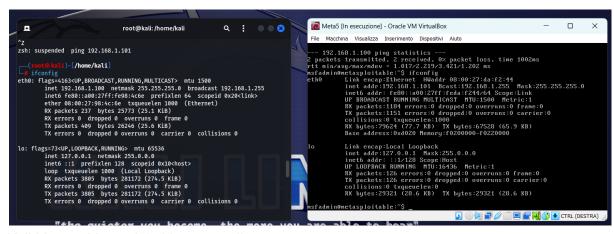
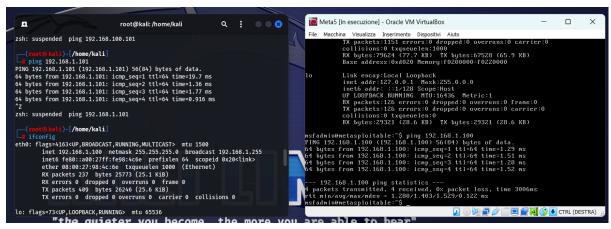
CONSEGNA S5/L3



Kali Linux e Metasploitable sono sulla stessa rete

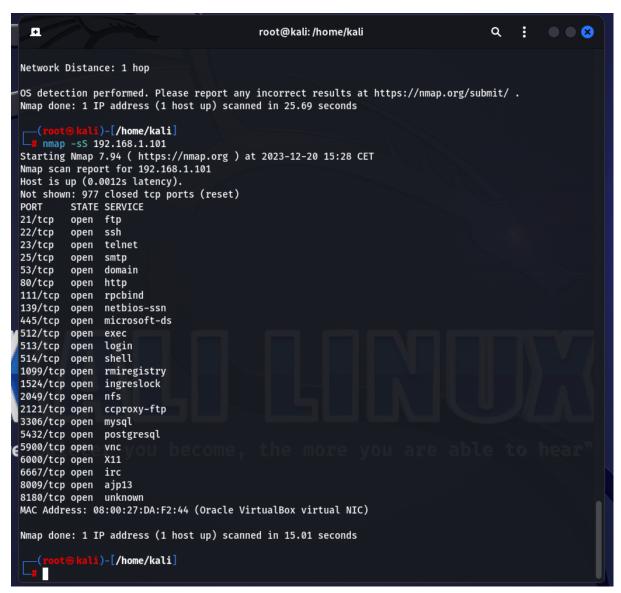


Le due macchine pingano correttamente

```
Q : 0 ×
  \blacksquare
                                            root@kali: /home/kali
(root@ kali)-[/home/kalinmap -0 192.168.1.101
     root⊛kali)-[/home/kali]
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 14:59 CET
Nmap scan report for 192.168.1.101
Host is up (0.0076s latency).
Not shown: 977 closed tcp ports (reset)
        STATE SERVICE
PORT
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
1099/tcp open rmiregistry
1524/tcp open ingreslock
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
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:DA:F2:44 (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=7.94%E=4%D=12/20%OT=21%CT=1%CU=32469%PV=Y%DS=1%DC=D%G=Y%M=080027%
OS:TM=6582F367%P=x86_64-pc-linux-gnu)SEQ(SP=CD%GCD=1%ISR=CD%TI=Z%CI=Z%II=I%
OS:TS=5)SEQ(SP=CF%GCD=1%ISR=CF%TI=Z%CI=Z%II=I%TS=5)SEQ(SP=D0%GCD=1%ISR=CF%T
OS:I=Z%CI=Z%II=I%TS=5)OPS(01=M5B4ST11NW7%02=M5B4ST11NW7%03=M5B4NNT11NW7%04=
OS:M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16
OS:A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW7%CC=N%Q=)T1(R=Y%
OS:DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=0%A=S+%
OS:F=AS%O=M5B4ST11NW7%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
```

```
53/tcp
         open domain
80/tcp open http
111/tcp open rpcbi
                rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
 512/tcp open
                exec
513/tcp open login
514/tcp open shell
 1099/tcp open
                rmiregistry
 1524/tcp open ingreslock
 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
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:DA:F2:44 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
OS:SCAN(V=7.94%E=4%D=12/20%OT=21%CT=1%CU=32469%PV=Y%DS=1%DC=D%G=Y%M=080027%
OS:TM=6582F367%P=x86_64-pc-linux-gnu)SEQ(SP=CD%GCD=1%ISR=CD%TI=Z%CI=Z%II=I%
OS:TS=5)SEQ(SP=CF%GCD=1%ISR=CF%TI=Z%CI=Z%II=I%TS=5)SEQ(SP=D0%GCD=1%ISR=CF%T
OS:I=Z%CI=Z%II=I%TS=5)OPS(01=M5B4ST11NW7%02=M5B4ST11NW7%03=M5B4NNT11NW7%04=
OS:M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16
OS:A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW7%CC=N%Q=)T1(R=Y%
OS:DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=0%A=S+%
OS:F=AS%O=M5B4ST11NW7%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.69 seconds
```

OS Fingerprint su Metasploitable



SYN Scan su Metasploitable

```
<mark>(ali</mark>)-[/home/kali]
 (root⊕ kali)-[/home/kal:
# nmap -sT 192.168.1.101
 Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 15:39 CET
 Nmap scan report for 192.168.1.101
 Host is up (0.022s latency).
 Not shown: 977 closed tcp ports (conn-refused)
 PORT
           STATE SERVICE
21/tcp
22/tcp
           open ftp
           open ssh
 23/tcp
25/tcp
           open telnet
           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
1099/tcp open rmiregistry
1524/tcp open ingreslock
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
6667/tcp open irc
 8009/tcp open ajp13
 8180/tcp open unknown
MAC Address: 08:00:27:DA:F2:44 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds
```

TCP Scan su Metasploitable

```
Q : 0 ×
  Ξ
                                              root@kali:/home/kali
Try: apt install <deb name>
             li)-[/home/kali]
 mmap 192.168.1.101 --script smb-os-discovery
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 16:06 CET
Nmap scan report for 192.168.1.101
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (reset)
PORT
          STATE SERVICE
21/tcp
          open ftp
22/tcp
          open ssh
23/tcp
         open telnet
25/tcp
          open smtp
         open domain
53/tcp
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsof0
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
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
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:DA:F2:44 (Oracle VirtualBox virtual NIC)
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: 2023-12-20T08:44:22-05:00
Nmap done: 1 IP address (1 host up) scanned in 15.01 seconds
```

Version detection su Metasploitable

```
li)-[/home/kali]
 map -0 192.168.1.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 16:11 CET
Nmap scan report for 192.168.1.102
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.1.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:CA:C7:C8 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedd
ed, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:mic
rosoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_se
rver_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Sta
ndard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.60 seconds
```

OS Fingerprint su Windows 7