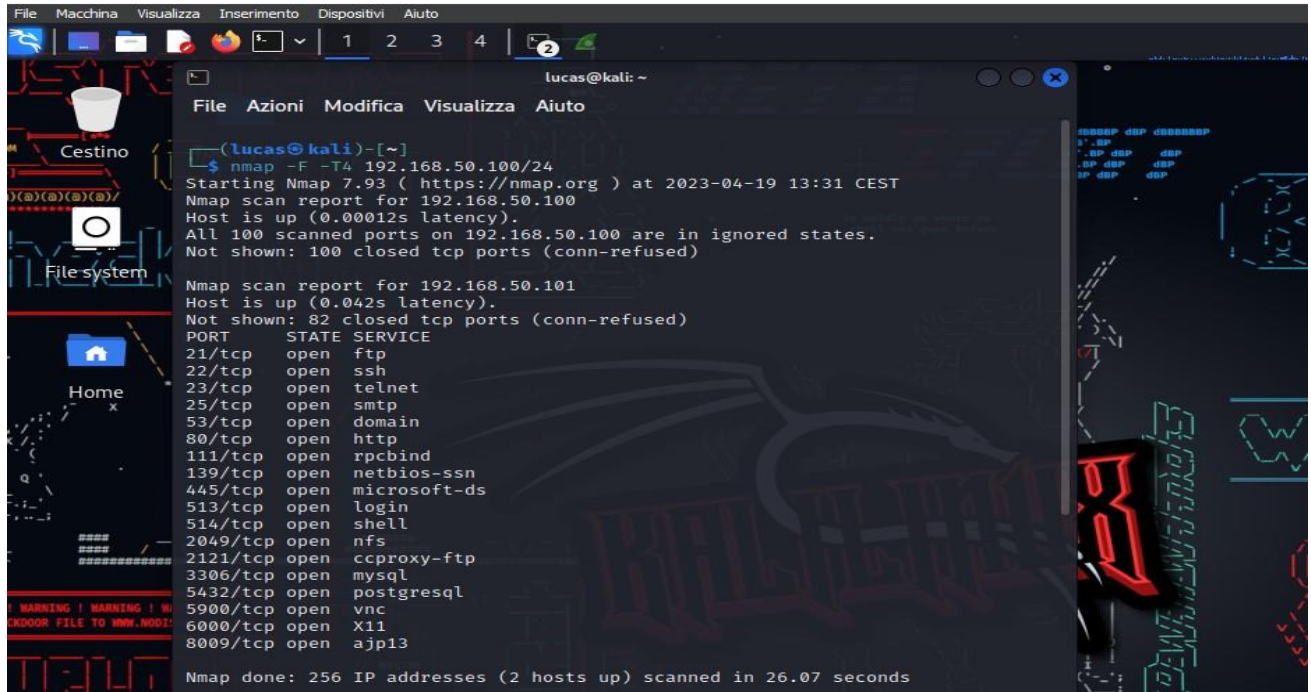
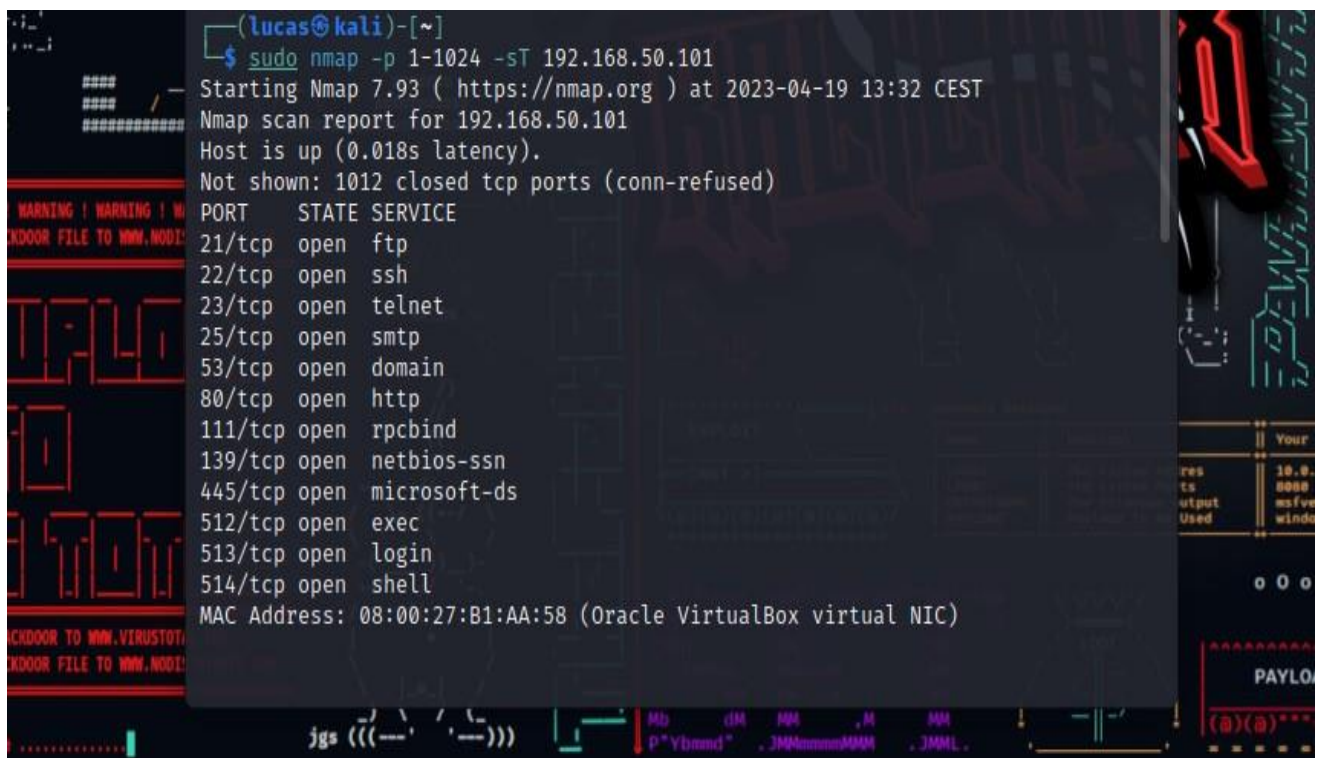


