

FACOLTATIVO

IP Metasploitable: 192.168.50.101

IP Kali: 192.168.50.100

Entrambe su rete interna.

Sistema operativo macchina target (Metasploitable): Linux 2.6.9 – 2.6.33

Tabelle riassuntive su porte aperte e servizi in ascolto con le relative versioni

| Porta | Proto | Stato | Servizio |
|-------|-------|-------|--------------|
| 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 |

| Porta | Servizio | Versione |
|-------|-------------|-------------------------------------|
| 21 | ftp | vsftpd 2.3.4 |
| 22 | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 |
| 23 | telnet | Linux telnetd |
| 25 | smtp | Postfix smtpd |
| 53 | domain | ISC BIND 9.4.2 |
| 80 | http | Apache httpd 2.2.8 ((Ubuntu) DAV/2) |
| 111 | rpcbind | 2 (RPC #100000) |
| 139 | netbios-ssn | Samba smbd 3.X - 4.X |
| 445 | netbios-ssn | Samba smbd 3.X - 4.X |
| 512 | exec | netkit-rsh rexecd |
| 513 | login | (unknown) |
| 514 | shell | Netkit rshd |
| 1099 | java-rmi | GNU Classpath grmiregistry |
| 1524 | bindshell | Metasploitable root shell |
| 2049 | nfs | 2-4 (RPC #100003) |
| 2121 | ftp | ProFTPD 1.3.1 |
| 3306 | mysql | MySQL 5.0.51a-3ubuntu5 |
| 5432 | postgresql | PostgreSQL DB 8.3.0 - 8.3.7 |
| 5900 | vnc | VNC (protocol 3.3) |
| 6000 | X11 | (access denied) |
| 6667 | irc | UnrealIRCd |
| 8009 | ajp13 | Apache Jserv (Protocol v1.3) |
| 8180 | http | Apache Tomcat/Coyote JSP engine 1.1 |

Principali differenze tra le due scansioni – reti diverse vs. stessa rete

1. Latenza:

Reti diverse: latenza leggermente più alta (0.0047s, 0.017s, 0.022s, 0.016s).

Stessa rete: latenza significativamente più bassa (0.0023s, 0.0078s, 0.00052s, 0.0053s).

