

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.

```
Session Actions Edit View Help
(kali@kali)~$ nmap -O 192.168.20.11
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:12 EST
Nmap scan report for 192.168.20.11
Host is up (0.0079s 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
No exact OS matches for host (if you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95E=AND-1/6KOT-21KCT=1KCU=41653NPV=YKDS=2KDC=IKG=YKTM=695D0884
OS:XP=X86_64-pc-linux-gnu)SEQ(SP=C3KGCD=1KISR=CFKTI=ZKII=IKTS=5)SEQ(SP=C5KG
OS:CD=1KISR=CEKTI=ZKII=IKTS=5)SEQ(SP=CCNGCD=1KISR=CFKTI=ZKII=IKTS=5)SEQ(SP=
OS:CEMGCD=1KISR=D1KTI=ZKII=IKTS=5)SEQ(SP=CFMGCD=1KISR=D3KTI=ZKII=IKTS=5)OPS
OS:(OI=MSBAST11NW7K02=MSBAST11NW7K03=MSBANNT11NW7K04=MSBAST11NW7K05=MSBAST1
OS:11NW7K06=MSBAST111WIN(KI=16A0XW2=16A0XW3=16A0XW4=16A0XW5=16A0XW6=16A0)ICN
OS:(R=YKDF=YKT=40XW=16D0X0=MSBANNSNW7KCC=NRQ)T1(R=YKDF=YKT=40XS=OXA=5+XF=A
OS:SKRD=0XQ)T2(R=N)T3(R=N)T4(R=N)T5(R=YKDF=YKT=40XW=0XS=ZKA=5+XF=ARX0=KRD=
OS:0XQ)T6(R=N)T7(R=N)U1(R=YKDF=NKT=40XKPL=164XUN=0XRIPL=GXRID=GXRIPCK=GXRU
OS:CK=GXRUD=0)IE(R=YKDF=NKT=40XCD=5)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.26 seconds
(kali@kali)~$
```

```
Session Actions Edit View Help
(kali@kali)~$ nmap -sV 192.168.20.11
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 19:35 EST
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 63.64% done; ETC: 19:36 (0:00:15 remaining)
Nmap scan report for 192.168.20.11
Host is up (0.038s 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?
25/tcp    open  smtp?
53/tcp    open  domain
512/tcp   filtered http
513/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  shell?
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  ccproxy-ftp?
3306/tcp  open  mysql?
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  unknown

Service Info: Host: 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 182.51 seconds
(kali@kali)~$
```

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)-[~]
$
```

12 0.075354713	192.168.50.151	192.168.20.11	TCP	58 56190 → 111 [SYN] Seq=0
22 0.084539473	192.168.20.11	192.168.50.151	TCP	58 111 → 56190 [SYN, ACK] Seq=
28 0.084583307	192.168.50.151	192.168.20.11	TCP	54 56190 → 111 [RST] Seq=1

- **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.

```

kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ nmap -sT 192.168.20.11
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 19:21 EST
Nmap scan report for 192.168.20.11
Host is up (0.021s 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    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 1.50 seconds

(kali@kali)-[~]
$ 

```

1964	7.253750034	192.168.50.151	192.168.20.11	TCP	74 39682 → 512 [SYN] Seq=0 W
2040	7.272935581	192.168.20.11	192.168.50.151	TCP	74 512 → 39682 [SYN, ACK] Se
2041	7.273002395	192.168.50.151	192.168.20.11	TCP	66 39682 → 512 [ACK] Seq=1 A

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).

```
kali@kali: ~  
Session Actions Edit View Help  
[kali@kali]~  
$ nmap -O 192.168.50.152  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 19:55 EST  
Nmap scan report for 192.168.50.152  
Host is up (0.0019s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:5C:8D:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Aggressive OS guesses: Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1 (95%), Microsoft Windows 2000 SP4 or Windows XP SP1a (95%), Microsoft Windows Server 2003 SP1 or SP2 or Windows XP SP1 (95%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows XP SP3 (92%), Microsoft Windows 2000 Server SP3 or SP4 (92%)  
No exact OS matches for host (test conditions non-ideal).  
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 9.20 seconds  
[kali@kali]~  
$
```

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.
