

Di seguito riporto la prima scansione TCP effettuata con comando nmap.

Con il metodo classico (senza aggiungere opzioni aggiuntive di esecuzione) ed analizzando i pacchetti con Wireshark, si nota che con questo metodo il programma effettua il processo completo di richiesta di collegamento, effettuando il three-way-handshake in modo completo. Lo si può notare dalle righe rosa che riportano ACK di risposta, stabilendo una connessione.



Di seguito riporto la scansione Completa effettuata con comando nmap -A

NMAP -A SCAN TYPE							
FONTE DELLO SCAN		TARGET SCAN		SCAN TYPE	SERVIZI ATTIVI		
Sistema Operativo	Ip Source	Sistema Operativo	Ip Target		Port N.	Stato	Version
Kali Linux Release 2023.3	192.168.50.100	Linux - Metasploitable 2.6.24	192.168.50.101	nmap - ALL	21	Open	vsftpd 2.3.4
					22	Open	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
					23	Open	Linux telnetd
					25	Open	Postfix smtpd
					53	Open	ISC BIND 9.4.2
					80	Open	Apache httpd 2.2.8 (Ubuntu DAV/2)
					111	Open	RPC #100000
					139	Open	Samba smbd 3.X - 4.X
					445	Open	Samba smbd 3.0.20-Debian
					512	Open	netkit-rsh rexecd
					513	Open	OpenBSD or Solaris rlogind
					514	Open	\

Anche questo comando effettua e completa i passaggi della three-way-handshake, ma risulta molto più invasivo e lento nella sua esecuzione. Questo perché nell'effettuare la scansione non ricerca solo le porte aperte con i relativi servizi, ma ne ricava anche più dati possibile di ognuna di esse. Nell'elenco sopra ho elencato la versione del servizio individuato aperto dalla scansione. Di sotto ne riporto gli screen completi di quanto individuato.

```
(kali@kali)-[~]
$ nmap -A 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-26 06:44 EST
Nmap scan report for 192.168.50.101
Host is up (0.00058s latency).
Not shown: 977 closed tcp ports (conn-refused)
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 192.168.50.100
|_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       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_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: 2023-12-26T11:44:54+00:00; 0s from scanner time.
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-title: Metasploitable2 - Linux
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_program version    port/proto  service
```



```

|_ 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-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      50874/tcp  mountd
|   100005   1,2,3      57459/udp  mountd
|   100021   1,3,4      44738/tcp  nlockmgr
|   100021   1,3,4      53774/udp  nlockmgr
|   100024   1          34305/udp  status
|_ 100024   1          55277/tcp  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       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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 11
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, Speaks41ProtocolNew, Support41Auth, LongColumnFlag, SupportsCompression, SwitchToSSLAfterHandshake, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: kS<pC<Aq8bcK/H]{qGK&
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| 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: 2023-12-26T11:44:54+00:00; 0s 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
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-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

```

Host script results:
|_clock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2023-12-26T06:44:46-05:00

```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 27.14 seconds

