

REPORT : Scansione dei servizi con NMAP

Introduzione e Scopo

Il report in questione ha lo scopo di presentare in modo strutturato i risultati delle attività di scansione di rete condotte con lo strumento Nmap. L'analisi si concentra su due sistemi target distinti, identificati come "**Metasploitable**" e "**Windows**", sui quali sono state eseguite diverse tipologie di scansione per la raccolta di informazioni. L'obiettivo principale è fornire una mappatura chiara e dettagliata della configurazione di rete dei sistemi, delle porte aperte e dei servizi esposti.

L'analisi procederà esaminando singolarmente ciascun target, iniziando con il sistema Metasploitable.

Analisi del Target 1: Metasploitable (192.168.0.181)

L'analisi del primo target si concentra sulla macchina virtuale **Metasploitable**, un sistema deliberatamente configurato con vulnerabilità note. L'importanza strategica di questa analisi risiede nell'identificare quella che è la sua configurazione di rete e la superficie d'attacco esposta, elementi fondamentali per comprendere le potenziali vie di accesso per un utente.

Identificazione dell'Host e del Sistema Operativo

La scansione iniziale di tipo **OS fingerprinting** ha permesso di raccogliere le informazioni fondamentali per l'identificazione univoca dell'host e del suo sistema operativo. I dati chiave emersi sono i seguenti:

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.0.181
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:05 EST
Nmap scan results for 192.168.0.181
Host is up [0.0013s 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  cccproxy-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: 08:00:27:85:01:A6 (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 1.71 seconds

(kali㉿kali)-[~]
```

Confronto tra Scansioni Porte: SYN Scan vs. TCP Connect

Per l'analisi approfondita della superficie di attacco esposta dal sistema, sono state impiegate due metodologie distinte e complementari di **port scanning**, finalizzate all'identificazione delle porte **TCP** (Transmission Control Protocol) attive e in ascolto. Nello specifico, la ricognizione è stata eseguita tramite una **SYN Scan** (nota anche come **half-open scanning**) e una **TCP Connect Scan** (o **full-open scanning**).

La **SYN Scan** sfrutta l'invio di pacchetti **SYN** (Synchronize) per avviare l'handshake TCP, ma, in caso di risposta **SYN/ACK** (indizio di porta aperta), interrompe immediatamente la procedura inviando un pacchetto **RST** (Reset) anziché completare l'handshake con l'**ACK** finale. Questo approccio è spesso preferito per la sua rapidità e per la minore "rumorosità" sui *log* di sistema, agendo in modo più furtivo.

La **TCP Connect Scan** è invece un metodo più diretto che tenta di stabilire una connessione TCP completa e tridirezionale (**SYN -> SYN/ACK -> ACK**). Questo tipo di scansione, pur essendo meno discreta e più facilmente rilevabile da sistemi di sicurezza, è considerato il più affidabile in termini di verifica dello stato di una porta, poiché simula esattamente il comportamento di un'applicazione client legittima.

Il confronto dei risultati ottenuti da queste due diverse tecniche di scansione ha prodotto un dato significativo: **entrambe le tecniche hanno identificato lo stesso identico set di porte aperte**. Non si è riscontrata alcuna differenza, nemmeno minima, tra l'elenco delle porte individuate dalla **SYNScan** e quello prodotto dalla **TCP Connect Scan**.

In altre parole, se fossero presenti meccanismi di sicurezza attivi in grado di monitorare lo stato delle connessioni (come un firewall stateful), ci si aspetterebbe che la **SYN Scan**, data la sua natura incompleta, venisse trattata in modo differente (ad esempio bloccata o ignorata) rispetto alla **TCP Connect Scan**, alterando potenzialmente i risultati. La perfetta sovrapposizione dei set di porte conferma, pertanto, che il traffico di scansione è stato trattato in modo indifferenziato dal sistema bersaglio o dai dispositivi di sicurezza di rete intermedi.

TCP SCAN:

(kali㉿kali)-[~]

```
$ nmap -sT 192.168.0.181
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:08 EST
Nmap scan report for 192.168.0.181
Host is up (0.0083s 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  cccproxy-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: 08:00:27:85:01:A6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

msfadmin@metasploitable:~\$ ifconfig

```
eth0      Link encap:Ethernet HWaddr 08:00:27:85:01:a6
          inet addr:192.168.0.181 Bcast:192.168.0.255 Mask:255.255.255.0
          inet6 addr: fdd7:21:9d01:1440:0:0:27ff:fe85:1a6/64 Scope:Global
            inet6 addr: fe80::a00:27ff:fe85:1a6/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:82 errors:0 dropped:0 overruns:0 frame:0
              TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:7643 (7.4 KB) TX bytes:6977 (6.8 KB)
              Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:92 errors:0 dropped:0 overruns:0 frame:0
            TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)
```

