Progetto S11 – L5

BONUS 1 – Esplorazione di Nmap

Executive Summary

In questo esercizio ho utilizzato **Nmap per esplorare host e servizi di rete**. Ho **analizzato le principali opzioni del tool, eseguito scansioni sul localhost, sulla rete locale e su un server pubblico di test, identificando porte aperte, servizi attivi e informazioni sul sistema operativo**. L'attività ha evidenziato il ruolo di Nmap sia come strumento di sicurezza sia come possibile strumento di ricognizione offensiva.

Introduzione

L'obiettivo dell'esercizio è acquisire familiarità con Nmap e comprenderne l'utilizzo nelle attività di network discovery e security assessment. **Attraverso scansioni mirate ho osservato come individuare host attivi, porte aperte e servizi in esecuzione, valutando le implicazioni di sicurezza legate all'esposizione dei servizi di rete**.

Nota metodologica

Nel presente esercizio BONUS **non sono stati inseriti screenshot a scopo dimostrativo, poiché l'attività si basa sull'analisi e interpretazione degli output testuali generati da Nmap e delle informazioni presenti nelle man pages**.

Le scansioni producono risultati standardizzati, riportati e descritti nel presente report; pertanto, la documentazione testuale è ritenuta sufficiente mente dettagliata.

Obiettivi

- Parte 1: Esplorazione di Nmap
- Parte 2: Scansione delle Porte Aperte

Parte 1 – Esplorazione di Nmap

Avvio la VM CyberOps Workstation e apro un terminale.
Eseguo il comando:
man nmap

per consultare la documentazione ufficiale del tool.

Domanda:

Cos’è Nmap?

Risposta:

Nmap (Network Mapper) è una potente utility di rete utilizzata per la scoperta di host e la scansione di porte e servizi. È ampiamente impiegata per attività di audit e analisi della sicurezza.

Domanda:

Per cosa viene usato nmap?

Risposta:

Nmap viene utilizzato per:

- Port scanning
- Identificazione dei servizi e delle versioni
- Rilevamento del sistema operativo
- Network discovery
- Valutazioni di sicurezza

Analizzando gli esempi presenti nella documentazione, individuo il comando:
nmap -A -T4 scanme.nmap.org

Domanda:

Qual è il comando nmap usato?

Risposta:

Il comando utilizzato è:
nmap -A -T4 scanme.nmap.org

Domanda:

Cosa fa l’opzione -A?

Risposta:

L’opzione -A abilita una scansione avanzata che include:

- Rilevamento dei servizi e delle versioni
- Identificazione del sistema operativo
- Esecuzione di script NSE
- Traceroute

Domanda:

Cosa fa l’opzione -T4?

Risposta:

L’opzione -T4 imposta un livello di timing aggressivo per velocizzare la scansione su reti affidabili.

Parte 2 – Scansione delle Porte Aperte

Scansione del localhost

Eseguo:
nmap -A -T4 localhost

Domanda:

Quali porte e servizi sono aperti?

Risposta:

Dall’output risultano aperte:

- 21/tcp – servizio FTP

Domanda:

Per ognuna delle porte aperte, registra il software che fornisce i servizi.

Risposta:

- 21/tcp (FTP) → vsftpd 2.0.8 o superiore

Scansione della rete locale

Eseguo:
ip address

per determinare indirizzo IP e subnet mask.

Domanda:

Registra l’indirizzo IP e la subnet mask per la tua VM.

Risposta:

- IP: 10.0.2.15

- Subnet mask: 255.255.255.0 (/24)

Domanda:

A quale rete appartiene la tua VM?

Risposta:

La rete di appartenenza è:

10.0.2.0/24

Per individuare altri host nella LAN eseguo:
nmap -A -T4 10.0.2.0/24

Domanda:

Quanti host sono attivi?

Risposta:

Risultano attivi:

- 4 host

Domanda:

Elenca gli indirizzi IP degli host sulla stessa LAN della tua VM e alcuni servizi disponibili.

Risposta:

Host attivi:

- 10.0.2.15
- 10.0.2.4
- 10.0.2.3
- 10.0.2.2

Servizi rilevati:

- 21/tcp – FTP (vsftpd)
- 22/tcp – SSH (OpenSSH)
- 23/tcp – Telnet

Scansione di un server remoto

Eseguo:
nmap -A -T4 scanme.nmap.org

Domanda:

Qual è lo scopo di questo sito?

Risposta:

È un server pubblico messo a disposizione dal team Nmap per consentire scansioni di test in modo legale e controllato.

Domanda:

Quali porte e servizi sono aperti?

Risposta:

- 22/tcp – SSH
- 80/tcp – HTTP
- 9929/tcp – Nping echo
- 31337/tcp – tcpwrapped

Domanda:

Quali porte e servizi sono filtrati?

Risposta:

- 25/tcp – SMTP
- 135/tcp – MSRPC
- 139/tcp – NetBIOS
- 445/tcp – Microsoft-DS
- 593/tcp – HTTP-RPC
- 4444/tcp – krb524

Domanda:

Qual è l’indirizzo IP del server?

Risposta:

45.33.32.156

Domanda:

Qual è il sistema operativo?

Risposta:

Linux

Domanda di Riflessione

Come può Nmap aiutare con la sicurezza della rete? Come può essere usato in modo malevolo?

Risposta:

Nmap aiuta la sicurezza perché consente di:

- Identificare porte aperte
- Individuare servizi esposti
- Rilevare configurazioni errate
- Supportare attività di hardening

Può essere utilizzato in modo malevolo per:

- Effettuare ricognizione
- Individuare servizi vulnerabili
- Preparare attacchi mirati

Conclusioni

L’esercitazione mi ha permesso di c**omprendere in modo pratico il funzionamento di Nmap e il suo utilizzo nell’analisi delle reti**.

Ho verificato come sia possibile **identificare host attivi, porte aperte e servizi esposti, elementi fondamentali per valutare la superficie di attacco di un sistema**.

L’attività conferma l’importanza di Nmap sia in ambito difensivo sia in fase di ricognizione offensiva.