OS fingerprint di Meta

```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -O 192.168.49.101
[sudo] password for alessio:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 06:30 CST
Nmap scan report for 192.168.49.101 (192.168.49.101)
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp open     ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
8180/tcp open     unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.29 (Gentoo)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.28 seconds
```

Scan di solo SYN

```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -sS 192.168.49.101
[sudo] password for alessio:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 07:10 CST
Nmap scan report for 192.168.49.101 (192.168.49.101)
Host is up (0.014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp open     ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
8180/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

Scan con TCP connect

```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -sT 192.168.49.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 07:10 CST
Nmap scan report for 192.168.49.101 (192.168.49.101)
Host is up (0.0045s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp open     ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
8180/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

Version Detection:

```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -sV -T5 192.168.49.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 07:31 CST
Nmap scan report for 192.168.49.101 (192.168.49.101)
Host is up (0.0045s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         vsftpd 2.3.4
22/tcp   open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet      Linux telnetd
25/tcp   open     smtp        Postfix smtpd
53/tcp   open     domain      ISC BIND 9.4.2
80/tcp   filtered http
111/tcp  open     rpcbind     2 (RPC #100000)
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec?
513/tcp  open     login       OpenBSD or Solaris rlogind
514/tcp  open     tcpwrapped
1099/tcp open     java-rmi    GNU Classpath grmiregistry
1524/tcp open     bindshell   Metasploitable root shell
2049/tcp open     nfs         2-4 (RPC #100003)
2121/tcp open     ftp         ProFTPD 1.3.1
3306/tcp open     mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc         VNC (protocol 3.3)
6000/tcp open     X11         (access denied)
6667/tcp open     irc         UnrealIRCd
8009/tcp open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; 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 66.01 seconds
```

OS fingertip detection su Win 7, alcuni risultati sono filtrati dal firewall di windows

```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 07:26 CST
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.00056s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 08:00:27:A1:50:9E (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|8|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::- cpe:
/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 S
P1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
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 7.62 seconds
```

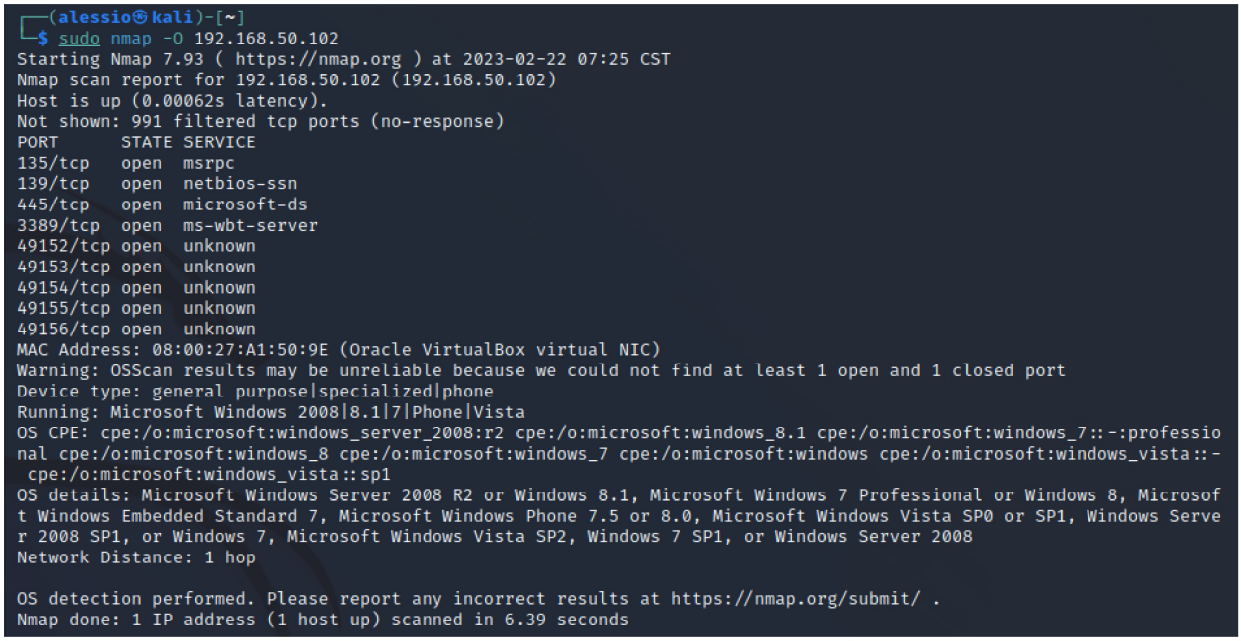
Provo a ingannare il firewall facendo arrivare le richieste dalla porta 80, ma ancora niente

```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102 --source-port 80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 07:40 CST
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.00050s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 08:00:27:A1:50:9E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds

┌──(alessio㉿kali)-[~]
```

Provo un altra strategia

```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102 --source-port 80 --badsum
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 07:43 CST
Nmap scan report for 192.168.50.102 (192.168.50.102)
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.50.102 (192.168.50.102) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:A1:50:9E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 25.39 seconds
```

Inserisco allora una regola su windows firewall per permettere tutti i protocolli:



Essendo il firewall di un client è difficile da ingannare