BONUS_S10_L5_Nmap_&_MySQL

Consegna_Bonus1

Topologia Obiettivi

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

Contesto / Scenario

La scansione delle porte fa solitamente parte di un attacco di ricognizione. Esistono diversi metodi di scansione delle porte utilizzabili. Esploreremo come usare l'utility Nmap. Nmap è una potente utility di rete usata per la scoperta della rete e l'audit di sicurezza.

Risorse Richieste

- Macchina virtuale CyberOps Workstation
- Accesso a Internet

Svolgimento_Bonus1

Cos'è Nmap? Per cosa viene usato nmap?

Nmap (Network Mapper) è uno strumento open-source ampiamente utilizzato nell'ambito della sicurezza informatica e dell'amministrazione di rete. Il suo scopo principale è identificare host e servizi presenti su una rete, rilevando porte aperte, sistemi operativi, applicazioni e potenziali vulnerabilità.

E' uno strumento fondamentale sia per amministratori di sistema sia per analisti di sicurezza. Fornisce una panoramica completa sulla superficie di attacco di un host o di una rete e, se utilizzato correttamente, aiuta a prevenire intrusioni e migliorare la sicurezza.

Guarda l'Esempio 1. Qual è il comando nmap usato? Cosa fa l'opzione A? Cosa fa l'opzione T4?

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

nmap: programma eseguibile.

-A: esegue l'OS detection, version detection, script scan e traceroute. Può aumentare rumore e tempo.

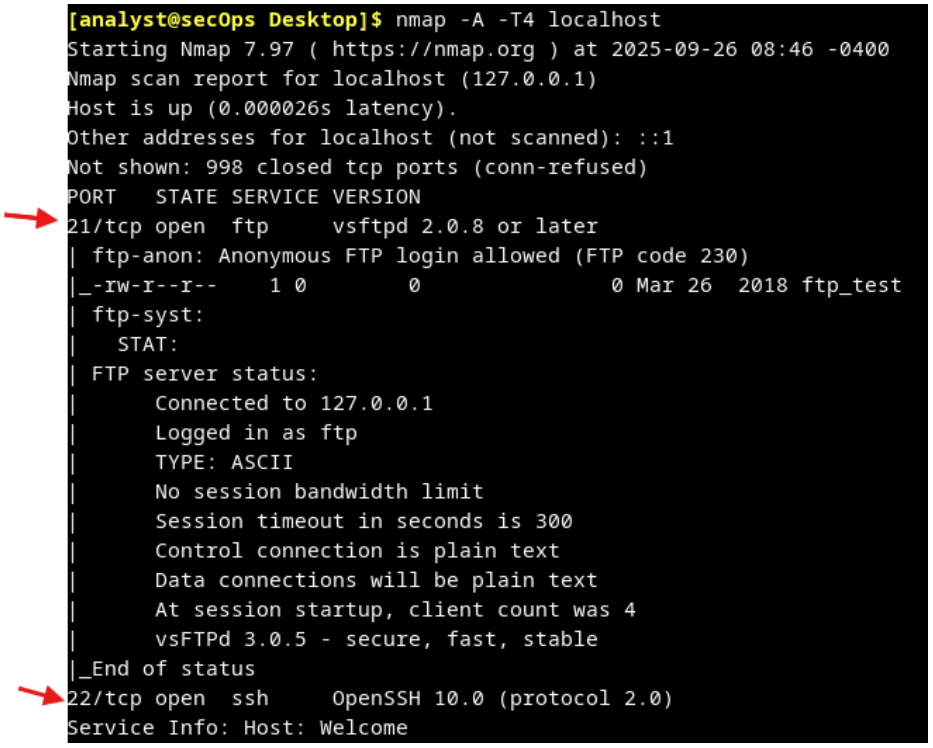
-T4: profilo di timing; possibili valori -T0..-T5 (da molto lento/stealth a molto veloce). -T4 è veloce, usabile solo su connessioni stabili; da evitare quando è richiesto lo stealth.

scanme.nmap.org: target; può essere un nome host, IP singolo, range CIDR o file di target.

Scansiona il tuo localhost. Quali porte e servizi sono aperti?

Le porte ed i servizi aperti sono:

-porta 21 tcp(File Transfer Protocol)software: vsftpd 2.0.8
-porta 22 tcp (secure shell)software:OpenSSH 7.7



Scansiona la tua rete. Registra l'indirizzo IP e la subnet mask per la tua VM. A quale rete appartiene la tua VM?

Essendo in rete NAT, anche la mia VM ha IP 10.0.2.15 ed appartiene alla rete 10.0.2.0/24.

Quanti host sono attivi?

