FICHA TRABALHO 8

MODALIDADE:	Aprendizagem +	Não aplicável	
CURSO:	Técnico/a de Cibersegurança		
UC:	Instalar e configurar ferramentas de análise e recolha de logs e evidências	CÓDIGO UC:	UC01485
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

- Saber como utilizar ferramentas para reconhecimento de sistemas e serviços numa rede de dados
- Exploração da ferramenta Nmap

Na segurança informática, mais especificamente, ao nível da rede, existem muitas ferramentas para avaliar se um sistema está vulnerável ou não. O resultado produzido por este tipo de ferramentas pode ser utilizado por pessoas mal-intencionadas para fins menos apropriados, ou por proprietários e administradores de sistemas para melhorarem a segurança dos seus sistemas.

Uma das ferramentas que permite facilmente identificar sistemas e serviços é o NMAP. Tal como referido, o NMAP é uma ferramenta usada para reconhecimento de sistemas e serviços numa rede de dados. Esta ferramenta é uma das mais populares neste segmento e disponibiliza imensas funcionalidades.

O sistema operativo Kali Linux já vem com Nmap pré-instalado, mas, também podemos utilizar esta ferramenta em outros sistemas operativos. Para tal fica aqui disponível a página oficial do Nmap.

Link para download: https://nmap.org/download.html

A saída do Nmap é uma lista de alvos analisados, com informações adicionais de cada um dependendo das opções utilizadas. Uma informação chave é a “tabela de portas”. Essa tabela lista o número da porta e o protocolo utilizado, o nome do serviço e o estado atual.

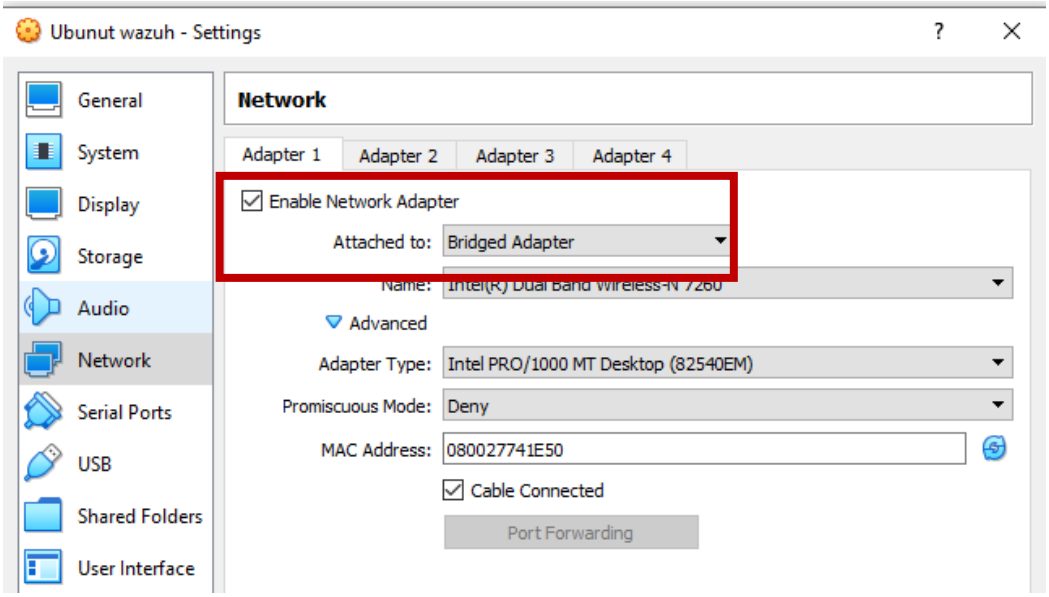
O estado pode ser aberto (***open***), filtrado (***filtered***), fechado (***closed***), ou não-filtrado (***unfilterd***).