Scan veloce della rete per trovare gli host up, partendo dall'IP della macchina attaccante con lo /24 per scansionare tutta la subnet



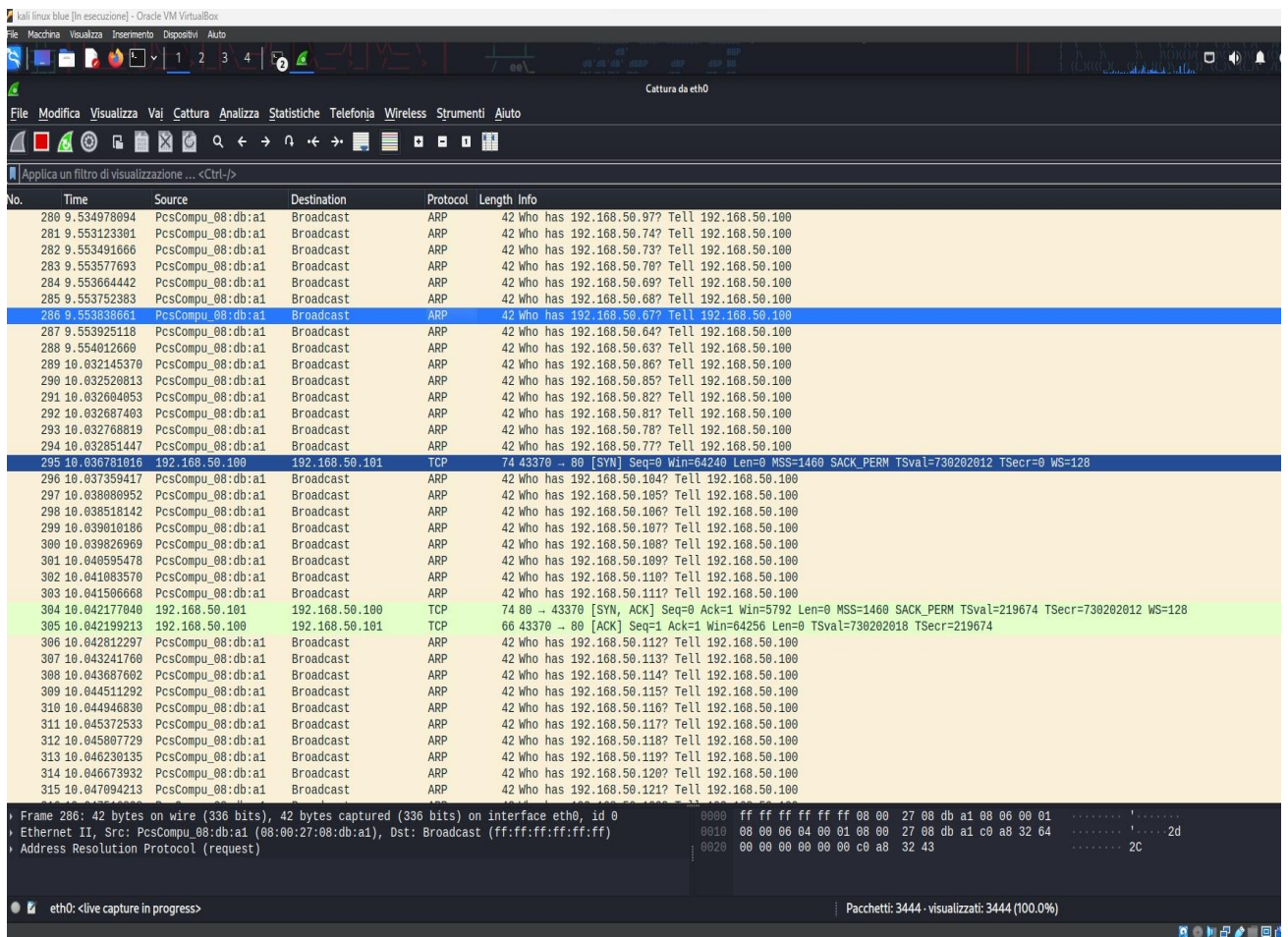
```
lucas@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(lucas@kali)-[~]  
$ nmap -F -T4 192.168.50.100/24  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19 13:31 CEST  
Nmap scan report for 192.168.50.100  
Host is up (0.00012s latency).  
All 100 scanned ports on 192.168.50.100 are in ignored states.  
Not shown: 100 closed tcp ports (conn-refused)  
  
Nmap scan report for 192.168.50.101  
Host is up (0.042s latency).  
Not shown: 82 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  
513/tcp   open  login  
514/tcp   open  shell  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
8009/tcp  open  ajp13  
  
Nmap done: 256 IP addresses (2 hosts up) scanned in 26.07 seconds
```

