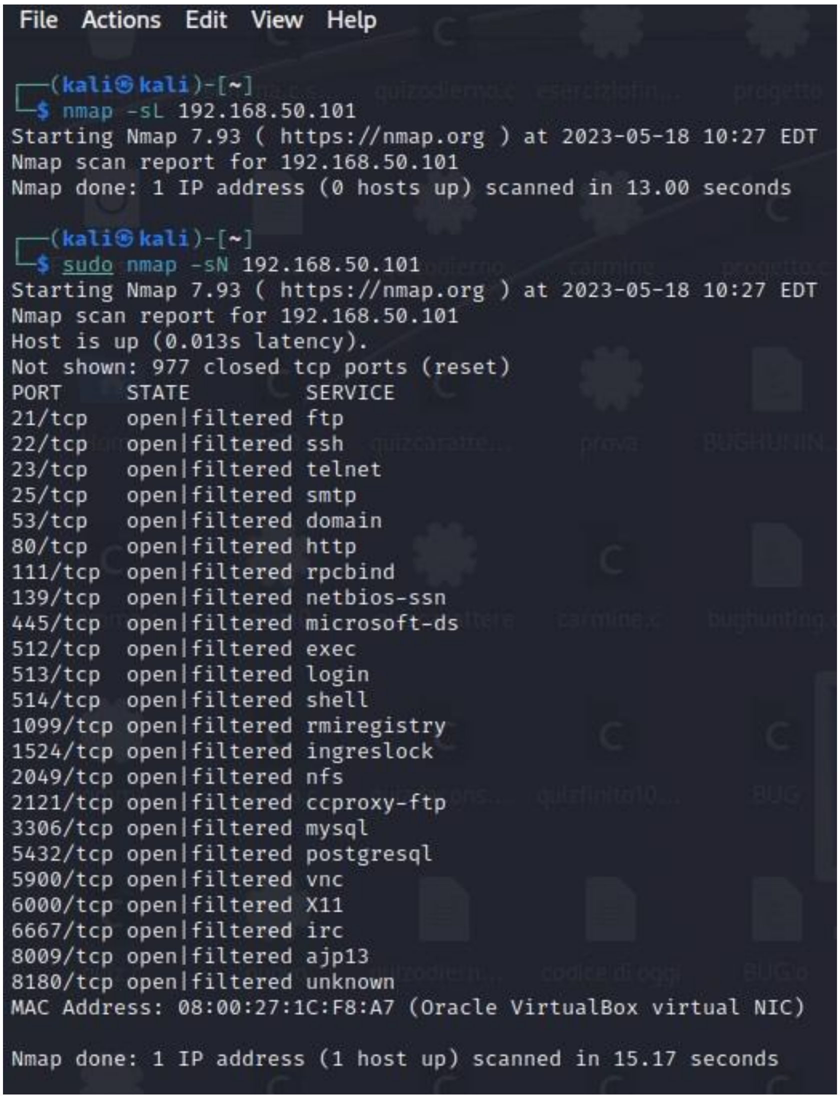
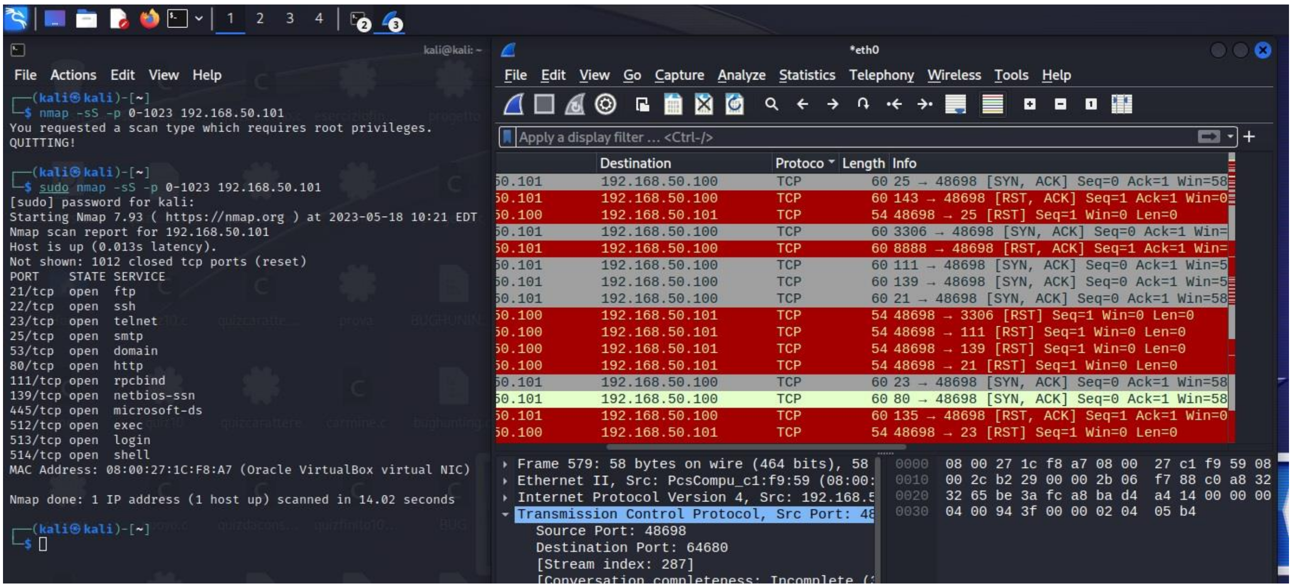
NMAP

Ho eseguito il comando nmap -sL 192.168.50.101 (ip di metasploitable) per avere la lista di tutte le macchine target da scansionare. Con il comando nmap -sN ho controllato se l'host trovato con il precedente comando è attivo tramite protocollo ping, senza effettuare nessun scan invasivo (poiché non vi è tentativo di creare una sessione)



```
┌──(kali㉿kali)-[~]
└─$ nmap -sL 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:27 EDT
Nmap scan report for 192.168.50.101
Nmap done: 1 IP address (0 hosts up) scanned in 13.00 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sN 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:27 EDT
Nmap scan report for 192.168.50.101
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:1C:F8:A7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.17 seconds
```

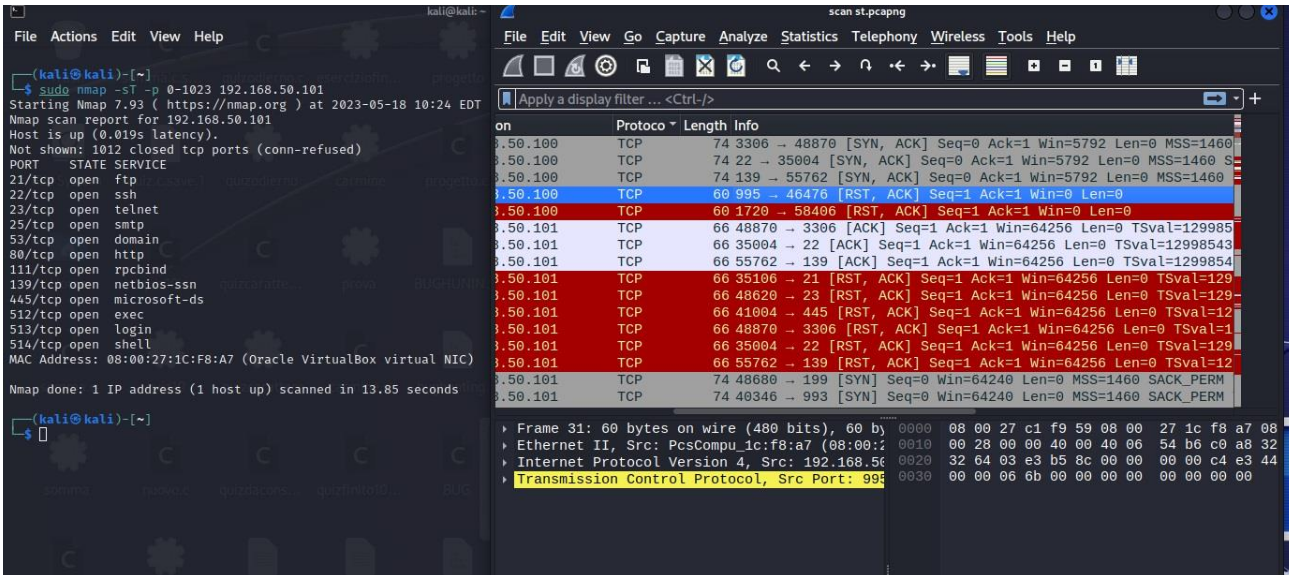
In seguito ho effettuato un syn scan con il comando nmap -Ss -P 0-1023 192.168.50.101, intercettando il traffico con Wireshark.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p 0-1023 192.168.50.101