2. Porte e Servizi:

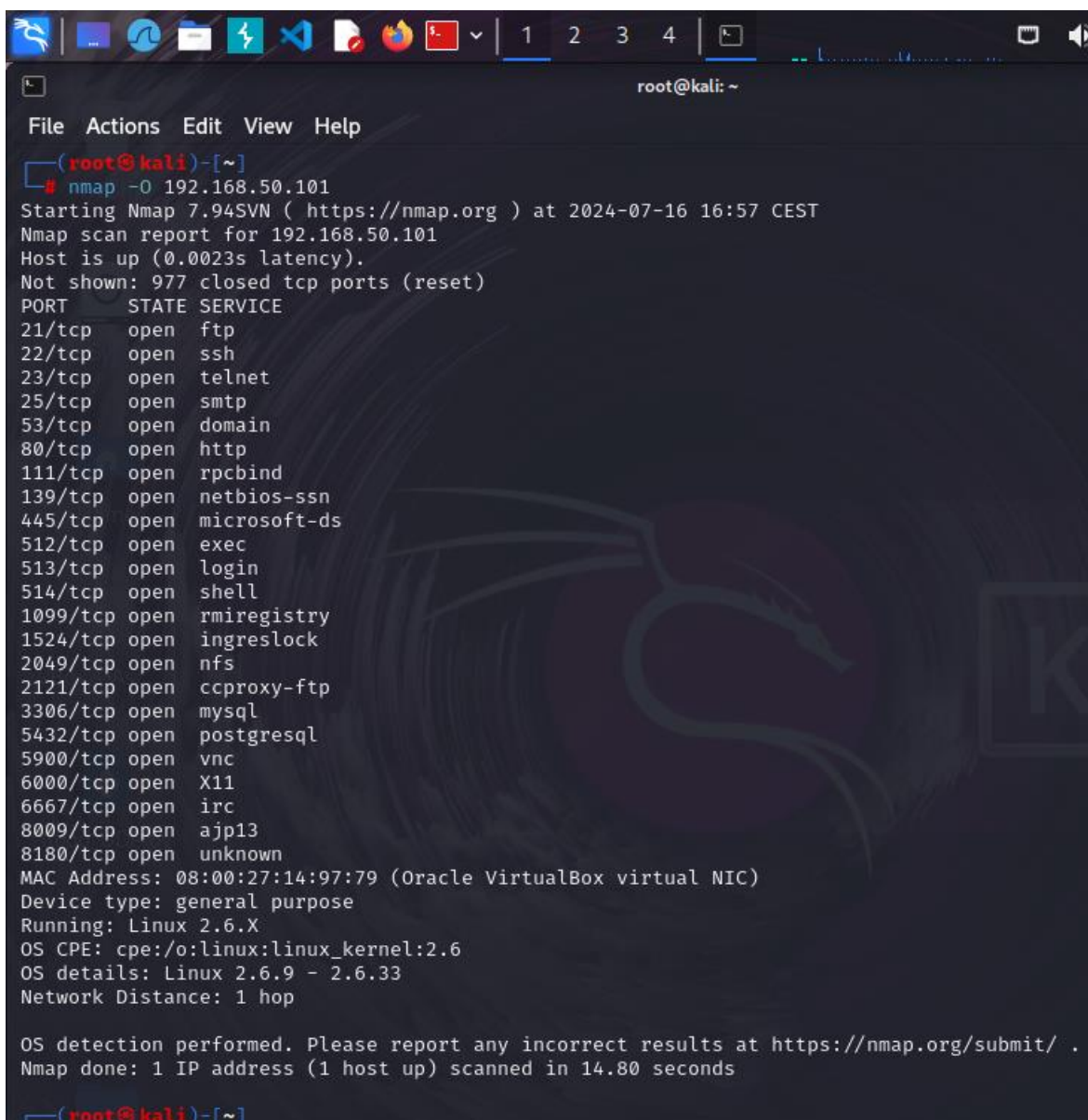
Reti diverse: la porta 80 è risultata filtrata.

Stessa rete: la porta 80 è risultata aperta e identificata come Apache httpd 2.2.8 ((Ubuntu) DAV/2).

3. Servizi con versione:

Reti diverse: servizi identificati senza ulteriori dettagli per alcune porte come 2121/tcp (ccproxy-ftp?), 513/tcp (login?), 6000/tcp (X11, access denied).

Stessa rete: 80/tcp è identificato come Apache httpd 2.2.8 ((Ubuntu) DAV/2), 2121/tcp è identificato come ProFTPD 1.3.1., 513/tcp rimane con identificazione incerta (login?), 6000/tcp rimane come X11 con access denied.



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~  
# nmap -O 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-16 16:57 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.0023s 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: 08:00:27:14:97:79 (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 14.80 seconds  
(root@kali)~
```

```
(root@kali)-[~]
# nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-16 16:58 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0078s 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: 08:00:27:14:97:79 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
```

```
Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds

(root@kali)-[~]
# nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-16 17:00 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00052s 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: 08:00:27:14:97:79 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.61 seconds
```

```
(root@kali)-[~]
#
```

Nmap done: 1 IP address (1 host up) scanned in 13.61 seconds

(root@kali)-[~]

nmap -sV 192.168.50.101

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-07-16 17:01 CEST

Nmap scan report for 192.168.50.101

Host is up (0.0053s 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 | netkit-rsh rexecd |
| 513/tcp | open | login? | |
| 514/tcp | open | shell | Netkit rshd |
| 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: 08:00:27:14:97:79 (Oracle VirtualBox virtual NIC)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: 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 66.11 seconds

(root@kali)-[~]