Consegna S5/L3

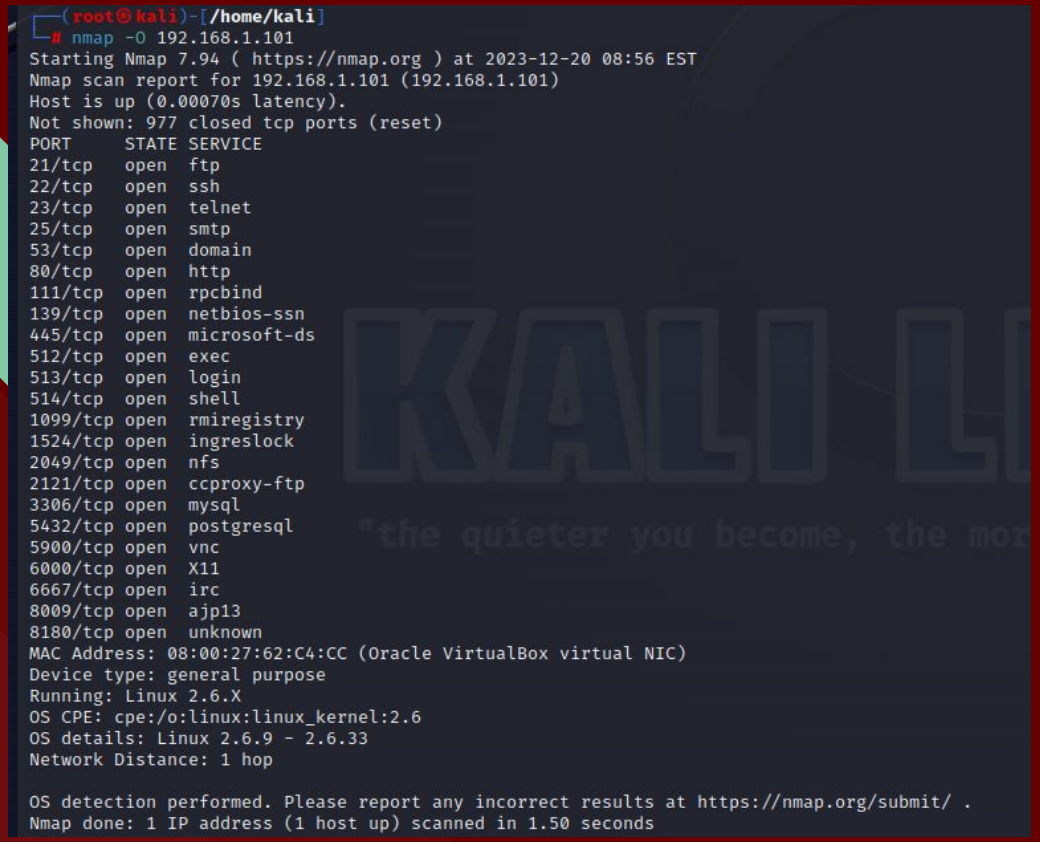
Come prima operazione verifichiamo il ping tra le due macchine

