EPICODE-CS0124
S9/L1 - Pratica

Flaviano Sedici

Indice

Riferimenti e versioni

Responsabile del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Riferimento	Data
1.0	Redazione documento	Responsabile	18/03/2024

1. Traccia

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno.

Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

La macchina Windows XP 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:

- Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
- Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection e -o nome file report per salvare in un file l'output)
- Abilitare il Firewall sulla macchina Windows XP
- Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch–sV.
- Trovare le eventuali differenze e motivarle.

Che differenze notate? E quale può essere la causa del risultato diverso?

Requisiti:

Configurate l'indirizzo di Windows XP come di seguito: **192.168.240.150**

Configurate l'indirizzo della macchina Kali come di seguito: **192.168.240.100**

1.1. Definizioni e impostazioni laboratorio

Prima di iniziare le scansioni richieste, definiamo il contesto operativo, gli strumenti utilizzati e impostiamo le Virtual Machine utilizzate per il nostro laboratorio.

1.1.1. Definizioni

Firewall

Un firewall è un dispositivo di sicurezza che monitora e controlla il traffico di rete per proteggere una rete o un sistema informatico da accessi non autorizzati e minacce informatiche. Filtra il traffico in base a regole predefinite, bloccando o consentendo il passaggio dei pacchetti in base a indirizzi IP, porte e protocolli. Possono anche implementare funzionalità avanzate come il rilevamento delle intrusioni e la prevenzione dei DDoS. Il suo scopo è quello di proteggere la rete e i dati da attacchi e intrusioni, mantenendo l'integrità e la sicurezza del sistema.

Nmap

Nmap è uno strumento di scansione di rete open source che consente agli amministratori di rete di esaminare la sicurezza e la configurazione di dispositivi e servizi in una rete. Utilizza tecniche avanzate di scansione per rilevare e mappare dispositivi, porte aperte e servizi in esecuzione su una rete. Fornisce informazioni dettagliate sulle vulnerabilità di sicurezza e l'architettura di rete, consentendo agli utenti di valutare e migliorare la sicurezza della propria infrastruttura IT. Nmap è ampiamente utilizzato per l'analisi delle reti, il test della sicurezza e la gestione della rete.

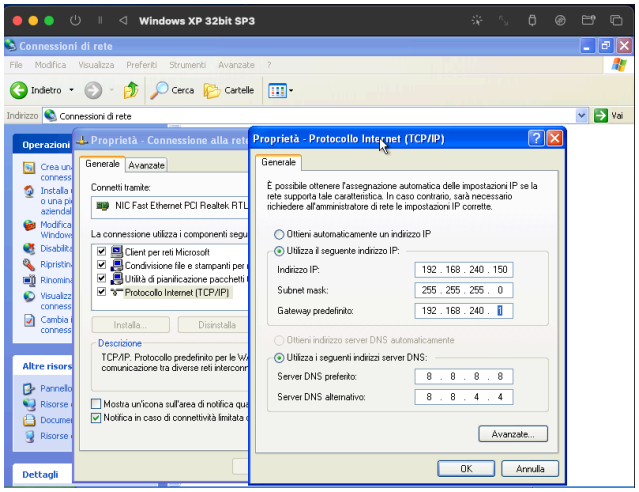
1.1.2.Impostazioni di laboratorio

Come richiesto nella traccia, gli indirizzi IP delle Macchine Virtuali sono stati impostati su:

