L’obiettivo di oggi è utilizzare nmap per scansionare diversi sistemi operativi.

Nmap è un software creato per effettuare port scanning, cioè, mirato all'individuazione di porte aperte su un computer bersaglio o anche su range di indirizzi IP, in modo da determinare quali servizi di rete siano disponibili.

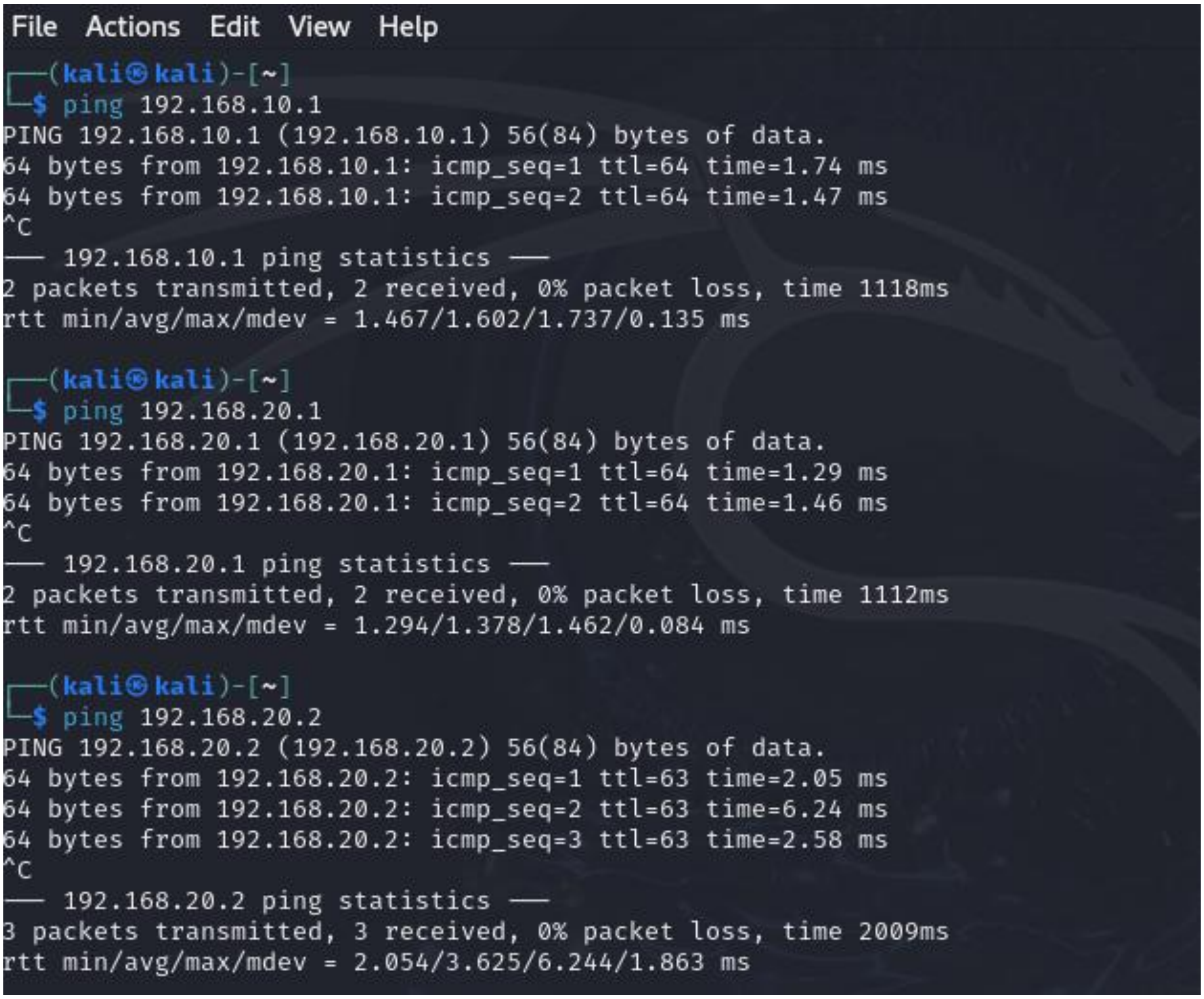
Inizio predisponendo pfsense, kali, metasploitable, win10. Faccio dei test di ping per verificare che la configurazione su rete locale sia corretta. In particolare avrò:

192.168.10.2 kali linux

192.198.20.2 meta

192.168.30.2 win10

192.168.xx.1 pfsense che fungerà da router e gateway.



