3 Way Handshake

```
┌──(nicholas㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
[sudo] password for nicholas:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 18:27 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers wi
Nmap scan report for 192.168.50.101
Host is up (0.00080s 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: CA:01:F0:3E:DD:B1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

┌──(nicholas㉿kali)-[~]
```

246	20.390012223	192.168.50.101	192.168.50.110	TCP	60 9000 → 58028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
247	20.390012261	192.168.50.101	192.168.50.110	TCP	60 6779 → 45722 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
248	20.390106311	192.168.50.101	192.168.50.110	TCP	60 667 → 32986 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
249	20.390162261	192.168.50.101	192.168.50.110	TCP	74 6000 → 39794 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TS…
250	20.390166086	192.168.50.110	192.168.50.101	TCP	66 39794 → 6000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1748318437 TSecr=42…
251	20.390266061	192.168.50.101	192.168.50.110	TCP	60 32782 → 46220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
252	20.390266136	192.168.50.101	192.168.50.110	TCP	60 32 → 51346 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
253	20.390475086	192.168.50.101	192.168.50.110	TCP	60 9101 → 36248 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
254	20.390475161	192.168.50.101	192.168.50.110	TCP	60 7007 → 57640 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
255	20.390597411	192.168.50.101	192.168.50.110	TCP	60 19 → 55246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
256	20.390597486	192.168.50.101	192.168.50.110	TCP	60 1097 → 56840 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
257	20.390731286	192.168.50.101	192.168.50.110	TCP	60 1110 → 56460 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
258	20.390731361	192.168.50.101	192.168.50.110	TCP	60 545 → 50812 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

420	20.413186173	192.168.50.101	192.168.50.110	TCP	60 4125 → 39398 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
421	20.413189998	192.168.50.101	192.168.50.110	TCP	60 1443 → 46410 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
422	20.413190036	192.168.50.101	192.168.50.110	TCP	60 16016 → 60168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
423	20.413200123	192.168.50.110	192.168.50.101	TCP	74 46168 → 16012 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=17483…
424	20.413205448	192.168.50.110	192.168.50.101	TCP	74 56910 → 1247 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=174831…
425	20.413381248	192.168.50.101	192.168.50.110	TCP	60 8290 → 42388 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
426	20.413381286	192.168.50.101	192.168.50.110	TCP	74 2121 → 53736 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TS…
427	20.413381323	192.168.50.101	192.168.50.110	TCP	60 2006 → 40450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
428	20.413381361	192.168.50.101	192.168.50.110	TCP	60 7627 → 52918 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
429	20.413381361	192.168.50.101	192.168.50.110	TCP	60 32780 → 39050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
430	20.413381398	192.168.50.101	192.168.50.110	TCP	60 2196 → 37022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
431	20.413381436	192.168.50.101	192.168.50.110	TCP	60 5925 → 39304 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
432	20.413381436	192.168.50.101	192.168.50.110	TCP	60 24800 → 51236 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
433	20.413398536	192.168.50.110	192.168.50.101	TCP	66 53736 → 2121 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1748318460 TSecr=42…
434	20.413432136	192.168.50.101	192.168.50.110	TCP	60 6101 → 33444 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
435	20.413432211	192.168.50.101	192.168.50.110	TCP	60 280 → 54860 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