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 0-1023 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:21 EDT
Nmap scan report for 192.168.50.101
Host is up (0.013s latency).
Not shown: 1012 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
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: 08:00:27:1C:F8:A7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.02 seconds

┌──(kali㉿kali)-[~]
└─$ ▯
```

```
        Destination     Protoco Length Info
50.101  192.168.50.100  TCP     60 25 → 48698 [SYN, ACK] Seq=0 Ack=1 Win=58
50.101  192.168.50.100  TCP     60 143 → 48698 [RST, ACK] Seq=1 Ack=1 Win=0
50.100  192.168.50.101  TCP     54 48698 → 25 [RST] Seq=1 Win=0 Len=0
50.101  192.168.50.100  TCP     60 3306 → 48698 [SYN, ACK] Seq=0 Ack=1 Win=
50.101  192.168.50.100  TCP     60 8888 → 48698 [RST, ACK] Seq=1 Ack=1 Win=
50.101  192.168.50.100  TCP     60 111 → 48698 [SYN, ACK] Seq=0 Ack=1 Win=5
50.101  192.168.50.100  TCP     60 139 → 48698 [SYN, ACK] Seq=0 Ack=1 Win=5
50.101  192.168.50.100  TCP     60 21 → 48698 [SYN, ACK] Seq=0 Ack=1 Win=58
50.100  192.168.50.101  TCP     54 48698 → 3306 [RST] Seq=1 Win=0 Len=0
