# Relazione Tecnica: Tecniche di Scansione con Nmap

Corso: Cyber Security & Ethical Hacking

Mirko Imbrogno

---

## 1. Introduzione e Obiettivi

La presente attività si focalizza sull'analisi della rete e l'identificazione dei servizi attivi su due target specifici:

- **Target 1:** Metasploitable (Linux-based).
- **Target 2:** Windows.
- **Scopo:** Eseguire OS fingerprinting, scansioni SYN e TCP Connect, e detection delle versioni dei servizi.

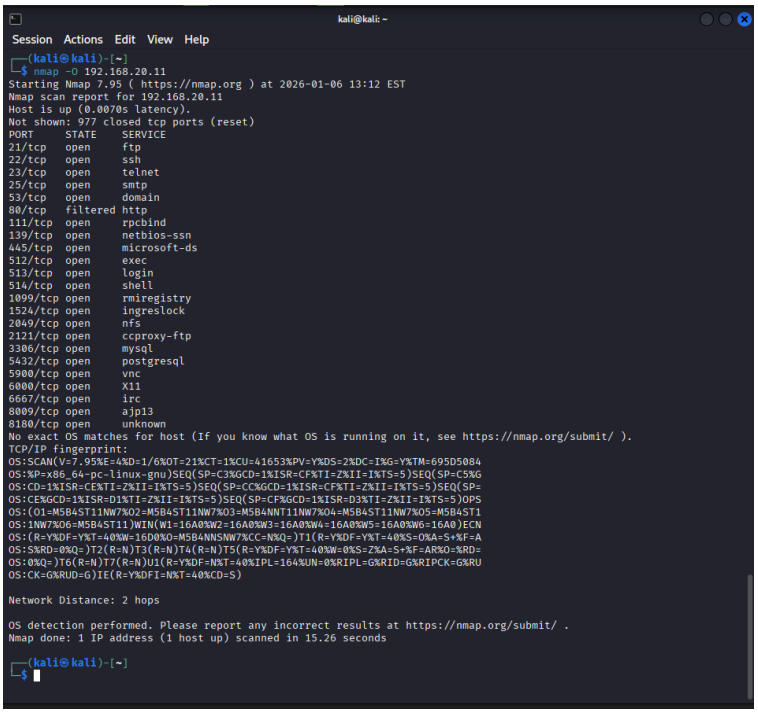
---

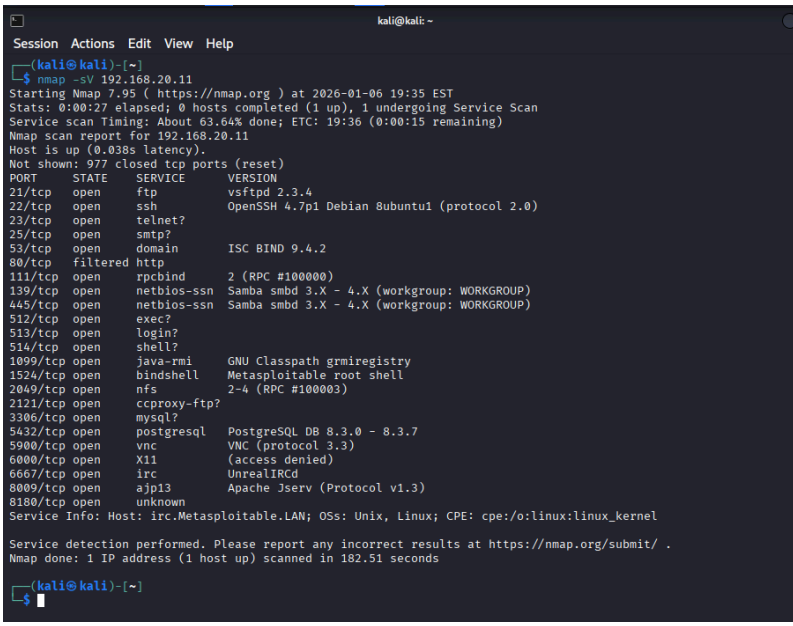
## 2. Analisi Target: Metasploitable (192.168.20.11)

### A. OS Fingerprinting & Service Detection

Dalla scansione effettuata con i flag -O e -sV, sono stati ottenuti i seguenti dati:

- **IP Target:** 192.168.20.11.
- **Sistema Operativo:** Linux (Kernel 2.6.X).
- **Servizi Critici Rilevati:**
  - **Porta 21:** vsftpd 2.3.4 (FTP).
  - **Porta 22:** OpenSSH 4.7p1.
  - **Porta 3306:** MySQL 5.0.51a.
  - **Porta 5432:** PostgreSQL 8.3.0.



