EPICODE

ESERCIZIO W18D1

SECURITY OPERATION

Azioni preventive

Mungiovì Fabio

TASK

Le azioni preventive mirano a ridurre la possibilità di attacchi provenienti dall'esterno.
Abbiamo visto che a livello di rete, possiamo configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.
La macchina Windows, che abbiamo utilizzato, ha di default il Firewall disabilitato.

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection)
3. Abilitare il Firewall sulla macchina Windows
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.
5. Trovare eventuali differenze e motivarle

Facoltativo:

Monitorare i log di Windows durante queste operazioni:

1. Quali log vengono modificati? (se vengono modificati)
2. Cosa si riesce a trovare?

ESECUZIONE

Per l'esecuzione dell'esercizio, è stata utilizzata una macchina Kali Linux come attaccante e una macchina Windows come target. Gli step seguiti sono i seguenti:

Scansione con Firewall Disattivato

Prima di procedere, è stato verificato che il Firewall sulla macchina Windows fosse disabilitato, come illustrato nella schermata di configurazione del Firewall di Windows[9].

È stata quindi eseguita la prima scansione Nmap con il comando nmap -sV 192.168.50.102.

Output della scansione:

```
┌──(fabiomun㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-24 07:51 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.00095s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:FA:CE:7E (VMware)
Service Info: Host: PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 60.35 seconds
```

Come mostrato in figura la scansione iniziale ha rivelato diverse porte aperte e i relativi servizi in esecuzione sulla macchina Windows:

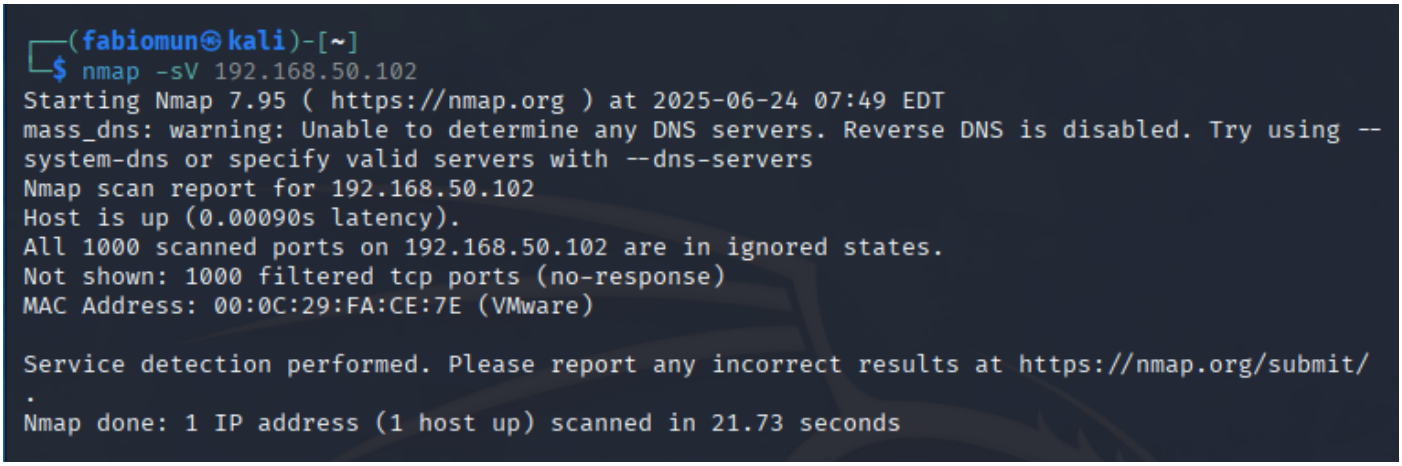
Attivazione del Firewall

Successivamente alla prima scansione, il Firewall di Windows è stato attivato sulla macchina target. Questo è stato eseguito modificando le impostazioni del servizio "Windows Firewall" e abilitando il Firewall tramite il Pannello di Controllo.

Scansione con Firewall Attivato

Dopo aver abilitato il Firewall, è stata eseguita una seconda scansione Nmap con lo stesso comando: nmap -sV 192.168.50.102.

Output della scansione:



Come mostrato in figura, il risultato della seconda scansione è significativamente diverso dalla precedente.

Nmap indica che "All 1000 scanned ports on 192.168.50.102 are in ignored states" e "Not shown: 1000 filtered tcp ports (no-response)".

Questo indica che nessuna porta è risultata aperta o che ha risposto attivamente alla scansione.

Analisi delle Differenze e Conclusioni

Il confronto tra le due scansioni Nmap evidenzia un impatto drastico dell'attivazione del Firewall di Windows sulla visibilità dei servizi esposti.