50.100  192.168.50.101  TCP     54 48698 → 111 [RST] Seq=1 Win=0 Len=0
50.100  192.168.50.101  TCP     54 48698 → 139 [RST] Seq=1 Win=0 Len=0
50.100  192.168.50.101  TCP     54 48698 → 21 [RST] Seq=1 Win=0 Len=0
50.101  192.168.50.100  TCP     60 23 → 48698 [SYN, ACK] Seq=0 Ack=1 Win=58
50.101  192.168.50.100  TCP     60 80 → 48698 [SYN, ACK] Seq=0 Ack=1 Win=58
50.101  192.168.50.100  TCP     60 135 → 48698 [RST, ACK] Seq=1 Ack=1 Win=0
50.100  192.168.50.101  TCP     54 48698 → 23 [RST] Seq=1 Win=0 Len=0

› Frame 579: 58 bytes on wire (464 bits), 58       0000  08 00 27 1c f8 a7 08 00  27 c1 f9 59 08
› Ethernet II, Src: PcsCompu_c1:f9:59 (08:00:      0010  00 2c b2 29 00 00 2b 06  f7 88 c0 a8 32
› Internet Protocol Version 4, Src: 192.168.5      0020  32 65 be 3a fc a8 ba d4  a4 14 00 00 00
⌄ Transmission Control Protocol, Src Port: 48     0030  04 00 94 3f 00 00 02 04  05 b4
    Source Port: 48698
    Destination Port: 64680
    [Stream index: 287]
    [Conversation completeness: Incomplete (
```

In seguito ho effettuato una scansione TCP sulle porte well know con target 192.168.50.101 con il comando nmap -sT -P 0-1023 192.168.50.101, catturando il traffico su Wireshark.



