L’esercizio chiedeva di effettuare delle scansioni sul target metasploitable

- OS fingerprint

```
# Nmap 7.94SVN scan initiated Tue Dec  3 14:56:51 2024 as: nmap -O -oN osfing_metas_report.txt 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.00060s 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: 08:00:27:32:14:16 (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
```

VERSIONE SISTEMA OPERATIVO: linux 2.6.X (quindi tra 2.6.9 e 2.6.33)
IP: 192.168.50.101

- Syn scan= qui ci sono le **porte aperte**

```
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Dec  3 14:57:06 2024 -- 1 IP address (1 host up) scanned in 14.53 seconds
# Nmap 7.94SVN scan initiated Tue Dec  3 15:03:21 2024 as: nmap -sS -oN synscan_metas_report.txt 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.000083s 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: 08:00:27:32:14:16 (Oracle VirtualBox virtual NIC)
```

- TCP connect=qui si trovano le **porte aperte**

```
# Nmap done at Tue Dec  3 15:03:34 2024 -- 1 IP address (1 host up) scanned in 13.23 seconds
# Nmap 7.94SVN scan initiated Tue Dec  3 15:04:54 2024 as: nmap -sT -oN tcpscan_metas_report.txt 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.00022s 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: 08:00:27:32:14:16 (Oracle VirtualBox virtual NIC)
```

LA DIFFERENZA TRA TCP E SYN

La differenza tra queste due scansioni si trova nella velocità di scansione e nella latenza, in quanto la syn risulta essere più veloce della tcp (syn=0.000083s, tcp=0.00022s) perché la syn non completa la connessione restituendo RST (reset), mentre la tpc stabilisce la connessione completa.

L'altra differenza è che, appunto, la syn non completa la connessione restituendo RST (reset), mentre la tcp restituisce connection refused.

- Version detection=qui si trovano i **servizi in ascolto con versione**

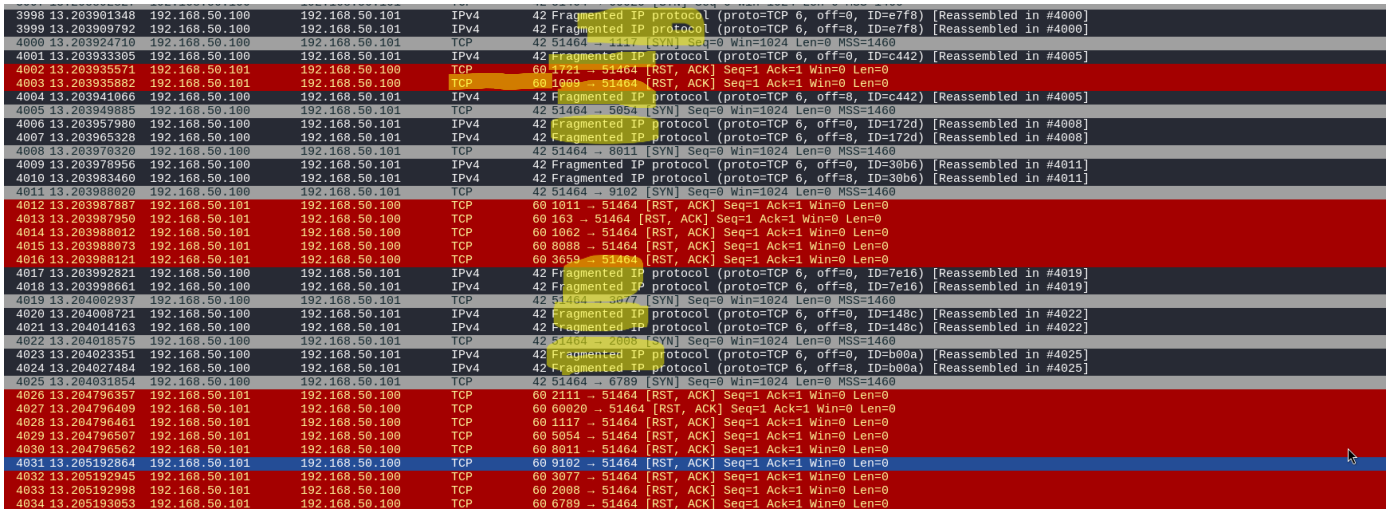
```
# Nmap 7.94SVN scan initiated Tue Dec  3 15:06:18 2024 as: nmap -sV -oN verdet_metas_report.txt 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   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: 08:00:27:32:14:16 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel
```

- OS fingerprint windows= qui dono elencati tutte le possibili **versioni del SO**.