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.661 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.547 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=0.625 ms
64 bytes from 192.168.1.101: icmp_seq=4 ttl=64 time=0.539 ms
64 bytes from 192.168.1.101: icmp_seq=5 ttl=64 time=0.547 ms
64 bytes from 192.168.1.101: icmp_seq=6 ttl=64 time=0.354 ms
64 bytes from 192.168.1.101: icmp_seq=7 ttl=64 time=0.568 ms
64 bytes from 192.168.1.101: icmp_seq=8 ttl=64 time=0.606 ms
64 bytes from 192.168.1.101: icmp_seq=9 ttl=64 time=0.672 ms
64 bytes from 192.168.1.101: icmp_seq=10 ttl=64 time=0.314 ms
64 bytes from 192.168.1.101: icmp_seq=11 ttl=64 time=0.531 ms
64 bytes from 192.168.1.101: icmp_seq=12 ttl=64 time=0.602 ms
64 bytes from 192.168.1.101: icmp_seq=13 ttl=64 time=0.591 ms
64 bytes from 192.168.1.101: icmp_seq=14 ttl=64 time=0.870 ms
64 bytes from 192.168.1.101: icmp_seq=15 ttl=64 time=0.767 ms
64 bytes from 192.168.1.101: icmp_seq=16 ttl=64 time=0.669 ms
64 bytes from 192.168.1.101: icmp_seq=17 ttl=64 time=0.724 ms
64 bytes from 192.168.1.101: icmp_seq=18 ttl=64 time=0.714 ms
64 bytes from 192.168.1.101: icmp_seq=19 ttl=64 time=0.937 ms
64 bytes from 192.168.1.101: icmp_seq=20 ttl=64 time=0.848 ms
64 bytes from 192.168.1.101: icmp_seq=21 ttl=64 time=0.795 ms
64 bytes from 192.168.1.101: icmp_seq=22 ttl=64 time=0.895 ms
64 bytes from 192.168.1.101: icmp_seq=23 ttl=64 time=0.553 ms
^C
── 192.168.1.101 ping statistics ──
23 packets transmitted, 23 received, 0% packet loss, time 22325ms
rtt min/avg/max/mdev = 0.314/0.649/0.937/0.154 ms
```

```
msfadmin@metasploitable:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.760 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.664 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.653 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=4.08 ms
64 bytes from 192.168.1.100: icmp_seq=5 ttl=64 time=0.604 ms
64 bytes from 192.168.1.100: icmp_seq=6 ttl=64 time=0.760 ms
64 bytes from 192.168.1.100: icmp_seq=7 ttl=64 time=1.02 ms
64 bytes from 192.168.1.100: icmp_seq=8 ttl=64 time=1.01 ms
64 bytes from 192.168.1.100: icmp_seq=9 ttl=64 time=0.871 ms
64 bytes from 192.168.1.100: icmp_seq=10 ttl=64 time=0.576 ms
64 bytes from 192.168.1.100: icmp_seq=11 ttl=64 time=0.737 ms

--- 192.168.1.100 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 9994ms
rtt min/avg/max/mdev = 0.576/1.068/4.087/0.965 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

OS fingerprint Metasploitable



Syn Scan Metasploitable

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sS 192.168.1.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 09:06 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:62:C4:CC (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linu
x; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 64.50 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sT 192.168.1.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 09:12 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00015s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:62:C4:CC (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linu
x; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 64.00 seconds
```

Stesso procedimento anche per Windows. Quindi come prima operazione verifichiamo il ping tra le due macchine

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.102
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
64 bytes from 192.168.1.102: icmp_seq=1 ttl=128 time=0.363 ms
64 bytes from 192.168.1.102: icmp_seq=2 ttl=128 time=0.268 ms
64 bytes from 192.168.1.102: icmp_seq=3 ttl=128 time=0.363 ms
64 bytes from 192.168.1.102: icmp_seq=4 ttl=128 time=0.311 ms
64 bytes from 192.168.1.102: icmp_seq=5 ttl=128 time=0.657 ms
64 bytes from 192.168.1.102: icmp_seq=6 ttl=128 time=0.490 ms
64 bytes from 192.168.1.102: icmp_seq=7 ttl=128 time=0.244 ms
64 bytes from 192.168.1.102: icmp_seq=8 ttl=128 time=0.313 ms
64 bytes from 192.168.1.102: icmp_seq=9 ttl=128 time=0.665 ms
64 bytes from 192.168.1.102: icmp_seq=10 ttl=128 time=0.698 ms
64 bytes from 192.168.1.102: icmp_seq=11 ttl=128 time=0.540 ms
64 bytes from 192.168.1.102: icmp_seq=12 ttl=128 time=0.294 ms
^C
── 192.168.1.102 ping statistics ──
12 packets transmitted, 12 received, 0% packet loss, time 11219ms
rtt min/avg/max/mdev = 0.244/0.433/0.698/0.160 ms
```

```
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

OS fingerprint Windows

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 09:58 EST
Nmap scan report for 192.168.1.102 (192.168.1.102)
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.1.102 (192.168.1.102) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:67:2C:55 (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 embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 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 22.16 seconds
```