- ***Aberto (open):*** significa que uma aplicação na máquina-alvo está a ouvir as conexões/pacotes naquela porta.
- ***Filtrado (filtered):*** significa que a firewall, filtro ou outro obstáculo de rede está a bloquear a porta de forma que o Nmap não consegue dizer se está aberta (open) ou fechada (closed).
- ***Portas fechadas (closed):*** não possuem uma aplicação a ouvir conexões, embora possam abrir a qualquer instante.

- ***Portas não filtradas (unfiltered):*** quando elas respondem às sondagens do Nmap, mas o Nmap não consegue determinar se as portas estão abertas ou fechadas. O Nmap reporta as combinações aberta|filtrada (open|filtered) e fechada|filtrada (closed|filtered), quando não consegue determinar qual dos dois estados descrevem melhor a porta.

A tabela de portas também pode incluir detalhes de versão de software quando a deteção de versão for solicitada. Quando um scan do protocolo IP é solicitado (-sO), o Nmap fornece informações dos protocolos IP suportados ao invés de portas que estão abertas. Além da tabela de portas, o Nmap pode fornecer informações adicionais sobre os alvos, incluindo nomes de DNS reverso, possível sistema operacional, tipos de dispositivos e endereços MAC.

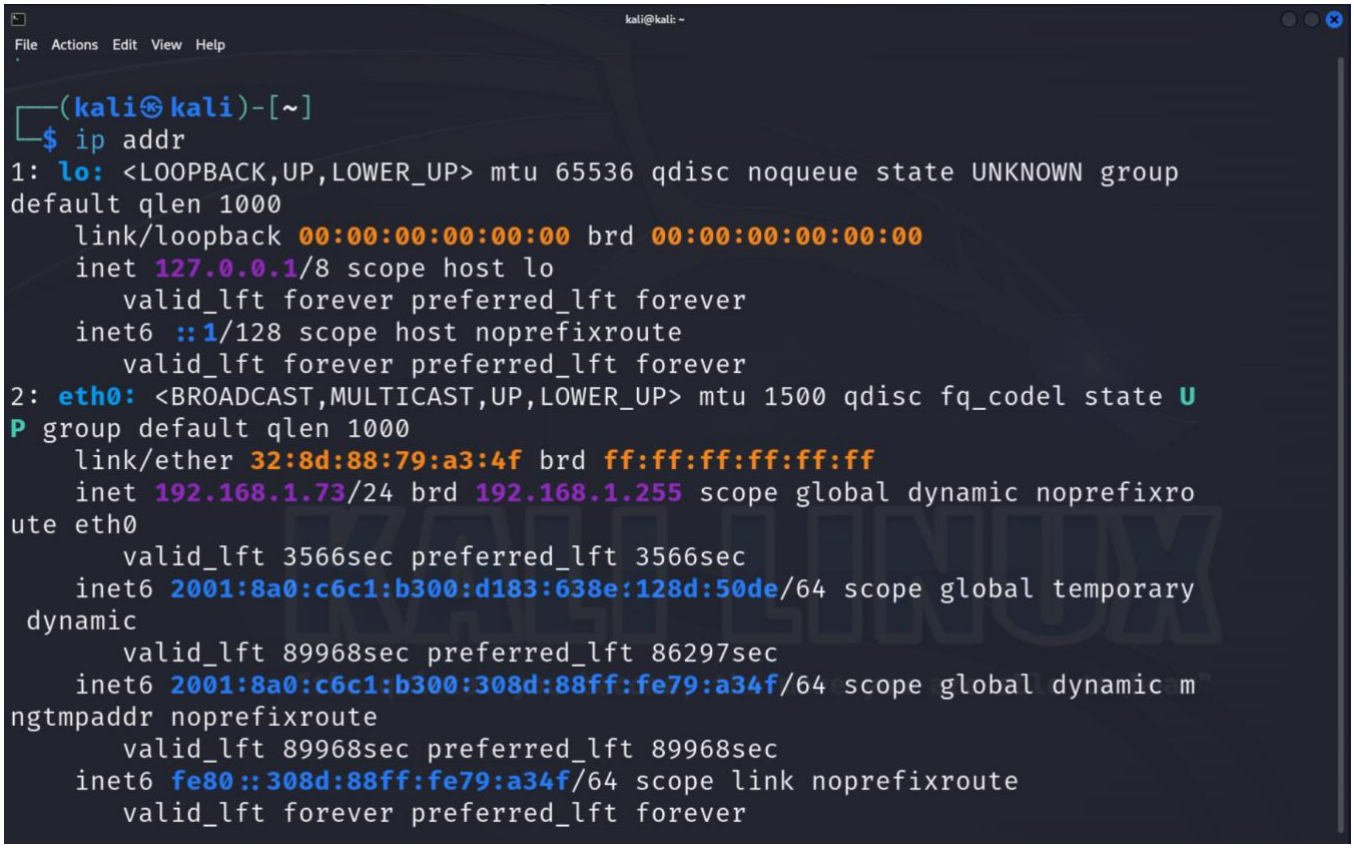
Passo 1 - Caso use o ***software virtual box***, nas configurações da placa de rede da máquina virtual deve colocar o adaptador de rede em ***bridge adapter***



