IP TARGET : 192.168.49.102 (METASPLOITABLE)
OS FINGERPRINT:

```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.49.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:07 EST
Nmap scan report for 192.168.49.102
Host is up (0.0026s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.53 seconds
```

SYN scan:

```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.49.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:08 EST
Nmap scan report for 192.168.49.102
Host is up (0.0027s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
```

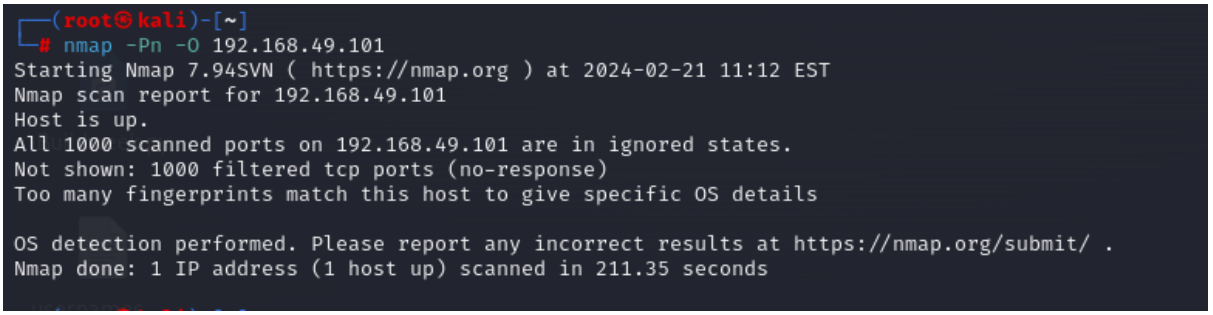
TCP scan:

```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.49.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:09 EST
Nmap scan report for 192.168.49.102
Host is up (0.0034s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds
```

La differenza che si nota tra SYN e TCP , il lasso di tempo aumenta in TCP e il latency del host aumenta.
VERSION scan:

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.49.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 11:10 EST
Nmap scan report for 192.168.49.102
Host is up (0.0029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   Unbound
80/tcp  open  http     nginx
443/tcp open  ssl/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 18.17 seconds
```

IP TARGET: 192.168.50.101 (WINDOWS 7):



Il motivo che windows si comporta in questo modo è perchè ha un firewall, per continuare la scansione basta usare “T0” o “T1” per aggirare il firewall, trovare un punto debole così da permetterci di passara da quel punto debole per riuscire a fare un scan TCP.