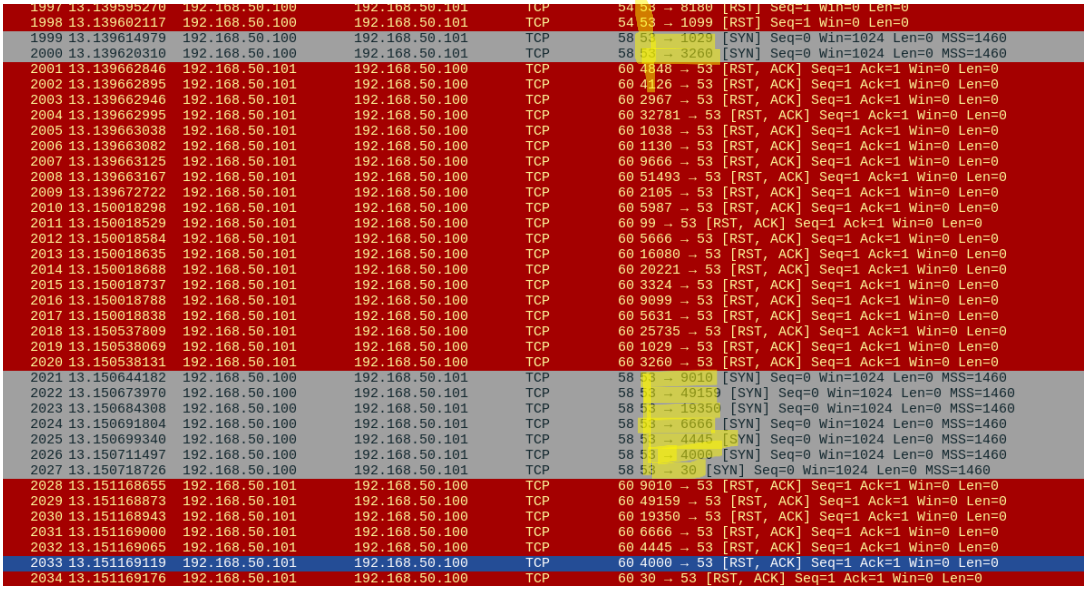
```
# Nmap 7.94SVN scan initiated Tue Dec  3 14:53:06 2024 as: nmap -O -oN osfing_win_report.txt 192.168.50.102
Nmap scan report for 192.168.50.102
Host is up (0.00080s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
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
Aggressive OS guesses: Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1 (95%), Microsoft Windows 2000 SP4 or Windows XP SP1a (95%),
Microsoft Windows Server 2003 SP1 or SP2 (95%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows XP SP3 (92%), Microsoft Windows 2000
Server SP3 or SP4 (92%)
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 14:53:27 2024 -- 1 IP address (1 host up) scanned in 21.60 seconds
```

EXTRA:

- comando -f= con questo comando si frammentano i pacchetti tcp/ip per eludere il firewall ed i sistemi IDS.

