W11D1 - Pratica (2)

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Traccia:

Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target **Windows 7**:

-OS fingerprint
-Syn Scan
-Version detection

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un report contenente le seguenti info (dove disponibili):
IP
Sistema Operativo
Porte Aperte
Servizi in ascolto con versione
Descrizione dei servizi

https://www.poftut.com/nmap-output/

nmap -oN report1 IP

Quesito extra (al completamento dei quesiti sopra):

Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

Non si capisce cosa possa essere perché il firewall sta facendo il suo lavoro:

└─$ sudo nmap -O 192.168.1.11
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-21 16:44 EST
Nmap scan report for 192.168.1.11
Host is up (0.00061s latency).
All 1000 scanned ports on 192.168.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E4:51:47 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.82 seconds

Le porte risultano filtrate, quindi la macchina è protetta da un firewall.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 16:51 EST
Nmap scan report for 192.168.1.11
Host is up (0.00055s latency).
All 1000 scanned ports on 192.168.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E4:51:47 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 24.59 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -sS -T1  192.168.1.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 16:56 EST
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.00% done
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.05% done
Stats: 0:02:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.30% done
Stats: 0:26:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.10% done; ETC: 01:22 (7:59:46 remaining)
Stats: 5:57:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.30% done; ETC: 01:17 (2:23:50 remaining)
Nmap scan report for 192.168.1.11
Host is up (0.00047s latency).
All 1000 scanned ports on 192.168.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E4:51:47 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 30081.45 seconds
```

In pratica Windows 7 è protetto da un firewall e quest'ultimo blocca tutto il traffico.
Non si riesce determinare con gli strumenti attuali, quali siano le porte aperte e chiuse.
Risponde con porte filtarate.

Cybersecurity Analyst 2023