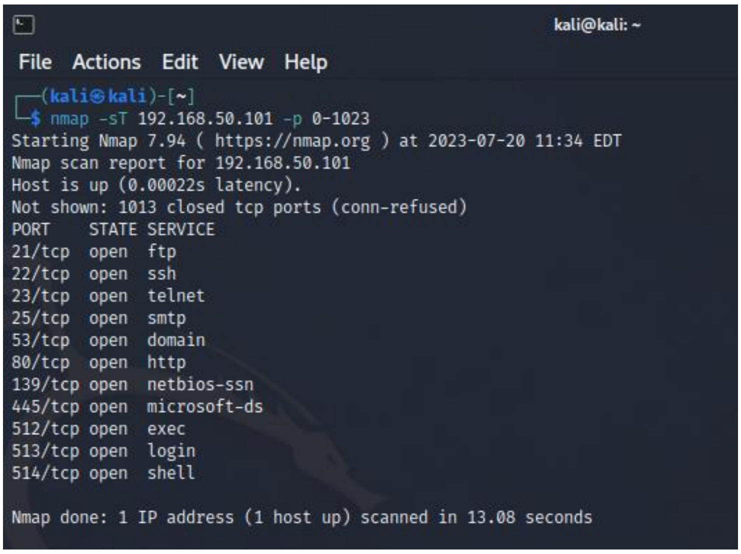
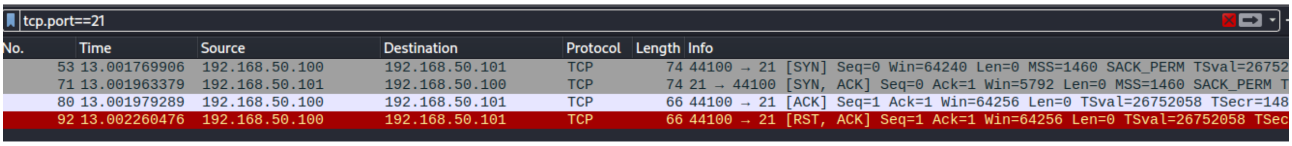
SCANSIONE TCP SULLE PORTE WELL-KNOWN



