

# Report Nmap

## Introduzione

In questo esercizio, sono stati eseguiti dei test di scansione su due macchine virtuali (VM) utilizzando Nmap per identificare i servizi e le vulnerabilità esposte. Le due macchine target erano:

- **Metasploitable**: una macchina Linux vulnerabile, utile per test di sicurezza e exploit.
- **Windows 10**: una macchina Windows, utile per testare la sicurezza di un sistema operativo di uso comune.

Gli indirizzi IP delle macchine sono stati ottenuti come segue:

- **Metasploitable** è stata configurata con l'IP 192.168.1.100.
- **Windows 10** è stata configurata con l'IP 192.168.1.81.

## 1. Metasploitable (192.168.1.100)

### Preparazione e Scansione

#### 1. Configurazione della macchina Metasploitable:

La macchina virtuale Metasploitable è stata avviata e configurata con l'indirizzo IP 192.168.1.100. Questo IP è stato identificato utilizzando il comando `ifconfig` direttamente sulla macchina Metasploitable.

#### 2. Esecuzione della scansione con Nmap:

Una volta ottenuto l'IP, è stata avviata la scansione con **Nmap** per raccogliere informazioni sui servizi esposti e sulle porte aperte. Il comando utilizzato per la scansione è stato il seguente:

```
nmap -sS -sV -O 192.168.1.100
```

### Opzioni di Nmap:

- -sS: Scansione SYN (meglio conosciuta come scansione furtiva).
- -sV: Rilevamento della versione dei servizi.
- -O: Rilevamento del sistema operativo.

### Risultati della Scansione

- **Sistema Operativo:** Linux 2.6.9 - 2.6.33
- **Porte Aperte e Servizi:**
  - Sono state identificate numerose porte aperte, tra cui **FTP (21/tcp)**, **SSH (22/tcp)**, **HTTP (80/tcp)** e **MySQL (3306/tcp)**.
  - I servizi in ascolto con le rispettive versioni sono stati identificati, ad esempio **vsftpd 2.3.4** per FTP, **OpenSSH 4.7p1** per SSH, e **Apache httpd 2.2.8** per HTTP.

### Conclusioni sulla Scansione di Metasploitable

- **Metasploitable** espone numerosi servizi vulnerabili, che possono essere utilizzati per testare varie tecniche di attacco e exploit.
- La macchina è stata configurata intenzionalmente con vulnerabilità per scopi didattici.

```
kali-linux-2025.1a-virtualbox-amd64 (clean) [in esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
kali@kali -
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -O 192.168.1.100

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 09:10 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00080s 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
33/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
6080/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:09:A8:A5 (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 8.33 seconds

(kali@kali)-[~]
$ nmap -sS 192.168.1.100

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 09:12 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00028s 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
33/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
6080/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:09:A8:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
kali-linux-2025.1a-virtualbox-amd64 (clean) [in esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
kali@kali:~$ nmap -sT 192.168.1.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 09:13 EDT
Nmap scan report for 192.168.1.100
Host is up (0.0013s 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
445/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:D9:AB:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 8.31 seconds

kali@kali:~$ nmap -sV 192.168.1.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 09:15 EDT
Nmap scan report for 192.168.1.100
Host is up (0.0016s 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/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)
513/tcp   open  exec         netkit-rsh rshexec
514/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tperwrapped
1099/tcp  open  java-rmi     GNU Classpath gmiRegistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2.4 (RPC #1800003)
2121/tcp  open  ftp          ProFTPD 1.1.1
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/2.2.8 (Protocol v1.2)
8180/tcp  open  http         Apache/2.2.8 (Protocol v1.2)
MAC Address: 08:00:27:D9:AB:A5 (PCS Systemtechnik/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 18.31 seconds
```

## 2. Windows 10 (192.168.1.81)

### Preparazione e Scansione

#### 1. Configurazione della macchina Windows 10:

- La macchina Windows 10 è stata configurata con l'IP **192.168.1.81**. Questo IP è stato determinato eseguendo il comando **ipconfig** sulla macchina Windows 10.

#### 2. Esecuzione della scansione con Nmap:

Una volta ottenuto l'IP, è stata avviata la scansione con **Nmap** per identificare le porte aperte e i servizi in esecuzione. Il comando utilizzato per la scansione è stato lo stesso di Metasploitable:

```
nmap -sS -sV -O 192.168.1.81
```

## Opzioni di Nmap:

- -sS: Scansione SYN per rilevare le porte aperte senza stabilire una connessione completa.
- -sV: Identificazione delle versioni dei servizi.
- -O: Rilevamento del sistema operativo.

