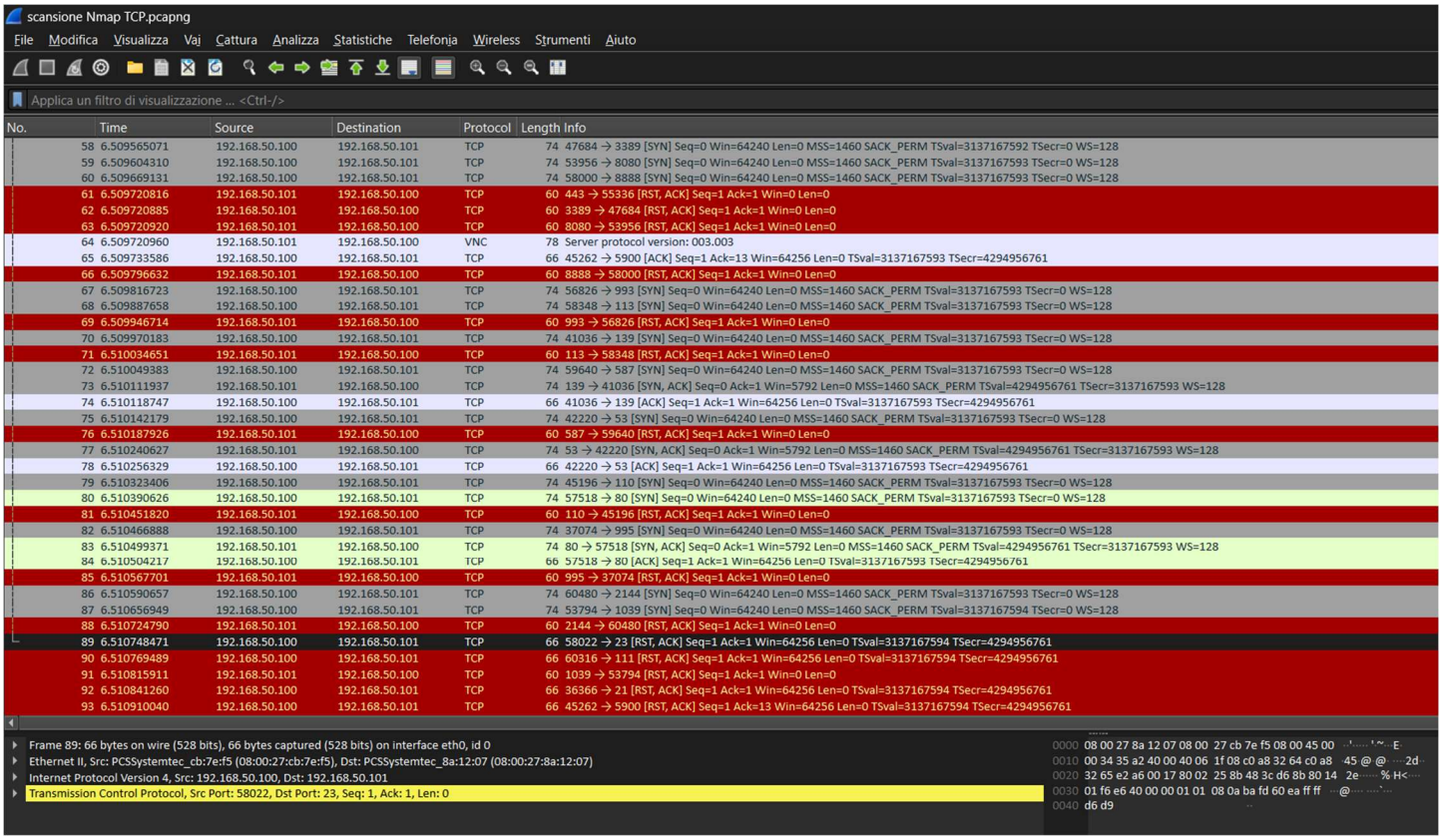
SCANSIONI NMAP

Effettuo le scansioni da macchina Kali-Linux a macchina Metasploitable.

