Esercizio 03/12/2024

- OS Fingerprint - Metasploitable

```
# Nmap 7.94SVN scan initiated Tue Dec  3 09:39:10 2024 as: /usr/lib/nmap/nmap --privileged -O -oN osfingerprint_report_metasploitable.txt
  192.168.10.10
Nmap scan report for 192.168.10.10
Host is up (0.00020s 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
MAC Address: 08:00:27:4D:E1:90 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Dec  3 09:39:24 2024 -- 1 IP address (1 host up) scanned in 14.56 seconds
```

- SYN Scan - Metasploitable

```
# Nmap 7.94SVN scan initiated Tue Dec  3 08:55:18 2024 as: /usr/lib/nmap/nmap --privileged -sS -oN SYCScan_report_metasploitable.txt 192.168.10.10
Nmap scan report for 192.168.10.10
Host is up (0.000069s 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
MAC Address: 08:00:27:4D:E1:90 (Oracle VirtualBox virtual NIC)

# Nmap done at Tue Dec  3 08:55:31 2024 -- 1 IP address (1 host up) scanned in 13.16 seconds

```

- TCP Connect Scan - Metasploitable

```
# Nmap 7.94SVN scan initiated Tue Dec  3 08:55:56 2024 as: /usr/lib/nmap/nmap --privileged -sT -oN TCPConnectScan_report_metasploitable.txt
  192.168.10.10
Nmap scan report for 192.168.10.10
Host is up (0.00020s 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
MAC Address: 08:00:27:4D:E1:90 (Oracle VirtualBox virtual NIC)

# Nmap done at Tue Dec  3 08:56:09 2024 -- 1 IP address (1 host up) scanned in 13.15 seconds

```

- Version Detection - Metasploitable

```
# Nmap 7.94SVN scan initiated Tue Dec  3 08:59:47 2024 as: /usr/lib/nmap/nmap --privileged -sV -oN VersionDetection_report_metasploitable.txt
  192.168.10.10
Nmap scan report for 192.168.10.10
Host is up (0.000068s 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   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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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
MAC Address: 08:00:27:4D:E1:90 (Oracle VirtualBox virtual NIC)
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 at Tue Dec  3 09:00:52 2024 -- 1 IP address (1 host up) scanned in 65.52 seconds

```

- OS FingerPrint - Win XP

```
# Nmap 7.94SVN scan initiated Tue Dec  3 08:44:58 2024 as: /usr/lib/nmap/nmap --privileged -O -oN osfingerprint_report_xp.txt 192.168.10.102
Nmap scan report for 192.168.10.102
Host is up (0.00036s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (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|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2008|2000 (97%), General Dynamics embedded (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/
  o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_2000::sp4
Aggressive OS guesses: Microsoft Windows XP SP3 (97%), Microsoft Windows Server 2003 SP1 or SP2 (95%), Microsoft Windows Server 2008 Enterprise SP2
  (95%), Microsoft Windows Server 2003 SP2 (94%), Microsoft Windows XP (94%), Microsoft Windows XP SP2 or Windows Server 2003 (93%), Microsoft Windows
  XP SP2 or SP3 (93%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (92%), Microsoft Windows XP SP2 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Dec  3 08:45:19 2024 -- 1 IP address (1 host up) scanned in 21.68 seconds

```

Differenze tra SYN Scan e TCP Connect Scan:

La differenza tra lo scan SYN e TCP sta nel fatto che:

- Nello scan SYN (-sS) le porte chiuse non vengono mostrate come "Connessione rifiutata". In pratica se una porta viene ritrovata chiusa da Nmap non viene mostrata nel report.

- Nello scan TCP (-sT) le porte chiuse sono riportate come "conn-refused".

Un'altra differenza sta nel tempo di scansione visto che SYNScan non effettua la connessione TCP ma si ferma al RST del SYN-ACT.