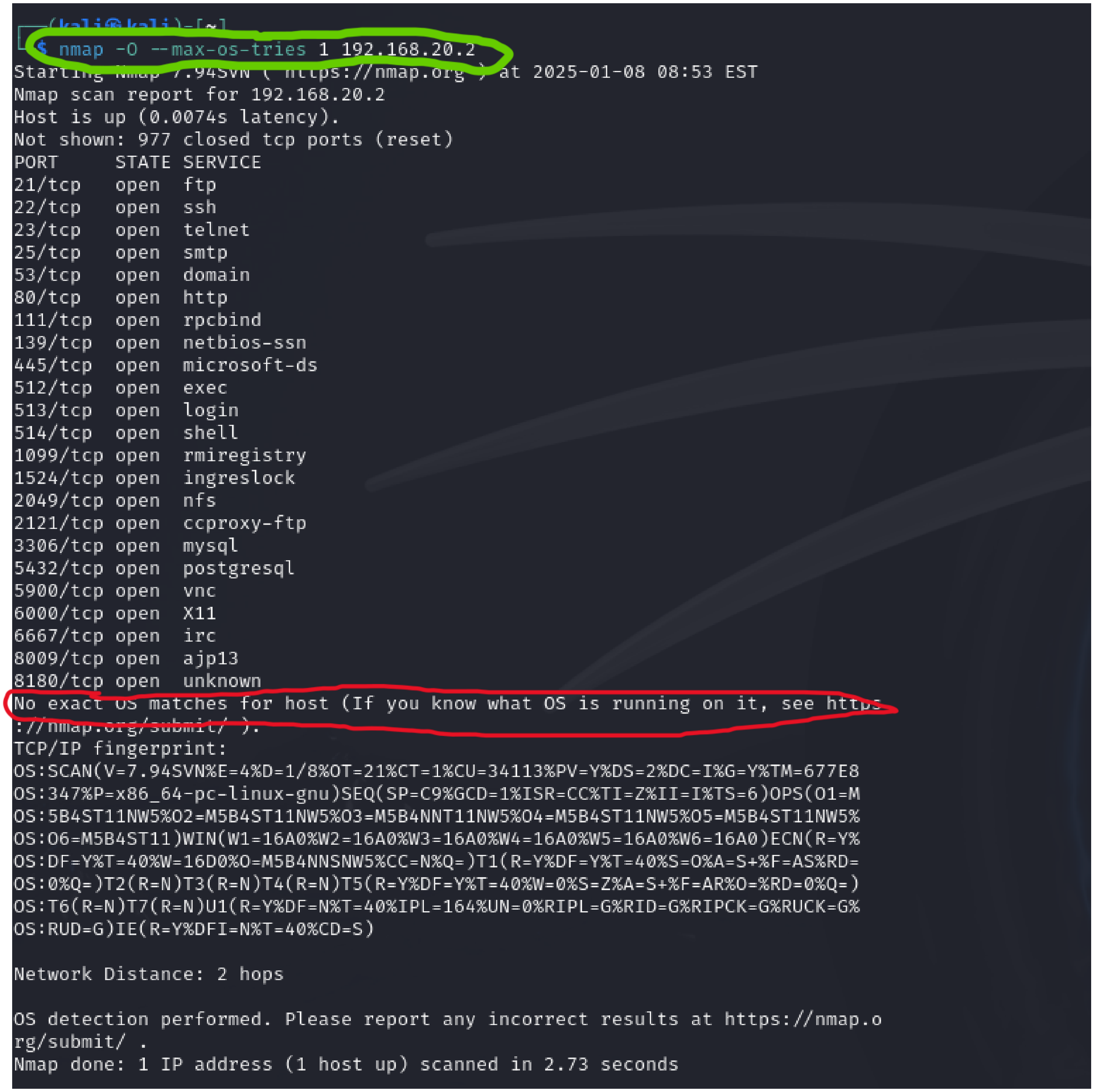
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=1.74 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=1.47 ms
^C
—— 192.168.10.1 ping statistics ——
2 packets transmitted, 2 received, 0% packet loss, time 1118ms
rtt min/avg/max/mdev = 1.467/1.602/1.737/0.135 ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=1.29 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=1.46 ms
^C
—— 192.168.20.1 ping statistics ——
2 packets transmitted, 2 received, 0% packet loss, time 1112ms
rtt min/avg/max/mdev = 1.294/1.378/1.462/0.084 ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.2
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.
64 bytes from 192.168.20.2: icmp_seq=1 ttl=63 time=2.05 ms
64 bytes from 192.168.20.2: icmp_seq=2 ttl=63 time=6.24 ms
64 bytes from 192.168.20.2: icmp_seq=3 ttl=63 time=2.58 ms
^C
—— 192.168.20.2 ping statistics ——
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 2.054/3.625/6.244/1.863 ms
```

Le macchine, ad eccezione di win10, si pingano e funzionano correttamente.

Scansione metasploitable

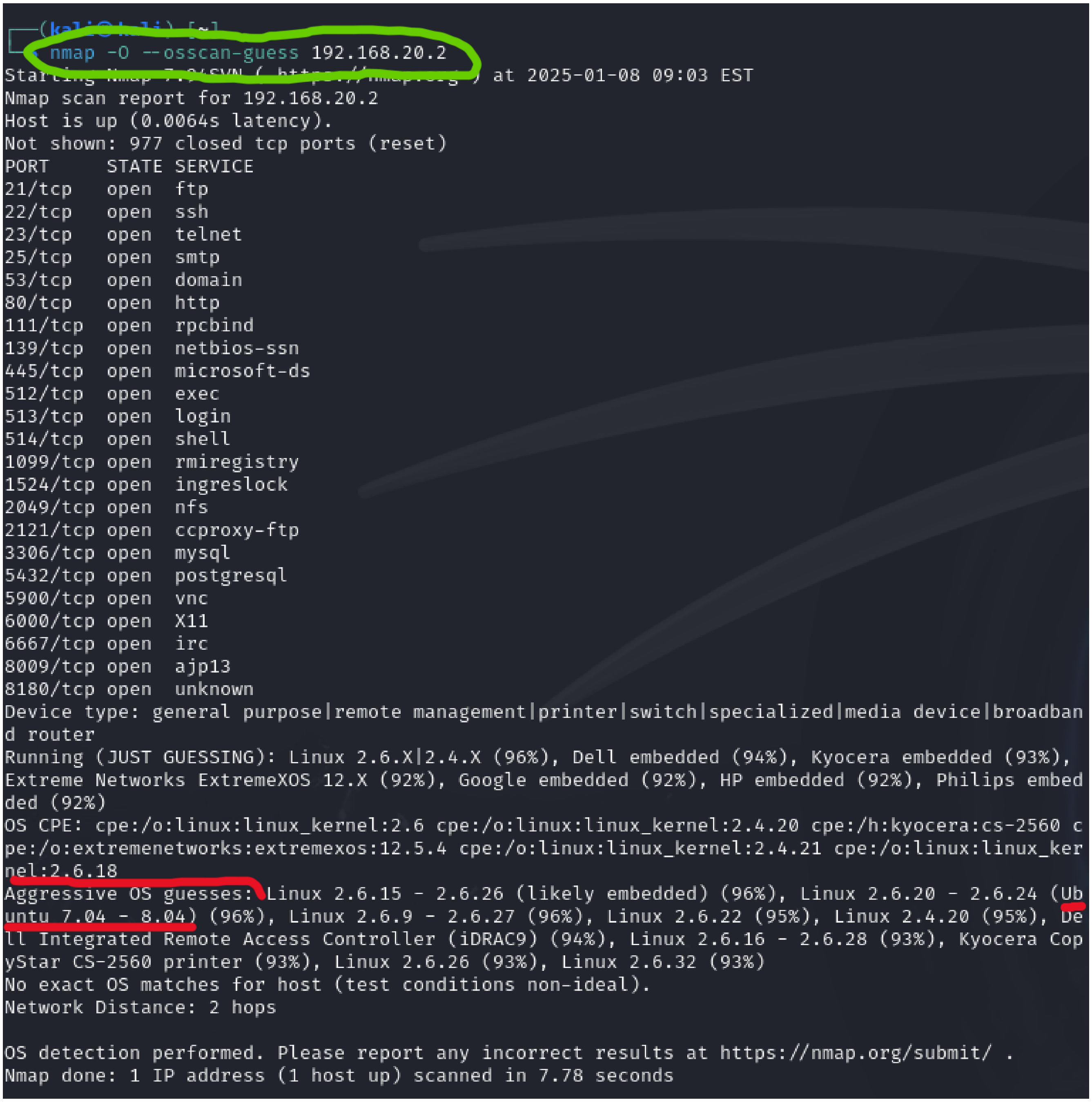
Inizio con una scansione usando nmap con lo switch -O --max-os-tries 1

Questo switch fa un guess dei sistemi operativi e li mostra solo se hanno il 100% di probabilità di essere corretti