Passo 2 – Vamos abrir no terminal a ferramenta do Nmap. Para tal, deve abrir um novo terminal no kali Linux e **entrarem modo de administrador**;

Passo 3 – Antes de mais nada, precisamos de obter informações sobre o endereço de rede da nossa máquina. Para tal, escreva o seguinte comando: ***ip addr.*** Este comando, irá mostrar todos as configurações das placas de rede do sistema operativo, mais especificamente, a permite que o utilizador configure e faça gestão dos endereços de IP integrados numa interface de rede. Com isso, podemos: associar, desvincular e verificar IPs ou desfazer configurações recentes.

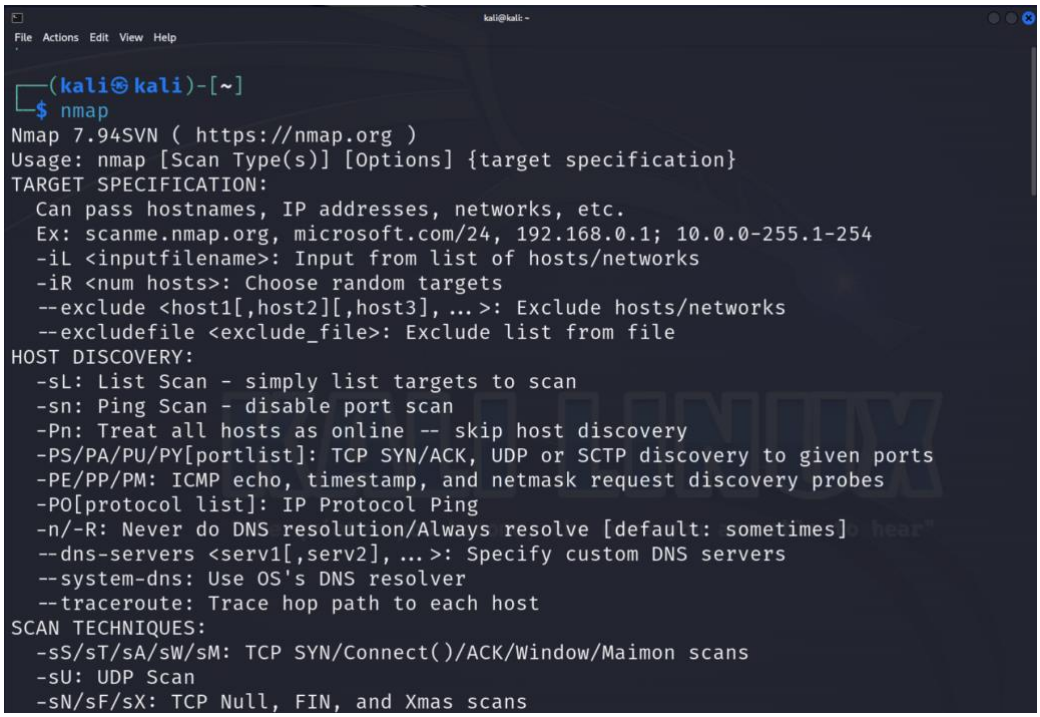
Neste contexto, queremos saber qual a gama de endereços IP onde está a rede, o domínio onde está a gama do IP e a máscara de rede:



Numa analise rápida, podemos verificar que a interface eth0 tem os seguintes dados:

- ***Endereço IP:*** 192.168.1.73
- ***Máscara de rede:*** 24 (255.255.255.0)
- ***Domínio:*** 192.168.1.0/24

Para saber como utilizar os comandos do Nmap e respetivas funcionalidades, escreva o comando ***nmap*** e este vai exibir qual a versão atual da ferramenta e uma listagem dos comandos que tem disponíveis e qual a utilidade:

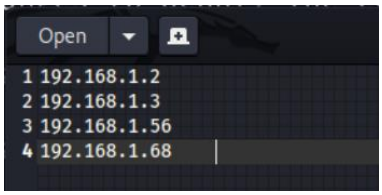


Passo 4 – Também podem indicar quais as máquinas individualmente em vez de toda a rede:

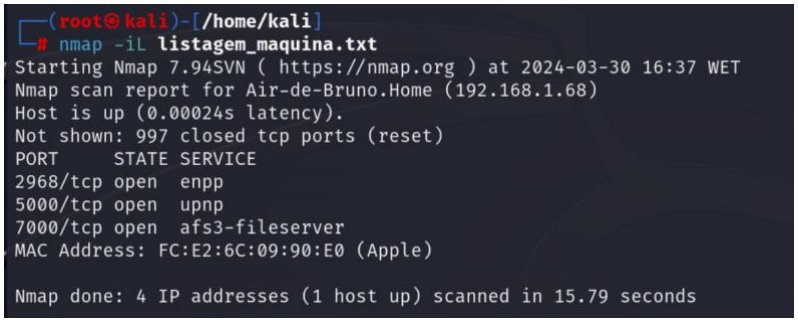
- ***Comando:*** nmap ***<endereço_IP_1> <endereço_IP_2> <endereço_IP_3> (...)***
- ***Exemplo:*** nmap ***192.168.1.2 192.168.1.3 192.168.1.4 (...)***

Ou então, podem construir uma listagem de endereços num ficheiro e pedir para que este siga essa informação:





Correr o nmap com base nos endereços colocados nos ficheiros. Para tal deve utilizar o comando: ***nmap -iL listagem_maquinas.txt***



Passo 4 – Descobrir endereços IP numa rede "ativos"

Caso pretenda saber quais os endereços IP "ativos" numa determinada rede de dados. Para tal basta que execute o comando ***nmap -sP <Rede>***. O resultado da execução deste comando permite, por exemplo, saber que outras máquinas que estão na rede:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 11:08 WET
Nmap scan report for Air-de-Bruno.Home (192.168.1.68)
Host is up (0.00076s latency).
Nmap scan report for kali.Home (192.168.1.73)
Host is up (0.00027s latency).
Nmap scan report for meo.Home (192.168.1.254)
Host is up (0.015s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.22 seconds
```

Passo 5 – Descobrir portos de comunicação abertos nos endereços IP "ativos"

Caso pretenda descobrir quais os portos lógicos abertos numa determinada máquina só tem de usar o comando ***nmap <dominio da rede> ou nmap <IP_Máquina>***. Como se pode ver pelo seguinte output, a máquina com o IP 192.168.10.130 tem o porto 22, associado ao protocolo SSH, aberto (à escuta):

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 11:05 WET
Nmap scan report for Air-de-Bruno.Home (192.168.1.68)
Host is up (0.00040s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
2968/tcp  open  enpp
5000/tcp  open  upnp
7000/tcp  open  afs3-fileserver
49152/tcp open  unknown

Nmap scan report for kali.Home (192.168.1.73)
Host is up (0.000042s latency).
All 1000 scanned ports on kali.Home (192.168.1.73) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for meo.Home (192.168.1.254)
Host is up (0.011s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
5431/tcp open  park-agent
8080/tcp open  http-proxy
8089/tcp open  unknown
9876/tcp open  sd
9877/tcp open  x510

Nmap done: 256 IP addresses (3 hosts up) scanned in 11.32 seconds
```