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

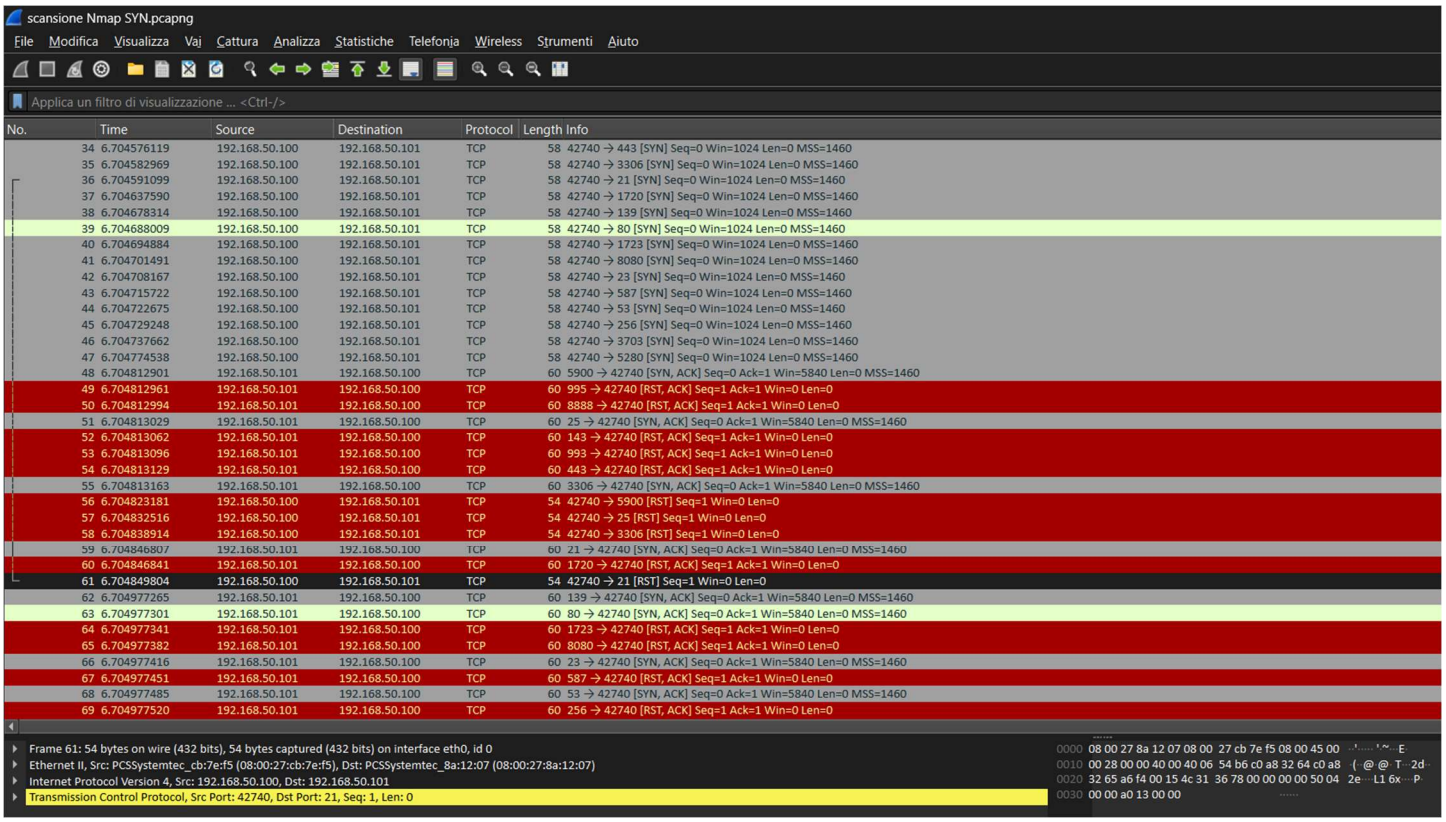
TCP SCAN TYPE								
FONTE DELLO SCAN		TARGET SCAN		SCAN TYPE	SERVIZI ATTIVI			
Sistema Operativo	Ip Source	Sistema Operativo	Ip Target		Port N.	Stato	Service	Version
Kali Linux Relase 2023.3	192.168.50.100	Linux - Metasploitable 2.6.24	192.168.50.101	nmap - TCP	21	Open	ftp	\
					22	Open	ssh	\
					23	Open	telnet	\
					25	Open	smtp	\
					53	Open	domain	\
					80	Open	http	\
					111	Open	rpcbind	\
					139	Open	netbios-ssn	\
					445	Open	microsoft-ds	\
					512	Open	exec	\
					513	Open	login	\
					514	Open	shell	\



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 SYN effettuata con comando nmap –sS

SYN SCAN TYPE								
FONTE DELLO SCAN		TARGET SCAN		SCAN TYPE	SERVIZI ATTIVI			
Sistema Operativo	Ip Source	Sistema Operativo	Ip Target		Port N.	Stato	Service	Version
Kali Linux Relase 2023.3	192.168.50.100	Linux - Metasploitable 2.6.24	192.168.50.101	nmap - TCP	21	Open	ftp	\
					22	Open	ssh	\
					23	Open	telnet	\
					25	Open	smtp	\
					53	Open	domain	\
					80	Open	http	\
					111	Open	rpcbind	\
					139	Open	netbios-ssn	\
					445	Open	microsoft-ds	\
					512	Open	exec	\
					513	Open	login	\
					514	Open	shell	\

