

# Esercizio S5L2:

## SVOLGIMENTO:

```

META2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Last login: Tue Apr 29 08:59:27 EDT 2025 on ttty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 1636 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:04:0e:a4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe04:e464 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

```

Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: wind3.hub
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::1164:77ba:872b:1467%4
    Indirizzo IPv4. . . . . : 192.168.1.13
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:2c98:3f43:68b9:d17
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::2c98:3f43:68b9:d17%5
    Gateway predefinito . . . . . : ::

Scheda Tunnel isatap.wind3.hub:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione: wind3.hub
```

```

(pistacchio@pistacchio)-[~]
$ ping -c4 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.157 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.212 ms
64 bytes from 192.168.1.12: icmp_seq=4 ttl=64 time=0.164 ms

— 192.168.1.12 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.157/0.225/0.368/0.085 ms

(pistacchio@pistacchio)-[~]
$ ping -c4 192.168.1.13
PING 192.168.1.13 (192.168.1.13) 56(84) bytes of data.
64 bytes from 192.168.1.13: icmp_seq=1 ttl=128 time=0.377 ms
64 bytes from 192.168.1.13: icmp_seq=2 ttl=128 time=0.248 ms
64 bytes from 192.168.1.13: icmp_seq=3 ttl=128 time=0.240 ms
64 bytes from 192.168.1.13: icmp_seq=4 ttl=128 time=0.237 ms

— 192.168.1.13 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.237/0.275/0.377/0.058 ms
```

```

(pistacchio@pistacchio)-[~]
$ nmap -O 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 15:27 CEST
Nmap scan report for 192.168.1.12 (192.168.1.12)
Host is up (0.00017s 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: 08:00:27:04:0E:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 1.55 seconds

```

```

(pistacchio@pistacchio)-[~]
$ nmap -O 192.168.1.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 15:27 CEST
Nmap scan report for 192.168.1.13 (192.168.1.13)
Host is up (0.00019s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:41:3A:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 22.91 seconds

```

```
(pistacchio@pistacchio)-[~]
$ nmap -sS 192.168.1.12 (192.168.1.12)
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 15:57 CEST
Nmap scan report for 192.168.1.12 (192.168.1.12)
Host is up (0.000086s 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: 08:00:27:04:0E:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

```
(pistacchio@pistacchio)-[~]
$ nmap -sS 192.168.1.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 15:57 CEST
Nmap scan report for 192.168.1.13 (192.168.1.13)
Host is up (0.0035s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msqm-mgmt
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:41:3A:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
```

```
(pistacchio@pistacchio)-[~]
$ nmap -sT 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 16:03 CEST
Nmap scan report for 192.168.1.12 (192.168.1.12)
Host is up (0.00017s 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: 08:00:27:04:0E:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

```
(pistacchio@pistacchio)-[~]
$ nmap -sT 192.168.1.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 16:10 CEST
Nmap scan report for 192.168.1.13 (192.168.1.13)
Host is up (0.00018s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msqm-mgmt
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:41:3A:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.95 seconds
```

```
(pistacchio@pistacchio)-[~]
$ nmap -sV 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 16:34 CEST
Nmap scan report for 192.168.1.12 (192.168.1.12)
Host is up (0.00012s 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 #000000)
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
1899/tcp  open  java-rmi     GNU Classpath gmrregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2.4 (RPC #000003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-Jubuntus
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: 08:00:27:04:0E:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 04.81 seconds
```

```
(pistacchio@pistacchio)-[~]
$ nmap -sV 192.168.1.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 16:36 CEST
Nmap scan report for 192.168.1.13 (192.168.1.13)
Host is up (0.00031s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime     Microsoft Windows International daytime
17/tcp    open  qotd        Windows qotd (English)
19/tcp    open  chargen
80/tcp    open  http        Microsoft IIS httpd 10.0
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp  open  msmq?
2103/tcp  open  msrpc       Microsoft Windows RPC
2105/tcp  open  msrpc       Microsoft Windows RPC
2107/tcp  open  msrpc       Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5432/tcp  open  postgresql?
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8443/tcp  open  ssl/https-alt
MAC Address: 08:00:27:41:3A:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104B1; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 178.31 seconds
```