## Risultati della Scansione

- **Sistema Operativo:** Microsoft Windows 10 pro
- **Porte Aperte e Servizi:**
  - Sono state identificate diverse porte aperte, tra cui **HTTP (80/tcp)**, **MSRPC (135/tcp)**, **RDP (3389/tcp)** e **PostgreSQL (5432/tcp)**.
  - I servizi in ascolto sono stati identificati, tra cui **Microsoft IIS 10.0** per HTTP, **Microsoft Windows RPC** per MSRPC, e **Microsoft Terminal Services (RDP)**.

## Conclusioni sulla Scansione di Windows 10

- **Windows 10** espone diversi servizi critici, tra cui **RDP**, che può essere vulnerabile a diversi attacchi.
  - La macchina Windows 10 è configurata in una rete di test, con i servizi di sistema come **MSRPC** attivi e visibili.
- 

## Report Finale:

### 1. Metasploitable (192.168.1.100)

#### Dettagli del Target:

- **IP:** 192.168.1.100
- **Sistema Operativo:** Linux 2.6.9 - 2.6.33

**Porte Aperte:**

- 21/tcp - FTP
- 22/tcp - SSH
- 23/tcp - Telnet
- 25/tcp - SMTP
- 53/tcp - Domain
- 80/tcp - HTTP
- 111/tcp - rpcbind
- 139/tcp - NetBIOS-SSN
- 445/tcp - Microsoft-DS
- 512/tcp - Exec
- 513/tcp - Login
- 514/tcp - Shell
- 1099/tcp - RMIRegistry
- 1524/tcp - Ingreslock
- 2049/tcp - NFS
- 2121/tcp - FTP (ProFTPD)
- 3306/tcp - MySQL
- 5432/tcp - PostgreSQL
- 5900/tcp - VNC
- 6000/tcp - X11
- 6667/tcp - IRC
- 8009/tcp - AJP13
- 8180/tcp - HTTP (Tomcat)

### **Servizi in Ascolto con Versione:**

- **FTP:** vsftpd 2.3.4
  - **SSH:** OpenSSH 4.7p1 Debian 8ubuntu1
  - **HTTP:** Apache httpd 2.2.8
  - **MySQL:** MySQL 5.0.51a-3ubuntu5
  - **VNC:** VNC (protocollo 3.3)
  - **Tomcat:** Apache Tomcat/Coyote JSP engine 1.1
- 

## **2. Windows 10 (192.168.1.81)**

### **Dettagli del Target:**

- **IP:** 192.168.1.81
- **Sistema Operativo:** Microsoft Windows 10 1507 - 1607

### **Porte Aperte:**

- 7/tcp - Echo
- 9/tcp - Discard
- 13/tcp - Daytime
- 17/tcp - QOTD
- 19/tcp - Chargen
- 80/tcp - HTTP
- 135/tcp - MSRPC
- 139/tcp - NetBIOS-SSN
- 445/tcp - Microsoft-DS
- 1801/tcp - MSMQ