```
┌──(kali㉿kali)-[~]
└─$ nmap -O --max-os-tries 1 192.168.20.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 08:53 EST
Nmap scan report for 192.168.20.2
Host is up (0.0074s 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   open  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
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/8%OT=21%CT=1%CU=34113%PV=Y%DS=2%DC=I%G=Y%TM=677E8
OS:347%P=x86_64-pc-linux-gnu)SEQ(SP=C9%GCD=1%ISR=CC%TI=Z%II=I%TS=6)OPS(O1=M
OS:5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O5=M5B4ST11NW5%
OS:O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%
OS:DF=Y%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.73 seconds
```

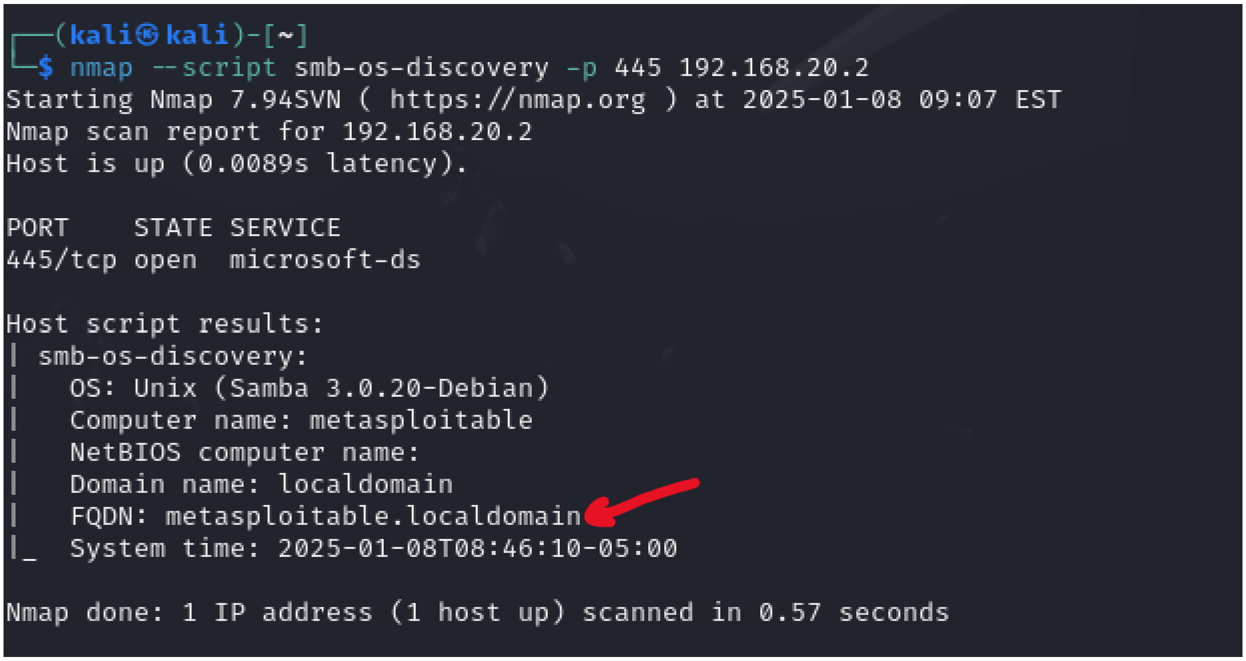
Non è possibile individuare con certezza il sistema operativo, riprovo con -O --osscan-guess