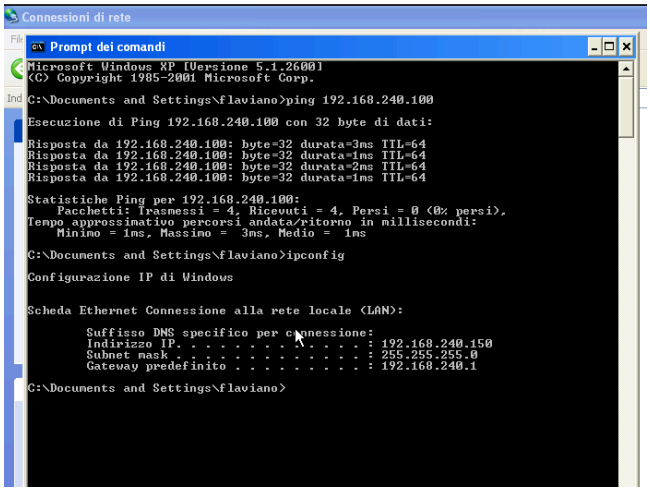
Kali Linux - 192.168.240.100/24

Windows XP - 192.168.240.150/24

Per verificare la corretta configurazione dell'ambiente di test, procediamo con un comando ping su entrambe le VM.



Impostazioni di rete Windows XP



Ping di test con la VM Kali

1.2. Esecuzione di nmap con firewall disattivato

1.2.1. Impostazione firewall Windows XP

Verifichiamo che il firewall di Windows XP sia disattivato.

Impostazione firewall Windows XP

1.2.2. Esecuzione del comando nmap

Eseguiamo il comando:

nmap 192.168.240.150 -SV -Pn -o report_no_firewall.txt

```
┌──(flaviano㉿kaliArm)-[~/Desktop/CSS_0124/S9]
└─$ nmap 192.168.240.150 -sV -Pn -o report_no_firewall.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:51 CET
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 192.168.240.150
Host is up (0.00093s latency).
Not shown: 996 closed tcp ports (conn-refused)
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 Vista Embedded microsoft-ds (workgroup: WORK
GROUP)
1025/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: FLAVIANO-XP; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:micros
oft:windows_vista

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 7.31 seconds
```

Risultato della scansione di Windows XP

Le porte aperte rilevate dalla scansione sono le 135, 139, 445 e la 1025.

1.3. Esecuzione di nmap con firewall attivato

1.3.1. Impostazione firewall Windows XP

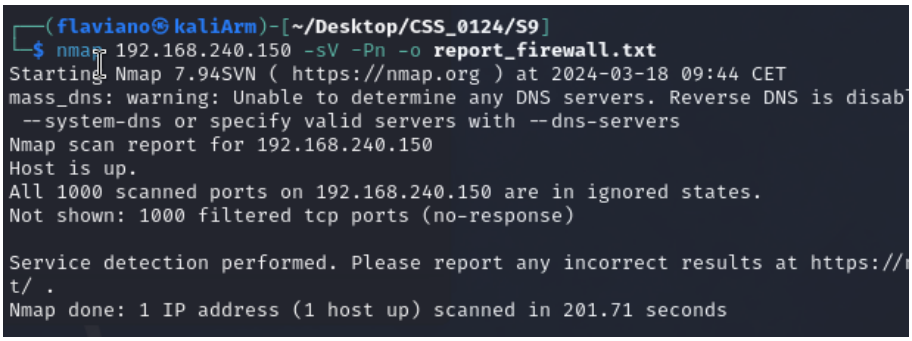
Verifichiamo che il firewall di Windows XP sia attivato.

Impostazione firewall Windows XP

1.3.2. Esecuzione del comando nmap

Eseguiamo il comando:

nmap 192.168.240.150 -SV -Pn -o report_firewall.txt



Risultato della scansione di Windows XP

Con l'utilizzo del firewall la scansione non produce alcun risultato, e le porte precedentemente scoperte non sono visibili.

Il firewall in questo caso impedisce questo tipo di scansioni rilevandole come "malevole".

Al fine di aggirare tale blocco, si potrebbe utilizzare una scansione più lenta tramite lo **switch -T2.** Questo renderebbe la nostra scansione più lenta e meno "intrusiva" non facendola rilevare come una minaccia da parte del firewall.

In alternativa si potrebbe procedere alla scansione delle singole porte cercando di identificare quelle che potenzialmente potrebbero contenere una vulnerabilità.