

Esercitazione WEEK 11 D1 (2)

Scansione dei servizi con Nmap (Windows 7)

Ettore Farris - 17/01/2024

Descrizione sintetica

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?

1) Scansione con host su reti diverse

Per prima cosa configuriamo le impostazioni di rete, assegnando gli indirizzi IP, modificando eventuali regole firewall che bloccano il traffico inbound e portando la VM Windows 7 su una rete interna diversa da quella in cui c'è Kali tramite le impostazioni di VirtualBox.

Ip Windows 7

```
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b0b9:3bd:84d0:e820%14
    IPv4 Address. . . . . : 192.168.32.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.32.1

Tunnel adapter isatap.{C8CD9050-8854-4D56-8D94-1904DAFE6B72}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

- OS fingerprint

Il sistema, come visibile, è stato individuato come probabile Windows 7.

```
(kali㉿kali) - [~]
$ sudo nmap -O 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 15:31 EST
Nmap scan report for 192.168.32.101
Host is up (0.0045s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.10 seconds
```

- *Syn Scan*

8 porte aperte individuate, tra cui quelle smb.

```
(kali㉿kali) - [~]
$ sudo nmap -sS 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 15:31 EST
Nmap scan report for 192.168.32.101
Host is up (0.0077s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.84 seconds
```

- *Version detection*

```
(kali㉿kali) - [~]
$ sudo nmap -sV 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 15:31 EST
Nmap scan report for 192.168.32.101
Host is up (0.0055s latency).
Not shown: 992 filtered tcp ports (no-response)
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-845Q99004PP; 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 63.42 seconds
```

I servizi che operano sulle 8 porte individuate, a differenza della scansione precedente, ora vengono mostrati con chiarezza.

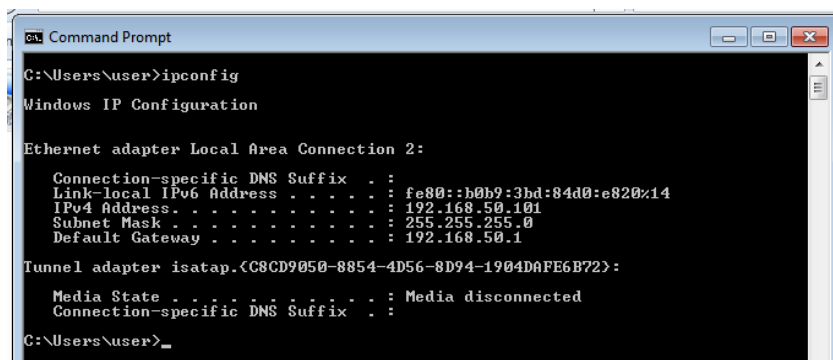
- Esportazione del report

```
(kali㉿kali) - [~]
$ cat report3.txt
# Nmap 7.94 scan initiated Thu Jan 18 15:39:17 2024 as: nmap -sV -oN report3.txt -v 192.168.32.101
Nmap scan report for 192.168.32.101
Host is up (0.0090s latency).
Not shown: 992 filtered tcp ports (no-response)
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jan 18 15:40:22 2024 -- 1 IP address (1 host up) scanned in 64.61 seconds
```

2) Scansione con host sulla stessa rete

Portiamo Windows 7 sulla stessa rete interna di quella di Kali e assegniamo un indirizzo ip appartenente allo stesso dominio di rete (192.168.50.0) dal pannello di controllo di Windows.



```
Command Prompt
C:\Users\User>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b0b9:3bd:84d0:e820%14
    IPv4 Address. . . . . : 192.168.50.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.50.1

Tunnel adapter isatap.{C8CD9050-8854-4D56-8D94-1904DAFE6B72}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
C:\Users\User>
```

Una volta assicurati che le macchine possano pingarsi a vicenda, procediamo con la creazione del report di una scansione -sV che include dettagli rilevanti su OS, porte in ascolto e versione dei servizi.

```
(kali㉿kali) - [~]
$ cat report4.txt
# Nmap 7.94 scan initiated Thu Jan 18 15:47:49 2024 as: nmap -sV -oN report4.txt -v 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.00064s latency).
Not shown: 992 filtered tcp ports (no-response)
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:97:4D:54 (Oracle VirtualBox virtual NIC)
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jan 18 15:48:53 2024 -- 1 IP address (1 host up) scanned in 64.52 seconds
```

3) Quesito extra

Uno dei motivi per i quali una scansione non potrebbe funzionare è a causa del firewall. Le soluzioni per poter continuare con successo l'attività di scan possono essere 2:

- disabilitare o modificare eventuali regole firewall che bloccano il traffico inbound;
- specificare una come *source-port* una *well-known port* (come quella FTP o HTTPS) in modo tale che il firewall (al netto di regole più stringenti) possa interpretare il traffico come non sospetto. Alla comando nmap di scansione, si aggiunge il flag "--source-port <numero porta>" come quella 443.