```
┌──(kali㉿kali)-[~]
└─$ nmap -O --osscan-guess 192.168.20.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:03 EST
Nmap scan report for 192.168.20.2
Host is up (0.0064s 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   open  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|remote management|printer|switch|specialized|media device|broadban
d router
Running (JUST GUESSING): Linux 2.6.X|2.4.X (96%), Dell embedded (94%), Kyocera embedded (93%),
Extreme Networks ExtremeXOS 12.X (92%), Google embedded (92%), HP embedded (92%), Philips embed
ded (92%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.4.20 cpe:/h:kyocera:cs-2560 c
pe:/o:extremenetworks:extremexos:12.5.4 cpe:/o:linux:linux_kernel:2.4.21 cpe:/o:linux:linux_ker
nel:2.6.18
Aggressive OS guesses: Linux 2.6.15 - 2.6.26 (likely embedded) (96%), Linux 2.6.20 - 2.6.24 (Ub
untu 7.04 - 8.04) (96%), Linux 2.6.9 - 2.6.27 (96%), Linux 2.6.22 (95%), Linux 2.4.20 (95%), De
ll Integrated Remote Access Controller (iDRAC9) (94%), Linux 2.6.16 - 2.6.28 (93%), Kyocera Cop
yStar CS-2560 printer (93%), Linux 2.6.26 (93%), Linux 2.6.32 (93%)
No exact OS matches for host (test conditions non-ideal).
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 7.78 seconds
```

L’aggressive os guess è quello corretto. Infatti, metasploitable è basato su ubuntu 8.04

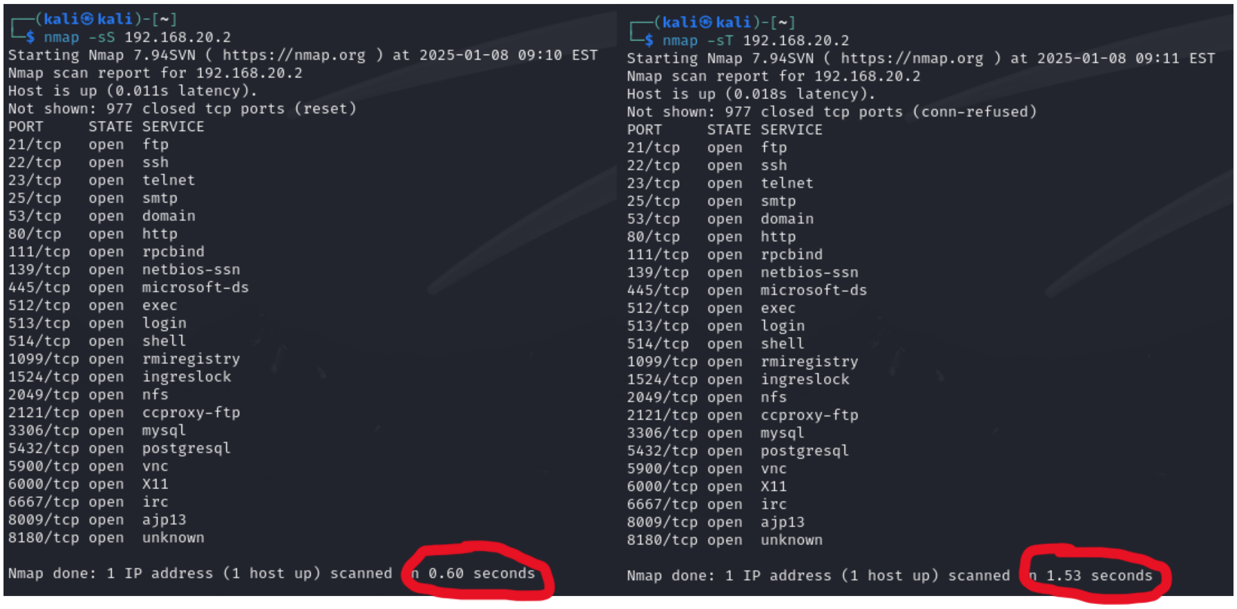
Faccio un tentative con lo script --script smb-os-discovery -p 445



```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-os-discovery -p 445 192.168.20.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:07 EST
Nmap scan report for 192.168.20.2
Host is up (0.0089s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-01-08T08:46:10-05:00

