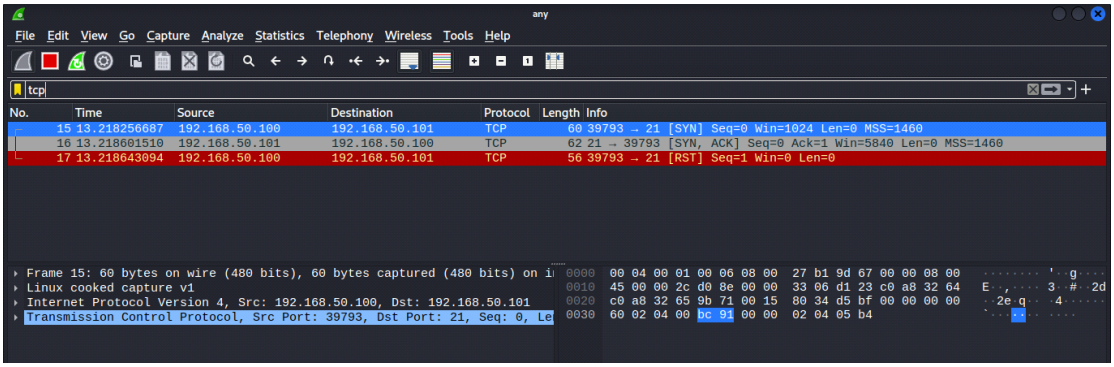
Questo primo comando: "nmap -sS" effetua una scansione leggera

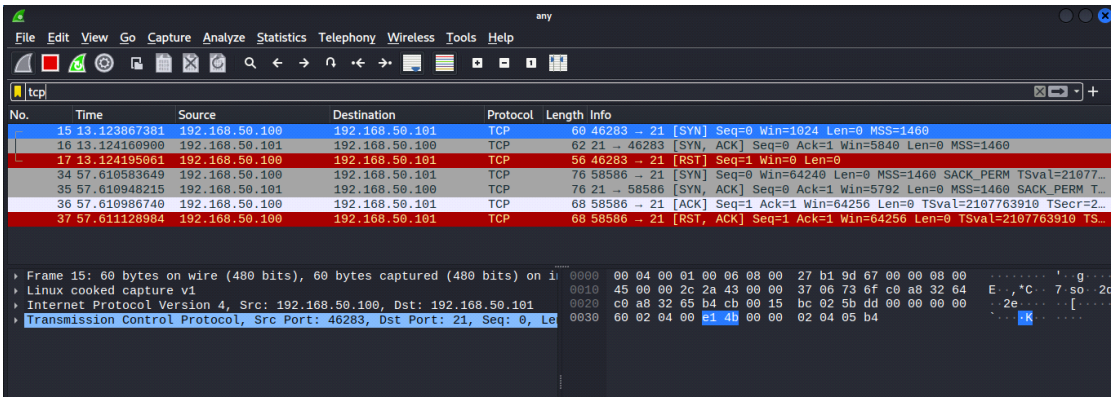
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p21 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 10:00 EST
Nmap scan report for 192.168.50.101
Host is up (0.00030s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 08:00:27:D1:6A:10 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
```

Di seguito con Wireshark possiamo vedere i pacchetti mandati e ricevuti durante la scansione:

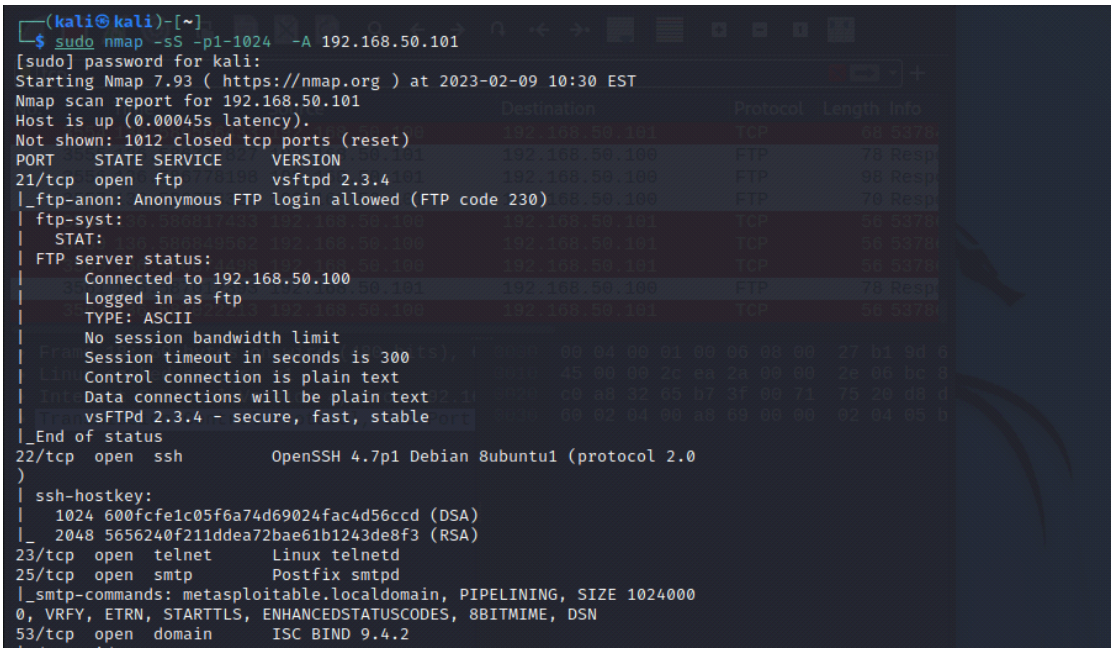


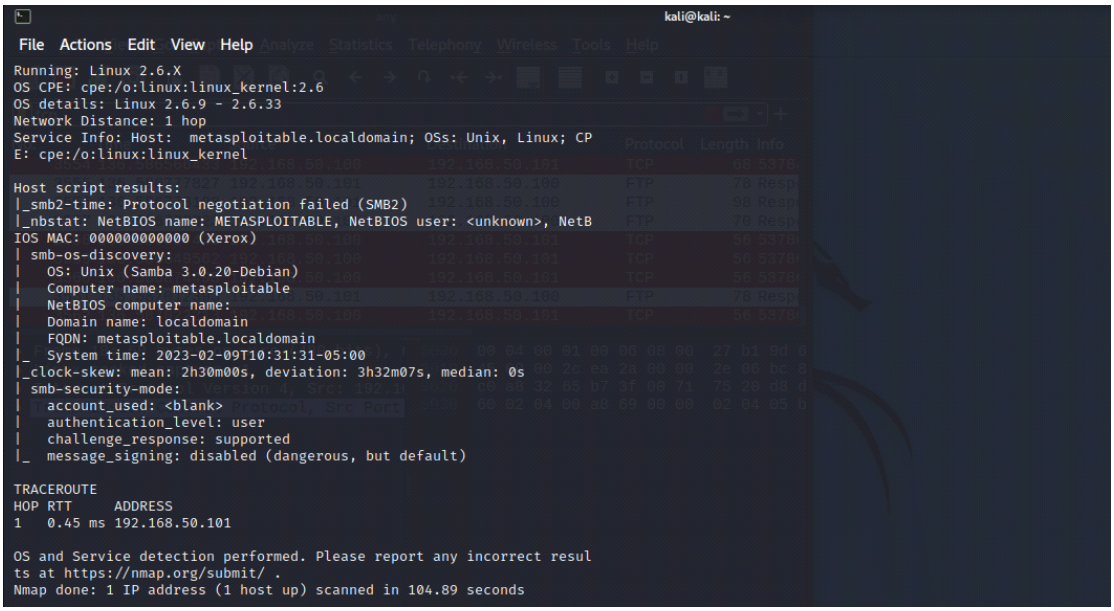
Questo secondo comando: "nmap -sT" esegue una scansione più invasiva

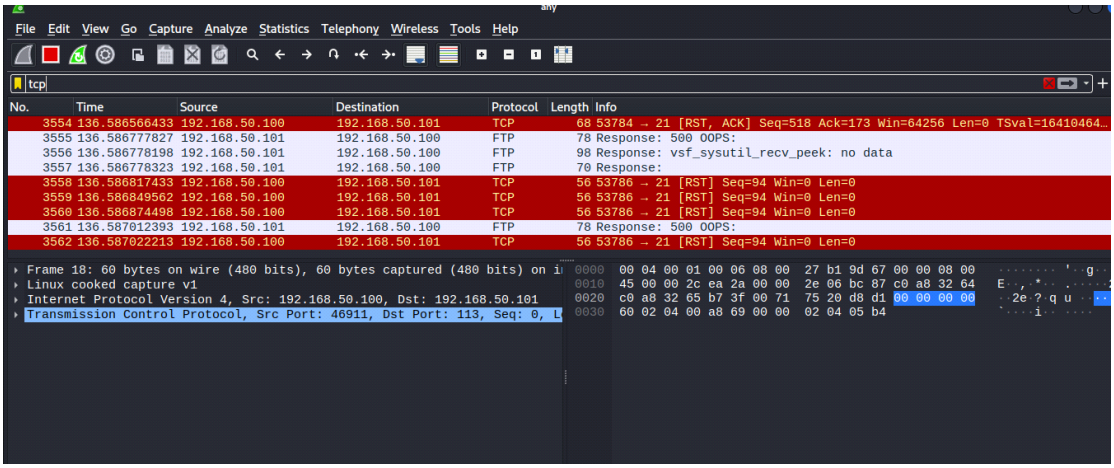
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -p21 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 10:11 EST
Nmap scan report for 192.168.50.101
Host is up (0.00033s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 08:00:27:D1:6A:10 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```