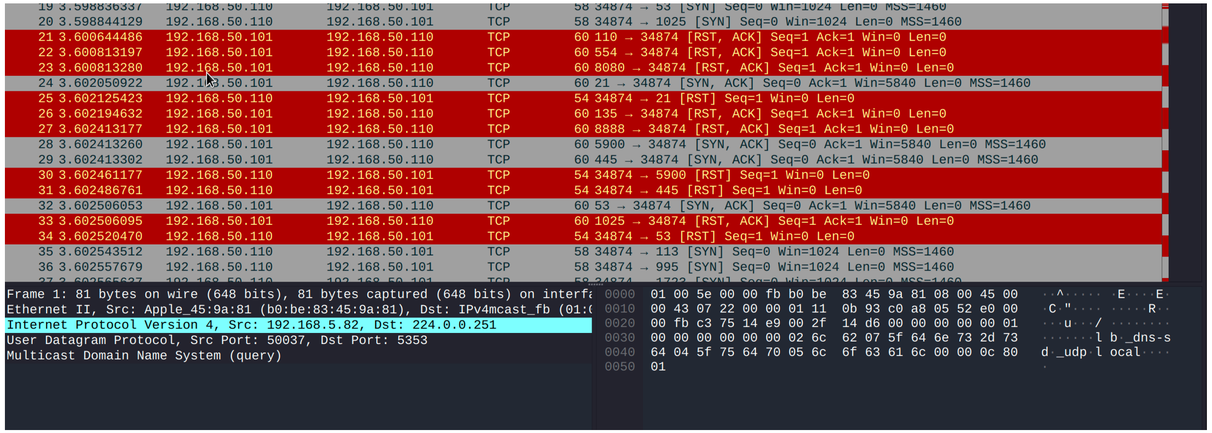
Frame 426: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on inte… 0000 00 0c 29 b3 f3 7c ca 01 f0 3e dd b1 08 00 45 00

Scansione nmap con switch -sT
Sorgente Kali 192.168.50.110
Target metasploitable 2 192.168.50.101
Risultati ottenuti sono quelli presenti in figura che corrispondono alle porte well known aperte su metasploitable
In wireshark si evidenzia il completamento del 3 way handshake con consegna del pacchetto SYN con ricevuta dal target SYN/ACK e risposta sempre dalla sorgente con ACK

Scansione SYN scan

```
└─$ sudo nmap -sS  192.168.50.101
[sudo] password for nicholas:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-24 19:11 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00055s latency).
Not shown: 978 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
8180/tcp open  unknown
MAC Address: CA:01:F0:3E:DD:B1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```



- Scansione in in nmap con switch -Ss
- Sorgente Kali 192.168.50.110
- Target metasploitable 192.168.50.101
- Risultati ottenuti: elenco di porte well-known aperte
- Questo tipo di scan è meno invasivo rispetto a -sT poiché non crude il 3 way handshake, ma una volta appurato che la porta è aperta si limita a chiudere la connessione come si evince nell' immagine di cattura con Wireshark. Dopo il pacchetto di risposta SYN/ACK, la sorgente provvede a chiudere direttamente la connessione con un pacchetto RST

Scansione in Aggressive

```
┌──(nicholas㉿kali)-[~]
└─$ sudo nmap -A 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-24 18:08 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.0016s 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 192.168.50.110
|      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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=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: 2023-07-24T16:09:18+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

```
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      46926/udp   mountd
|   100005  1,2,3      48979/tcp   mountd
|   100021  1,3,4      54531/udp   nlockmgr
|   100021  1,3,4      58005/tcp   nlockmgr
|   100024  1          50285/tcp   status
|_  100024  1          58704/udp   status
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        netkit-rsh rexecd
513/tcp  open  login
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsCompression, SupportsTransactions, ConnectWithDatabase, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, LongColumnFlag
|   Status: Autocommit
|_  Salt: |<TrbuC0c#$)?Cq4ISGK
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-07-24T16:09:17+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=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
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)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

```
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
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: CA:01:F0:3E:DD:B1 (Unknown)
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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: 2023-07-24T12:09:09-04:00
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   1.64 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.75 seconds

