

# Scansione dei servizi

## nmap

### Indice

Traccia dell'esercizio principale .....	2
Traccia dell'esercizio facoltativo.....	2
Configurazione laboratorio virtuale.....	2
Svolgimento traccia principale .....	3
1. OS Fingerprinting (nmap -O) .....	3
2. TCP Connect Scan (nmap -sT) .....	3
3. SYN Scan (nmap -sS) .....	3
4. Version Detection (nmap -sV) .....	3
Report di Scansione Nmap su Windows 7 .....	4
Porte Aperte e Servizi .....	4
Rilevazione del Sistema Operativo.....	4
Descrizione dei Servizi .....	5
Conclusione .....	5
Svolgimento esercizio facoltativo .....	5
Confronto dei Report Nmap .....	5

## Traccia dell'esercizio principale

Si richiede allo studente di effettuare le scansioni dell'esercizio precedente con Nmap sul target **Windows 7**.

Elencare tutti i passaggi compiuti ed i tipi di scansione, con i relativi risultati, durante la fase di scrittura report.

## Traccia dell'esercizio facoltativo

Spostare il target **Windows 7** nella stessa rete dell'attaccante e ripetere le scansioni.




## Configurazione laboratorio virtuale

La configurazione è impostata seguendo la logica del report M3 W9 D5

pfSense come Server DHCP

Kali Linux su rete 192.168.1.0/24

Windows 7 su rete 192.168.50.0/24

Interfaces				
 WAN	↑	1000baseT <full-duplex>	10.0.2.15	
 LAN	↑	1000baseT <full-duplex>	192.168.1.1	
 LAN2	↑	1000baseT <full-duplex>	192.168.50.1	

# Svolgimento traccia principale

## 1. OS Fingerprinting (nmap-O)

```
(kali@kali)-[~]
└─$ sudo nmap -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 17:56 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0044s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
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 7.16 seconds
```

## 2. TCP Connect Scan (nmap-sT)

```
(kali@kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 17:56 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0078s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
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 4.16 seconds
```

## 3. SYN Scan (nmap-sS)

```
(kali@kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 17:57 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0069s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
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 4.82 seconds
```

## 4. Version Detection (nmap-sV)

```
(kali@kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 17:58 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0076s latency).
Not shown: 991 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)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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: CORSO-PC; 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 65.07 seconds
```

## Report di Scansione Nmap su Windows 7

**Indirizzo IP:** 192.168.50.101

**Stato dell'host:** Attivo (latenza: 0.0044s)

**Nome host:** CORSO-PC

**Sistema Operativo:** Microsoft Windows Embedded Standard 7 / Windows Phone 7.5 o 8.0

**CPE:** cpe:/o:microsoft, cpe:/o:microsoft

**Common Platform Enumeration**, ed è uno standard utilizzato per identificare in modo univoco sistemi operativi, applicazioni e hardware.

---

### Porte Aperte e Servizi

Porta	Stato	Servizio	Versione/Descrizione
<b>135/tcp</b>	Aperta	msrpc	Microsoft Windows RPC
<b>139/tcp</b>	Aperta	netbios-ssn	Microsoft Windows netbios-ssn
<b>445/tcp</b>	Aperta	microsoft-ds	Microsoft Windows 7 - 10, SMB (Workgroup: WORKGROUP)
<b>5357/tcp</b>	Aperta	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
<b>49152/tcp</b>	Aperta	msrpc	Microsoft Windows RPC
<b>49153/tcp</b>	Aperta	msrpc	Microsoft Windows RPC
<b>49154/tcp</b>	Aperta	msrpc	Microsoft Windows RPC
<b>49155/tcp</b>	Aperta	msrpc	Microsoft Windows RPC
<b>49156/tcp</b>	Aperta	msrpc	Microsoft Windows RPC

---

### Rilevazione del Sistema Operativo

- Il sistema sembra essere **Microsoft Windows Embedded Standard 7 o Windows Phone 7.5/8.0**.
  - La rilevazione dell'OS potrebbe essere inaffidabile a causa del numero insufficiente di porte aperte/chiusure per un'identificazione precisa.
-

## Descrizione dei Servizi

### 1. **135/tcp (msrpc):**

- Questo è il servizio Microsoft Remote Procedure Call (RPC). Permette alle applicazioni di comunicare tra loro in rete, in particolare per la gestione remota del sistema.

### 2. **139/tcp (netbios-ssn):**

- Il servizio NetBIOS Session Service viene utilizzato per la condivisione di file e stampanti su una rete Windows.

### 3. **445/tcp (microsoft-ds):**

- Questa porta è utilizzata dai Directory Services di Microsoft per la condivisione di file e SMB (Server Message Block). È comunemente associata alla rete Windows per accedere a risorse condivise.

### 4. **5357/tcp (http):**

- Questa porta è associata al server Microsoft HTTPAPI httpd 2.0, utilizzato per il protocollo SSDP (Simple Service Discovery Protocol) e la scoperta di dispositivi UPnP (Universal Plug and Play) su una rete.

### 5. **49152-49156/tcp (msrpc):**

- Queste porte dinamiche sono utilizzate per i servizi RPC di Microsoft. Fanno parte dell'intervallo di porte dinamiche utilizzato da Windows per le comunicazioni aggiuntive tramite RPC.

---

## Conclusione

Il sistema scansionato all'indirizzo IP 192.168.50.101 sembra eseguire una versione di Windows, probabilmente Windows Embedded Standard 7. Le diverse porte aperte, in particolare quelle relative ai servizi RPC e SMB di Microsoft, indicano che il target potrebbe essere coinvolto in attività di condivisione file e gestione remota all'interno di una rete. Questi servizi, soprattutto SMB, potrebbero rappresentare un rischio per la sicurezza se non adeguatamente protetti. Potrebbe essere necessario un ulteriore approfondimento per valutare le eventuali vulnerabilità.

## Svolgimento esercizio facoltativo

Impostare la macchina virtuale Windows 7 alla rete **intnet** la stessa di Kali Linux.

### Confronto dei Report Nmap

**Distanza di rete:** la latenza è inferiore in quanto il traffico non passa attraverso pfSense.

**Porte aperte e servizi** sono identici in entrambe le scansioni.