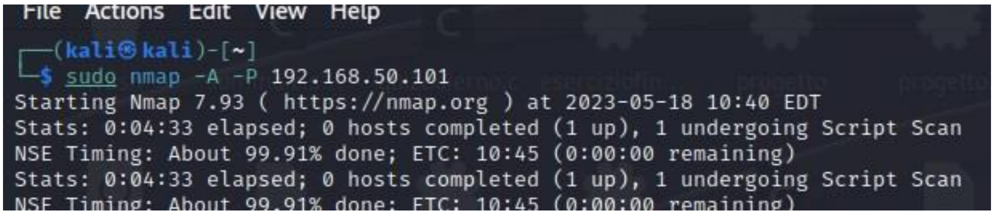
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -p 0-1023 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:24 EDT
Nmap scan report for 192.168.50.101
Host is up (0.019s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
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: 08:00:27:1C:F8:A7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.85 seconds

┌──(kali㉿kali)-[~]
└─$ ▯
```

```
on       Protoco Length Info
.50.100  TCP     74 3306 → 48870 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
.50.100  TCP     74 22 → 35004 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 S
.50.100  TCP     74 139 → 55762 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
.50.100  TCP     60 995 → 46476 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100  TCP     60 1720 → 58406 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.101  TCP     66 48870 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=129985
.50.101  TCP     66 35004 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=12998543
.50.101  TCP     66 55762 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1299854
.50.101  TCP     66 35106 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=129
.50.101  TCP     66 48620 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=129
.50.101  TCP     66 41004 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=12