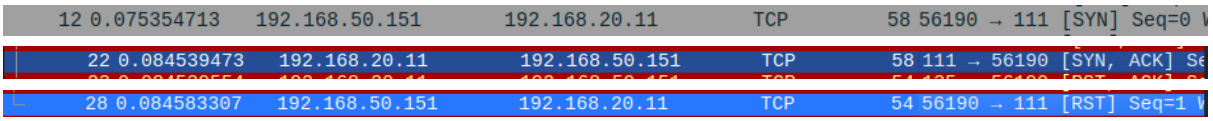



## B. Confronto Tecniche di Scansione

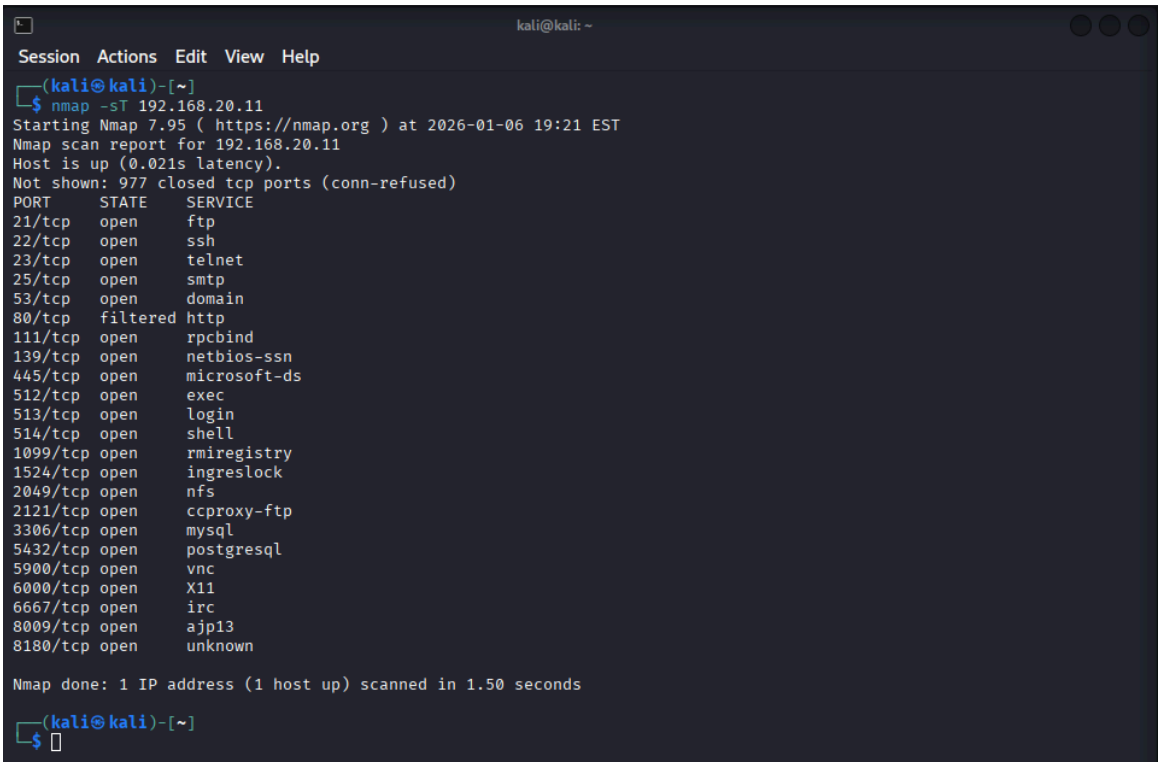
Come richiesto dalla traccia, sono state confrontate le metodologie **SYN Scan** (-sS) e **TCP Connect** (-sT):

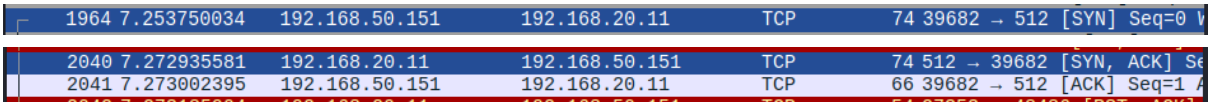
- **SYN Scan (Stealth):** Nmap invia un pacchetto SYN e, ricevuto il SYN/ACK, invia immediatamente un RST. La connessione non viene mai completata, rendendo la scansione meno visibile nei log applicativi.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.20.11
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:15 EST
Nmap scan report for 192.168.20.11
Host is up (0.027s 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   filtered 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