SYN SCAN:

(kali㉿kali)-[~]

```
$ sudo nmap -sS 192.168.0.181
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:07 EST
Nmap scan report for 192.168.0.181
Host is up (0.0020s 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  cccproxy-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: 08:00:27:85:01:A6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

msfadmin@metasploitable:~\$ ifconfig

```
eth0      Link encap:Ethernet HWaddr 08:00:27:85:01:a6
          inet addr:192.168.0.181 Bcast:192.168.0.255 Mask:255.255.255.0
          inet6 addr: fdd7:21:9d01:1440:0:0:27ff:fe85:1a6/64 Scope:Global
            inet6 addr: fe80::a00:27ff:fe85:1a6/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:82 errors:0 dropped:0 overruns:0 frame:0
              TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:7643 (7.4 KB) TX bytes:6977 (6.8 KB)
              Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:92 errors:0 dropped:0 overruns:0 frame:0
            TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)
```

Analisi dei Servizi e delle Versioni

La scansione di rilevamento delle versioni ([Version detection](#)) fornisce le informazioni più significative, associando a ogni porta aperta uno specifico servizio software e, dove possibile, la sua esatta versione. Questa informazione è cruciale per la successiva fase di ricerca di vulnerabilità note. I risultati di tale scansione sono catalogati nella tabella sottostante.

The screenshot shows two windows. On the left, a terminal window on Kali Linux displays the results of a Nmap scan against the IP 192.168.0.181. The output includes a table of open ports with their services and versions, such as vsftpd 2.3.4, OpenSSH 4.7p1, and Apache httpd 2.2.8. It also shows service detection results like Java RMI and MySQL. On the right, a Metasploitable host running in Oracle VirtualBox is shown in a graphical interface. The interface shows network configuration details for the host, including MAC address, IP, and subnet information. The host's name is 'Metasploitable2-Linux'.

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.0.181
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:14 EST
Nmap scan report for 192.168.0.181
Host is up (0.00046s 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
514/tcp   open  tcpwrapped
109/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: 08:00:27:85:01:A6 (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 65.35 seconds

(kali㉿kali)-[~]
```

Metasploitable2-Linux [In esecuzione] - Oracle VirtualBox

No mail.

eth0 Link encap:Ethernet HWaddr 08:00:27:85:01:a6
inet6 addr: fdd7:21:9d01:1440:a0:27ff:fe85:1a6/64 Scope:Global
inet6 addr: 2a0e:43d:1a54:0:a0:27ff:fe85:1a6/64 Scope:Global
inet6 addr: fe80::a00:27ff:fe85:1a6/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:82 errors:0 dropped:0 overruns:0 frame:0
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:7643 (7.4 KB) TX bytes:6977 (6.8 KB)
Base address:0xd020 Memory:f0200000-f0220000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:92 errors:0 dropped:0 overruns:0 frame:0
TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~\$
msfadmin@metasploitable:~\$

Dall'analisi emergono diverse criticità di sicurezza che richiedono attenzione immediata. La presenza di un servizio di [Metasploitable root shell](#) sulla porta 1524 rappresenta un'esposizione diretta e non autenticata al sistema con i massimi privilegi. Inoltre, il servizio [vsftpd 2.3.4](#) è una versione notoriamente vulnerabile a un backdoor, che consente l'esecuzione di comandi remoti. Infine, la presenza di software datati come [OpenSSH 4.7p1](#) e [Apache httpd 2.2.8](#) introduce ulteriori rischi, poiché queste versioni sono affette da multiple vulnerabilità pubblicamente note.

Analisi del Target 2: Windows (192.168.0.230)

