SCANSIONE DEI SERVIZI CON NMAP W11D4

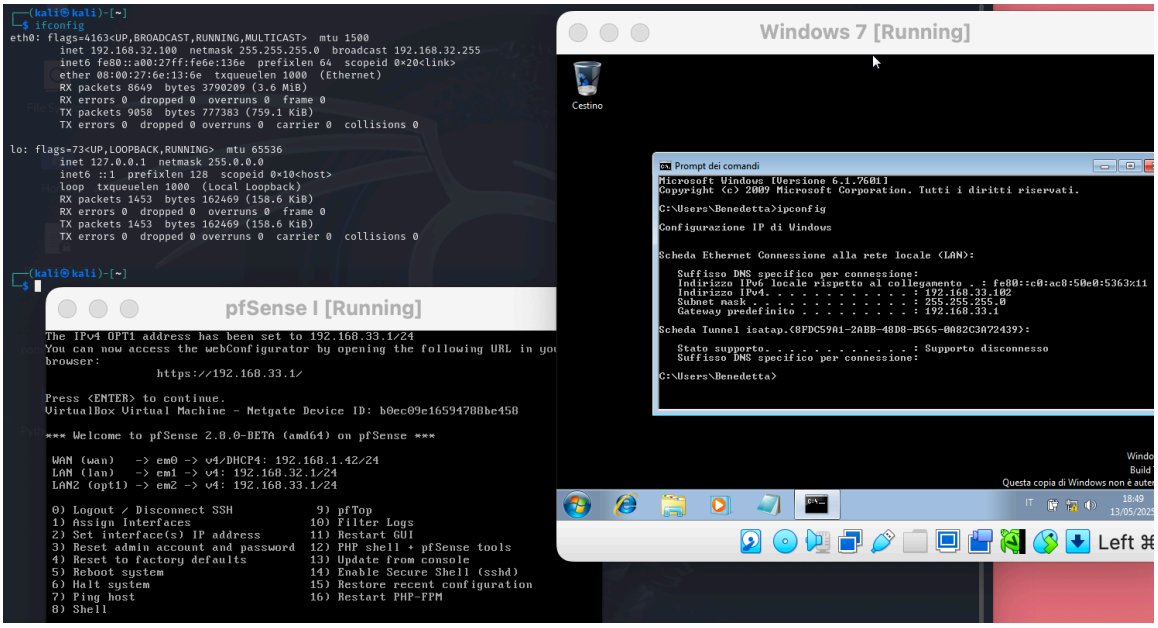
TRACCIA:

Effettuare queste scansioni sul target Windows (con Windows Firewall abilitato e disabilitato):

1. OS Fingerprint
2. Syn Scan
3. TCP Connect
4. Version Detection

SOLUZIONE:

Configurare Kali, Windows e Pfsense come segue



SCANSIONI CON FIREWALL ABILITATO:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.33.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 12:50 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.56 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.33.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 12:50 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.22 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.33.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 12:50 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.33.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 12:51 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.40 seconds
```

SCANSIONI CON FIREWALL DISABILITATO:

1. OS Fingerprint: scan per trovare dettagli sul sistema operativo del target

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.33.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 13:08 EDT
Nmap scan report for 192.168.33.102
Host is up (0.010s latency).
Not shown: 992 closed tcp ports (reset)
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
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 SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.60 seconds
```

2. Syn Scan: esegue una scansione SYN sul target

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.33.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 13:08 EDT
Nmap scan report for 192.168.33.102
Host is up (0.037s latency).
Not shown: 992 closed tcp ports (reset)
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 13.98 seconds
```

3. TCP Connect: esegue una scansione TCP sul target

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.33.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 13:10 EDT
Nmap scan report for 192.168.33.102
Host is up (0.045s latency).
Not shown: 992 closed tcp ports (conn-refused)
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 13.82 seconds
```

4. Version Detection: esegue una scansione TCP sul target, specificando la versione dei servizi

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.33.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 13:10 EDT
Nmap scan report for 192.168.33.102
Host is up (0.017s latency).
Not shown: 992 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
Service Info: Host: BENEDETTA-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 73.06 seconds
```