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds

┌──(kali㉿kali)-[~]
└─$
```



- **TCP Connect:** Nmap completa il "Three-Way Handshake" (SYN -> SYN/ACK -> ACK). Questa tecnica è più lenta e facilmente tracciabile, poiché il sistema operativo target registra l'avvenuta connessione.



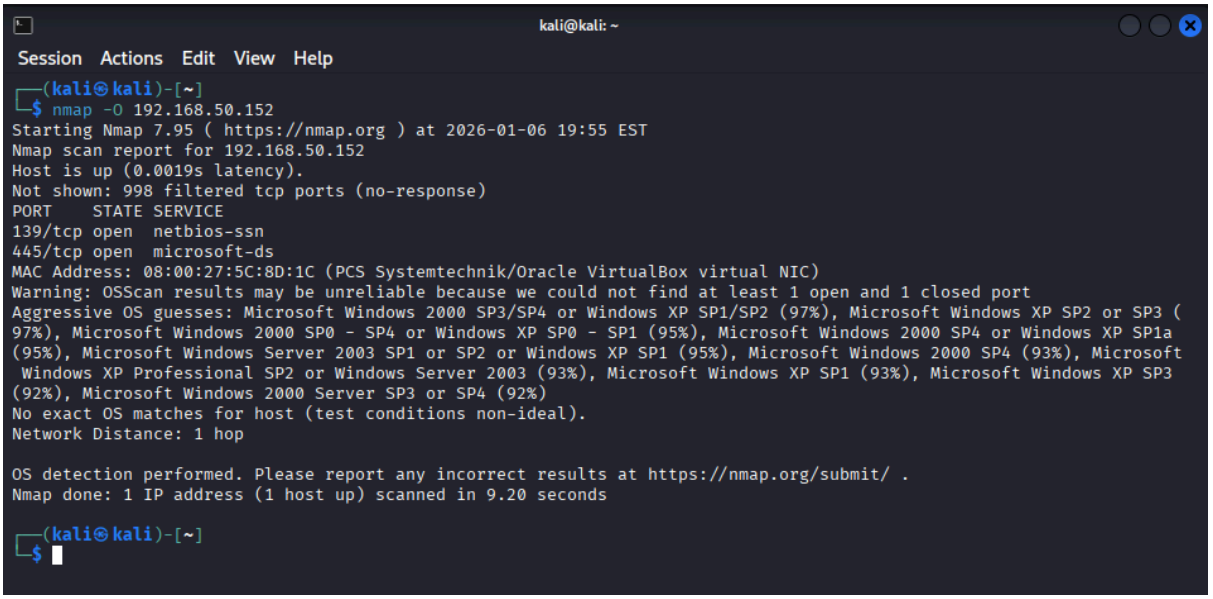
---

# 3. Analisi Target: Windows (192.168.50.152)

### OS Fingerprinting

Sulla macchina Windows è stata eseguita una scansione per l'identificazione del sistema operativo:

- **IP Target:** 192.168.50.152.
- **Risultato Fingerprint:** Nmap indica con un'accuratezza del 97% la presenza di **Microsoft Windows XP (SP1/SP2)** o **Windows 2000**.
- **Porte Aperte Rilevate:**
    - **139/tcp:** netbios-ssn.
    - **445/tcp:** microsoft-ds (SMB).



## 4. Report Sintetico dei Servizi

Seguendo le linee guida della traccia, ecco il riepilogo finale:

| IP | Sistema Operativo | Porte Aperte | Servizi e Versioni |
|---|---|---|---|
| **192.168.20.11** | Linux (Kernel 2.6.X) | 21, 22, 23, 445, 3306 | vsftpd 2.3.4, OpenSSH 4.7p1, Samba |
| **192.168.50.152** | Windows XP/2000 | 139, 445 | NetBIOS-ssn, Microsoft-ds |

## 5. Conclusioni

L'attività ha permesso di mappare la superficie di attacco dei target. La macchina Metasploitable presenta vulnerabilità critiche dovute a versioni di servizi obsolete (es. vsftpd 2.3.4), mentre il fingerprinting su Windows ha evidenziato un sistema operativo non più supportato e potenzialmente vulnerabile.