┌──(nicholas㉿kali)-[~]
└─$
```

```
  2853 17.601835332  192.168.50.110  192.168.50.101  TCP      66 49814 → 25 [ACK] Seq=23 Ack=205 Win=64128 Len=0 TSval=1764554047 TSecr=163
  2854 17.616496984  192.168.50.110  192.168.50.101  TCP      66 42966 → 8180 [ACK] Seq=316 Ack=8840 Win=64128 Len=0 TSval=1764554062 TSecr
  2855 17.636447361  192.168.50.101  192.168.50.110  FTP     100 Response: 331 Please specify the password.
  2856 17.644703181  192.168.50.110  192.168.50.101  TCP      66 50232 → 2121 [ACK] Seq=19 Ack=131 Win=64256 Len=0 TSval=1764554090 TSecr=1
  2857 17.645427393  192.168.50.101  192.168.50.110  TCP      66 22 → 43482 [ACK] Seq=39 Ack=21 Win=5824 Len=0 TSval=16341 TSecr=1764554045
  2858 17.645610300  192.168.50.101  192.168.50.110  TCP      98 22 → 43482 [PSH, ACK] Seq=39 Ack=21 Win=5824 Len=32 TSval=16341 TSecr=1764
  2859 17.645610467  192.168.50.101  192.168.50.110  TCP      66 22 → 43482 [FIN, ACK] Seq=71 Ack=21 Win=5824 Len=0 TSval=16341 TSecr=17645
  2860 17.650299431  192.168.50.110  192.168.50.101  TCP      66 50232 → 2121 [RST, ACK] Seq=19 Ack=131 Win=64256 Len=0 TSval=1764554096 TS
  2861 17.650502379  192.168.50.110  192.168.50.101  TCP      66 34132 → 8009 [FIN, ACK] Seq=98 Ack=8775 Win=64128 Len=0 TSval=1764554096 T
  2862 17.650868943  192.168.50.110  192.168.50.101  TCP      74 35208 → 6000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=17645540
  2863 17.651107139  192.168.50.110  192.168.50.101  FTP      80 Request: PASS IEUser@
  2864 17.651179844  192.168.50.110  192.168.50.101  HTTP    233 PROPFIND / HTTP/1.1
  2865 17.651221759  192.168.50.110  192.168.50.101  HTTP     84 GET / HTTP/1.0
  2866 17.651258840  192.168.50.101  192.168.50.110  TCP      74 6000 → 35208 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSva
  2867 17.651290547  192.168.50.110  192.168.50.101  TCP      66 35208 → 6000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1764554097 TSecr=1634
  2868 17.651575657  192.168.50.101  192.168.50.110  TCP      66 21 → 53200 [ACK] Seq=55 Ack=31 Win=5824 Len=0 TSval=16341 TSecr=1764554097
  2869 17.651701151  192.168.50.101  192.168.50.110  TCP      66 80 → 43954 [ACK] Seq=1 Ack=168 Win=6912 Len=0 TSval=16341 TSecr=1764554097
  2870 17.651701317  192.168.50.101  192.168.50.110  TCP      66 80 → 43964 [ACK] Seq=1 Ack=19 Win=5824 Len=0 TSval=16341 TSecr=1764554097

Frame 1: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on int
Ethernet II, Src: TendaTec_5c:c5:d8 (d8:32:14:5c:c5:d8), Dst: Broadcast (ff:f
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 11113, Dst Port: 11111
Data (129 bytes)

0000  ff ff ff ff ff ff d8 32  14 5c c5 d8 08 00 45 00   ·····2 ·\····E·
0010  00 9d 4c 22 00 00 40 11  2e 2f 00 00 00 00 ff ff   ··L"··@· ./····
0020  ff ff 2b 69 2b 67 00 89  6c d0 f1 f2 f3 f4 e3 bd   ··+i+g·· l·····
0030  3d fa cf 93 f1 92 01 05  54 65 6e 64 61 02 06 4d   =······ Tenda··M
0040  57 35 2d 76 32 03 01 01  0a 06 d8 32 14 5c c5 d8   W5-v2··· ···2·\··
0050  04 04 01 05 a8 c0 05 01  00 06 01 01 07 01 00 08   ········ ········
0060  04 c3 c4 0e 00 09 04 22  b0 be 64 0d 12 45 38 38   ·······" ··d··E88
0070  38 32 30 31 31 30 33 30  35 30 30 30 34 38 34 0b   82011030 5000484·
0080  0b 43 61 73 61 5f 4e 61  73 69 6e 69 0c 10 30 32   ·Casa_Na sini··02
0090  30 30 37 32 31 31 34 35  39 31 39 37 33 31 0e 01   00721145 919731··
00a0  05 10 08 db c2 50 c5 85  01 00 00                  ·····P·· ···
```

- Scansione in map con switch -A
- Sorgente Kali 192.168.50.110
- Target metasploitable 2 192.168.50.101
- Con scansione in Aggressive è possibile recuperare più informazioni sul target oltre che le porte aperte come info sul sistema operativo e i servizi in ascolto sulle porte aperte, poiché è uno Scan più invasivo. Le info ottenute sono visibile nell’immagini della slide precedente