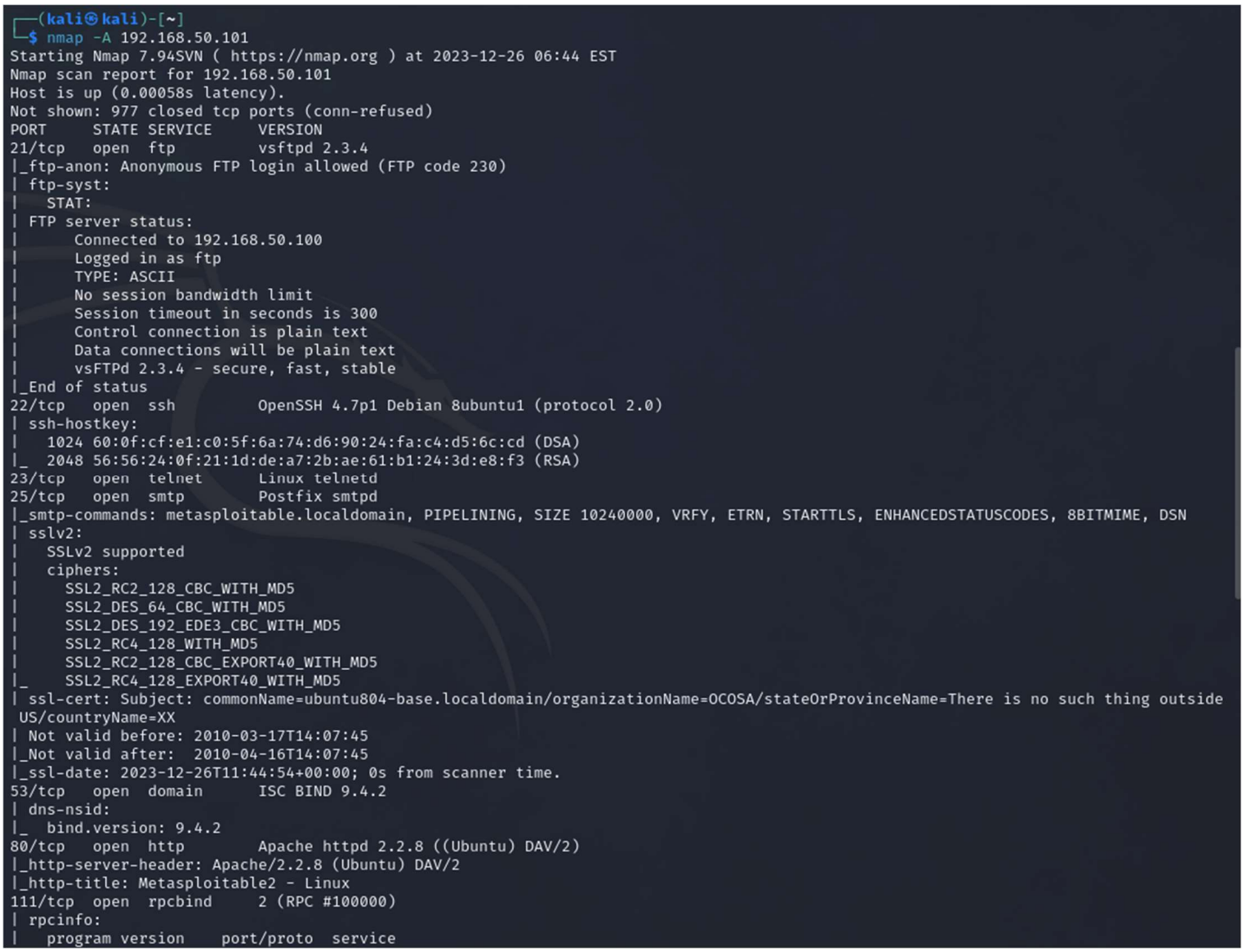


A differenza del metodo precedente, questo non completa la three-way-handshake. È meno invasivo e non effettua una connessione qual ora la porta fosse aperta e attiva. Ma semplicemente alla ricezione del pacchetto SYN-ACK il comando chiude la connessione.