Riepilogo

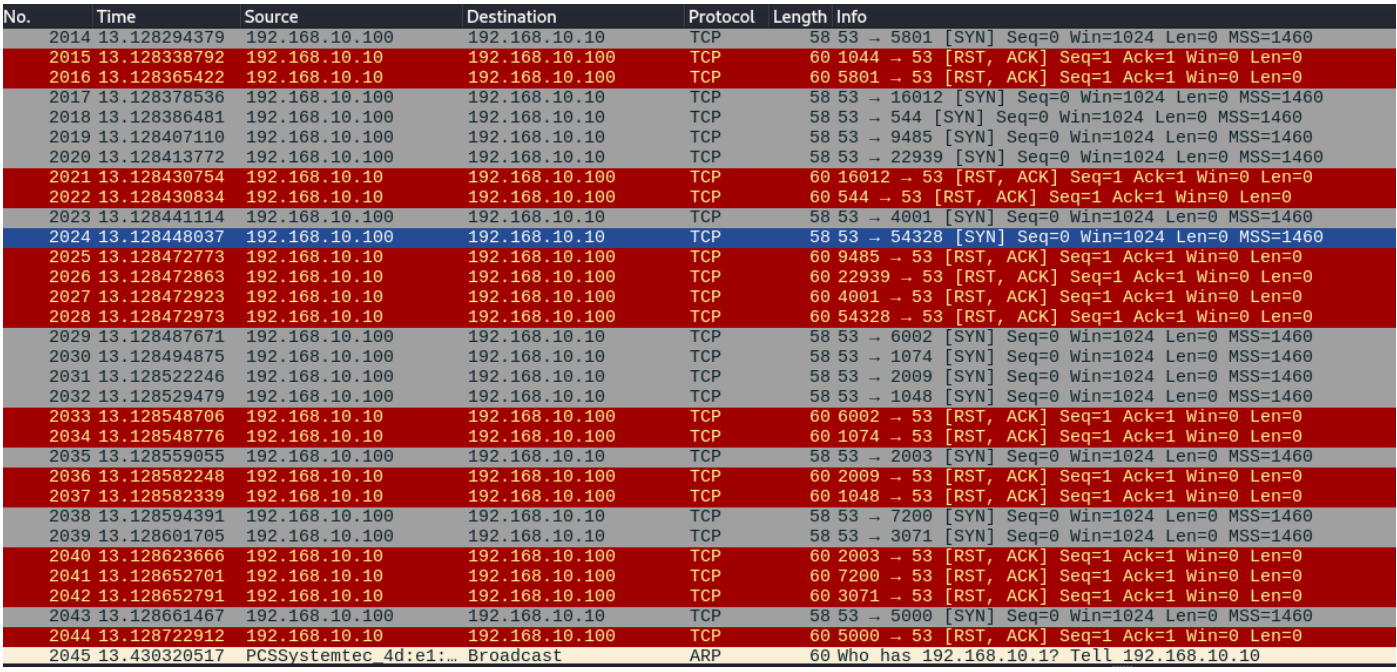
Info	Comando	Report
IP	Qualsiasi	Tutti
Sistema Operativo	nmap -O	OS Fingerprint
Porte Aperte	nmap -sS, nmap -sT	SYN Scan e TCP Connect Scan
Servizi in Ascolto con Versione	nmap -sV	Version Detection

Extra 03/12/2024

Utilizzo dei comandi “-g” “-f” “-D”

Comando “-g”:

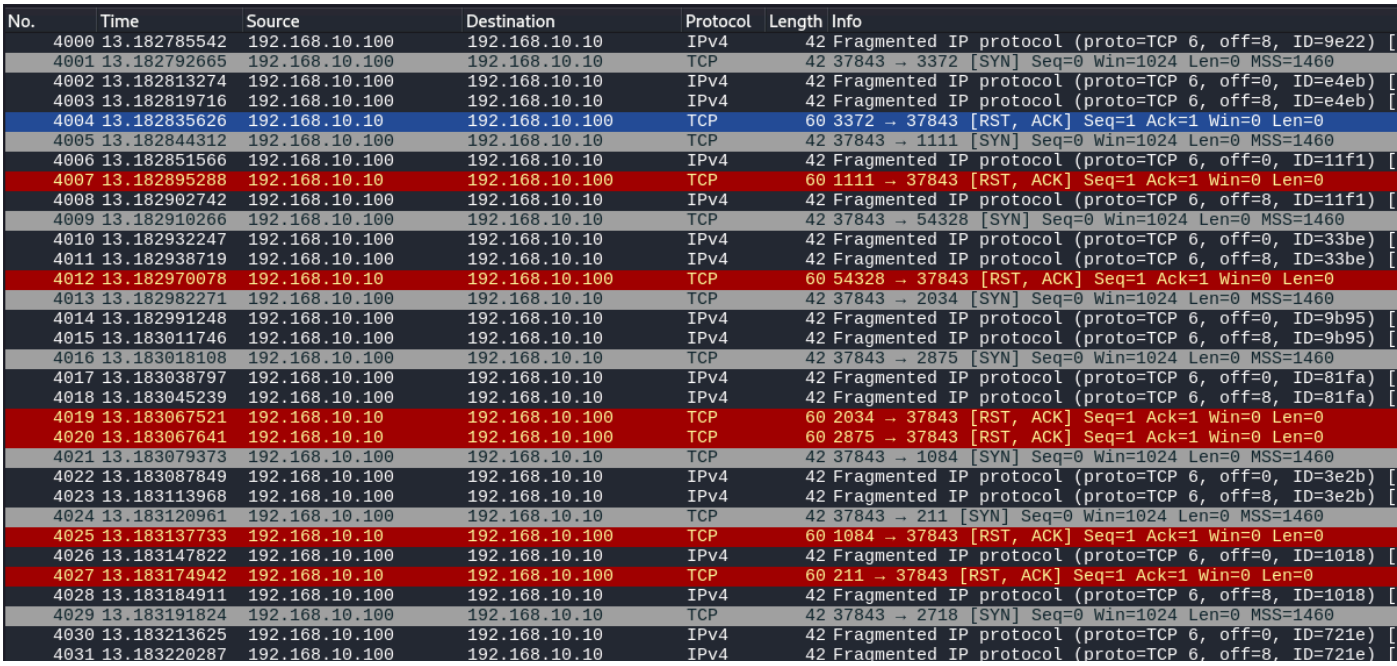
Il comando -g permette di avviare la scansione attraverso una porta predefinita scelta al momento di avvio della scansione.



