

CONSEGNA S5/L3

The image shows two side-by-side terminal windows. The left window is a Kali Linux terminal with the prompt 'root@kali: /home/kali'. It displays the output of the 'ifconfig' command for the 'eth0' interface, showing IP address 192.168.1.100, netmask 255.255.255.0, and broadcast 192.168.1.255. It also shows the output of 'lo: flags=73<UP,LOOPBACK,RUNNING>' for the loopback interface. The right window is a Metasploitable VM terminal with the prompt 'msfadmin@metasploitable:~'. It displays the output of the 'ifconfig' command for the 'eth0' interface, showing IP address 192.168.1.101, netmask 255.255.255.0, and broadcast 192.168.1.255. It also shows the output of 'lo: flags=73<UP,LOOPBACK,RUNNING>' for the loopback interface.

```
root@kali: /home/kali
^Z
zsh: suspended ping 192.168.1.101

(root@kali)~[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe98:4c6e prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:98:4c:6e txqueuelen 1000 (Ethernet)
    RX packets 237 bytes 25773 (25.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 409 bytes 26246 (25.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3805 bytes 281172 (274.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3805 bytes 281172 (274.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msfadmin@metasploitable:~
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.101 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe98:4c6e prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:98:4c:6e txqueuelen 1000 (Ethernet)
    RX packets 237 bytes 25773 (25.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 409 bytes 26246 (25.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3805 bytes 281172 (274.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3805 bytes 281172 (274.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Kali Linux e Metasploitable sono sulla stessa rete

The image shows two side-by-side terminal windows. The left window is a Kali Linux terminal with the prompt 'root@kali: /home/kali'. It displays the output of the 'ping 192.168.1.101' command, showing successful ping results with 64 bytes of data and a time of 19.7 ms. The right window is a Metasploitable VM terminal with the prompt 'msfadmin@metasploitable:~'. It displays the output of the 'ping 192.168.1.100' command, showing successful ping results with 64 bytes of data and a time of 1.29 ms.

```
root@kali: /home/kali
zsh: suspended ping 192.168.1.101

(root@kali)~[/home/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=19.7 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=1.36 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=1.77 ms
64 bytes from 192.168.1.101: icmp_seq=4 ttl=64 time=0.916 ms
^Z
zsh: suspended ping 192.168.1.101

(root@kali)~[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe98:4c6e prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:98:4c:6e txqueuelen 1000 (Ethernet)
    RX packets 237 bytes 25773 (25.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 409 bytes 26246 (25.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

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=1.29 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=1.51 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=1.28 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=1.52 ms

--- 192.168.1.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/ndev = 1.280/1.403/1.529/0.122 ms
msfadmin@metasploitable:~
```

Le due macchine pingano correttamente

```
root@kali: /home/kali

(root@kali)-[/home/kali]
# nmap -O 192.168.1.101
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)
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
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(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=
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=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%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  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(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=
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%O=%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

```
root@kali: /home/kali

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

(root@kali)-[/home/kali]
# nmap -sS 192.168.1.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 15:28 CET
Nmap scan report for 192.168.1.101
Host is up (0.0012s 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
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 15.01 seconds

(root@kali)-[/home/kali]
#
```

SYN Scan su Metasploitable

```
(root@kali)-[/home/kali]
# 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    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)

Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds
```

TCP Scan su Metasploitable

```
root@kali: /home/kali
Try: apt install <deb name>

(root@kali)-[/home/kali]
# nmap 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
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft
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


```
(root@kali)-[/home/kali]
# nmap -o 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 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 36.60 seconds
```

OS Fingerprint su Windows 7