Scan con TCP



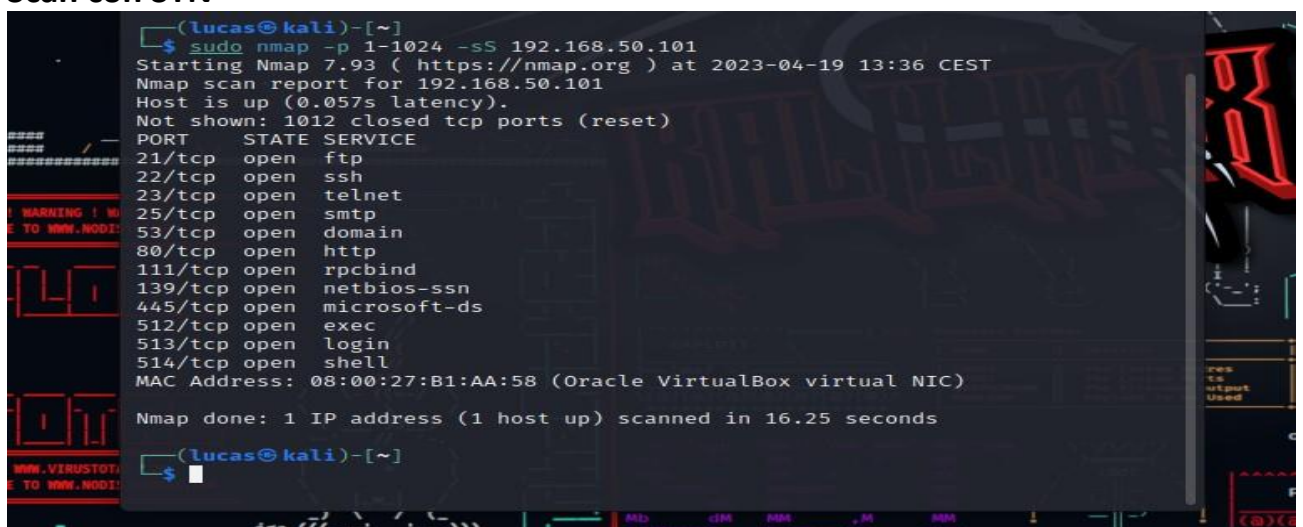
```
(lucas@kali)-[~]  
$ sudo nmap -p 1-1024 -sT 192.168.50.101  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19 13:32 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.018s latency).  
Not shown: 1012 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    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  
MAC Address: 08:00:27:B1:AA:58 (Oracle VirtualBox virtual NIC)
```