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

Qui vedo che FQDN (nome di dominio non ambiguo) è metasploitable.localdomain

Ora uso sysscan con -sS e -sT



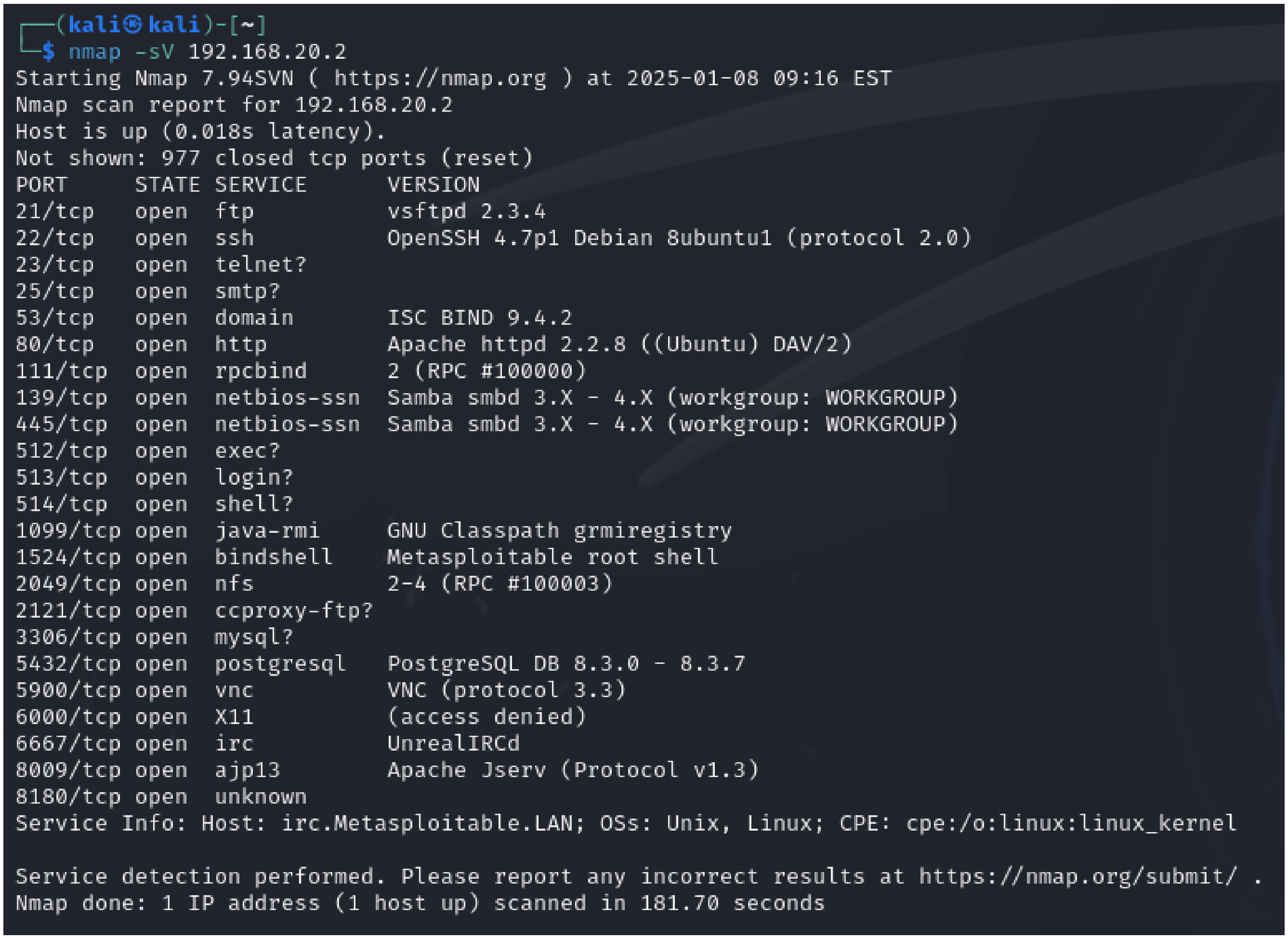
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.20.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:10 EST
Nmap scan report for 192.168.20.2
Host is up (0.011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  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 0.60 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.20.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:11 EST
Nmap scan report for 192.168.20.2
Host is up (0.018s 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   open  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 1.53 seconds
```

