

W11D1 - Pratica (2)



Esercizio

Scansione dei servizi

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

```
windows7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. Tutti i diritti riservati.

PS C:\Users\gio> ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::adb9:397:eb9f:5c91%11
    Indirizzo IPv4. . . . . : 192.168.26.41
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.26.214

Scheda Tunnel isatap.{DBC19055-F2D4-41D7-BD44-5C3557146556}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:
PS C:\Users\gio> ping 192.168.26.95

Esecuzione di Ping 192.168.26.95 con 32 byte di dati:
Risposta da 192.168.26.95: byte=32 durata=2ms TTL=64
Risposta da 192.168.26.95: byte=32 durata<1ms TTL=64
Risposta da 192.168.26.95: byte=32 durata=1ms TTL=64
Risposta da 192.168.26.95: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.26.95:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo = 2ms, Medio = 0ms
PS C:\Users\gio>
```

```
(giovanni@kali)-[~]
$ sudo nmap -O 192.168.26.41
[sudo] password for giovanni:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-20 21:30 CET
Nmap scan report for 192.168.26.41
Host is up (0.00090s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
5357/tcp  open  wsddapi
10243/tcp open  unknown
MAC Address: 08:00:27:DC:D3:4B (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|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
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 15.89 seconds
```