Con questo comando ho eseguito la scansione di tipo TCP sulle porte well-know. L'IP 192.168.50.101 è attivo e nmap ha trovato diversi servizi in porte aperte




kali@kali: ~
File Actions Edit View Help
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CP
E: cpe:/o:linux:linux_kernel
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetB
IOS MAC: 000000000000 (Xerox)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2023-02-09T10:31:31-05:00
|_clock-skew: mean: 2h30m00s, deviation: 3h32m07s, median: 0s
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
TRACEROUTE
HOP RTT ADDRESS
1 0.45 ms 192.168.50.101
OS and Service detection performed. Please report any incorrect resul
ts at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 104.89 seconds


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
3554 136.586566433 192.168.50.100 192.168.50.101 TCP 68 53784 → 21 [RST, ACK] Seq=518 Ack=173 Win=64256 Len=0 TSval=16410464…
3555 136.586777827 192.168.50.101 192.168.50.100 FTP 78 Response: 500 OOPS:
3556 136.586778198 192.168.50.101 192.168.50.100 FTP 98 Response: vsf_sysutil_recv_peek: no data
3557 136.586778323 192.168.50.101 192.168.50.100 FTP 70 Response:
3558 136.586817433 192.168.50.100 192.168.50.101 TCP 56 53786 → 21 [RST] Seq=94 Win=0 Len=0
3559 136.586849562 192.168.50.100 192.168.50.101 TCP 56 53786 → 21 [RST] Seq=94 Win=0 Len=0
3560 136.586874498 192.168.50.100 192.168.50.101 TCP 56 53786 → 21 [RST] Seq=94 Win=0 Len=0
3561 136.587012393 192.168.50.101 192.168.50.100 FTP 78 Response: 500 OOPS:
3562 136.587022213 192.168.50.100 192.168.50.101 TCP 56 53786 → 21 [RST] Seq=94 Win=0 Len=0
Frame 18: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on i
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
Transmission Control Protocol, Src Port: 46911, Dst Port: 113, Seq: 0, L
0000 00 04 00 01 00 06 08 00 27 b1 9d 67 00 00 08 00
0010 45 00 00 2c ea 2a 00 00 2e 06 bc 87 c0 a8 32 64
0020 c0 a8 32 65 b7 3f 00 71 75 20 d8 d1 00 00 00 00
0030 60 02 04 00 a8 69 00 00 02 04 05 b4