- Parto con una scansione os fingerprint per rilevare il sistema operativo della macchina

sudo nmap -Pn -O 192.168.50.1 (nmap 192.168.50.1 --script smb-os-discovery)

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 04:56 EDT
Nmap scan report for 192.168.50.1
Host is up (0.00056s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
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: general purpose
Running: FreeBSD 11.X
OS CPE: cpe:/o:freebsd:freebsd:11.2
OS details: FreeBSD 11.2-RELEASE

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.22 seconds
```

- vado a fare una scansione SYN

sudo nmap -sS 192.168.50.1

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:01 EDT
Nmap scan report for 192.168.50.1
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.72 seconds
```

- vado a fare una scansione TCP

sudo nmap -sT 192.168.50.1

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:03 EDT
Nmap scan report for 192.168.50.1
Host is up (0.00063s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds
```

- vado a fare una scansione aggressiva

sudo nmap -A 192.168.50.1

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:01 EDT
Nmap scan report for 192.168.50.1
Host is up (0.00039s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound
80/tcp open  http    nginx
|_http-title: pfSense - Login
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: FreeBSD 11.X
OS CPE: cpe:/o:freebsd:freebsd:11.2
OS details: FreeBSD 11.2-RELEASE
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.33 ms 192.168.50.1

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 21.05 seconds
```

- controllo la versione dei servizi per ogni porta aperta

sudo nmap -sV 192.168.50.1

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:07 EDT
Nmap scan report for 192.168.50.1
Host is up (0.00051s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound
80/tcp open  http    nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.15 seconds
```