 Descoberta de Rede Avançada

Para a realização desta descoberta foi utilizada a flag '-sS'

```
(kali㉿kali)-[~]
└─$ nmap -sS 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 11:12 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0089s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for 192.168.0.2
Host is up (0.010s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman

Nmap scan report for 192.168.0.3
Host is up (0.0090s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for 192.168.0.4
Host is up (0.0095s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap scan report for 192.168.0.254
Host is up (0.0082s latency).
All 1000 scanned ports on 192.168.0.254 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 6.47 seconds
```

Figura 3.2: Descoberta de Rede Avançada

Devido à natureza e modo de operação deste ataque é possível não só fazer um reconhecimento da rede como das portas TCP abertas nas diversas máquinas.

3.4 Descoberta dos Sistemas Operativos

Para a realização desta descoberta, foi utilizada a flag '-O'

```
└─$ nmap -O 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 11:30 EDT
Nmap scan report for 192.168.0.1
Host is up (0.012s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 3 hops

Nmap scan report for 192.168.0.2
Host is up (0.010s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
Aggressive OS guesses: Microsoft Windows Server 2022 (99%), Microsoft Win
dows 10 1703 or Windows 11 21H2 (97%), Microsoft Windows Server 2016 or S
erver 2019 (97%), Microsoft Windows 11 21H2 (96%), Windows Server 2019 (9
5%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (9
4%), Microsoft Windows 10 1703 (94%), Microsoft Windows Server 2016 (94%)
, Microsoft Windows 10 1507 - 1607 (94%), Microsoft Windows Server 2012 o
r 2012 R2 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 3 hops

Nmap scan report for 192.168.0.3
Host is up (0.012s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 3 hops

Nmap scan report for 192.168.0.4
Host is up (0.011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
Device type: general purpose
Running: Microsoft Windows 10|11
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11
OS details: Microsoft Windows 10 1703 or Windows 11 21H2
Network Distance: 3 hops
```

Figura 3.3: Descoberta dos Sistemas Operativos

Através desta experiência, podemos visualizar mais detalhadamente a ver
são dos Sistemas Operativos de cada equipamento presente na rede e quais por
tas TCP se encontram abertas.

3.5 Descoberta de rede Intensiva

Para a realização desta descoberta foi utilizada a flag '-A'

```
L$ nmap -A 192.168.0.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 11:18 EDT
Nmap scan report for 192.168.0.4
Host is up (0.011s latency).
Not shown: 997 closed tcp ports (reset)
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 Windows 10 Enterprise Evaluation 15063 microsoft-ds (workgroup: WORKGROUP)
Device type: general purpose
Running: Microsoft Windows 10|11
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11
OS details: Microsoft Windows 10 1703 or Windows 11 21H2
Network Distance: 3 hops
Service Info: Host: DESKTOP-608G4N7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|     Message signing enabled but not required
|_nbstat: NetBIOS name: DESKTOP-608G4N7, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d5:d3:b6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -20m01s, deviation: 34m38s, median: -1s
| smb2-time:
|   date: 2025-06-04T15:18:33
|_ start_date: 2025-06-04T14:50:54
| smb-os-discovery:
|   OS: Windows 10 Enterprise Evaluation 15063 (Windows 10 Enterprise Evaluation 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10:-
|   Computer name: DESKTOP-608G4N7
|   NetBIOS computer name: DESKTOP-608G4N7\x00
|   Workgroup: WORKGROUP\x00
|_ system_time: 2025-06-04T16:18:33+01:00

TRACEROUTE (using port 554/tcp)
HOP RTT      ADDRESS
1  0.62 ms  192.168.200.254
2  4.98 ms  192.168.1.1
3  5.42 ms  192.168.0.4

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 14.02 seconds
```

Figura 3.4: Descoberta de rede Intensiva

Após a realização do ataque à VM que corre Windows 10 standard, podemos concluir que o alvo foi encontrado, e tem 3 portas TCP abertas, conseguimos saber o nome da máquina, o seu *workgroup* e conseguimos também o sistema operativo, a distância lógica e o resultados dos scripts NSE: Sabe-se que o nível de autenticação é de user, está com uma conta guest e não tem *message signing*, isto pode ser perigoso pois permite ataques man-in-the-middle.

