

## Scansione nmap -sT

PORTA	FONTE	TARGET	TIPO DI SCAN	SERVIZIO
21	192.168.50.100	192.168.50.101	Nmap -sT	ftp
22	192.168.50.100	192.168.50.101	Nmap -sT	Ssh
23	192.168.50.100	192.168.50.101	Nmap -sT	telnet
25	192.168.50.100	192.168.50.101	Nmap -sT	Smtp
53	192.168.50.100	192.168.50.101	Nmap -sT	Domain
80	192.168.50.100	192.168.50.101	Nmap -sT	http
111	192.168.50.100	192.168.50.101	Nmap -sT	Rpcbind
139	192.168.50.100	192.168.50.101	Nmap -sT	Netbios-ssn
445	192.168.50.100	192.168.50.101	Nmap -sT	Microsoft-ds
512	192.168.50.100	192.168.50.101	Nmap -sT	Exec
513	192.168.50.100	192.168.50.101	Nmap -sT	Login
514	192.168.50.100	192.168.50.101	Nmap -sT	shell

## Esempio di intercettazione sulla porta 80 con nmap-sT

tcp.port == 80					
No.	Time	Source	Destination	Protocol	Length Info
47	13.072787389	192.168.50.100	192.168.50.101	TCP	74 58700 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=372785006 TSecr=0 WS=128
62	13.074661054	192.168.50.101	192.168.50.100	TCP	74 80 → 58700 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=189858 TSecr=372785
64	13.074716659	192.168.50.100	192.168.50.101	TCP	66 58700 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=372785008 TSecr=189858

## Scansione nmap -sS

PORTA	FONTE	TARGET	TIPO DI SCAN	SERVIZIO
21	192.168.50.100	192.168.50.101	Nmap -sS	ftp
22	192.168.50.100	192.168.50.101	Nmap -sS	Ssh
23	192.168.50.100	192.168.50.101	Nmap -sS	telnet
25	192.168.50.100	192.168.50.101	Nmap -sS	Smtp
53	192.168.50.100	192.168.50.101	Nmap -sS	Domain
80	192.168.50.100	192.168.50.101	Nmap -sS	http
111	192.168.50.100	192.168.50.101	Nmap -sS	Rpcbind
139	192.168.50.100	192.168.50.101	Nmap -sS	Netbios-ssn
445	192.168.50.100	192.168.50.101	Nmap -sS	Microsoft-ds
512	192.168.50.100	192.168.50.101	Nmap -sS	Exec
513	192.168.50.100	192.168.50.101	Nmap -sS	Login
514	192.168.50.100	192.168.50.101	Nmap -sS	shell

## Esempio di intercettazione sulla porta 80 con nmap-sS

tcp.port == 80					
No.	Time	Source	Destination	Protocol	Length Info
28	13.129884147	192.168.50.100	192.168.50.101	TCP	58 35914 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	13.130387149	192.168.50.101	192.168.50.100	TCP	60 80 → 35914 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
33	13.130409053	192.168.50.100	192.168.50.101	TCP	54 35914 → 80 [RST] Seq=1 Win=0 Len=0

La differenza principale che si può notare dalle due scansioni è che con “nmap -sT” (che è più invasiva) la scansione completa la 3-way-handshake creando così la connessione. Mentre nella scansione “nmap -sS” (meno invasiva) non completa la connessione e chiude la comunicazione con un pacchetto di reset (RST)

## Scansione nmap -A

```
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-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
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
|_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            36279/udp  mountd
|_100005 1,2,3            39634/tcp  mountd
|_100021 1,3,4            49769/udp  nlockmgr
|_100021 1,3,4            53015/tcp  nlockmgr
|_100024 1                44822/udp  status
|_100024 1                57234/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 rshcd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
```

A differenza delle altre scansioni, la scansione “nmap-A” fa una scansione più ampia prendendo molte altre informazioni come, per esempio, la versione del servizio. Rispetto alle altre due però è molto più lungo come procedimento proprio perché intercetta molte più cose.