- **Firewall Disattivato:** Con il Firewall disattivato, Nmap è stato in grado di rilevare diverse porte aperte e i servizi associati, come RPC, NetBIOS e SMB (port 445).
  Questo scenario rappresenta una superficie di attacco ampia, dove un attaccante potrebbe identificare vulnerabilità nei servizi esposti per compromettere la macchina.
- **Firewall Attivato:** Con il Firewall attivato, tutte le porte scansionate sono risultate "filtered" (filtrate). Questo significa che il Firewall ha intercettato e bloccato i tentativi di connessione di Nmap, impedendo al tool di determinare lo stato delle porte e la versione dei servizi in ascolto.
  In questo caso, il Firewall agisce come una barriera, riducendo drasticamente la superficie di attacco visibile dall'esterno.

Motivazione delle Differenze:

Le differenze sono motivate dal ruolo fondamentale del Firewall come strumento di sicurezza perimetrale.
Quando il Firewall è attivo e configurato correttamente, esso filtra il traffico di rete in entrata e in uscita in base a regole predefinite.
Nel nostro caso, il Firewall di Windows ha bloccato le richieste di Nmap, che tentavano di stabilire connessioni ai servizi sulla macchina target. Di conseguenza, Nmap ha ricevuto risposte di tipo "filtrato" o "nessuna risposta", non potendo così identificare i servizi o le porte aperte.

Questo esercizio dimostra chiaramente come l'implementazione di un Firewall sia un'azione preventiva cruciale per la sicurezza di rete. Un Firewall ben configurato può mitigare significativamente la possibilità di attacchi esterni, rendendo molto più difficile per gli attaccanti individuare e sfruttare le vulnerabilità presenti sui sistemi.

FACOLTATIVO

Durante le operazioni di attivazione e disattivazione del Firewall, e le conseguenti scansioni di rete, è consigliabile monitorare i log di sistema di Windows per osservare gli eventi generati.

Sebbene non siano stati acquisiti specifici log per questo esercizio, di seguito si descrivono quali tipi di log sarebbero tipicamente influenzati e cosa si potrebbe aspettare di trovare.

Log Interessati

I log di Windows che verrebbero principalmente modificati e che meriterebbero un'attenzione particolare durante un esercizio di questo tipo sono:

- **Log di Sicurezza (Security Log):** Questo log registra eventi relativi alla sicurezza del sistema, inclusi i tentativi di accesso, le modifiche alle policy di sicurezza e le attività del Firewall.
- **Log di Sistema (System Log):** Contiene eventi generati dai componenti del sistema operativo, inclusi gli avvii e gli arresti dei servizi (come il servizio Windows Firewall), errori hardware e di sistema.
- **Log "Windows Firewall con Sicurezza Avanzata" (specifico di Windows Firewall):** Questo log, se abilitato e configurato, registra attività più dettagliate relative al Firewall, come le connessioni bloccate, le regole applicate e i tentativi di accesso non autorizzati.

Cosa si Potrebbe Trovare nei Log

Analizzando i log durante le operazioni descritte nell'esercizio, ci si aspetterebbe di trovare eventi che confermano le azioni intraprese e le loro conseguenze:

- **Disattivazione del Firewall:**
    - Nel **Log di Sistema**, si potrebbero trovare eventi relativi all'arresto del servizio "Windows Firewall" (event ID specifici per l'arresto del servizio).
    - Nel **Log di Sicurezza**, potrebbero esserci audit di modifiche alle policy del Firewall o all'alterazione delle sue impostazioni.
- **Scansione Nmap con Firewall Disattivato:**
    - In assenza di un Firewall attivo, i log potrebbero essere meno eloquenti riguardo ai tentativi di connessione in entrata, a meno che non ci siano altri sistemi di auditing o servizi che registrano tentativi di connessione a porte specifiche (es. log di IIS per il traffico web, se presente).
- **Attivazione del Firewall:**
    - Nel **Log di Sistema**, si vedrebbero eventi relativi all'avvio del servizio "Windows Firewall" (event ID specifici per l'avvio del servizio).
    - Nel **Log di Sicurezza**, si registrerebbero eventi di audit legati all'applicazione di nuove regole o all'abilitazione delle policy del Firewall.
- **Scansione Nmap con Firewall Attivato:**
    - Nel **Log "Windows Firewall con Sicurezza Avanzata",** se il logging delle connessioni bloccate è abilitato, si troverebbero numerosi eventi che indicano tentativi di connessione in entrata bloccati, con dettagli sugli indirizzi IP di origine (quello della macchina Kali), le porte di destinazione e le regole che hanno causato il blocco. Questo fornirebbe una prova diretta dell'efficacia del Firewall nel filtrare il traffico malevolo o indesiderato.
    - Il **Log di Sicurezza** potrebbe mostrare eventi di "audit failure" o "dropped packets" se configurato per registrare tentativi di connessione non riusciti.