3.6 Descoberta de Vulnerabilidades

Para a realização desta descoberta, foi utilizada a flag '--script vuln'

```
(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 11:42 EDT
Nmap scan report for 192.168.0.1
Host is up (0.025s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for 192.168.0.2
Host is up (0.020s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman

Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false

Nmap scan report for 192.168.0.3
Host is up (0.022s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for 192.168.0.4
Host is up (0.019s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Nmap scan report for 192.168.0.254
Host is up (0.025s latency).
All 1000 scanned ports on 192.168.0.254 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 32.43 seconds
```

Figura 3.5: Descoberta de Vulnerabilidades

Através desta experiência podemos ver que nenhuma máquina tem alguma vulnerabilidade que possa ser ativamente explorável.

3.7 Descoberta de Protocolos

Para a realização desta descoberta foi utilizada a flag '-sO'

```
(kali㉿kali)-[~]
└─$ nmap -sO 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 12:04 EDT
Warning: 192.168.0.1 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.0.1
Host is up (0.010s latency).
Not shown: 250 closed n/a protocols (proto-unreach)
PORTCOL STATE      SERVICE
1      open       icmp
2      open|filtered  igmp
6      open       tcp
17     open       udp
103    open|filtered pim
136    open|filtered udplite

Nmap scan report for 192.168.0.2
Host is up (0.016s latency).
Not shown: 250 closed n/a protocols (proto-unreach)
PORTCOL STATE      SERVICE
1      open       icmp
2      open|filtered  igmp
6      open       tcp
17     open       udp
50     open|filtered esp
51     open|filtered ah

Nmap scan report for 192.168.0.3
Host is up (0.010s latency).
Not shown: 237 closed n/a protocols (proto-unreach)
PORTCOL STATE      SERVICE
1      open       icmp
2      open|filtered  igmp
6      open       tcp
17     open       udp
34     open|filtered 3pc
61     open|filtered anyhost
103    open|filtered pim
105    open|filtered scps
113    open|filtered pgm
135    open|filtered mobility-hdr
136    open|filtered udplite
142    open|filtered rohc
154    open|filtered unknown
155    open|filtered unknown
162    open|filtered unknown
178    open|filtered unknown
184    open|filtered unknown
220    open|filtered unknown
242    open|filtered unknown
```

Figura 3.6: Descoberta de Protocolos

Através da experiência, podemos visualizar que todas as máquinas aceitam pacotes ICMP (1), TCP (6) e UDP (17).

4. Mitigação

A utilização de scanners é um tema controverso, a maioria deles são automatizados por worms, investigadores ou pessoas curiosas.

Sistemas de log raramente conseguem detetar estes scans eficazmente, principalmente do tipo SYN (o modo 'normal' do Nmap[2]), que não estabelecem ligações completas. Existem ferramentas especializadas como o PortSentry que oferecem melhor deteção podendo bloquear automaticamente IPs que considere suspeitos, mas este tipo de resposta é arriscada pois é difícil distinguir acessos normais de scans.

No entanto, quem se preocupa com scans também quer analisar e monitorizar ameaças mais avançadas, para isso usam sistemas de deteção de intrusões (IDS) como o Snort, uma solução muito popular.

Apesar de úteis, os IDS não são infalíveis, por isso devem ser usados como uma parte da estratégia de segurança e não como a única linha de defesa.