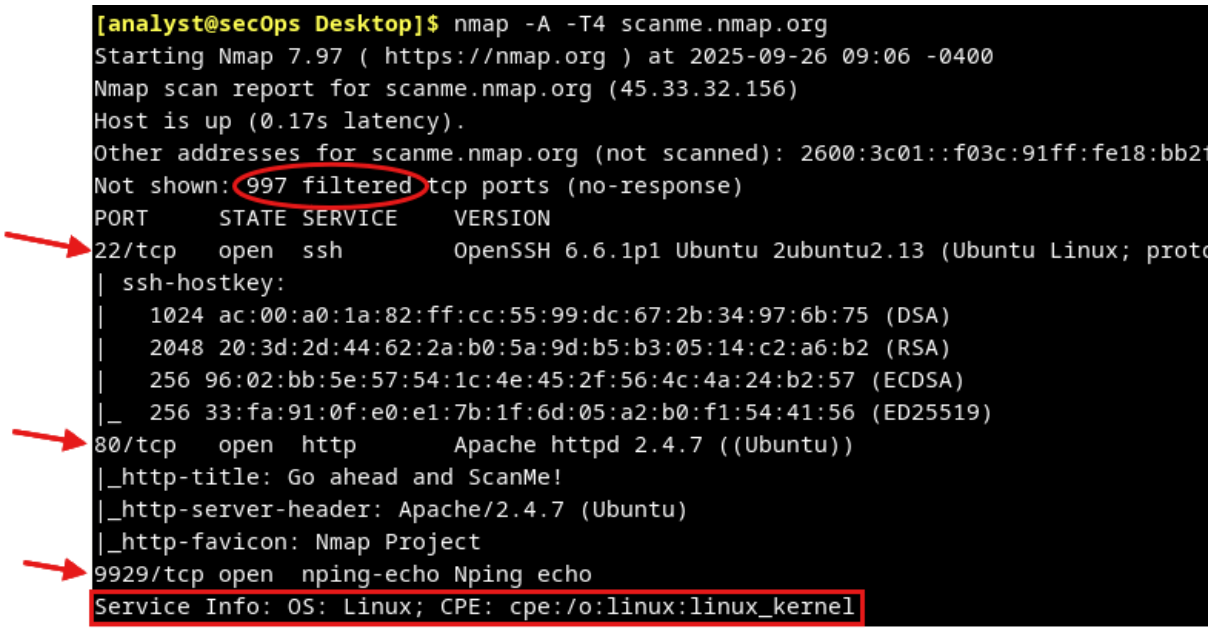
Non avendo altre VM operative all'interno della rete, l'unico dispositivo rilevato è quello precedentemente descritto con ip 10.0.2.15 e con le porte elencate in precedenza.

Qual è lo scopo del sito scanme.nmap.org?

Aiutare le persone a conoscere Nmap e ad esercitarsi con esso permettendo loro di avere un target verso cui testare le varie tipologie di scansioni.

Al prompt del terminale, inserisci nmap A T4 scanme.nmap.org. Quali porte e servizi sono aperti? Quali porte e servizi sono filtrati? Qual è l'indirizzo IP del server? Qual è il sistema operativo?

Utilizzando il comando proposto ricaviamo le seguenti informazioni:



open ports:

22ssh → OpenSSH 6.6.1p1
80http → Apache httpd 2.4.7
9929nping

Filtered Ports (no-response): le restanti 997 che prende in considerazione la scansione

OS: Linux

Domanda di Riflessione Nmap è uno strumento potente per l'esplorazione e la gestione della rete. Come può Nmap aiutare con la sicurezza della rete? Come può Nmap essere usato da un attore malevolo come strumento nefasto?

Nmap aiuta la sicurezza di rete permettendoti di:

a) Valutare delle Vulnerabilità tramite identificazioni di porte aperte o rilevamento servizi vulnerabili.
b) Fare Audit di Sicurezza e Penetration Testing tramite simulazioni di attacchi o verifica delle regole dei firewall.
c) Verificare configurazioni errate o non autorizzate
d) Gestire la rete, es:monitoraggio rete o rilevamento dispositivi

La stessa potenza di Nmap che lo rende prezioso per la difesa, lo rende anche un'arma formidabile nelle mani di un attaccante perché gli permette di:

a) fare ricognizione scoprendo obiettivi,identificare punti deboli o conoscere il sistema operativo per usare exploit specifici
b) gli permette di preparare bene un exploitation
c) permette una mappatura per attacchi mirati

Conclusione:

Nmap aiuta la sicurezza mappando la rete: trova host attivi, porte e servizi, identifica versioni/OS e permette di verificare patch, policy di firewall e cambiamenti rispetto alla baseline — utile per inventari, auditing e response.