SYN Scan (-sS): Più veloce, meno rilevabile nei log del sistema target. Necessita di privilegi di root in teoria, ma funziona ugualmente. Più veloce

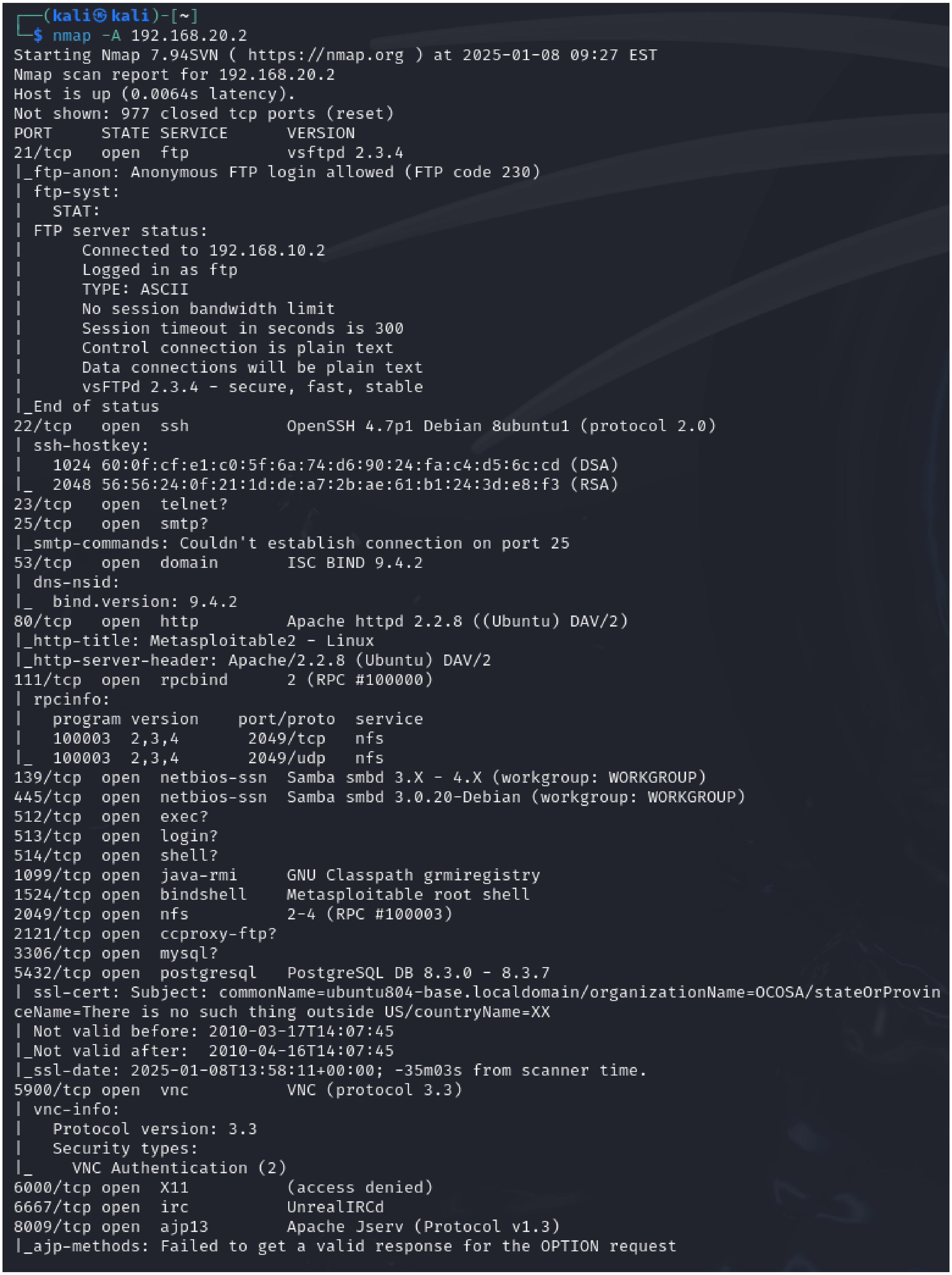
TCP Connect (-sT): Rilevabile nei log (poiché completa la connessione), ma non richiede privilegi elevati. Più lento.

nmap -sV invece cverifica I servizi e le versioni associate alle porte aperte. Richiede circa 3 minuti.

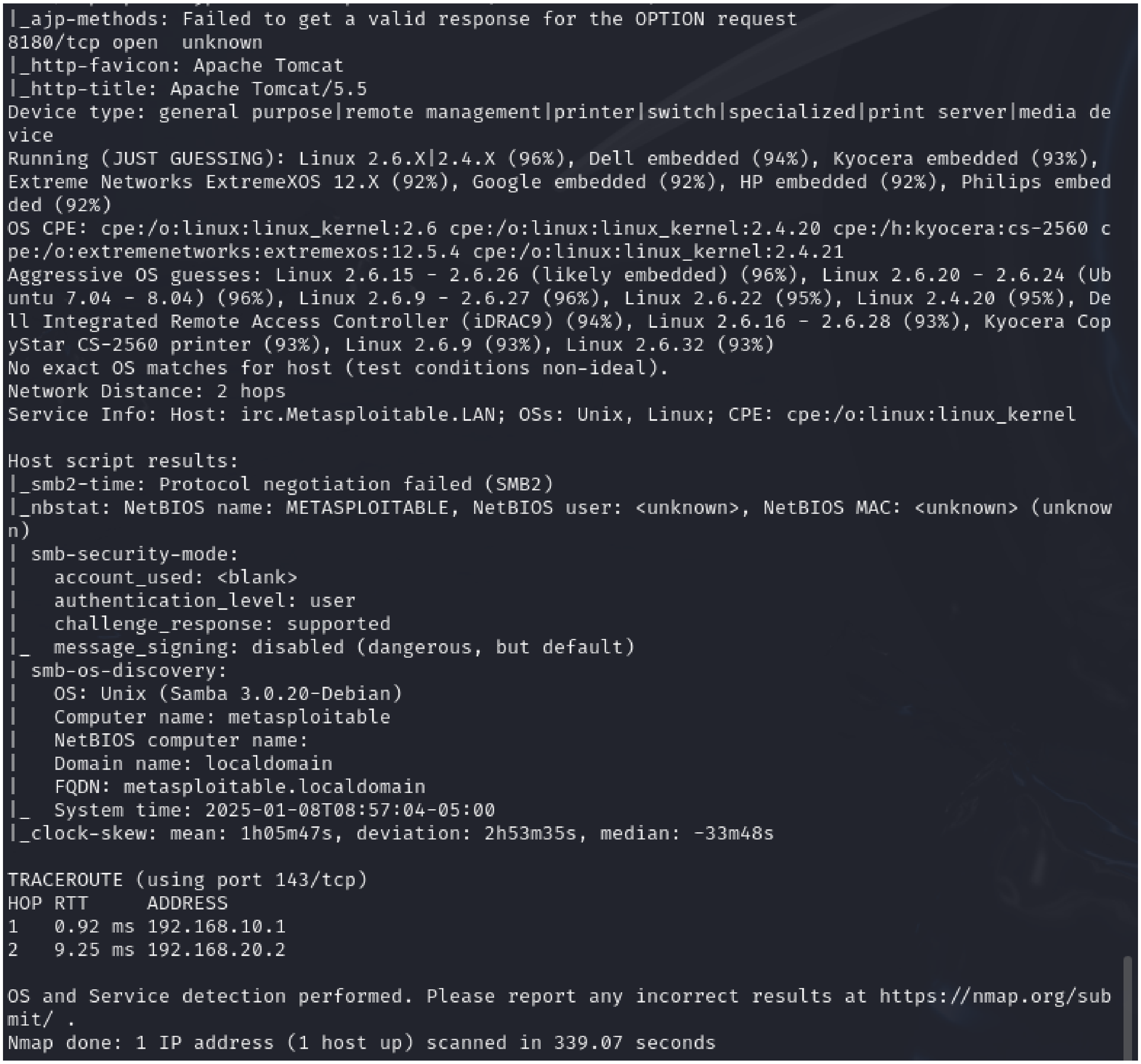


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.20.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:16 EST
Nmap scan report for 192.168.20.2
Host is up (0.018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
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?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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  unknown
Service Info: Host: 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 181.70 seconds
```