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.101 -p 0-1023
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 11:34 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00022s latency).
Not shown: 1013 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
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
```

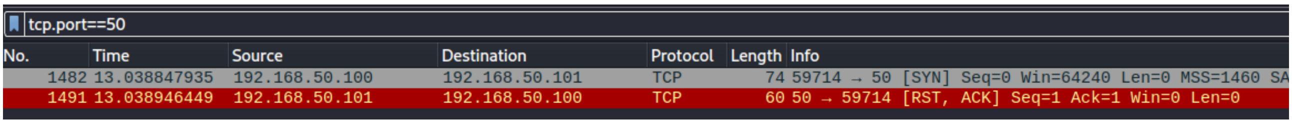
3-way handshake terminato con successo sulla porta 21 in quanto risulta aperta per il servizio ftp



tcp.port==21

No.	Time	Source	Destination	Protocol	Length	Info
53	13.001769906	192.168.50.100	192.168.50.101	TCP	74	44100 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=26752
71	13.001963379	192.168.50.101	192.168.50.100	TCP	74	21 → 44100 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM T
80	13.001979289	192.168.50.100	192.168.50.101	TCP	66	44100 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=26752058 TSecr=148
92	13.002260476	192.168.50.100	192.168.50.101	TCP	66	44100 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=26752058 TSec

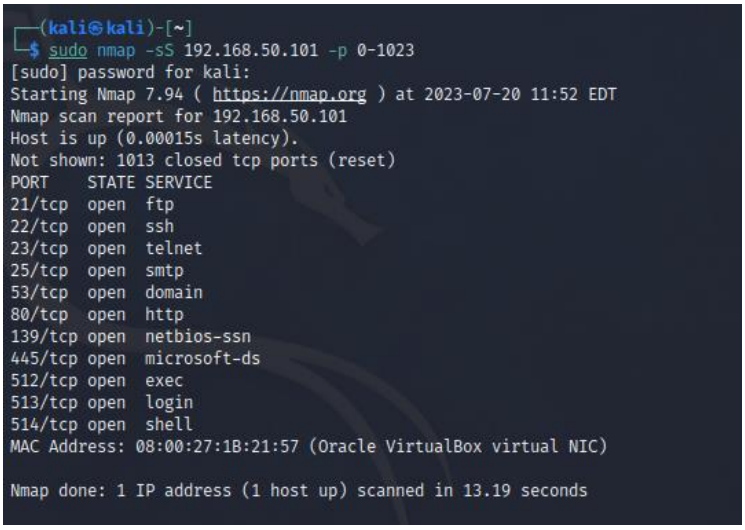
3-way handshake non terminato in quanto la porta 50 risulta chiusa



tcp.port==50

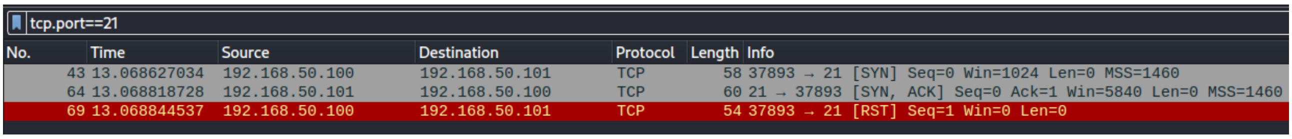
No.	Time	Source	Destination	Protocol	Length	Info
1482	13.038847935	192.168.50.100	192.168.50.101	TCP	74	59714 → 50 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
1491	13.038946449	192.168.50.101	192.168.50.100	TCP	60	50 → 59714 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

SCANSIONE SYN SULLE PORTE WELL-KNOWN



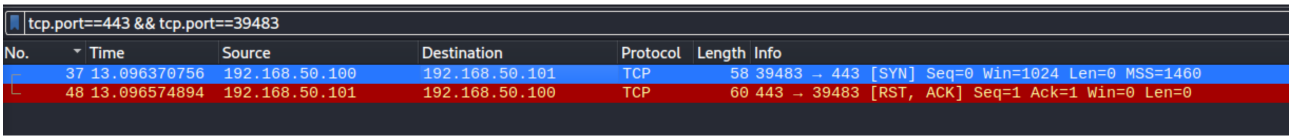
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101 -p 0-1023
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 11:52 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00015s latency).
Not shown: 1013 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:1B:21:57 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

SYN scan completata con successo sulla porta 21 in quanto aperta. Possiamo notare l'invio del pacchetto RST inviato per concludere la connessione prima della conclusione del 3-way handshake