.50.101  TCP     66 48870 → 3306 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1
.50.101  TCP     66 35004 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=129
.50.101  TCP     66 55762 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=12
.50.101  TCP     74 48680 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
.50.101  TCP     74 40346 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM

› Frame 31: 60 bytes on wire (480 bits), 60 by     0000  08 00 27 c1 f9 59 08 00  27 1c f8 a7 08
› Ethernet II, Src: PcsCompu_1c:f8:a7 (08:00:2    0010  00 28 00 00 40 00 40 06  54 b6 c0 a8 32
› Internet Protocol Version 4, Src: 192.168.50    0020  32 64 03 e3 b5 8c 00 00  00 00 c4 e3 44
› Transmission Control Protocol, Src Port: 995    0030  00 00 06 6b 00 00 00 00  00 00 00 00
```

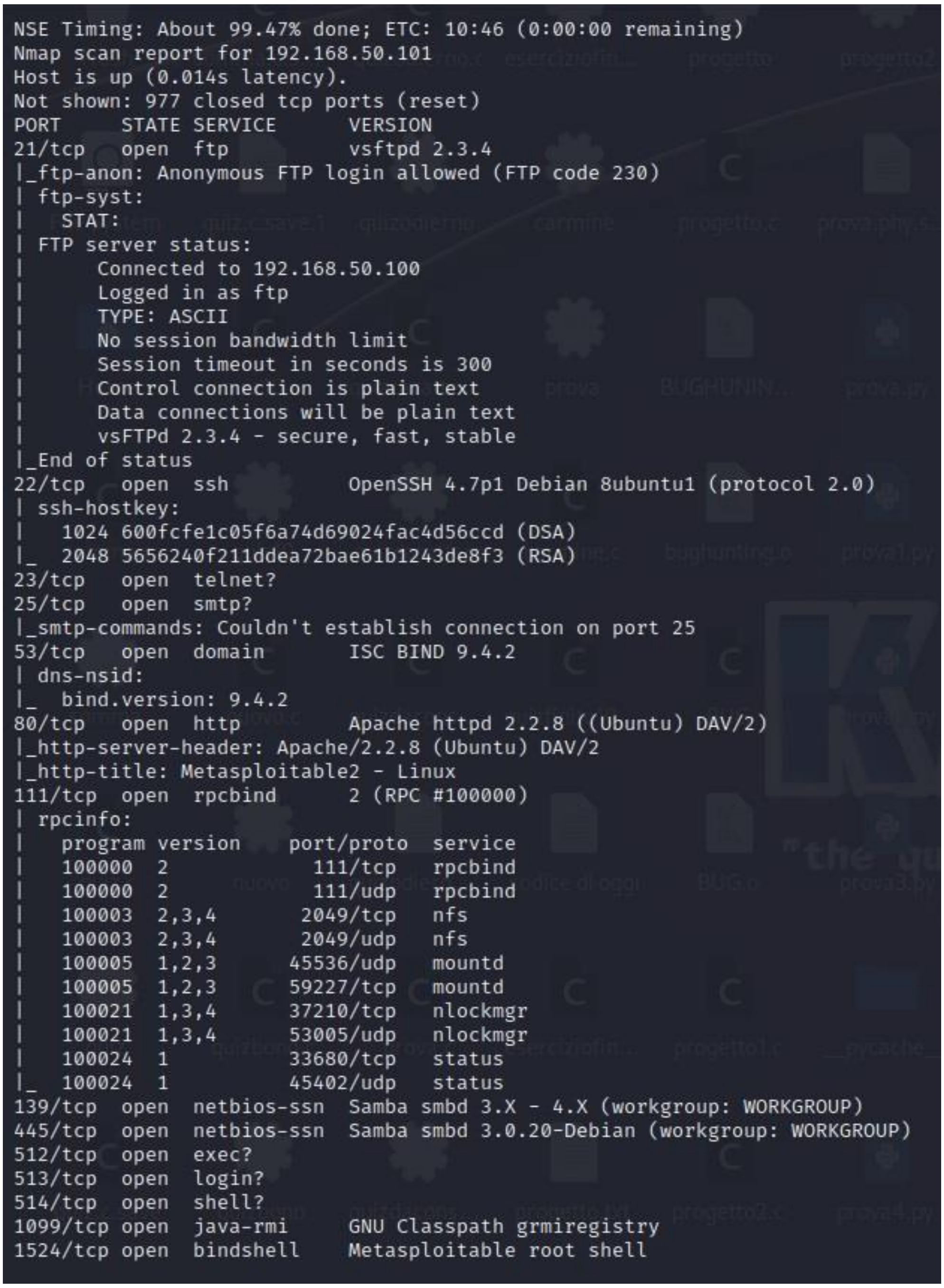
DIFFERENZA SYN SCAN E TCP SCAN

Dopo aver intercettato il traffico con Wireshark ho notato una differenza sostanziale. Con il syn scan (nmap -sS) ho notato che questo metodo, essendo meno invasivo rispetto al TCP Scan (nmap -sT), una volta appurato che una porta è aperta chiudeva la comunicazione, non completando i passaggi del 3-way-handshake. Nello specifico ho trovato che nelle info dei vari pacchetti intercettati ho trovato [RST], mentre nel TCP Scan ho notato che nelle info vi è [RST, ACK], e non il singolo [RST].