Nmap -A scansione aggressiva senza filtraggio dei risultati, per filtrarsi basta usare **| grep "OS details"**

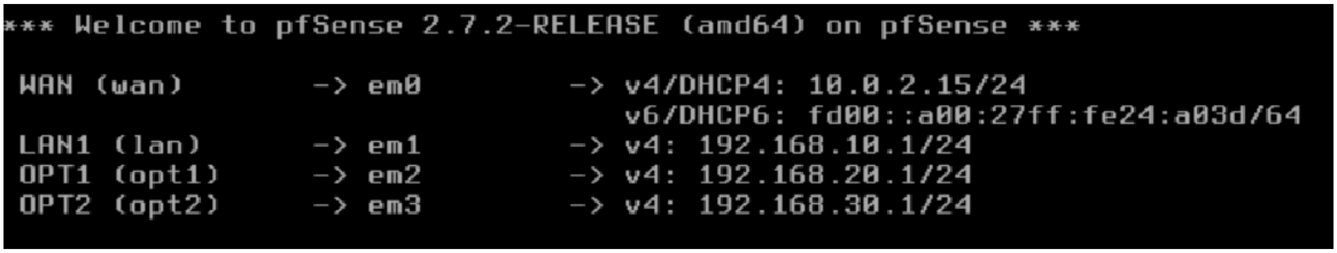


```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.20.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:27 EST
Nmap scan report for 192.168.20.2
Host is up (0.0064s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.10.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet?
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100003  2,3,4       2049/tcp   nfs
|_  100003  2,3,4       2049/udp   nfs
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvin
ceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-01-08T13:58:11+00:00; -35m03s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
```



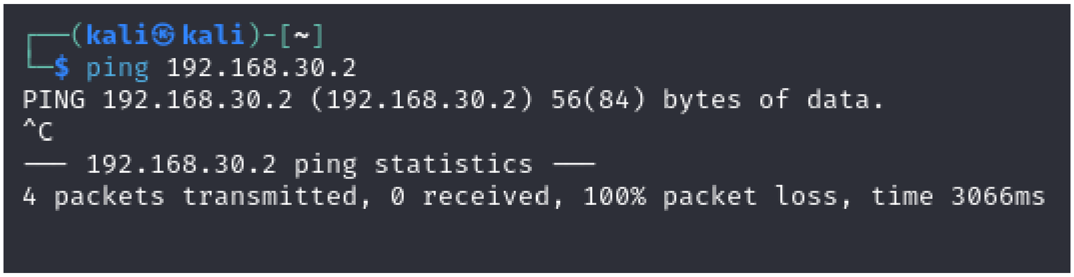
```
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
Device type: general purpose|remote management|printer|switch|specialized|print server|media de
vice
Running (JUST GUESSING): Linux 2.6.X|2.4.X (96%), Dell embedded (94%), Kyocera embedded (93%),
Extreme Networks ExtremeXOS 12.X (92%), Google embedded (92%), HP embedded (92%), Philips embed
ded (92%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.4.20 cpe:/h:kyocera:cs-2560 c
pe:/o:extremenetworks:extremexos:12.5.4 cpe:/o:linux:linux_kernel:2.4.21
Aggressive OS guesses: Linux 2.6.15 - 2.6.26 (likely embedded) (96%), Linux 2.6.20 - 2.6.24 (Ub
untu 7.04 - 8.04) (96%), Linux 2.6.9 - 2.6.27 (96%), Linux 2.6.22 (95%), Linux 2.4.20 (95%), De
ll Integrated Remote Access Controller (iDRAC9) (94%), Linux 2.6.16 - 2.6.28 (93%), Kyocera Cop
yStar CS-2560 printer (93%), Linux 2.6.9 (93%), Linux 2.6.32 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknow
n)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-01-08T08:57:04-05:00
|_clock-skew: mean: 1h05m47s, deviation: 2h53m35s, median: -33m48s

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
1   0.92 ms 192.168.10.1
2   9.25 ms 192.168.20.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 339.07 seconds
```

Configuro la rete per win10



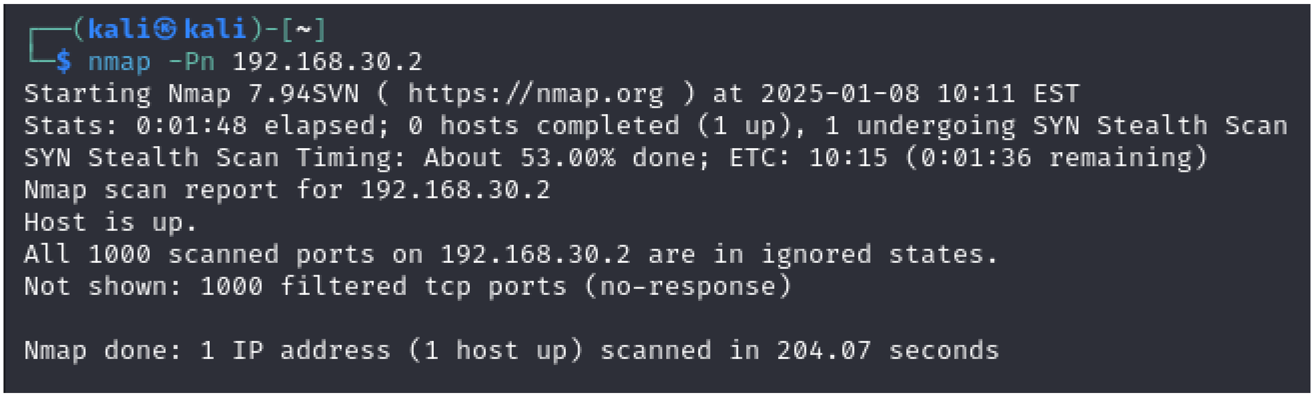
```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.15/24
                                  v6/DHCP6: fd00::a00:27ff:fe24:a03d/64
 LAN1 (lan)      -> em1        -> v4: 192.168.10.1/24
 OPT1 (opt1)     -> em2        -> v4: 192.168.20.1/24
 OPT2 (opt2)     -> em3        -> v4: 192.168.30.1/24
```