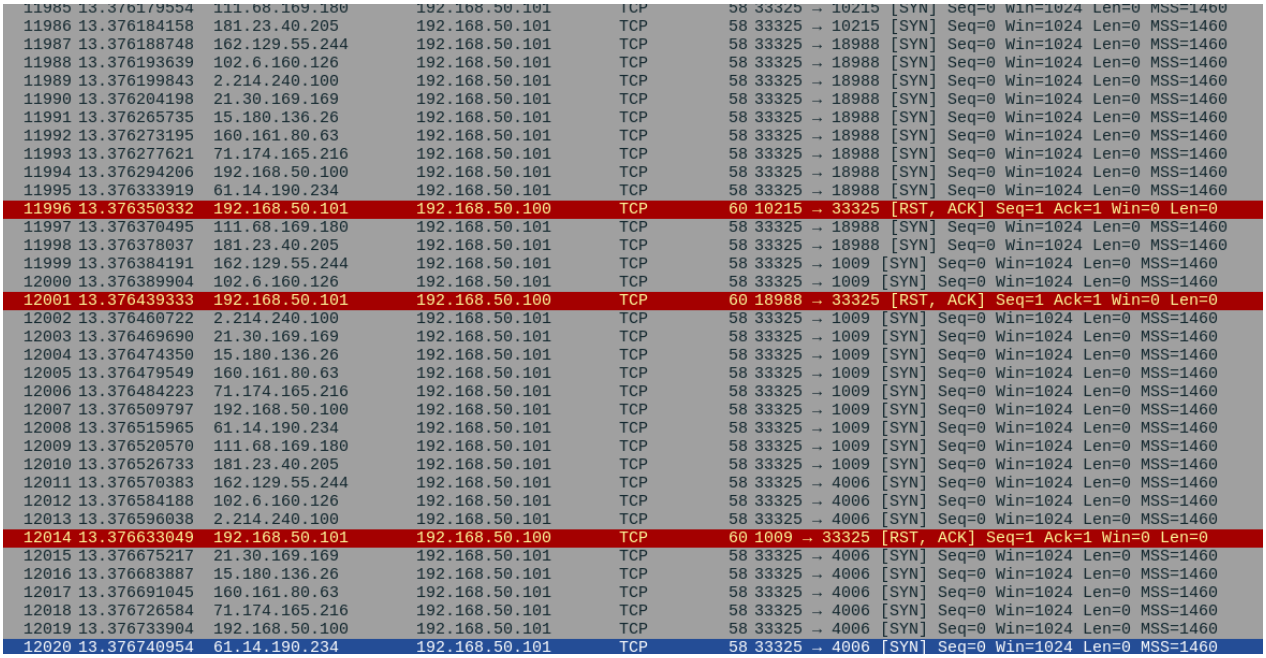


- comado -g {source port}= tramite questo comando si sceglie la porta da cui far partire la scansione.