No.	Time	Source	Destination	Protocol	Length	Info
2014	13.128294379	192.168.10.100	192.168.10.10	TCP	58	53 → 5801 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2015	13.128338792	192.168.10.10	192.168.10.100	TCP	60	1044 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2016	13.128365422	192.168.10.10	192.168.10.100	TCP	60	5801 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2017	13.128378536	192.168.10.100	192.168.10.10	TCP	58	53 → 16012 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2018	13.128386481	192.168.10.100	192.168.10.10	TCP	58	53 → 544 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2019	13.128407110	192.168.10.100	192.168.10.10	TCP	58	53 → 9485 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2020	13.128413772	192.168.10.100	192.168.10.10	TCP	58	53 → 22939 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2021	13.128430754	192.168.10.10	192.168.10.100	TCP	60	16012 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2022	13.128430834	192.168.10.10	192.168.10.100	TCP	60	544 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2023	13.128441114	192.168.10.100	192.168.10.10	TCP	58	53 → 4001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2024	13.128448037	192.168.10.100	192.168.10.10	TCP	58	53 → 54328 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2025	13.128472773	192.168.10.10	192.168.10.100	TCP	60	9485 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2026	13.128472863	192.168.10.10	192.168.10.100	TCP	60	22939 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2027	13.128472923	192.168.10.10	192.168.10.100	TCP	60	4001 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2028	13.128472973	192.168.10.10	192.168.10.100	TCP	60	54328 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2029	13.128487671	192.168.10.100	192.168.10.10	TCP	58	53 → 6002 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2030	13.128494875	192.168.10.100	192.168.10.10	TCP	58	53 → 1074 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2031	13.128522246	192.168.10.100	192.168.10.10	TCP	58	53 → 2009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2032	13.128529479	192.168.10.100	192.168.10.10	TCP	58	53 → 1048 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2033	13.128548706	192.168.10.10	192.168.10.100	TCP	60	6002 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2034	13.128548776	192.168.10.10	192.168.10.100	TCP	60	1074 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2035	13.128559055	192.168.10.100	192.168.10.10	TCP	58	53 → 2003 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2036	13.128582248	192.168.10.10	192.168.10.100	TCP	60	2009 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2037	13.128582339	192.168.10.10	192.168.10.100	TCP	60	1048 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2038	13.128594391	192.168.10.100	192.168.10.10	TCP	58	53 → 7200 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2039	13.128601705	192.168.10.100	192.168.10.10	TCP	58	53 → 3071 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2040	13.128623666	192.168.10.10	192.168.10.100	TCP	60	2003 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2041	13.128652701	192.168.10.10	192.168.10.100	TCP	60	7200 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2042	13.128652791	192.168.10.10	192.168.10.100	TCP	60	3071 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2043	13.128661467	192.168.10.100	192.168.10.10	TCP	58	53 → 5000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2044	13.128722912	192.168.10.10	192.168.10.100	TCP	60	5000 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2045	13.430320517	PCSSystemtec_4d:e1:…	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.10

Comando “-f”:

Il comando -f permette l’invio di pacchetti frammentati, l’utilizzo di questo comando è utile per passare firewall e IDS che analizzano solo pacchetti completi.