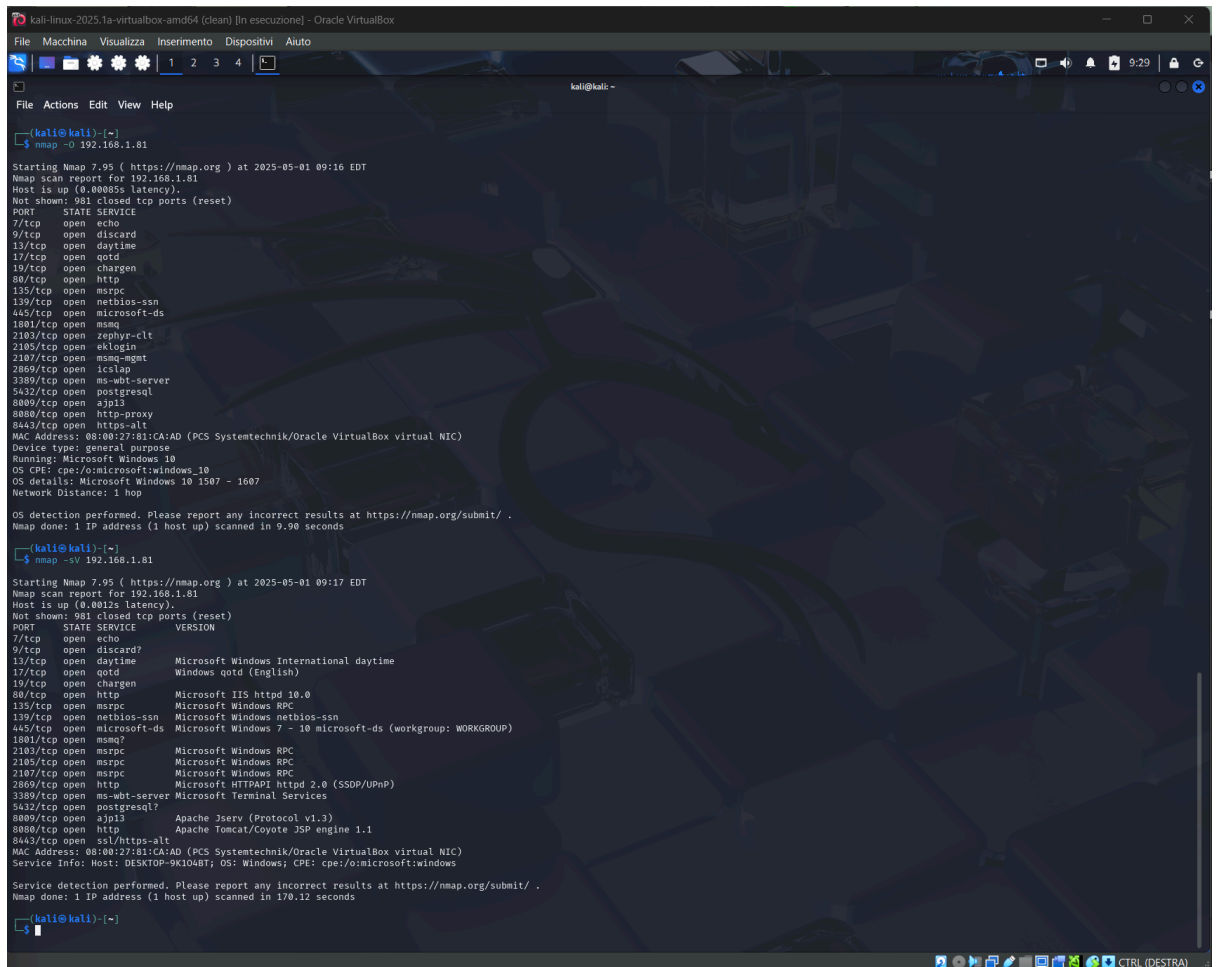
- 2103/tcp - MSRPC
- 2105/tcp - MSRPC
- 2107/tcp - MSRPC
- 2869/tcp - HTTP (Microsoft HTTPAPI)
- 3389/tcp - RDP (Microsoft Terminal Services)
- 5432/tcp - PostgreSQL
- 8009/tcp - AJP13
- 8080/tcp - HTTP (Tomcat)
- 8443/tcp - HTTPS-Alt

**Servizi in Ascolto con Versione:**

- **HTTP:** Microsoft IIS httpd 10.0
- **MSRPC:** Microsoft Windows RPC
- **RDP:** Microsoft Terminal Services (3389)
- **PostgreSQL:** versione sconosciuta



- **Tomcat:** Apache Tomcat/Coyote JSP engine 1.1



```
kali-linux-2025.1a-virtualbox-amd64 (clean) [in esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
kali@kali:~$ nmap -O 192.168.1.81
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 09:16 EDT
Nmap scan report for 192.168.1.81
Host is up (0.00085s latency).
Not shown: 981 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  wklogin
2107/tcp  open  msmq-mgmt
2809/tcp  open  iclslap
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8080/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:81:CA:AD (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 9.90 seconds

kali@kali:~$ nmap -v 192.168.1.81
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 09:17 EDT
Nmap scan report for 192.168.1.81
Host is up (0.0012s latency).
Not shown: 981 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
2809/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5432/tcp  open  postgresql?
8080/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: 08:00:27:81:CA:AD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT, 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 170.12 seconds

kali@kali:~$
```

Antonio Ercolamento