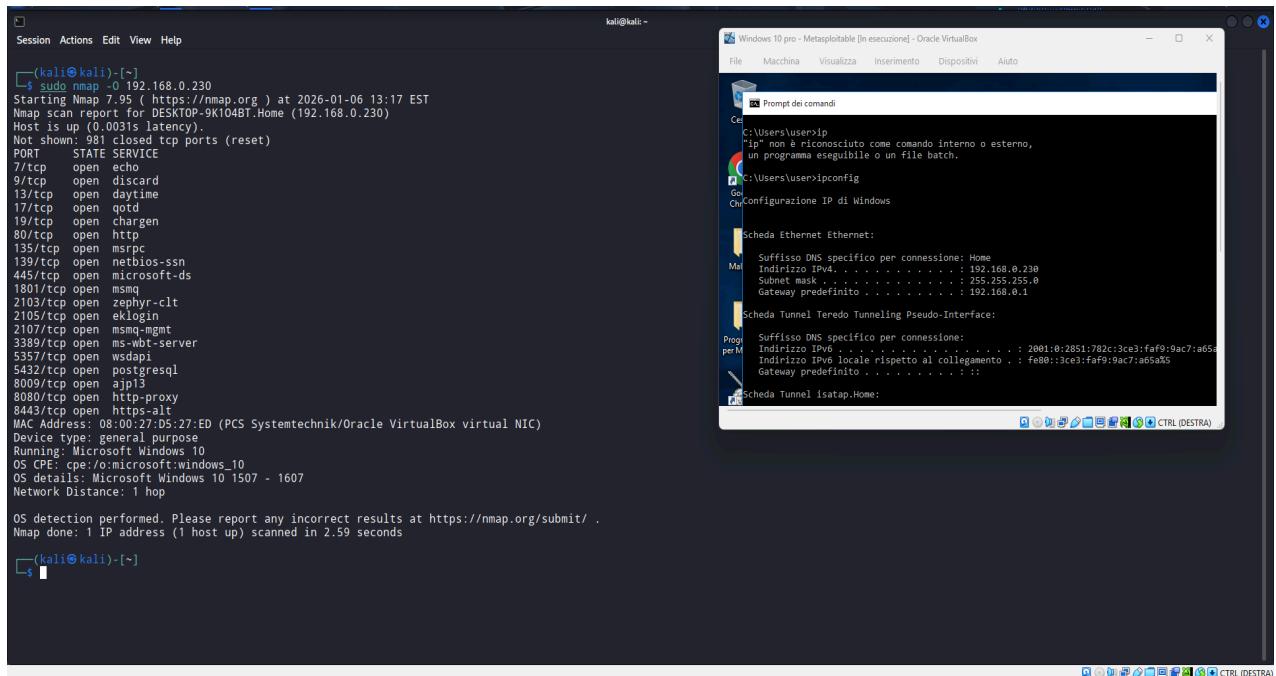
L'analisi si sposta ora sul secondo target identificato nella rete, una macchina con indirizzo IP **192.168.0.230**. Per questo host, l'obiettivo dell'attività era l'identificazione del sistema operativo e la mappatura delle porte aperte.

3.1 Identificazione dell'Host e del Sistema Operativo

La scansione **OS fingerprinting** ha fornito le seguenti informazioni identificative per l'host:

- **Indirizzo IP:** 192.168.0.230
- **Hostname:** DESKTOP-9K1048T.Home
- **Indirizzo MAC:** 08:00:27:DE:27:ED
- **Produttore Scheda di Rete:** PCS Systemtechnik/Oracle VirtualBox virtual NIC
- **Sistema Operativo Rilevato:** Microsoft Windows 10 (versione stimata 1507 – 1607).

OS fingerprinting



```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.0.230
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:17 EST
Nmap scan report for DESKTOP-9K1048T.Home (192.168.0.230)
Host is up (0.0031s 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  eklogin
2107/tcp   open  msmq-mgmt
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
5432/tcp   open  postgresql
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
MAC Address: 08:00:27:DE:27:ED (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 2.59 seconds

(kali㉿kali)-[~]
```

La scansione ha identificato il tipo di sistema operativo e un set di porte TCP aperte sull'host Windows.

Conclusioni

La scansione di rete ha delineato chiaramente la situazione della sicurezza dei sistemi esaminati. I principali riscontri sono:

1. È stata ottenuta una corretta identificazione di entrambi i sistemi target: una macchina **Linux (Metasploitable)** e una macchina **Microsoft Windows 10**.
2. Per il sistema Metasploitable, la mappatura dei servizi ha rivelato una postura di sicurezza estremamente critica. La presenza di servizi critici come una **root shell remota** (porta 1524), versioni di software **notoriamente vulnerabili** (es. vsftpd 2.3.4) e protocolli di gestione **non cifrati** (Telnet) contribuisce a una superficie d'attacco eccezionalmente ampia e a rischio elevato.
3. Il confronto tra le scansioni di tipo **SYN** e **TCP Connect** sul target ha confermato che entrambe le metodologie hanno prodotto **risultati identici**, suggerendo l'assenza di meccanismi di filtraggio di base sulla rete.