```
tcp.port==21
No.   Time          Source          Destination     Protocol Length Info
   43 13.068627034  192.168.50.100  192.168.50.101  TCP      58 37893 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   64 13.068818728  192.168.50.101  192.168.50.100  TCP      60 21 → 37893 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
   69 13.068844537  192.168.50.100  192.168.50.101  TCP      54 37893 → 21 [RST] Seq=1 Win=0 Len=0
```

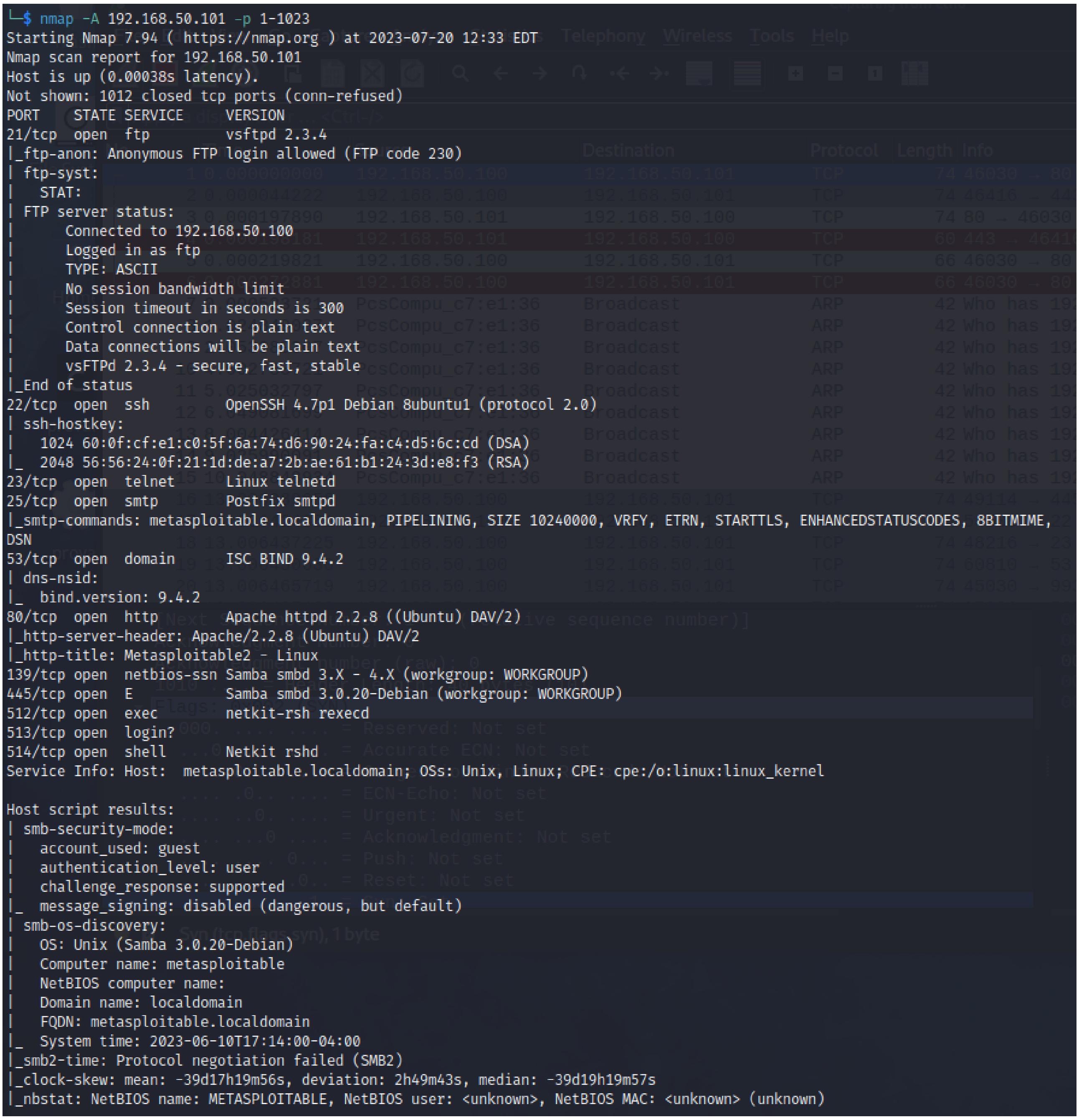
SYN scan fallito in quanto effettuato sulla porta 43 che risulta chiusa



```
tcp.port==443 && tcp.port==39483
No.   Time          Source          Destination     Protocol Length Info
   37 13.096370756  192.168.50.100  192.168.50.101  TCP      58 39483 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   48 13.096574894  192.168.50.101  192.168.50.100  TCP      60 443 → 39483 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

FONTE SCAN	**TARGET SCAN**	**TIPO SCAN**	**RISULTATI**
192.168.50.100	192.168.50.101:0-1023	nmap -sT	porta 21 aperta – ftp
			porta 22 aperta – ssh
			porta 23 aperta – telnet
			porta 25 aperta – smtp
			porta 53 aperta – domain
			porta 80 aperta – http
			porta 139 aperta – netbios-ssn
			porta 445 aperta – microsoft-ds
			porta 512 aperta – exec
			porta 513 aperta – login
			porta 514 aperta – shell
192.168.50.100	192.168.50.101:0-1023	nmap -sS	porta 21 aperta – ftp
			porta 22 aperta – ssh
			porta 23 aperta – telnet
			porta 25 aperta – smtp
			porta 53 aperta – domain
			porta 80 aperta – http
			porta 139 aperta – netbios-ssn
			porta 445 aperta – microsoft-ds
			porta 512 aperta – exec
			porta 513 aperta – login
			porta 514 aperta – shell

SCANSIONE CON SWITCH «-A» SULLE PORTE WELL-KNOWN



```
└─$ nmap -A 192.168.50.101 -p 1-1023
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 12:33 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00038s latency).
Not shown: 1012 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
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
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  E           Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-06-10T17:14:00-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: -39d17h19m56s, deviation: 2h49m43s, median: -39d19h19m57s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

Abbiamo recuperato quante più informazioni possibili della macchina target che nel nostro caso si tratta di una macchina Metasploitable