Win10 non è pingabile con icmp



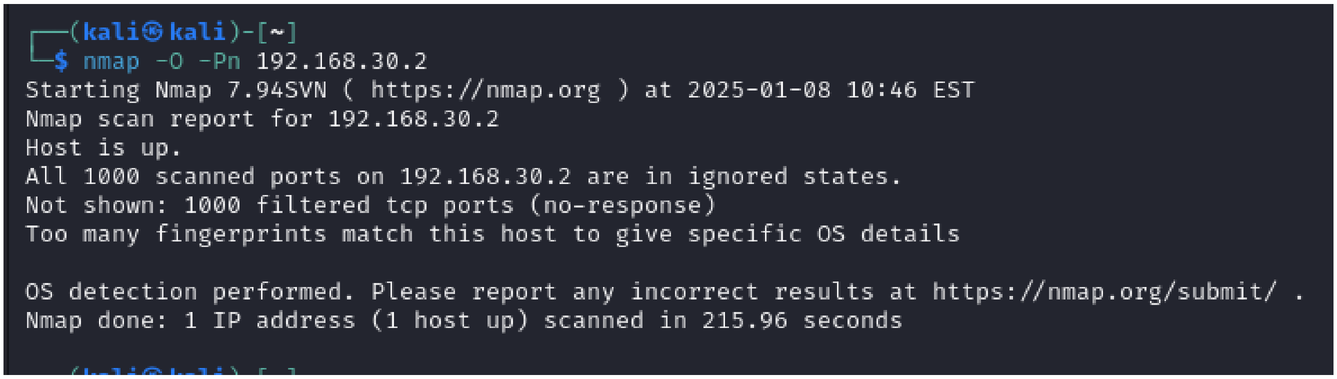
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.30.2
PING 192.168.30.2 (192.168.30.2) 56(84) bytes of data.
^C
--- 192.168.30.2 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3066ms
```

Provo quindi usando -Pn, che non usa icmp. L'host è up



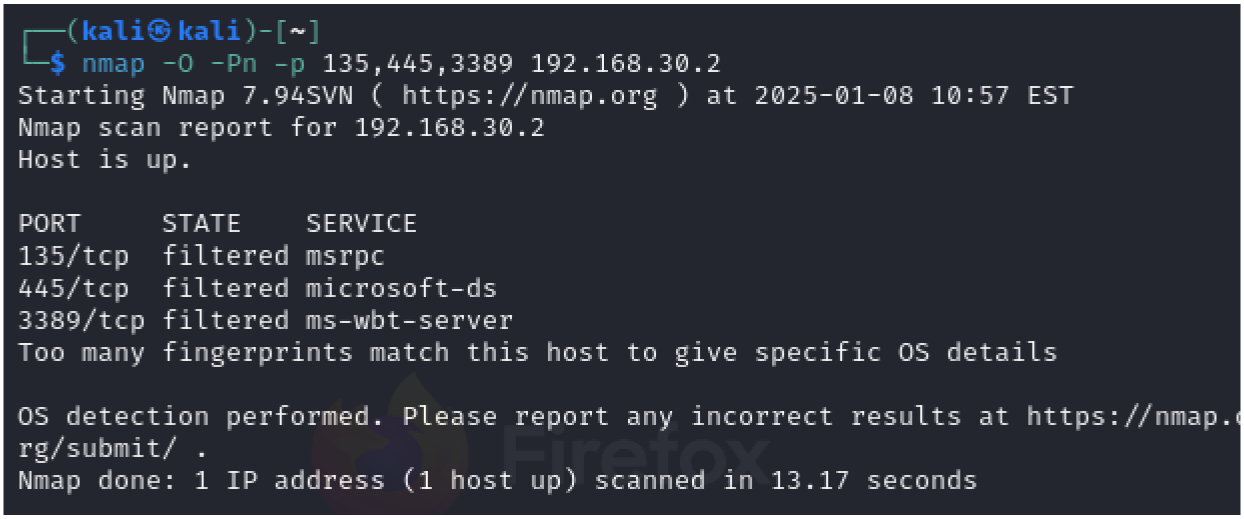
```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.30.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:11 EST
Stats: 0:01:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 53.00% done; ETC: 10:15 (0:01:36 remaining)
Nmap scan report for 192.168.30.2
Host is up.
All 1000 scanned ports on 192.168.30.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 204.07 seconds
```

Usando switch -O e -Pn ho troppe fingerprint per avere un risultato specifico.



```
┌──(kali㉿kali)-[~]
└─$ nmap -O -Pn 192.168.30.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:46 EST
Nmap scan report for 192.168.30.2
Host is up.
All 1000 scanned ports on 192.168.30.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.96 seconds

┌──(kali㉿kali)-[~]
```

Usando il comando precedente su porte mirate (135, 445, 3389):



```
┌──(kali㉿kali)-[~]
└─$ nmap -O -Pn -p 135,445,3389 192.168.30.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:57 EST
Nmap scan report for 192.168.30.2
Host is up.

PORT     STATE    SERVICE
135/tcp  filtered msrpc
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

Riesco a identificare che si tratta di una macchina windows