EPICODE

Daily projects
Week 9

S9/L1 - Firewall to protect services

PIO srl
Protecting is better than being safe

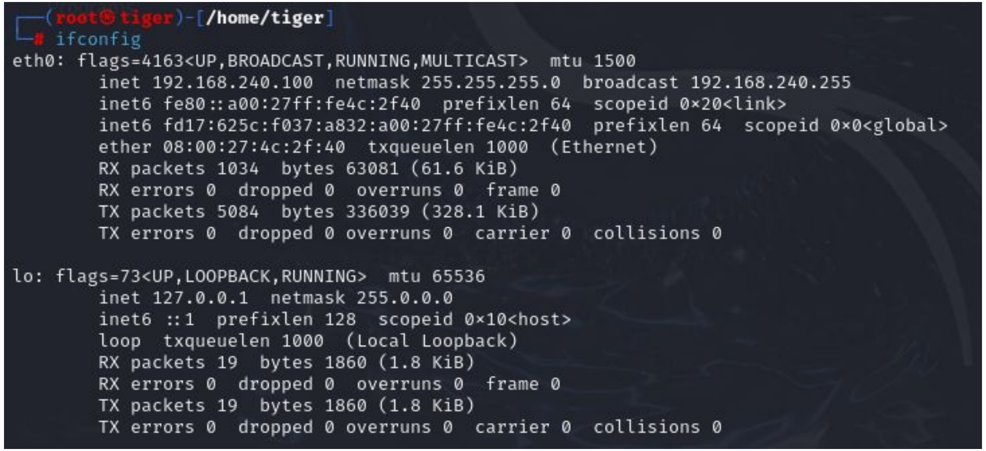
Daily projects

S9/L1 - Firewall to protect services

Try to use NMAP tool to prove that firewall can hide ports when an attacker try to find opened ports and view the versions of the services are running

