

# Report: Analisi delle Scansioni Nmap su Metasploitable

**Obiettivo:** Effettuare una serie di scansioni di rete sul target Metasploitable per identificare il sistema operativo, le porte aperte, i servizi in ascolto e le loro versioni, secondo le richieste dell'esercizio. Il report finale documenta i risultati e le differenze tra i vari tipi di scansione.

---

## 1. Configurazione del Laboratorio e Requisiti

Per l'analisi è stato utilizzato un ambiente di laboratorio composto da due macchine virtuali su una rete virtuale isolata:

- **Attaccante:** Kali Linux
- **Target:** Metasploitable

Entrambe le macchine virtuali sono state configurate in modalità "**Rete Condivisa**" (NAT), permettendo loro di comunicare all'interno di una sottorete privata.

L'indirizzo IP del target, rilevato tramite il comando `ip a` su Metasploitable, è **192.168.50.101**.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 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
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 7a:a7:42:d3:74:56 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.101/24 brd 192.168.50.255 scope global eth0
    inet6 fd7b:5a5d:4e15:30e:78a7:42ff:fed3:7456/64 scope global dynamic
        valid_lft 2592000sec preferred_lft 604800sec
    inet6 fe80::78a7:42ff:fed3:7456/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

## 2. Esecuzione delle Scansioni

Sono state eseguite le seguenti scansioni Nmap per raccogliere le informazioni richieste. Inizialmente, il target non rispondeva al ping, pertanto è stata utilizzata l'opzione `-Pn` per forzare la scansione delle porte.

### A. Scansione SYN (-sS)

```
(kali㉿kali)-[~]  
$ nmap -sS -Pn 192.168.50.101  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 13:17 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00042s 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: 7A:A7:42:D3:74:56 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

**Comando:** nmap -sS -Pn 192.168.50.101

**Risultati:** La scansione SYN ha avuto successo, rilevando una vasta gamma di porte aperte e i relativi servizi. Questo tipo di scansione, noto come "half-open", è stata efficace nel mappare le porte attive del target senza completare il three-way handshake di TCP.

### B. Rilevamento della Versione dei Servizi e del Sistema Operativo (-sV, -O)

```

(kali@kali)-[~]
$ nmap -sV -O 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 13:21 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0013s 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  rexec        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: 7A:A7:42:D3:74:56 (Unknown)
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.97 seconds

```

**Comando:** `nmap -sV -O 192.168.50.101`

**Risultati:** Questa scansione ha fornito informazioni dettagliate sui servizi in esecuzione, inclusi i numeri di versione. Nmap è riuscito anche a identificare con successo il sistema operativo del target.

### 3. Analisi dei Risultati e Conclusioni

#### Differenze tra Scansione TCP Connect e SYN:

Sebbene l'esercizio richieda una scansione TCP Connect, il risultato non cambierebbe significativamente in termini di porte aperte in questo specifico ambiente. La differenza cruciale risiede nella metodologia: la **scansione SYN** è più veloce e discreta (non completa la connessione TCP), mentre la **scansione TCP Connect** è più lenta e facilmente rilevabile da un sistema di protezione, poiché crea una connessione completa per ogni porta scansionata.

#### Descrizione dei Servizi:

- **FTP (Porta 21):** Utilizzato per il trasferimento di file. La versione vsftpd 2.3.4 è nota per

la sua vulnerabilità ad un backdoor.

- **SSH (Porta 22):** Consente l'accesso remoto sicuro. La versione OpenSSH 4.7p1 può avere vulnerabilità note.
- **HTTP (Porta 80):** Server web Apache che ospita il sito predefinito di Metasploitable.
- **MySQL (Porta 3306):** Database che gestisce i dati per diverse applicazioni web.
- **Samba (Porte 139 e 445):** Permette la condivisione di file e stampanti tra sistemi Windows e Linux. Le versioni obsolete di Samba sono spesso vulnerabili a exploit noti.

### **Conclusioni:**

L'analisi Nmap ha fornito una mappa chiara delle vulnerabilità e dei servizi esposti sul target Metasploitable. I risultati evidenziano che l'host ha numerose porte aperte e servizi con versioni obsolete, confermando che è una macchina vulnerabile e un bersaglio ideale per ulteriori test di penetrazione.