Passo 6 – Saber quais os portos TCP abertos de uma máquina

Caso pretenda saber se um determinado porto lógico está aberto numa determinada máquina. Com o nmap o processo é bastante simples sendo apenas necessário indicar o porto lógico e a máquina: ***nmap -p <porto> <máquina>***:

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 192.168.1.254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 11:42 WET
Nmap scan report for meo.Home (192.168.1.254)
Host is up (0.0094s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

Passo 7 – Saber o sistema operativo de uma determinada máquina

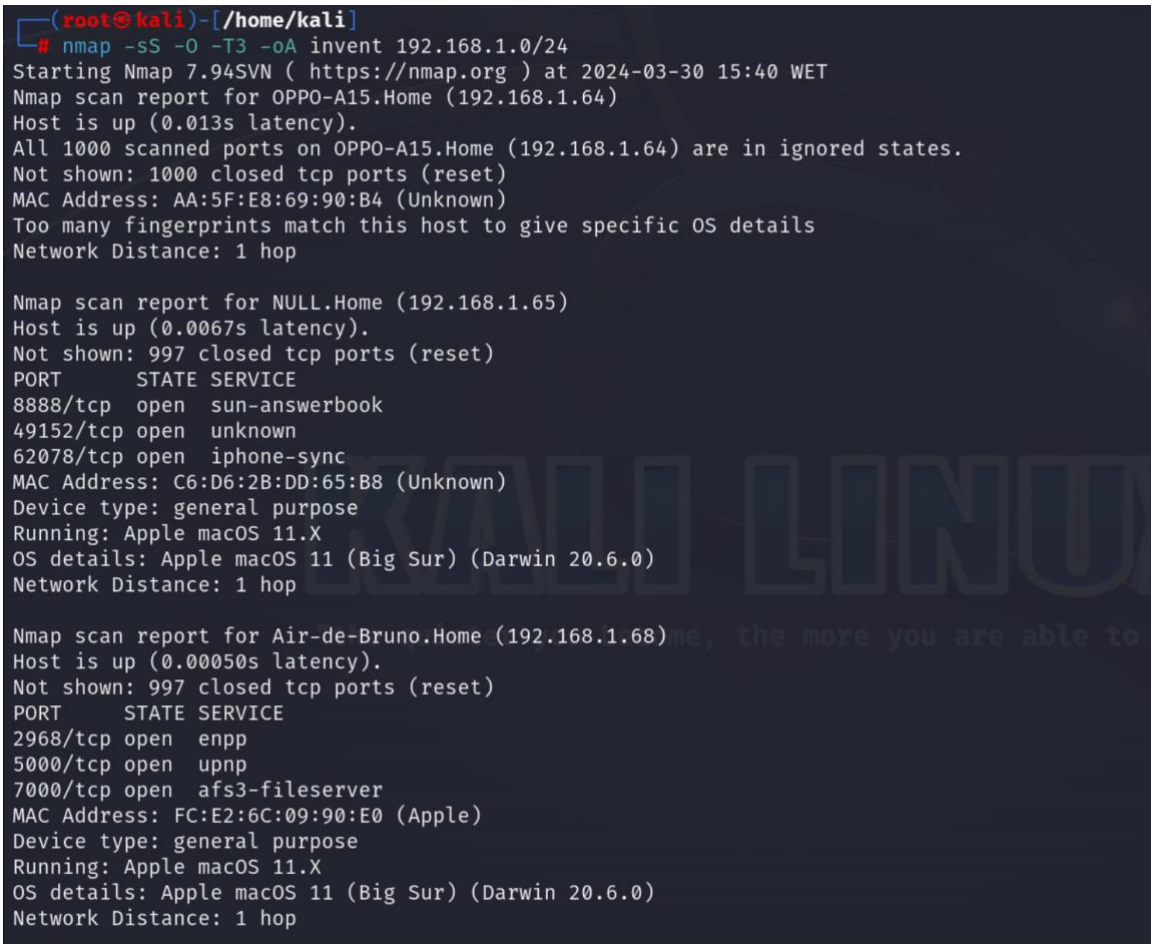
Caso pretenda saber remotamente qual o sistema operativo usado numa determinada máquina? O NMAP consegue, geralmente saber qual o sistema instalado (incluindo a versão). Para obter essa informação pode usar o comando: ***nmap -O <IP_Máquina>***