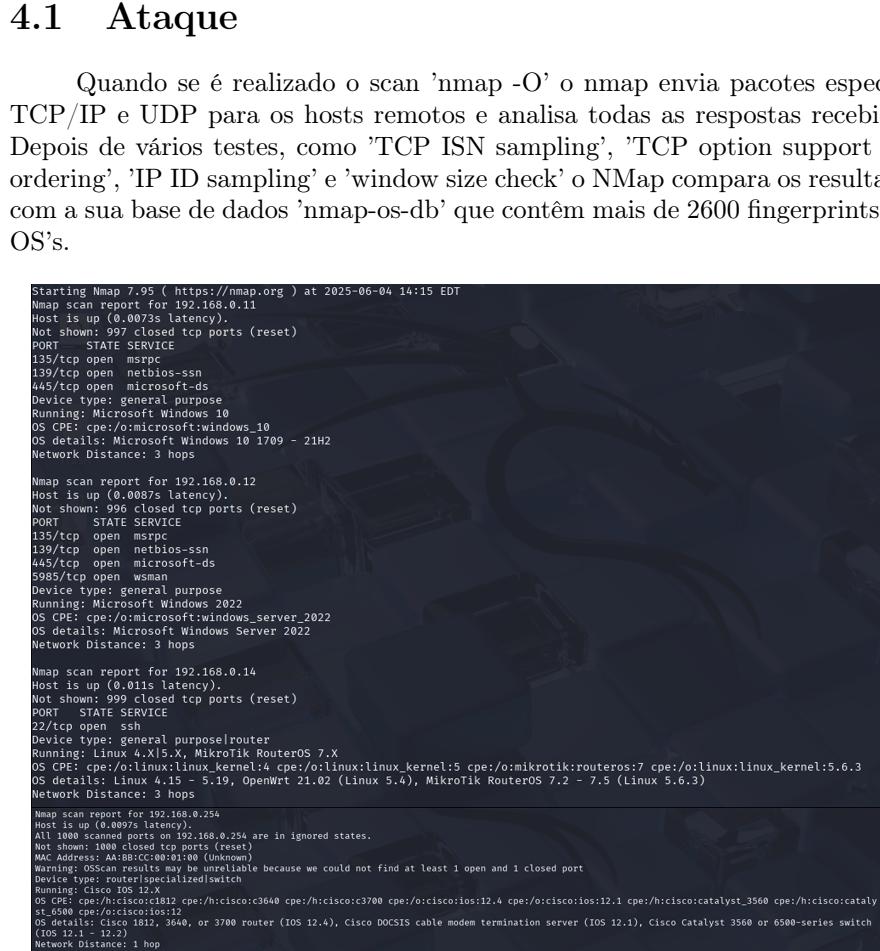
Alguns administradores também usam medidas ativas como serviços falsos para confundir ou desencorajar ferramentas de varrimentos, como o Nmap, estas táticas frequentemente causam mais problemas do que resolvem, muitas têm falhas críticas, como no caso do FakeBO que permitia o atacante instalar um backdoor. Além disso, estas medidas baseiam-se em "segurança por obscuridade" e podem desviar recursos que seriam melhores investidos em outras situações, sendo apenas úteis quando a rede já tem uma segurança firme. Exemplos destas medidas são:

- Esconder serviços em portos incomuns
- Port Knocking
- Honeypots / Honeynets
- OS Spoofing
- Tar Pits
- Reactive Port Scan Detection
- Escalating Arms Race

Concluindo, a proteção completa destas ferramentas é extremamente difícil de implementar e a melhor forma é mitigar a quantidade de informação que quem fez o scan consegue descobrir, como foi feito na nossa mitigação de scans de OS.

4.1 Ataque

Quando se é realizado o scan 'nmap -O' o nmap envia pacotes especiais TCP/IP e UDP para os hosts remotos e analisa todas as respostas recebidas. Depois de vários testes, como 'TCP ISN sampling', 'TCP option support and ordering', 'IP ID sampling' e 'window size check' o NMap compara os resultados com a sua base de dados 'nmap-os-db' que contém mais de 2600 fingerprints dos OS's.



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 14:15 EDT
Nmap scan report for 192.168.0.11
Host is up (0.007s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 21H2
Network Distance: 3 hops

Nmap scan report for 192.168.0.12
Host is up (0.0087s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5985/tcp   open  wsman
Device type: general purpose
Running: Microsoft Windows 2022
OS CPE: cpe:/o:microsoft:windows_server_2022
OS details: Microsoft Windows Server 2022
Network Distance: 3 hops

Nmap scan report for 192.168.0.14
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
Device type: general purpose/router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:ruteros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.19 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 3 hops

