Dettaglio delle scansioni in -A:

```
┌──(davide㉿kali)-[~]
└─$ nmap -sT 192.168.50.101 -p 0-1023
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-20 18:26 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00033s latency).
Not shown: 1012 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

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
```

```
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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
```

```
23/tcp  open  telnet      Linux telnetd
```

```
25/tcp  open  smtp        Postfix smtpd
|_ssl-date: 2023-04-20T18:29:10+00:00; +1h59m59s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
ch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
```

```
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      40465/tcp   mountd
|   100005  1,2,3      53118/udp   mountd
|   100021  1,3,4      41977/tcp   nlockmgr
|   100021  1,3,4      57382/udp   nlockmgr
|   100024  1          40764/tcp   status
|_  100024  1          42974/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
```

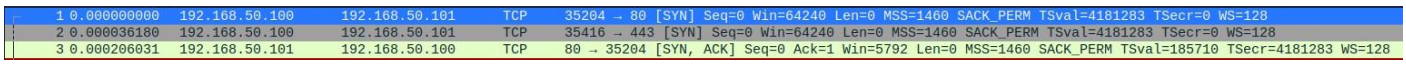
```
513/tcp open  login       OpenBSD or Solaris rlogind
```

```
514/tcp open  shell       Netkit rshd
Service Info: Host:  metasploitable.localdomain; 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: 2023-04-20T14:29:05-04:00
| smb-security-mode:
|   account_used: guest
|   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: 000000000000 (Xerox)
|_clock-skew: mean: 3h20m03s, deviation: 2h18m41s, median: 1h59m58s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.27 seconds
```

Intercettazione pacchetti con WireShark:

Possiamo notare la differenza fra i due tipi di scansione (-sS e -sT) effettuati entrambi ad hoc sulla porta 21.

Nella scansione -sT (la più invasiva) nmap stabilisce di fatto una connessione come possiamo vedere dallo scambio dei pacchetti SYN – SYN ACK – ACK.



Nella scansione -sS nmap invece apre una connessione con la porta e, al posto di inviare l'ultimo protocollo ACK per stabilire la connessione, va invece in RST (reset).

Fonte	Target	Tipo di scan	Porta	Servizio	Versione	Risultato
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	21	FTP	vsftpd 2.3.4	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	22	SSH	OpenSSH 4.7p1 Debian	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	23	Telnet	Linux telnetd	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	25	SMTP	Postfix smtpd	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	53	Domain	ISC BIND 9.4.2	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	80	HTTP	Apache httpd	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	111	RPCBind	RPC #100000	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	139	Netbios-ssn	Samba smbd 3.X - 4.X	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	445	Netbios-ssn	Samba smbd 3.X - 4.X	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	512	Exec	netkit-rsh rexecd	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	513	Login	OpenBSD or Solaris logind	Open
192.168.50.100 - Kali Linux	192.168.50.101 - Metaesploitable	sT con Ping	514	Shell	Netkit-rsh	Open