

Esercitazione W11D1 - Pratica 2

Nmap

Fabio Benevento - 16/01/2024

Traccia

Si richiede allo studente di effettuare le seguenti scansioni sul target Windows 7:

- OS fingerprint
- Syn Scan
- Version detection

Implementazione

Nelle seguenti pagine sono illustrati i comandi utilizzati per ricavare le informazioni richieste.

Entrambe le macchine sono collocate sulla stessa sottorete (192.168.50.x) con indirizzi rispettivamente di 192.168.50.100 per Kali Linux e di 192.168.50.102 per Windows 7

OS Fingerprinting (-O)

Tramite l'opzione -O è possibile individuare la versione del sistema operativo che viene stampata in basso al termine della scansione dei servizi come mostrato nell'immagine sottostante.

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 12:08 EST
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: 08:00:27:8A:67:81 (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 53.75 seconds
```

Syn Scan (-S)

Tramite l'opzione -S è possibile effettuare la scansione senza effettuare la connessione completa con three-way handshake

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 12:16 EST
Nmap scan report for 192.168.50.102
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:8A:67:81 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 46.58 seconds
```

Version detection (-V)

Il seguente test non è stato condotto in quanto, come emerso con i precedenti comandi, non risultano porte aperte. Ciò potrebbe esser dovuto alla presenza di un firewall / IPS che blocca le richieste in ingresso. Per aggirare queste limitazioni andrebbero adottati metodi specifici che possono riuscire a bypassare il blocco.

Report finale

Di seguito il report in forma tabellare con le informazioni trovate

Fonte	Kali Linux - IP: 192.168.50.100		
Target	Windows 7 - IP: 192.168.50.102		
Tipo di scan	Nmap (varie modalità)		
Numero servizi trovati	nessuna porta esposta		
Porta	Servizio	Versione	Descrizione