REPORT ESERCITAZIONE: SCANSIONE DEI SERVIZI CON NMAP

Corso: Cyber Security & Ethical Hacking

Modulo: Tecniche di Scansione ed Enumerazione

Studente: Rocco Paolo Caccamo

Data: 06/01/2026

---

1. OBIETTIVO E CONFIGURAZIONE DEL LABORATORIO

L'esercitazione ha l'obiettivo di analizzare target vulnerabili utilizzando diverse tecniche di scansione con il tool Nmap, identificando sistemi operativi, servizi attivi e differenze nel traffico di rete generato.

Configurazione di Rete (Laboratorio Virtuale):

- **Macchina Attaccante (Kali Linux):** 192.168.50.12
- **Target 1 (Metasploitable 2):** 192.168.50.10
- **Target 2 (Windows XP):** 192.168.50.13

---

2. ANALISI TARGET 1: METASPLOITABLE (LINUX)

A. Identificazione del Sistema Operativo

È stato eseguito il fingerprinting dello stack TCP/IP per determinare il sistema operativo del target.

- **Comando:** nmap -O 192.168.50.10
- **Risultato:** Linux 2.6.9 - 2.6.33

B. Analisi Comparativa: TCP Connect vs SYN Scan

Come richiesto dalla traccia, è stato analizzato il comportamento di due diverse tecniche di scansione osservando il traffico di rete tramite Wireshark.

1. **SYN Scan (Scansione Stealth - Opzione -sS)**
    - **Analisi del traffico:** La macchina attaccante invia un pacchetto **SYN**. Alla ricezione del **SYN/ACK** dal target, la macchina attaccante invia immediatamente un pacchetto **RST (Reset)**.
    - **Differenza:** La connessione non viene mai completata ("half-open"). Questa tecnica è più rapida e spesso evita di essere registrata nei log delle applicazioni del server target.
2. **TCP Connect Scan (Opzione -sT)**

- **Analisi del traffico:** La macchina attaccante completa interamente il *Three-Way Handshake* (SYN SYN/ACK ACK).
- **Differenza:** La connessione viene stabilita completamente prima di essere chiusa. Rispetto alla SYN scan, questa tecnica è più "rumorosa" e lascia tracce evidenti nei log di sistema del bersaglio.

C. Porte Aperte e Version Detection

Utilizzando il comando nmap -sV, è stato possibile enumerare i servizi in ascolto e le relative versioni. Il target espone una superficie d'attacco critica con servizi obsoleti.

Tabella dei Servizi Rilevati:

Porta	Protocollo	Stato	Servizio	Versione Rilevata
21	TCP	Open	FTP	vsftpd 2.3.4
22	TCP	Open	SSH	OpenSSH 4.7p1 Debian 8ubuntu1
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
445	TCP	Open	Microsoft-ds	Samba smbd 3.X - 4.X

512	TCP	Open	Exec	netkit-rsh rexecd
513	TCP	Open	Login	OpenBSD rlogind
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

---

3. ANALISI TARGET 2: WINDOWS XP

A. Identificazione del Sistema Operativo

È stata effettuata una scansione specifica sul secondo target per identificare la versione del sistema.

- **Comando:** nmap -O 192.168.50.13
- **IP Target:** 192.168.50.13
- **Sistema Operativo Rilevato:** Microsoft Windows XP SP2 o SP3
- **Affidabilità rilevamento:** 98%

B. Porte e Servizi Rilevati

Contestualmente all'identificazione del SO, sono state rilevate le porte standard per la condivisione di risorse in ambiente Windows:

- **Porta 139/tcp:** netbios-ssn
- **Porta 445/tcp:** microsoft-ds

---

4. CONCLUSIONI

L'attività ha permesso di verificare nella pratica le differenti risposte dei sistemi operativi e dei protocolli di rete. L'analisi del traffico con Wireshark ha evidenziato come la scansione SYN (Half-open) sia preferibile in contesti di *Penetration Testing* per la sua rapidità e la minore probabilità di essere loggata rispetto alla scansione TCP Connect completa. Il target Metasploitable si conferma altamente vulnerabile, esponendo numerosi servizi critici e shell remote senza autenticazione adeguata.