1997	13.139595270	192.168.50.100	192.168.50.101	TCP	54 53 → 8180 [RST] Seq=1 Win=0 Len=0
1998	13.139602117	192.168.50.100	192.168.50.101	TCP	54 53 → 1099 [RST] Seq=1 Win=0 Len=0
1999	13.139614979	192.168.50.100	192.168.50.101	TCP	58 53 → 1029 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2000	13.139620310	192.168.50.100	192.168.50.101	TCP	58 53 → 3260 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2001	13.139662846	192.168.50.101	192.168.50.100	TCP	60 4848 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2002	13.139662895	192.168.50.101	192.168.50.100	TCP	60 4126 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2003	13.139662946	192.168.50.101	192.168.50.100	TCP	60 2967 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2004	13.139662995	192.168.50.101	192.168.50.100	TCP	60 32781 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2005	13.139663038	192.168.50.101	192.168.50.100	TCP	60 1038 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2006	13.139663082	192.168.50.101	192.168.50.100	TCP	60 1130 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2007	13.139663125	192.168.50.101	192.168.50.100	TCP	60 9666 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2008	13.139663167	192.168.50.101	192.168.50.100	TCP	60 51493 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2009	13.139672722	192.168.50.101	192.168.50.100	TCP	60 2105 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2010	13.150018298	192.168.50.101	192.168.50.100	TCP	60 5987 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2011	13.150018529	192.168.50.101	192.168.50.100	TCP	60 99 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2012	13.150018584	192.168.50.101	192.168.50.100	TCP	60 5666 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2013	13.150018635	192.168.50.101	192.168.50.100	TCP	60 16080 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2014	13.150018688	192.168.50.101	192.168.50.100	TCP	60 20221 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2015	13.150018737	192.168.50.101	192.168.50.100	TCP	60 3324 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2016	13.150018788	192.168.50.101	192.168.50.100	TCP	60 9099 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2017	13.150018838	192.168.50.101	192.168.50.100	TCP	60 5631 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2018	13.150537809	192.168.50.101	192.168.50.100	TCP	60 25735 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2019	13.150538069	192.168.50.101	192.168.50.100	TCP	60 1029 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2020	13.150538131	192.168.50.101	192.168.50.100	TCP	60 3260 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2021	13.150644182	192.168.50.100	192.168.50.101	TCP	58 53 → 9010 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2022	13.150673970	192.168.50.100	192.168.50.101	TCP	58 53 → 49159 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2023	13.150684308	192.168.50.100	192.168.50.101	TCP	58 53 → 19350 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2024	13.150691804	192.168.50.100	192.168.50.101	TCP	58 53 → 6666 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2025	13.150699340	192.168.50.100	192.168.50.101	TCP	58 53 → 4445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2026	13.150711497	192.168.50.100	192.168.50.101	TCP	58 53 → 4000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2027	13.150718726	192.168.50.100	192.168.50.101	TCP	58 53 → 30 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2028	13.151168655	192.168.50.101	192.168.50.100	TCP	60 9010 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2029	13.151168873	192.168.50.101	192.168.50.100	TCP	60 49159 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2030	13.151168943	192.168.50.101	192.168.50.100	TCP	60 19350 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2031	13.151169000	192.168.50.101	192.168.50.100	TCP	60 6666 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2032	13.151169065	192.168.50.101	192.168.50.100	TCP	60 4445 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2033	13.151169119	192.168.50.101	192.168.50.100	TCP	60 4000 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2034	13.151169176	192.168.50.101	192.168.50.100	TCP	60 30 → 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- Comando -d= tramite questo comando si creano dei decoy (ip falsi) in modo da mascherare/confondere l'ip d'origine da cui è partita la scansione.
- Comando -d RND:10= questo comando permette di impostare un range di decoy.



11985	13.376179554	111.68.169.180	192.168.50.101	TCP	58 33325 → 10215 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11986	13.376184158	181.23.40.205	192.168.50.101	TCP	58 33325 → 10215 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11987	13.376188748	162.129.55.244	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11988	13.376193639	102.6.160.126	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11989	13.376199843	2.214.240.100	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11990	13.376204198	21.30.169.169	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11991	13.376265735	15.180.136.26	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11992	13.376273195	160.161.80.63	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11993	13.376277621	71.174.165.216	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11994	13.376294206	192.168.50.100	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11995	13.376333919	61.14.190.234	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11996	13.376350332	192.168.50.101	192.168.50.100	TCP	60 10215 → 33325 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11997	13.376370495	111.68.169.180	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11998	13.376378037	181.23.40.205	192.168.50.101	TCP	58 33325 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11999	13.376384191	162.129.55.244	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12000	13.376389904	102.6.160.126	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12001	13.376439333	192.168.50.101	192.168.50.100	TCP	60 18988 → 33325 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12002	13.376460722	2.214.240.100	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12003	13.376469690	21.30.169.169	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12004	13.376474350	15.180.136.26	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12005	13.376479549	160.161.80.63	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12006	13.376484223	71.174.165.216	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12007	13.376509797	192.168.50.100	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12008	13.376515965	61.14.190.234	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12009	13.376520570	111.68.169.180	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12010	13.376526733	181.23.40.205	192.168.50.101	TCP	58 33325 → 1009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12011	13.376570383	162.129.55.244	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12012	13.376584188	102.6.160.126	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12013	13.376596038	2.214.240.100	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12014	13.376633049	192.168.50.101	192.168.50.100	TCP	60 1009 → 33325 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12015	13.376675217	21.30.169.169	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12016	13.376683887	15.180.136.26	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12017	13.376691045	160.161.80.63	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12018	13.376726584	71.174.165.216	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12019	13.376733904	192.168.50.100	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12020	13.376740954	61.14.190.234	192.168.50.101	TCP	58 33325 → 4006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

- Comando -p u:53,t:400 è sbagliato perché dovrebbe essere nmap -sU -sT -p U:53,T:200.