S7-L5 Vulnerabilità Java Metasploitable 2

INDICE

Sommario

ESERCIZIO

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 in formato OVA che abbiamo utilizzato nella Unit 2 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 XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

IP WINDOWS XP & KALI LINUX

Come prima cosa andiamo a cambiare i settaggi delle schede di rete delle due macchine. Entrambe le macchine virtuali sono impostate in “RETE INTERNA” e configurandole, come si può vedere di seguito tramite le slide, facciamo in modo che comunichino una con l’altra impostando gli IP richiesti dall’esercizio assegnatoci.

Kali: 192.168.240.100

Windows XP: 192.168.240.150

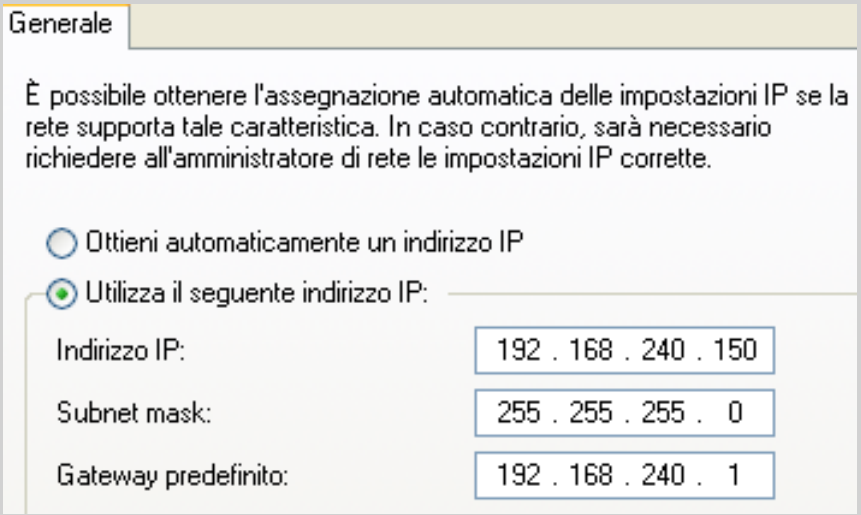
Gateway: 192.168.240.1

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.240.1
```



PRIMA SCANSIONE NMAP

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 17:06 CET
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.240.150
Host is up (0.00029s latency).
Not shown: 996 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 XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:DD:AA:BF (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.62 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 17:07 CET
Nmap scan report for 192.168.240.150
Host is up (0.00032s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:DD:AA:BF (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.72 seconds
```

Come possiamo vedere nella foto successiva, andremo ad utilizzare NMAP tramite il comando “sudo nmap -sV 192.168.240.150” per poter vedere tutte le porte disponibili e vedere se sono aperte o chiuse.

Il comando -sV andrà a mostrarci ogni singolo servizio relativo ad ogni porta che verrà individuata, invece il comando -T3 imposta una scansione di tempistica media, così da non essere troppo invadente (non interrompendo la scansione per via delle restrizioni di time sleep), ma riuscendo ugualmente a carpire abbastanza informazioni che ci servono.

SECONDA SCANSIONE NMAP

Dopodiché attiviamo il Firewall sulla macchina Windows XP e riutilizziamo lo stesso comando per NMAP e vediamo quali porte ci trova.

Nel secondo caso possiamo notare che delle 4 porte che prima erano aperte ce ne rileva solamente 1, ovvero la 3389.

Cos’è NMAP:

Nmap, acronimo di Network Mapper, è uno strumento di scansione di rete ampiamente utilizzato per esaminare, mappare e valutare la sicurezza di reti informatiche. Si tratta di un'applicazione open-source dotata di diverse funzionalità che consentono agli amministratori di sistema e agli esperti di sicurezza di condurre analisi approfondite su reti e dispositivi connessi.

Nmap è in grado di individuare e identificare dispositivi all'interno di una rete, determinare le porte aperte e i servizi in esecuzione su tali porte. Questa capacità di rilevare le caratteristiche della rete aiuta a comprendere la topologia di una rete e a individuare eventuali punti vulnerabili. Gli amministratori di sistema possono utilizzare Nmap per verificare la configurazione di sicurezza di una rete, identificare potenziali falle di sicurezza e valutare l'esposizione di servizi ai potenziali attacchi.

CONSIDERAZIONI FINALI

Differenze notate:

Nella prima scansione senza il Firewall attivo, potreste ottenere un elenco completo dei servizi aperti sulla macchina Windows XP.

Nella seconda scansione con il Firewall attivo, potrebbero esserci differenze nei risultati. Alcuni servizi potrebbero essere invisibili o non rilevuti a causa delle regole di filtraggio del Firewall.

Cause del risultato diverso:

Il Firewall blocca alcuni servizi: Il Firewall potrebbe impedire l'accesso a determinati servizi, rendendoli invisibili durante la scansione.

Regole di filtraggio personalizzate: Se sono state configurate regole di filtraggio personalizzate, potrebbero influenzare la visibilità dei servizi durante la scansione.

Porte chiuse dal Firewall: Il Firewall potrebbe chiudere alcune porte, rendendo i servizi associati a tali porte non accessibili esternamente.