Nmap scan report for 192.168.0.254
Host is up (0.0097s latency).
All 1000 scanned ports on 192.168.0.254 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: AA:BB:CC:00:01:00 (unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: router|specialized|switch
Running: Cisco IOS 12.1
OS CPE: cpe:/h:cisco:c1821 cpe:/h:cisco:c3600 cpe:/h:cisco:c3700 cpe:/o:cisco:ios:12.4 cpe:/o:cisco:ios:12.1 cpe:/h:cisco:catalyst_3560 cpe:/h:cisco:catalyst_6500 cpe:/o:cisco:ios:12
OS details: Cisco 1812, 3640, or 3700 router (IOS 12.4), Cisco DOCSIS cable modem termination server (IOS 12.1), Cisco Catalyst 3560 or 6500-series switch (IOS 12.1 - 12.2)
Network Distance: 1 hop
```

Figura 4.1: Ataque sem Mitigação

Cada fingerprint contem informação sobre o OS e uma classificação que permite identificar o fornecedor(ex: Microsoft), o OS, a versão (ex: Windows 10) e o tipo da máquina (router, laptop, etc.). A maior parte das fingerprints também têm uma Common Platform Enumeration que permite descobrir o kernel que está a ser utilizado.

Se o NMap[4] não conseguir saber o OS e tiver as condições necessárias ele tenta adivinhar o OS.

4.2 Mitigação do Ataque

Primeiro começamos por delimitar o número de portos permitidos e bloqueamos todos os não 'essenciais', vamos usar uma ACL para permitir apenas os portos 22(ssh) e o porto 80(tcp). Isto por si só não protege a rede de um scan de OS, mas quando for realizado um scan apenas vai encontrar estes dois portos, mesmo tendo mais abertos.

Configuração de ACL:

- ip access-list extended PORTS
- permit tcp any any eq 22
- permit tcp any any eq 80
- deny ip any any

Aplicação da ACL:

- interface Serial2/0
- ip access-group PORTS in

Figura 4.2: Mitigação ACL

Através da ACL a cima, já afetamos o uso do NMap, negando-lhe o acesso a estes portos, ele fica com a informação reduzida, permitindo apenas que ele adivinhe o OS. Mesmo assim, ele consegue adquirir informação útil, como o tipo CTE e o tipo da máquina.

Para mitigarmos melhor vamos utilizar o TCP Intercept que é usado para a defesa de ataques DoS, mas também é eficiente contra o uso do NMap.

Começamos por criar uma lista definindo assim o que vai ser visto pelo TCP Intercept. Pode ser dado os IP's ou portos, neste caso, vamos dar os mesmos portos da ACL.

Configuração:

- ip access-list extended PROTECTED_PORTS
- permit tcp any any eq 22
- permit tcp any any eq 90
 - Ativação de TCP Intercept
- ip tcp intercept list PROTECTED_PORTS
 - Alteração do modo de TCP Intercept
- ip tcp intercept mode intercept
 - Alteração do tempo de demora até uma conexão TCP é gerida pelo TCP Intercept antes de dar drop ao pacote
- ip tcp intercept connection-timeout 5
 - Definimos o quanto tempo o IOS deve esperar pela conexão TCP
- ip tcp intercept watch-timeout 10
 - Definimos o numero mínimo de conexões TCP para o IOS sair do modo 'agressivo' e o numero máximo de conexões TCP incompletas permitidas antes do IOS entrar em modo 'agressivo'
- ip tcp intercept max-incomplete low 15 high 30

Agora efetuamos novamente o scan e analisamos o resultado.

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 14:43 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0083s latency).
Not shown: 998 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running (JUST GUESSING): Ness embedded (86%)
Aggressive OS guesses: Ness Mi-WiFi home automation interface (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for 192.168.0.2
Host is up (0.0083s latency).
Not shown: 998 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running (JUST GUESSING): Ness embedded (86%)
Aggressive OS guesses: Ness Mi-WiFi home automation interface (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for 192.168.0.14
Host is up (0.011s latency).
Not shown: 998 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge/wireless adapter/WiFi/firewall/broadband router
Running (JUST GUESSING): D-Link embedded (87%), Cisco embedded (86%), Compaq embedded (85%), Zyxel ZyWOS (85%), Scientific Atlanta embedded (85%), Siemens embedded (85%)
OS CPE: cpe:/o:zyxel:zyos cpe:/h:scientificatlanta:webstar_epc2203 cpe:/h:siemens:c2-810-1
Aggressive OS guesses: D-Link PortServer, Serial-to-Ethernet bridge (87%), Cisco VG248 Analog Phone Gateway (86%), Compaq IPaq CP-2W Connection Point WAP (85%), Zyxel ZYWALL 2 Plus Firewall (85%), Scientific Atlanta WebSTAR EPC2203 cable modem (85%), Siemens C2-810-1 ADSL modem (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for 192.168.0.19
Host is up (0.0093s latency).
Not shown: 998 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Compaq IPaq CP-2W Connection Point WAP (88%), Kaba-Bennigton time and attendance terminal (86%), Zyxel Prestige 202 ISDN router (ZyNOS 2.4-1) (86%), Zyxel Prestige 400-series ADSL router (86%), Zyxel XGS880 ethernet network simulator (86%), Lucent 54500 NTP server (86%), Siemens C2-810-1 ADSL modem (86%), GNU Hurd 0.3 (86%), Dell PowerConnect 3324 switch (86%), Dell PowerConnect 3348 switch (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for 192.168.0.234
Host is up (0.019s latency).
Not shown: 998 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    closed http
MAC Address: CC:CC:00:00:00:00 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: router|specialized|switch
Running: Cisco IOS 12.X
OS CPE: cpe:/a:cisco:c1812 cpe:/h:cisco:c3640 cpe:/h:cisco:c3700 cpe:/o:cisco:ios:12.4 cpe:/o:cisco:ios:12.1 cpe:/h:cisco:catalyst_3560 cpe:/h:cisco:catalyst_3560
+ cisco1800 or cisco1812
OS details: Cisco 1812, 3640, or 3700 router (IOS 12.4), Cisco DOCSIS cable modem termination server (IOS 12.1), Cisco Catalyst 3560 or 6500-series switch (IOS 12.1 - 12.2)
Network Distance: 1 hop