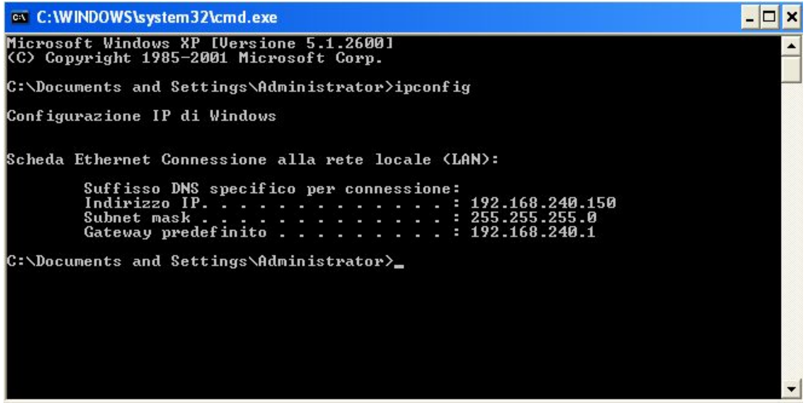
Machine info

Attacker info - Kali Linux



```
┌──(root㉿tiger)-[/home/tiger]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.240.100  netmask 255.255.255.0  broadcast 192.168.240.255
        inet6 fe80::a00:27ff:fe4c:2f40  prefixlen 64  scopeid 0x20<link>
        inet6 fd17:625c:f037:a832:a00:27ff:fe4c:2f40  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:4c:2f:40  txqueuelen 1000  (Ethernet)
        RX packets 1034  bytes 63081 (61.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5084  bytes 336039 (328.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 19  bytes 1860 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 1860 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Target info - Windows XP

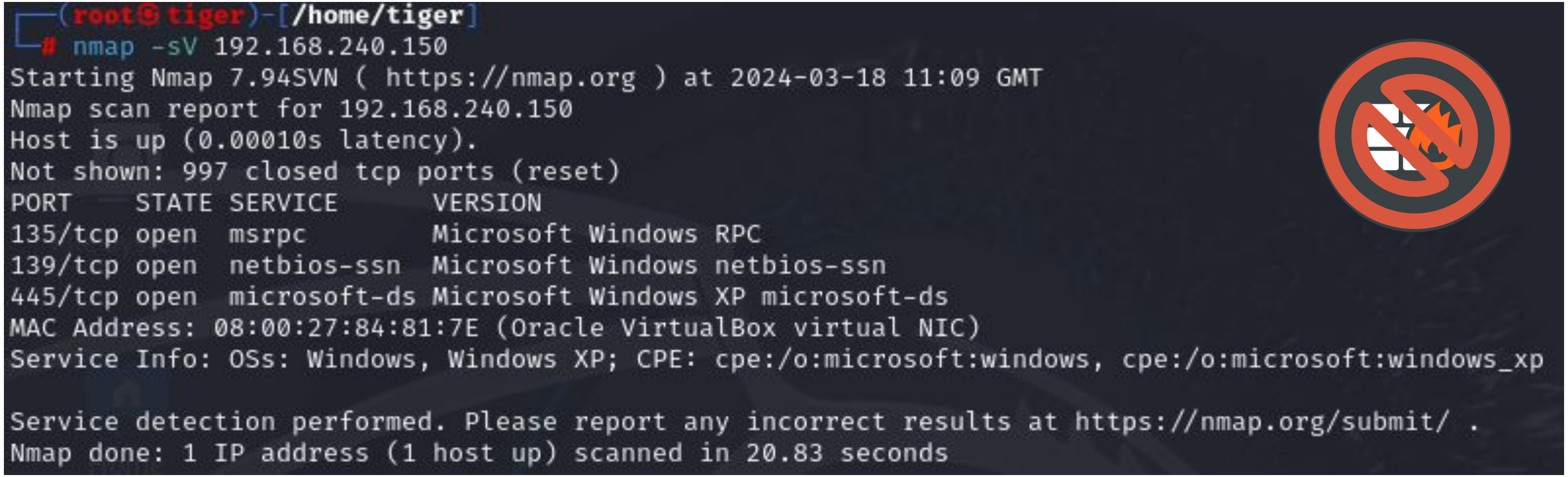


```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Configurazione IP di Windows


Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 192.168.240.150
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . : 192.168.240.1

C:\Documents and Settings\Administrator>_
```

NMAP tool report

Run an NMAP from Kali to Windows XP without Firewall.

We can see some opened ports and services running

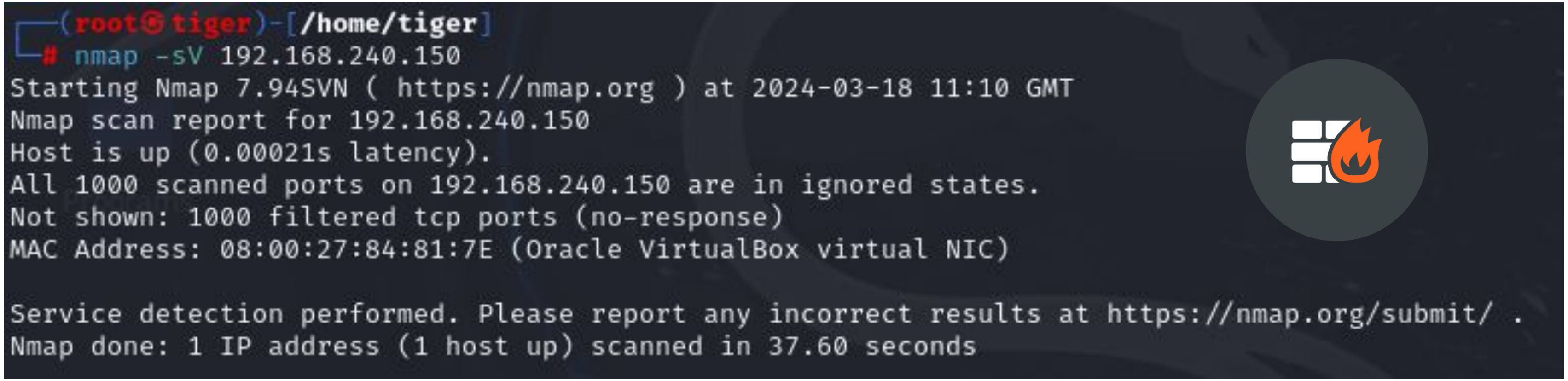


```
┌──(root㉿tiger)-[/home/tiger]
└─# nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 11:09 GMT
Nmap scan report for 192.168.240.150
Host is up (0.00010s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:84:81:7E (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.83 seconds
```

NMAP tool report

Run an NMAP from Kali to Windows XP without Firewall.

In this case, the firewall is on and hide to scan a port that can contain a vulnerability version of service



```
┌──(root㉿tiger)-[/home/tiger]
└─# nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 11:10 GMT
Nmap scan report for 192.168.240.150
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:84:81:7E (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.60 seconds
```