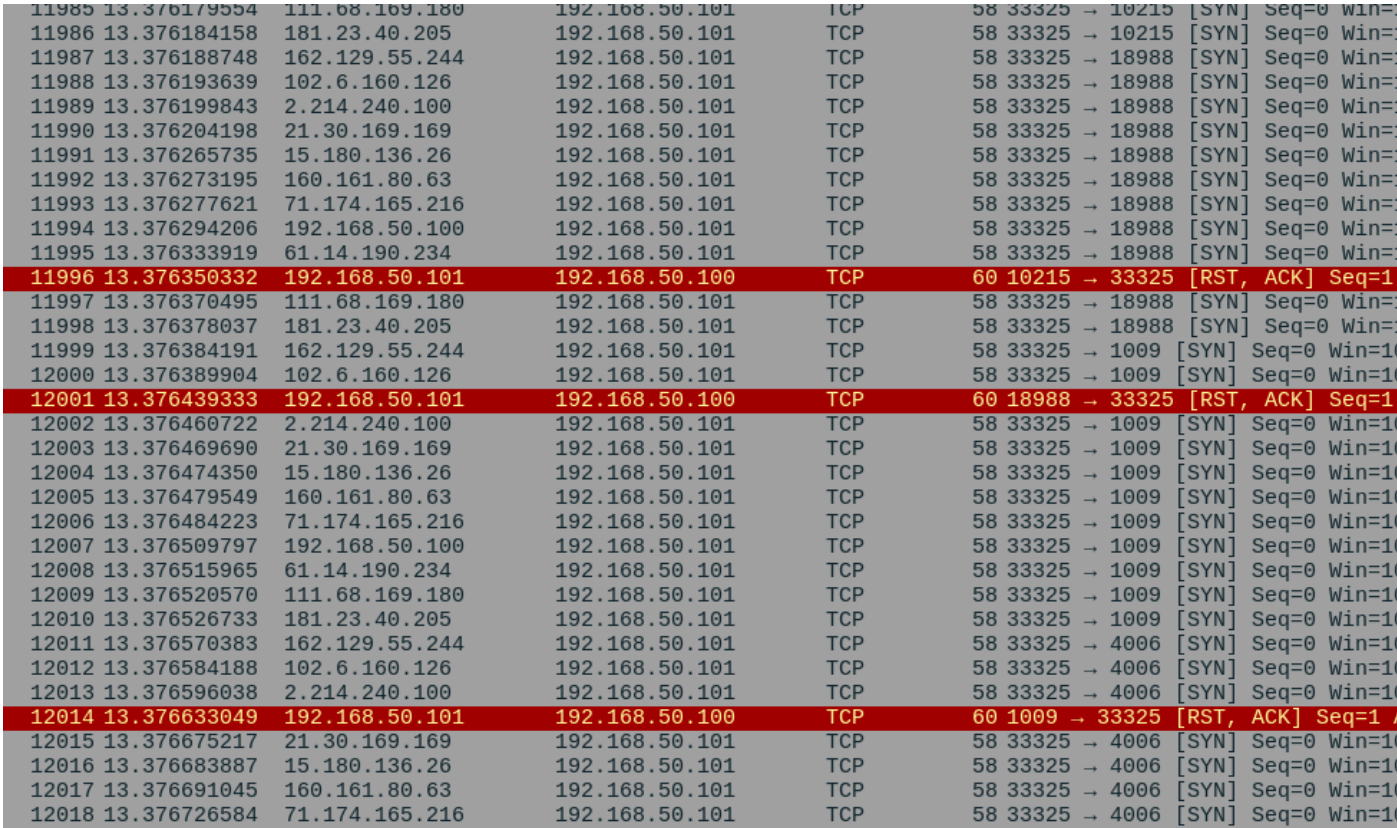
No.	Time	Source	Destination	Protocol	Length	Info
4000	13.182785542	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=9e22) [
4001	13.182792665	192.168.10.100	192.168.10.10	TCP	42	37843 → 3372 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4002	13.182813274	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e4eb) [
4003	13.182819716	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=e4eb) [
4004	13.182835626	192.168.10.10	192.168.10.100	TCP	60	3372 → 37843 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4005	13.182844312	192.168.10.100	192.168.10.10	TCP	42	37843 → 1111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4006	13.182851566	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=11f1) [
4007	13.182895288	192.168.10.10	192.168.10.100	TCP	60	1111 → 37843 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4008	13.182902742	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=11f1) [
4009	13.182910266	192.168.10.100	192.168.10.10	TCP	42	37843 → 54328 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4010	13.182932247	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=33be) [
4011	13.182938719	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=33be) [
4012	13.182970078	192.168.10.10	192.168.10.100	TCP	60	54328 → 37843 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4013	13.182982271	192.168.10.100	192.168.10.10	TCP	42	37843 → 2034 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4014	13.182991248	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=9b95) [
4015	13.183011746	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=9b95) [
4016	13.183018108	192.168.10.100	192.168.10.10	TCP	42	37843 → 2875 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4017	13.183038797	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=81fa) [
4018	13.183045239	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=81fa) [
4019	13.183067521	192.168.10.10	192.168.10.100	TCP	60	2034 → 37843 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4020	13.183067641	192.168.10.10	192.168.10.100	TCP	60	2875 → 37843 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4021	13.183079373	192.168.10.100	192.168.10.10	TCP	42	37843 → 1084 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4022	13.183087849	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=3e2b) [
4023	13.183113968	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=3e2b) [
4024	13.183120961	192.168.10.100	192.168.10.10	TCP	42	37843 → 211 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4025	13.183137733	192.168.10.10	192.168.10.100	TCP	60	1084 → 37843 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4026	13.183147822	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=1018) [
4027	13.183174942	192.168.10.10	192.168.10.100	TCP	60	211 → 37843 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4028	13.183184911	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=1018) [
4029	13.183191824	192.168.10.100	192.168.10.10	TCP	42	37843 → 2718 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4030	13.183213625	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=721e) [
4031	13.183220287	192.168.10.100	192.168.10.10	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=721e) [