```

Figura 4.3: Mitigaçāo ACL e TCP intercept

Com este layer de proteção, o NMap[5] não conseguiu obter nenhuma informação útil que pudesse ajudar um atacante, apenas mostrando os resultados que não se encontram perto da realidade no nosso subsistema.

Porém o NMap ainda consegue obter os enderecos de IP das maquinas conectadas à rede, para impedir isso teríamos de implementar uma *deny-by-default* firewall que permitiria apenas casos únicos, por exemplo numa empresa que permita *remote working*, apenas permitir tráfego no porto 22 de IPs conhecidos, ou através de uma VPN.

5. Conclusão

Através destas experiências e com a realização deste Projeto Autoproposto usando o Nmap, foi possível obter uma visão clara das capacidades da aplicação, desde a identificação de host's ativos, serviços disponíveis, sistemas operativos a potenciais vulnerabilidades. A utilização de diferentes opções do Nmap, como os modos de *sweeping* (-sS, -sO, -A, -sn), a deteção de sistema operativo (-O), a enumeração de versões de serviços (-sV) e a execução de scripts NSE (*-script vuln*), demonstrou a versatilidade, profundidade e robustez da ferramenta.

Verificou-se que alguns dispositivos da rede apresentavam portas críticas abertas, como as associadas ao protocolo SMB (porta 445), que foram alvo de scripts de deteção de vulnerabilidades conhecidas. Embora não tenham sido encontradas vulnerabilidades exploráveis diretamente, a presença desses serviços evidencia a importância de uma gestão ativa de segurança e de uma política de atualização contínua.

O Nmap provou ser uma ferramenta essencial para o diagnóstico de segurança de redes, permitindo identificar rapidamente pontos fracos que poderiam ser explorados por atacantes. A realização regular deste tipo de análises, complementada por outras ferramentas e técnicas, é fundamental para garantir a integridade, disponibilidade e confidencialidade dos sistemas informáticos.

Bibliografia

- [1] NMap.org. (2025). *Página oficial do Nmap*. <https://nmap.org>
- [2] NMap.org. (2025). *Técnicas de defesa contra varredura*. <https://nmap.org/book/nmap-defenses-trickery.html>
- [3] NMap.org. (2025). *Tutorial de varredura de portas*. <https://nmap.org/book/port-scanning-tutorial.html>
- [4] NMap.org. (2025). *Detecção do sistema operativo*. <https://nmap.org/book/man-os-detection.html>
- [5] Cisco. (2025). *Configuração do TCP Intercept*. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_dos_atprvn/configuration/15-mt/sec-data-dos-atprvn-15-mt-book/sec-cfg-tcp-intercpt.html