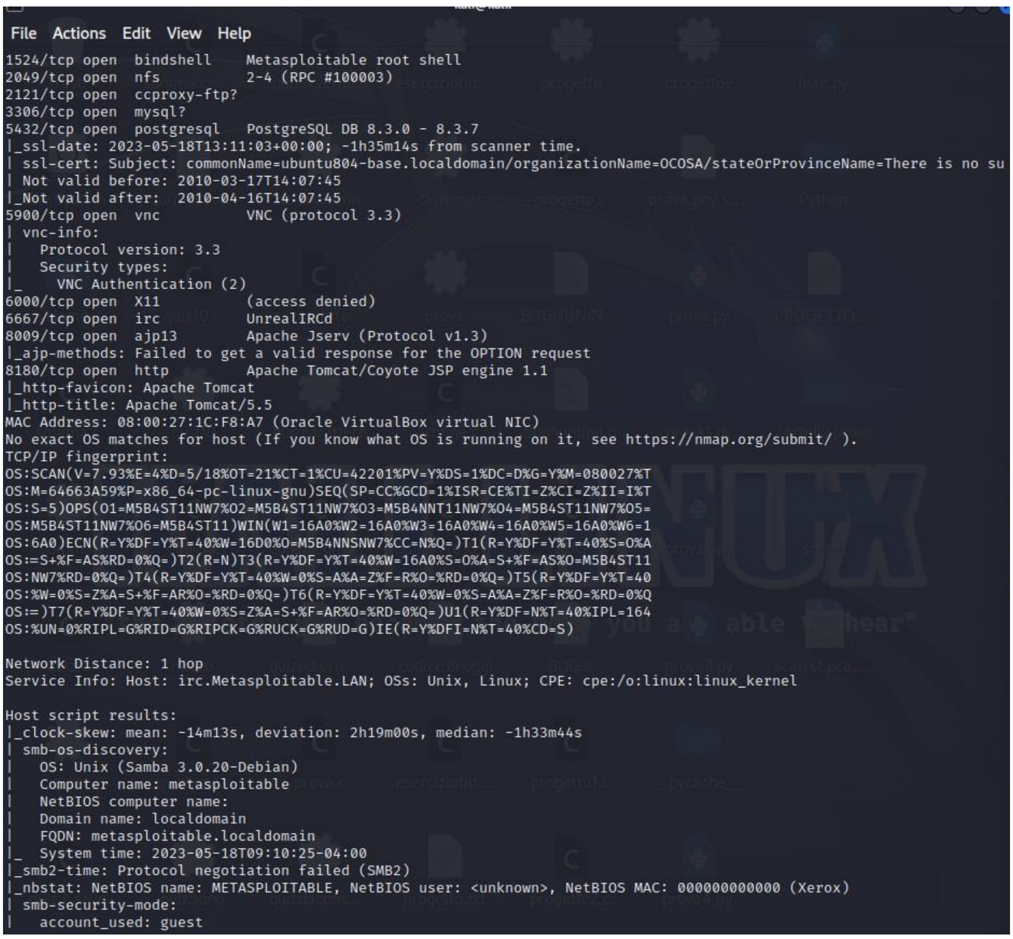
Ho eseguito altresì una scan aggressive con il comando sudo nmap -A 192.168.50.101. Opzione che abilita l'OS detenction -O, il version scanning -sv, lo script scanning -sc e il traceroute –traceroute. Ho utilizzato il comando sudo per inviare il comando, attivando i permessi di root.