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	Service	Version
Kali Linux Relase 2023.3	192.168.50.100	Linux - Metasploitable 2.6.24	192.168.50.101	nmap - ALL	21	Open	ftp	vsftpd 2.3.4
					22	Open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
					23	Open	telnet	Linux telenetd
					25	Open	smtp	Postfix smtpd
					53	Open	domain	ISC BIND 9.4.2
					80	Open	http	Apache httpd 2.2.8 (Ubuntu DAV/2)
					111	Open	rpcbind	RPC #100000
					139	Open	netbios-ssn	Samba smbd 3.X - 4.X
					445	Open	microsoft-ds	Samba smbd 3.0.20-Debian
					512	Open	exec	netkit-rsh rexecd
					513	Open	login	OpenBSD or Solaris rlogind
					514	Open	shell	\

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
```

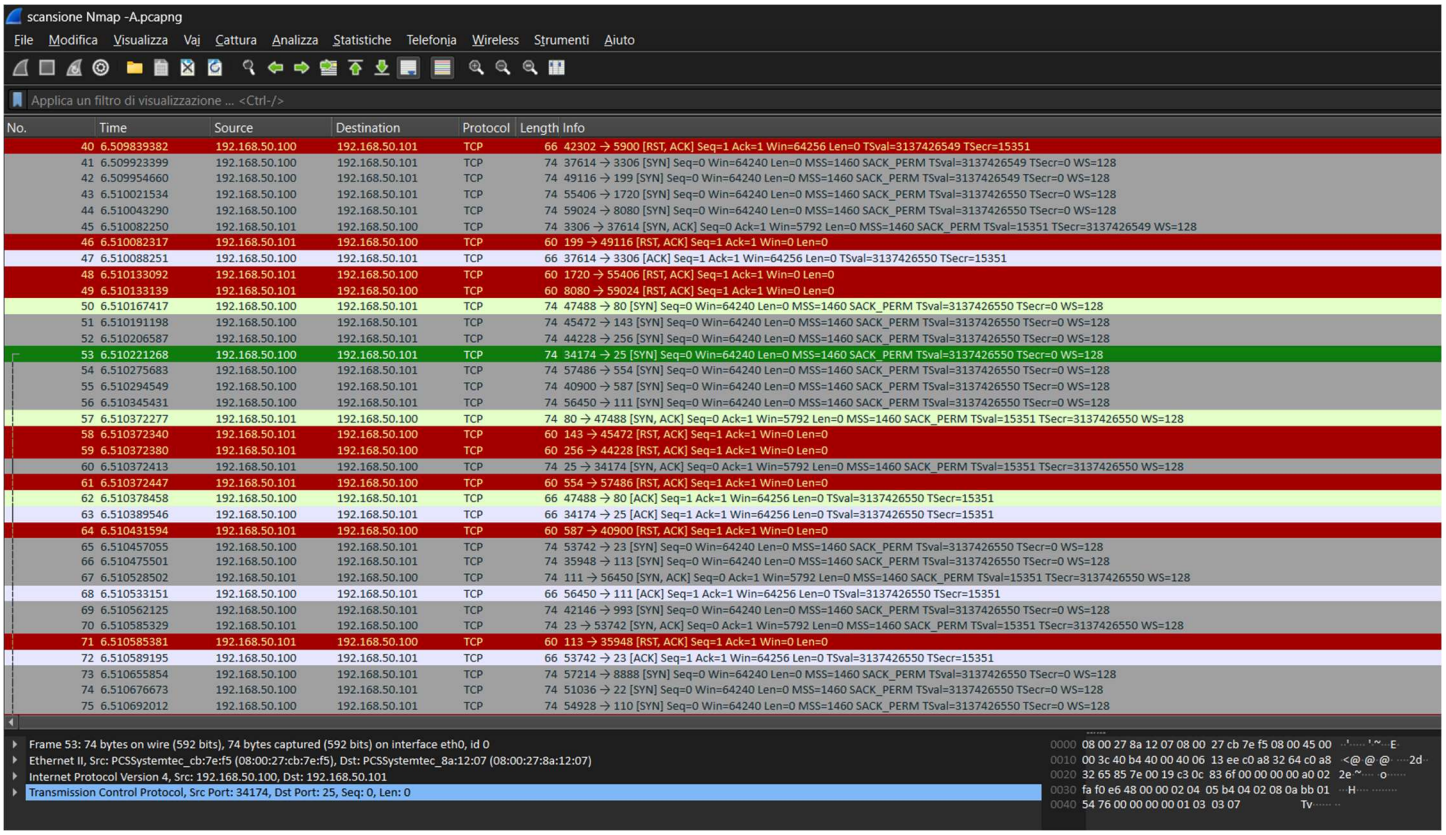
```
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            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, SwitchToSSLAft
erHandshake, 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)-[~]
└─$
```



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.