Wireshark del TCP

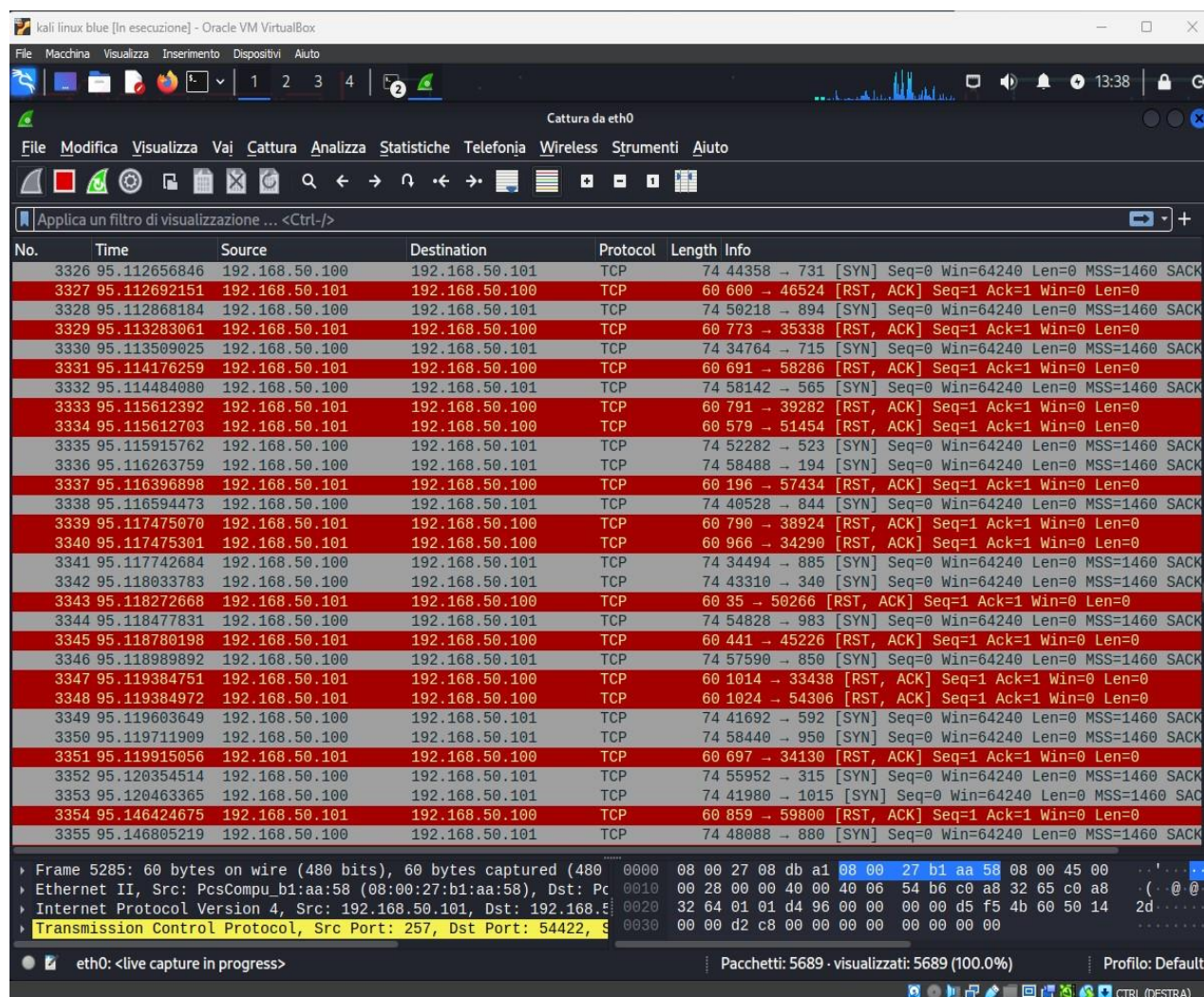


Qui possiamo vedere a sinistra la source in questo caso il pacchetto 384 è la risposta di meta alla richiesta di SYN di kali, dopo la freccina la porta sulla quale stanno comunicando, il pacchetto 385 indica la risposta del protocollo TCP, che non ci sarebbe stata con il SYN. concludendo il 3-way-handshake, stabiliamo un canale di comunicazione.

Scan con SYN



Wireshark con SYN



Qui si nota che non ci sono risposte da parte di kali alla ACK di meta perche la porta chiusa con RST,ACK e non conclude il 3-way-handshake ritornando indietro, non risultano servizi attivi.

Scansione con -A

```
Nmap done: 1 IP address (1 host up) scanned in 16.25 seconds
(lucas@kali)-[~]
$ sudo nmap -p 1-1024 -A 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19 13:42 CEST
Nmap scan report for 192.168.50.101
Host is up (0.023s latency).
Not shown: 1012 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet?
25/tcp    open  smtp
|_smtp-commands: Couldn't establish connection on port 25
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         42552/tcp  mountd
|_   100005  1,2,3         60255/udp  mountd
|_   100021  1,3,4         48430/tcp  nlockmgr
|_   100021  1,3,4         51885/udp  nlockmgr
|_   100024  1             33767/tcp  status
|_   100024  1             46571/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?
513/tcp   open  login?
```



```
File Azioni Modifica Visualizza Aiuto
|_ 100024 1 46571/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?
