Esercitazione 4 Modulo 5 - Alessio Russo

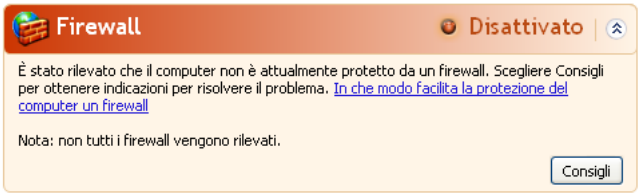
Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. 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 e -o nomefilereport per 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 eventuali differenze e motivarle

Firewall Attivo Windows:


```
└─$ sudo nmap -sV 192.168.50.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-06 19:28 CET
Nmap scan report for 192.168.50.200
Host is up (0.0011s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
2869/tcp closed icslap
MAC Address: 08:00:27:96:7F:A9 (Oracle VirtualBox virtual NIC)
```

Firewall non attivo:




```
└─$ sudo nmap -sV 192.168.50.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-06 19:30 CET
Nmap scan report for 192.168.50.200
Host is up (0.00062s 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: 08:00:27:96:7F:A9 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:mi
crosoft:windows_xp
```

Differenze:

Le differenze principali tra le due scansioni, dove nella prima il firewall è attivo e nella seconda il firewall non è attivo, si concentrano sui risultati delle porte e sui servizi rilevati:

Nella prima scansione (con firewall attivo):
- È stata rilevata solo una porta, la porta 2869/tcp, che è stata contrassegnata come "closed". Questo significa che il servizio associato a quella porta non ha risposto alle richieste di connessione di Nmap. Il firewall potrebbe aver bloccato le richieste di Nmap a questa porta, impedendo quindi la connessione.
- Tutte le altre porte (999 porte) sono state contrassegnate come "filtered", il che significa che Nmap non ha ricevuto alcuna risposta da queste porte. Questo potrebbe essere dovuto al firewall che ha bloccato le richieste di Nmap verso queste porte.
- Non sono stati rilevati altri servizi attivi.

Nella seconda scansione (con firewall non attivo):
- Sono state rilevate tre porte TCP aperte e associate a servizi attivi: la porta 135/tcp per il servizio Microsoft Windows RPC, la porta 139/tcp per il servizio Microsoft Windows netbios-ssn, e la porta 445/tcp per il servizio Microsoft Windows XP microsoft-ds.
- Queste porte sono state contrassegnate come "open", indicando che i servizi associati a queste porte sono in ascolto e rispondono alle richieste di connessione.
- Questo suggerisce che senza il firewall attivo, Nmap ha avuto successo nell'interrogare questi servizi e nel ricevere risposte dai servizi attivi.

In sintesi, l'attivazione del firewall ha influenzato la capacità di Nmap di rilevare servizi attivi sulle porte specifiche. Con il firewall attivo, molte porte sono state filtrate o non hanno risposto, mentre senza il firewall, Nmap è stato in grado di rilevare i servizi attivi sulle porte specificate.