Un attore malevolo usa Nmap per ricognizione: scopre servizi vulnerabili, versioni da sfruttare e punti di ingresso per pianificare attacchi o movimento laterale.

Consegna_Bonus2

Obiettivi

In questo laboratorio, visualizzerai un file PCAP di un attacco precedente contro un database SQL.

- Parte 1 Aprire Wireshark e caricare il file PCAP.
- Parte 2 Visualizzare l'attacco di SQL Injection.
- Parte 3 L'attacco di SQL Injection continua...
- Parte 4 L'attacco di SQL Injection fornisce informazioni di sistema.
- Parte 5 L'attacco di SQL Injection e le informazioni sulle tabelle
- Parte 6 L'attacco di SQL Injection si conclude.

Contesto / Scenario

Gli attacchi di SQL injection consentono agli hacker malintenzionati di digitare istruzioni SQL in un sito web e ricevere una risposta dal database. Ciò permette agli aggressori di manomettere i dati correnti nel database, falsificare identità e compiere varie azioni dannose. È stato creato un file PCAP per consentirti di visualizzare un attacco precedente contro un database SQL. In questo laboratorio, visualizzerai gli attacchi al database SQL e risponderai alle domande.

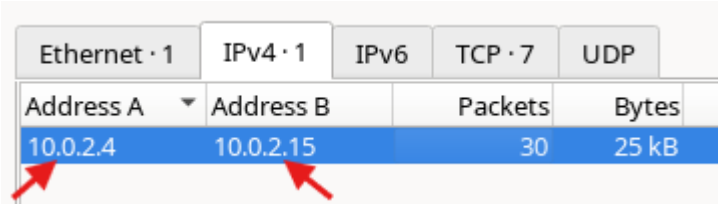
Risorse Richieste

- Macchina virtuale CyberOps Workstation

Svolgimento_Bonus2

Quali sono i due indirizzi IP coinvolti in questo attacco di SQL injection in base alle
informazioni visualizzate?

Gli indirizzi interessati sono il 10.0.2.4 (attaccante) che invia diverse richieste GET ed il 10.0.2.15(macchina target) che risponde alle richieste.



Qual è la versione?

5.7.12-0ubuntu1.1

Quale utente ha l'hash della password di 8d3533d75ae2c3966d7e0d4fcc69216b?

L'utente è il 1337:

Qual è la password in chiaro?

La psw in chiaro è charley.

Domande di Riflessione

1. Qual è il rischio che le piattaforme utilizzino il linguaggio SQL?

Usare SQL espone i sistemi al rischio di **SQL injection**, che permette a un attaccante di manipolare query e accedere/modificare dati sensibili; la gravità dipende dai privilegi che la query può raggiungere e dall'abilità dell'attaccante.

2. Naviga in internet ed esegui una ricerca per "prevenire attacchi di SQL injection". Quali sono 2 metodi o passaggi che possono essere adottati per prevenire gli attacchi di SQL injection?

Usare query parametrizzate / prepared statements (o stored procedure ben progettate) per separare il codice SQL dai dati, quindi i valori forniti dall'utente vengono trattati come *dati* e non come parte dell'istruzione SQL.

Quando usarlo: sempre, è la prima difesa raccomandata per qualsiasi input destinato al DB. Limiti: richiede supporto dal driver/ORM e corretta implementazione; non sostituisce altre difese.

Validare/filtrare l'input (whitelisting) e mettere controlli perimetrali come un WAF + principio del minimo privilegio sul DB per rendere la validazione rigida (accettare solo formati/valori previsti) e ridurre la lettura di dati malevoli; il WAF può bloccare pattern noti di SQLi e il principio del minimo privilegio limita l'impatto se una query viene manipolata.

Quando usarlo: insieme alle query parametrizzate per difesa in profondità. Limiti: la sola validazione non è infallibile; il WAF può generare falsi positivi/negativi.

Conclusioni

Il laboratorio combina due competenze fondamentali: l'uso di **Nmap** per la ricognizione e la gestione della superficie di attacco, e l'analisi forense di un **attacco SQL injection** tramite file PCAP.

Dall'esercitazione emergono tre messaggi chiave:

- Conoscere la propria rete (inventario di host, porte e servizi) riduce la sorpresa e facilita patch e containment.

- Le tecniche di attacco viste (ricognizione con Nmap, iniezione SQL) sfruttano difetti semplici ma comuni nelle configurazioni e nel trattamento dell'input.

- La difesa efficace richiede più livelli: hardening dei servizi, query parametrizzate/prepared statements, validazione input, privilegi minimi, WAF e monitoraggio continuo.