SECURITY OPERATION AZIONI PREVENTIVE

MATTIA PASTORELLI

COMANDA:

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:
1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP 2.Effettuate una scansione con nmapsulla macchina target (utilizzate lo switch–sV, per la service detectione -o nomefilereportper salvare in un file l'output)
3.Abilitare il Firewall sulla macchina Windows XP
4.Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch–sV.
5.Trovare le eventuali differenze e motivarle.

NMAP

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 192.168.240.150 -o report.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 07:20 EST
Nmap scan report for 192.168.240.150
Host is up (0.0014s latency).
Not shown: 997 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
MAC Address: 08:00:27:C5:CE:78 (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/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.49 seconds
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 192.168.240.150 -o reportFirewall.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 07:21 EST
Nmap scan report for 192.168.240.150
Host is up (0.0023s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C5:CE:78 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.60 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

Settati gli IP statici richiesti (192.168.240.100 per Kali e 192.168.240.150 per Windows XP).

Startiamo il servizio nmap attraverso il comando:

nmap -sV 192.168.240.150 -o file_testo.txt

namp è lo strumento che utilizziamo per fare la scansione di rete.

-sV= specifica di eseguire una scansione di versione, cercando di identificare i servizi e le loro versioni in esecuzione sulle porte aperte dell'host.

Ip vittima

-o + file_testo.txt = comando utilizzato per creare un file.txt con all’interno un report della scansione.

REPORT

```
1 # Nmap 7.94SVN scan initiated Mon Feb  5 07:20:38 2024 as: nmap -sV -o
  report.txt 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0014s latency).
4 Not shown: 997 closed tcp ports (reset)
5 PORT    STATE SERVICE      VERSION
6 135/tcp open  msrpc        Microsoft Windows RPC
7 139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
9 MAC Address: 08:00:27:C5:CE:78 (Oracle VirtualBox virtual NIC)
10 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
  cpe:/o:microsoft:windows_xp
11
12 Service detection performed. Please report any incorrect results at
  https://nmap.org/submit/ .
13 # Nmap done at Mon Feb  5 07:21:03 2024 -- 1 IP address (1 host up)
  scanned in 24.49 seconds
14
```

```
1 # Nmap 7.94SVN scan initiated Mon Feb  5 07:21:46 2024 as: nmap -sV -o
  reportFirewall.txt 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0023s latency).
4 All 1000 scanned ports on 192.168.240.150 are in ignored states.
5 Not shown: 1000 filtered tcp ports (no-response)
6 MAC Address: 08:00:27:C5:CE:78 (Oracle VirtualBox virtual NIC)
7
8 Service detection performed. Please report any incorrect results at
  https://nmap.org/submit/ .
9 # Nmap done at Mon Feb  5 07:22:25 2024 -- 1 IP address (1 host up)
  scanned in 38.60 seconds
10
```

Al termine delle 2 scansioni nmap avrà generato automaticamente i Report visibili nelle immagini a lato.

Possiamo notare nella prima immagine che la scansione, senza firewall attivo, ha generato un output con 3 porte porte aperte e relative versioni.

Mentre nel secondo caso, con firewall attivo, ci è stato restituito un output in cui ci viene espressamente detto che sono state scansionate 1000 porte ma sono state ignorate.
Ovvero, il firewall è stato impostato per ignorare le richieste di scansione da parte di un utente esterno.