Comando -D:

Il comando -D permette la scansione creando una varietà di ip fasulli al fine di far confondere il vero Ip del mandante delle richieste.

Comando -D RND:10:

L’aggiunta di RND:10 specifica il numero di IP fasulli da creare



11985	13.376179554	111.68.169.180	192.168.50.101	TCP	58 33325 → 10215 [SYN] Seq=0 Win=
11986	13.376184158	181.23.40.205	192.168.50.101	TCP	58 33325 → 10215 [SYN] Seq=0 Win=
11987	13.376188748	162.129.55.244	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11988	13.376193639	102.6.160.126	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11989	13.376199843	2.214.240.100	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11990	13.376204198	21.30.169.169	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11991	13.376265735	15.180.136.26	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11992	13.376273195	160.161.80.63	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11993	13.376277621	71.174.165.216	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11994	13.376294206	192.168.50.100	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11995	13.376333919	61.14.190.234	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11996	13.376350332	192.168.50.101	192.168.50.100	TCP	60 10215 → 33325 [RST, ACK] Seq=1
11997	13.376370495	111.68.169.180	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11998	13.376378037	181.23.40.205	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=
11999	13.376384191	162.129.55.244	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12000	13.376389904	102.6.160.126	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12001	13.376439333	192.168.50.101	192.168.50.100	TCP	60 18988 → 33325 [RST, ACK] Seq=1
12002	13.376460722	2.214.240.100	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12003	13.376469690	21.30.169.169	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12004	13.376474350	15.180.136.26	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12005	13.376479549	160.161.80.63	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12006	13.376484223	71.174.165.216	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12007	13.376509797	192.168.50.100	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12008	13.376515965	61.14.190.234	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12009	13.376520570	111.68.169.180	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12010	13.376526733	181.23.40.205	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1
12011	13.376570383	162.129.55.244	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1
12012	13.376584188	102.6.160.126	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1
12013	13.376596038	2.214.240.100	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1
12014	13.376633049	192.168.50.101	192.168.50.100	TCP	60 1009 → 33325 [RST, ACK] Seq=1
12015	13.376675217	21.30.169.169	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1
12016	13.376683887	15.180.136.26	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1
12017	13.376691045	160.161.80.63	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1
12018	13.376726584	71.174.165.216	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1
12019	13.376733904	192.168.50.100	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1
12020	13.376740954	61.14.190.234	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1

Comando -p u:53,t:200:

Il comando se inviato così è sbagliato.
La sintassi corretta del comando con Nmap è:

nmap -sU -sT -p U:53,T:200 <IP Target>

In questo caso è possibile ricevere “Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn ”.

Per ovviare a questo basta usare -Pn.