



W11D2

SCANSIONE SERVIZI NMAP SU WINDOWS 7

La traccia

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

La traccia

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):

Scansione win7 rete diversa da kali

```
kali@kali: ~  
File Actions Edit View Help  
— 192.168.100.4 ping statistics —  
8 packets transmitted, 8 received, 0% packet loss, time 7008ms  
rtt min/avg/max/mdev = 1.757/2.372/4.393/0.794 ms  
  
(kali@kali)-[~]  
$ nmap -O -sS -sV 192.168.100.4  
You requested a scan type which requires root privileges.  
QUITTING!  
  
(kali@kali)-[~]  
$ sudo nmap -O -sS -sV 192.168.100.4  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 17:36 EST  
Nmap scan report for 192.168.100.4  
Host is up (0.0039s latency).  
Not shown: 944 closed tcp ports (reset), 49 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
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  
49157/tcp  open  msrpc        Microsoft Windows RPC  
Device type: general purpose  
Running: Microsoft Windows Vista|2008|7  
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7  
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP 2, Windows 7 SP1, or Windows Server 2008  
Network Distance: 2 hops  
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 62.57 seconds  
  
(kali@kali)-[~]  
$
```

Di fianco la scansione di win7 , la prima opzione è la -O per verificare la versione del sistema operativo.

Le altre due opzioni invece servono a fare una SYN scan e ad elencare i servizi attivi. Come nel lavoro precedente anche qui avremo meno servizi visualizzati.

Scansione win7 rete uguale a kali

```
(kali㉿kali)-[~]  
$ sudo nmap -sV 192.168.50.4 -oN reportwin7  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 17:50 EST  
Nmap scan report for 192.168.50.4  
Host is up (0.00051s latency).  
Not shown: 991 closed tcp ports (reset)  
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  
49157/tcp  open  msrpc        Microsoft Windows RPC  
MAC Address: 08:00:27:72:3D:A5 (Oracle VirtualBox virtual NIC)  
Service Info: Host: WIN7; 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 60.36 seconds
```

Di fianco la scansione di win7, la prima opzione è la `-sV` che elenca i servizi , la seconda `-oN` invece salva il risultato della scansione in un file. Potremmo spiegare il risultato delle scansioni per evidenziare i diversi servizi disponibili in base ad esse. Per continuarle potremmo cambiare le opzioni.