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 11:58 WET
Nmap scan report for Air-de-Bruno.Home (192.168.1.68)
Host is up (0.00060s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
2968/tcp open  enpp
5000/tcp open  upnp
7000/tcp open  afs3-fileserver
MAC Address: FC:E2:6C:09:90:E0 (Apple)
Device type: phone|general purpose|media device
Running: Apple iOS 11.X|12.X|13.X, Apple macOS 10.13.X|10.14.X|10.15.X|11.X, Apple OS X 10.11.X
OS CPE: cpe:/o:apple:iphone_os:11 cpe:/o:apple:iphone_os:12 cpe:/o:apple:iphone_os:13 cpe:/o:apple:mac_os_x:10.13 cpe:
/o:apple:mac_os_x:10.14 cpe:/o:apple:mac_os_x:10.15 cpe:/o:apple:mac_os_x:10.11
OS details: Apple macOS 10.13 (High Sierra) - 10.15 (Catalina) or iOS 11.0 - 13.4 (Darwin 17.0.0 - 19.6.0), Apple Mac
OS X 10.11 (El Capitan) or iOS 12.4 - 13.6 (Darwin 15.6.0 - 19.6.0), Apple macOS 11 (Big Sur) (Darwin 20.6.0), Apple m
acOS 10.15 (Catalina) (Darwin 19.6.0)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.47 seconds
```

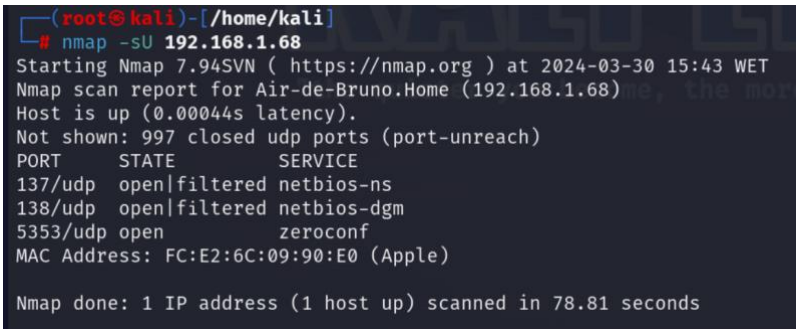
Passo 8 – Inventário de todas as máquinas de uma determinada rede

Para obter um inventário de todas as máquinas de uma determinada rede devemos utilizar o comando ***nmap -sS -O -T3 -oA invent <dominio>*** podemos saber para cada PC da rede indicada quais os portos abertos, MacAddress das máquinas, qual o sistema operativo, latência, etc.



Passo 9 – Inventário de todas as máquinas de uma determinada rede

Numa máquina existem ***65536 portos lógicos TCP*** e ***65536 portos lógicos UDP***. Para fazer um scan aos portos UDP, devem usar os argumentos -sU. Exemplo: ***nmap -sU <IP da máquina>***



Passo 10 – Saber scan a todos os portos lógicos

Se necessitar de fazer um scan a todos os portos lógicos, podem usar o argumento -p. Exemplo: ***nmap -p <n_porto> <IP da máquina>***

- ***Exemplo para percorrer vários portos ao mesmo tempo: nmap -p 80,443 <IP da máquina>***
- ***Exemplo para um intervalo de valores use o comando: nmap -p 1000-3000 <IP da máquina>***

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 138 192.168.1.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 15:47 WET
Nmap scan report for Air-de-Bruno.Home (192.168.1.68)
Host is up (0.00029s latency).

PORT    STATE  SERVICE
138/tcp closed netbios-dgm
MAC Address: FC:E2:6C:09:90:E0 (Apple)

Nmap done: 1 IP address (1 host up) scanned in 6.65 seconds
```