513/tcp open login?
514/tcp open shell?
MAC Address: 08:00:27:B1:AA:58 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=4/19%OT=21%CT=1%CU=44161%PV=Y%DS=1%DC=D%G=Y%M=080027%TOS:M=643FD4F7%P=x86_64-pc-linux-gnu)SEQ(SP=C8%GCD=1%ISR=D2%TI=Z%CI=Z%II=I%TOS:S=4)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=OS:M5B4ST11NW7%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=1OS:6A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=0%AOS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=0%A=S+%F=AS%O=M5B4ST11OS:NW7%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40OS:%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%QOS:=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164OS:%UN=0%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 7m26s, deviation: 2h49m43s, median: -1h52m34s
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-os-discovery:
|_OS: Unix (Samba 3.0.20-Debian)
|_Computer name: metasploitable
|_NetBIOS computer name:
|_Domain name: localdomain
|_FQDN: metasploitable.localdomain
|_System time: 2023-04-19T05:53:21-04:00
|_smb-security-mode:
|_account_used: guest
|_authentication_level: user
|_challenge_response: supported
|_message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT ADDRESS
1 23.25 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 326.82 seconds

(lucas@kali)-[~]
```

Scan -A ci permette di recuperare molte informazioni utili sull'ip target, sistema operativo servizi disponibili in ascolto sulle porte aperte. é lo scan piu invasivo.

Wireshark di -A

[illegible]