REPORT W9D1

NMAP

INDICE

1. Introduzione

La scansione dei servizi di rete rappresenta il primo passo per individuare quali applicazioni o servizi in esecuzione su una macchina possano presentare vulnerabilità sfruttabili.
Ambiente di test: scansioni eseguite in ambiente controllato, con macchina target Metasploitable.

2. Metodologia

Strumento utilizzato: *Nmap*
Tipologie di scansione effettuate:
- Scansione **TCP** - comando → *nmap -sT 192.168.50.101*
- Scansione **SYN** - comando → *nmap -sV 192.168.50.101*
- Scansione con switch **-A** (OS detection, versione, script e traceroute) – comando → *nmap -A 192.168.50.101*

Note operative: privilegi di root richiesti per alcune tipologie di scansione (Scansione **SYN**)

---

3. Report dei Risultati

Fonte dello scan	Target dello scan	Tipo di scan	Risultati ottenuti
Kali Linux IP 192.168.1.100	Metasploitable IP 192.168.50.101	TCP Connect Scan sulle well-known ports **Comando usato**: *nmap -sT IP*	23 porte aperte; numerosi servizi in ascolto (ftp, ssh, telnet, http)
Kali Linux IP 192.168.1.100	Metasploitable IP 192.168.50.101	SYN Scan sulle well-known ports **Comando usato**: *nmap -sV IP*	23 porte rilevate; rilevati servizi uguali alla scansione precedente;
Kali Linux IP 192.168.1.100	Metasploitable IP 192.168.50.101	Scan completa (-A) **Comando usato**: *nmap -A IP*	OS: Linux; Versioni dei servizi;

4. Analisi dei Risultati

Le scansioni effettuate sulla macchina Metasploitable hanno fornito una panoramica dettagliata dei servizi attivi e delle potenziali vulnerabilità presenti. Di seguito, un'analisi approfondita per ciascun tipo di scansione:

1. Scansione TCP (Connect Scan) - nmap -sT

- **Comportamento:** La scansione TCP ha stabilito una connessione completa con ciascuna porta.
- **Risultati:** Sono state identificate numerose porte aperte, tra cui:
    - **Porta 21 (FTP):** Servizio attivo, potenzialmente vulnerabile a brute-force o exploit noti.
    - **Porta 22 (SSH):** Servizio attivo, verificare la versione per eventuali vulnerabilità.
    - **Porta 23 (Telnet):** Servizio attivo, noto per trasmettere dati in chiaro, rappresenta un rischio significativo.
    - **Porta 80 (HTTP):** Servizio web attivo, possibile presenza di vulnerabilità nelle applicazioni web ospitate.
- **Considerazioni:** La presenza di servizi come Telnet e FTP senza cifratura rappresenta una superficie d'attacco ampia per un potenziale aggressore.

2. Scansione SYN (Half-Open Scan) - nmap -sS

- **Comportamento:** La scansione SYN ha inviato pacchetti SYN alle porte target senza completare la stretta di mano TCP, rendendola meno rilevabile dai sistemi di difesa.
- **Risultati:** Ha confermato la presenza delle stesse porte aperte rilevate dalla scansione TCP, con tempi di risposta leggermente inferiori.
- **Considerazioni:** Questa tecnica potrebbe non rilevare servizi che rispondono solo a connessioni complete.

---

3. Scansione con switch -A - nmap -A

- **Comportamento:** La scansione con l'opzione -A ha effettuato una rilevazione approfondita, includendo:
    - **Identificazione del sistema operativo:** Rilevato Linux con kernel 2.6.
    - **Versione dei servizi:** Ad esempio, Apache 2.2.8 su porta 80.
    - **Script NSE:** Esecuzione di script per rilevare vulnerabilità note.
    - **Traceroute:** Mappatura del percorso di rete fino al target.
- **Risultati:** Sono emerse ulteriori informazioni, come:
    - **Servizio Samba su porta 445:** Potenzialmente vulnerabile a exploit noti.
    - **Servizio MySQL su porta 3306:** Verificare configurazioni di sicurezza e versioni.

- **Considerazioni:** Questa scansione fornisce una visione completa del sistema target, essenziale per valutare il livello di esposizione e pianificare eventuali interventi di mitigazione.

---

5. Conclusioni

Le attività di scansione condotte sulla macchina Metasploitable hanno evidenziato una serie di servizi attivi, alcuni dei quali notoriamente vulnerabili. In particolare:

- **Servizi non cifrati:** La presenza di Telnet e FTP rappresenta un rischio elevato, in quanto trasmettono dati in chiaro, facilitando potenziali intercettazioni.
- **Servizi con vulnerabilità note:** Servizi come Samba e versioni obsolete di Apache possono essere sfruttati da aggressori per ottenere accesso non autorizzato o eseguire codice arbitrario.
- **Informazioni dettagliate:** La scansione con l'opzione -A ha fornito dati preziosi per una valutazione approfondita della sicurezza del sistema.

FACOLTATIVO:

1. Procedura Operativa

Passo 1: Avviare Wireshark

- Avvia Wireshark sulla macchina da cui si effettuano le scansioni.
- Seleziona l'interfaccia di rete attiva (es. eth0 o wlan0).
- Applica un filtro per semplificare l'analisi:
  - *tcp.port == 80 || tcp.flags.syn == 1*

Passo 2: Eseguire una scansione TCP completa

- *nmap -sT 192.168.50.101*

- Nmap stabilirà connessioni **completamente aperte** (3-way handshake completo).
- In Wireshark vedrai:
  - Pacchetti **SYN** →
  - Risposte **SYN-ACK** ←
  - Pacchetti **ACK** → (connessione completata)
  - Eventuali **RST** se la porta è chiusa

Passo 3: Eseguire una scansione SYN (half-open)

- *sudo nmap -sS 192.168.50.101*

- Nmap **non completa** la connessione.
- In Wireshark vedrai:
  - Pacchetti **SYN** →
  - Risposte **SYN-ACK** ←
  - Pacchetti **RST** → (per interrompere la connessione)