Passo 11 – Saber a versão de um determinado serviço

Para saber a versão de um determinado serviço que esteja a correr numa máquina remota devem usar a opção -sV. Para tal utilize o comando: ***nmap -sV -O*** <endreço_IP> ***-p*** <porto>.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O 192.168.1.68 -p 138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 15:49 WET
Nmap scan report for Air-de-Bruno.Home (192.168.1.68)
Host is up (0.00042s latency).

PORT    STATE  SERVICE     VERSION
138/tcp closed netbios-dgm
MAC Address: FC:E2:6C:09:90:E0 (Apple)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

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 8.34 seconds
```

Passo 12 – Aumentar a verbosity do resultado

Para quem pretender ter mais informação nos resultados basta aumentar a verbosity. Isso pode ser feito usando a opção -vv. Para tal utilize o comando: ***nmap -sV*** <endreço_IP> ***-p*** <porto> ***-vv***

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.68 -p 138 -vv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 16:18 WET
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 16:18
Scanning 192.168.1.68 [1 port]
Completed ARP Ping Scan at 16:18, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:18
Completed Parallel DNS resolution of 1 host. at 16:18, 6.53s elapsed
Initiating SYN Stealth Scan at 16:18
Scanning Air-de-Bruno.Home (192.168.1.68) [1 port]
Completed SYN Stealth Scan at 16:18, 0.02s elapsed (1 total ports)
Initiating Service scan at 16:18
NSE: Script scanning 192.168.1.68.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:18
Completed NSE at 16:18, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:18
Completed NSE at 16:18, 0.00s elapsed
Nmap scan report for Air-de-Bruno.Home (192.168.1.68)
Host is up, received arp-response (0.00032s latency).
Scanned at 2024-03-30 16:18:18 WET for 0s

PORT    STATE  SERVICE     REASON       VERSION
138/tcp closed netbios-dgm reset ttl 64
MAC Address: FC:E2:6C:09:90:E0 (Apple)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (68B)
```

Passo 13 – Fazer scan em "Modo Agreesivo"

O nmap tem uma opção para realizar um scan de forma agressiva. Para tal, basta usar a opção --ossscan-guess. Também podem usar o argumento ***-A***. Esta opção permite uma deteção melhorada de serviços, sistema operativo, etc. Para tal utilize o comando: ***nmap -A*** <endreço_IP> ***-p*** <porto> ***-vv***

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.1.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 16:20 WET
Nmap scan report for Air-de-Bruno.Home (192.168.1.68)
Host is up (0.00095s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
2968/tcp open  enpp?
5000/tcp open  rtsp    AirTunes rtspd 745.13.4
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
7000/tcp open  rtsp    AirTunes rtspd 745.13.4
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
|_irc-info: Unable to open connection
MAC Address: FC:E2:6C:09:90:E0 (Apple)
Device type: general purpose
Running: Apple macOS 11.X
OS details: Apple macOS 11 (Big Sur) (Darwin 20.6.0)
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.95 ms Air-de-Bruno.Home (192.168.1.68)

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 181.32 seconds
```

Passo 14 – Fazer scan para saber informações da Firewall

A deteção das configurações da firewall pode ser útil durante testes de penetração e verificações de vulnerabilidades. Várias funções podem ser usadas para detetar configurações de firewall em determinados hosts, mas o sinalizador -sA é o mais comum. Para tal utilize o comando: ***nmap -sA*** <endereço_IP>