CONSEGNA W18D2

Traccia: 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 e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.
5. Trovare le eventuali differenze e motivarle.

Come richiesto dalla traccia facciamo due scansioni dalla nostra Kali avendo come target la macchina Windows con Ip 192.168.50.102, dove nella prima scansione avremo il firewall disattivo mentre nella seconda lo attiveremo. Lo scopo dell'esercitazione è quello di vedere se ed eventualmente argomentare le differenze presenti.
Partiamo con una prima scansione usando il comando nmap -sV (ricordiamo comando che serve ad identificare i servizi, e le versioni di questi ultimi, in esecuzione su porte aperte) verso il target e otteniamo il risultato mostrato nella figura seguente.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 23:42 CET
Nmap scan report for 192.168.50.102
Host is up (0.00039s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime       Microsoft Windows International daytime
17/tcp   open  qotd          Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http          Microsoft IIS httpd 10.0
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)
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5432/tcp open  postgresql?
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:32:C4:74 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; 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 174.80 seconds
```

Eseguiamo poi la stessa scansione attivando però il firewall sulla macchina target

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 23:50 CET
Nmap scan report for 192.168.50.102
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:32:C4:74 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.30 seconds
```

Analizzando le due scansioni notiamo come il firewall nasconde completamente la superficie di attacco:

visto che non può rilevare né porte né servizi. Disattivandolo Nmap rivela servizi critici come possiamo notare dalla prima figura.
Vediamo infatti che con:
Firewall disattivato Nmap riesce a stabilire connessioni TCP con i servizi attivi, ottenendo dettagli sul sistema operativo oltre che dettagli sui servizi. Questo espone la macchina a potenziali attacchi.
Firewall attivato tutte le porte risultano inaccessibili. Il firewall blocca le richieste di scansione, impedendo a Nmap di determinare lo stato delle porte e di identificare i servizi. Anche il fingerprinting dell'OS fallisce.

CARATTERISTICHE	**FIREWALL DISATTIVATO**	**FIREWALL ATTIVATO**
Host	Rilevato attivo	Rilevato attivo
Porte aperte rilevate	135,139,445,3306	Nessuna porta aperta rilevata
Stato delle porte	Porte specifiche su OPEN	Non rilevato
Fingerprint OS	Windows	Nessuna informazione rilevata
Servizi identificati	RPC, NetBIOS, SMB, MySQL, HTTP	Nessun servizio rilevato
Distanza di rete	1 Hop	Non rilevata

Da questa esercitazione notiamo come avere un firewall attivo e ben configurato riduce drasticamente la superfice di attacco diventando non rintracciabile e non scansionabile.