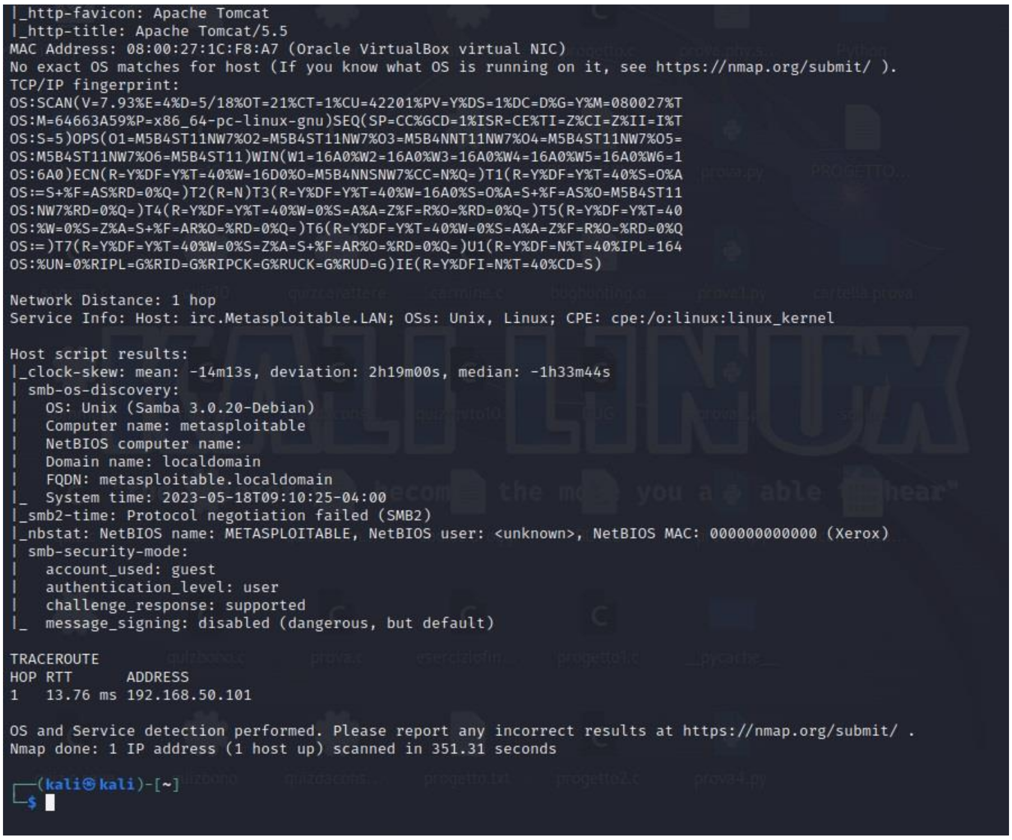
```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -P 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 10:40 EDT
Stats: 0:04:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.91% done; ETC: 10:45 (0:00:00 remaining)
Stats: 0:04:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.91% done; ETC: 10:45 (0:00:00 remaining)
```



```
NSE Timing: About 99.47% done; ETC: 10:46 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.014s latency).
Not shown: 977 closed tcp ports (reset)
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?
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      45536/udp   mountd
|   100005  1,2,3      59227/tcp   mountd
|   100021  1,3,4      37210/tcp   nlockmgr
|   100021  1,3,4      53005/udp   nlockmgr
|   100024  1          33680/tcp   status
|_  100024  1          45402/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?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
```



```
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-05-18T13:11:03+00:00; -1h35m14s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc          VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:1C:F8:A7 (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=5/18%OT=21%CT=1%CU=42201%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=64663A59%P=x86_64-pc-linux-gnu)SEQ(SP=CC%GCD=1%ISR=CE%TI=Z%CI=Z%II=I%T
OS:S=5)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=1
OS:6A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11
OS: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=40
OS:%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%Q
OS:=)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=164
OS:%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -14m13s, deviation: 2h19m00s, median: -1h33m44s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-05-18T09:10:25-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-security-mode:
|   account_used: guest
```



```
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:1C:F8:A7 (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=5/18%OT=21%CT=1%CU=42201%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=64663A59%P=x86_64-pc-linux-gnu)SEQ(SP=CC%GCD=1%ISR=CE%TI=Z%CI=Z%II=I%T
OS:S=5)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=1
OS:6A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11
OS: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=40
OS:%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%Q
OS:=)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=164
OS:%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -14m13s, deviation: 2h19m00s, median: -1h33m44s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-05-18T09:10:25-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT      ADDRESS
1   13.76 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 351.31 seconds

┌──(kali㉿kali)-[~]
└─$ 
```