```

(kali@kali)-[~]
$

```

scansione Nmap -Apcapng

File Modifica Visualizza Vaj Cattura Analisi Statistiche Telefonja Wireless Strumenti Aiuto

Applica un filtro di visualizzazione ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
40	6.509839382	192.168.50.100	192.168.50.101	TCP	66	42302 → 5900 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3137426549 TSecr=15351
41	6.509923399	192.168.50.100	192.168.50.101	TCP	74	37614 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426549 TSecr=0 WS=128
42	6.509934660	192.168.50.100	192.168.50.101	TCP	74	49116 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426549 TSecr=0 WS=128
43	6.510021534	192.168.50.100	192.168.50.101	TCP	74	55406 → 1720 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
44	6.510043290	192.168.50.100	192.168.50.101	TCP	74	59024 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
45	6.510082250	192.168.50.101	192.168.50.100	TCP	74	3306 → 37614 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=15351 TSecr=3137426549 WS=128
46	6.510082317	192.168.50.101	192.168.50.100	TCP	60	199 → 49116 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
47	6.510088251	192.168.50.100	192.168.50.101	TCP	66	37614 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3137426550 TSecr=15351
48	6.510133092	192.168.50.101	192.168.50.100	TCP	60	1720 → 55406 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	6.510133139	192.168.50.101	192.168.50.100	TCP	60	8080 → 59024 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
50	6.510167417	192.168.50.100	192.168.50.101	TCP	74	47488 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
51	6.510191198	192.168.50.100	192.168.50.101	TCP	74	45472 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
52	6.510206587	192.168.50.100	192.168.50.101	TCP	74	44228 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
53	6.510221268	192.168.50.100	192.168.50.101	TCP	74	34174 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
54	6.510275683	192.168.50.100	192.168.50.101	TCP	74	57486 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
55	6.510294549	192.168.50.100	192.168.50.101	TCP	74	40900 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
56	6.510345431	192.168.50.100	192.168.50.101	TCP	74	56450 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
57	6.510372277	192.168.50.101	192.168.50.100	TCP	74	80 → 47488 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=15351 TSecr=3137426550 WS=128
58	6.510372340	192.168.50.101	192.168.50.100	TCP	60	143 → 45472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	6.510372380	192.168.50.101	192.168.50.100	TCP	60	256 → 44228 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60	6.510372418	192.168.50.101	192.168.50.100	TCP	74	25 → 34174 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=15351 TSecr=3137426550 WS=128
61	6.510372447	192.168.50.101	192.168.50.100	TCP	60	554 → 57486 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	6.510378458	192.168.50.100	192.168.50.101	TCP	66	47488 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3137426550 TSecr=15351
63	6.510389546	192.168.50.100	192.168.50.101	TCP	66	34174 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3137426550 TSecr=15351
64	6.510431594	192.168.50.101	192.168.50.100	TCP	60	587 → 40900 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	6.510457055	192.168.50.100	192.168.50.101	TCP	74	53742 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
66	6.510475501	192.168.50.100	192.168.50.101	TCP	74	35948 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
67	6.510528502	192.168.50.101	192.168.50.100	TCP	74	111 → 56450 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=15351 TSecr=3137426550 WS=128
68	6.510533151	192.168.50.100	192.168.50.101	TCP	66	56450 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3137426550 TSecr=15351
69	6.510562125	192.168.50.100	192.168.50.101	TCP	74	42146 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
70	6.510585329	192.168.50.101	192.168.50.100	TCP	74	23 → 53742 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=15351 TSecr=3137426550 WS=128
71	6.510585381	192.168.50.101	192.168.50.100	TCP	60	113 → 35948 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
72	6.510589195	192.168.50.100	192.168.50.101	TCP	66	53742 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3137426550 TSecr=15351
73	6.510655854	192.168.50.100	192.168.50.101	TCP	74	57214 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
74	6.510676673	192.168.50.100	192.168.50.101	TCP	74	51036 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128
75	6.510692012	192.168.50.100	192.168.50.101	TCP	74	54928 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3137426550 TSecr=0 WS=128

Frame 53: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0  
Ethernet II, Src: PCSSystemtec\_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PCSSystemtec\_8a:12:07 (08:00:27:8a:12:07)  
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101  
Transmission Control Protocol, Src Port: 34174, Dst Port: 25, Seq: 0, Len: 0

0000 08 00 27 8a 12 07 08 00 27 cb 7e f5 08 00 45 00 .....E  
0010 00 3c 40 b4 40 00 40 06 13 ee c0 a8 32 64 c0 a8 <@ @ @ .....2d  
0020 32 65 85 7e 00 19 c3 0c 83 6f 00 00 00 00 a0 02 2e ~.....o  
0030 fa f0 e6 48 00 00 02 04 05 b4 04 02 08 0a bb 01 H.....  
0040 54 76 00 00 00 00 01 03 03 07 .....TV.....

La scansione effettuata con Wireshark risulterà la stessa di quella eseguita con il metodo TCP, mostrando quindi tutti i passaggi della three-way-handshake. Il comando chiude la connessione una volta effettuato l'analisi di tutto quello che può rilevare da quella porta aperta.