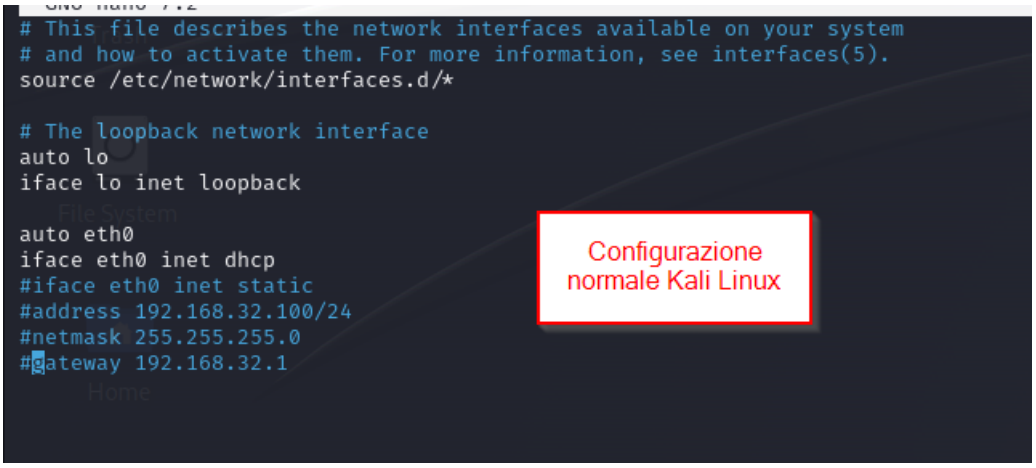
ESERCIZIO W11D1 PARTE 2

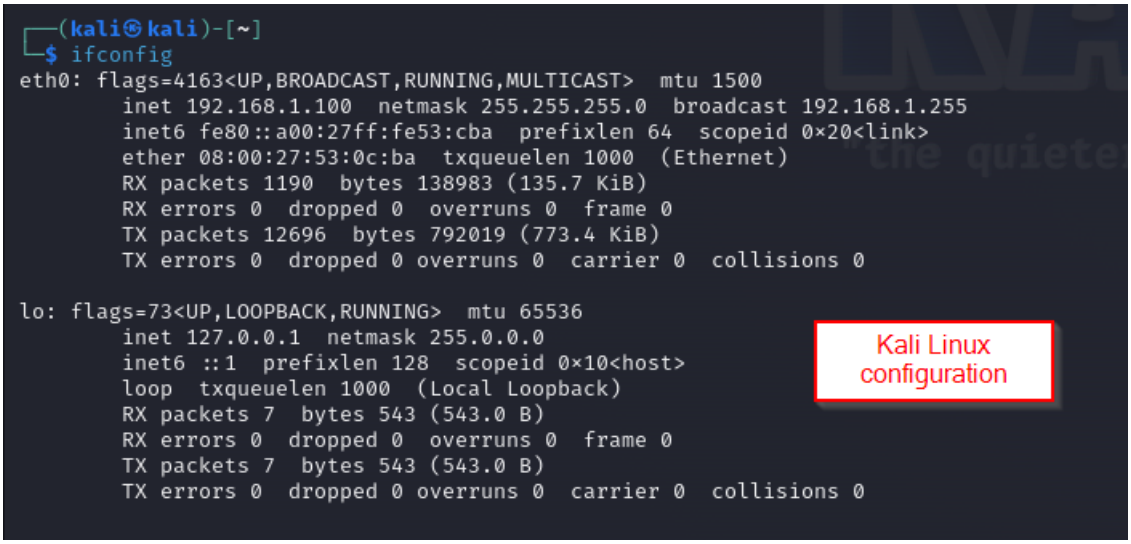
L'esercizio prevede di mettere due macchine virtuali all'interno della stessa rete e di saggiarne le suddette scansioni nmap:

- OS fingerprinting
- SYN scan
- Version detection

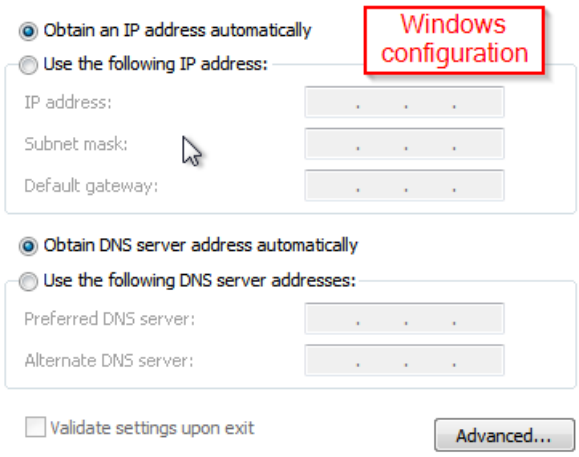
Configurazione di rete macchine virtuali

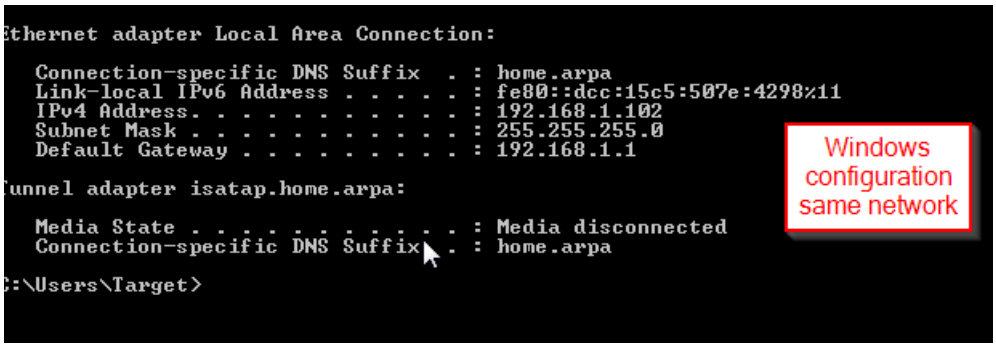



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
#iface eth0 inet static
#address 192.168.32.100/24
#netmask 255.255.255.0
#gateway 192.168.32.1
```

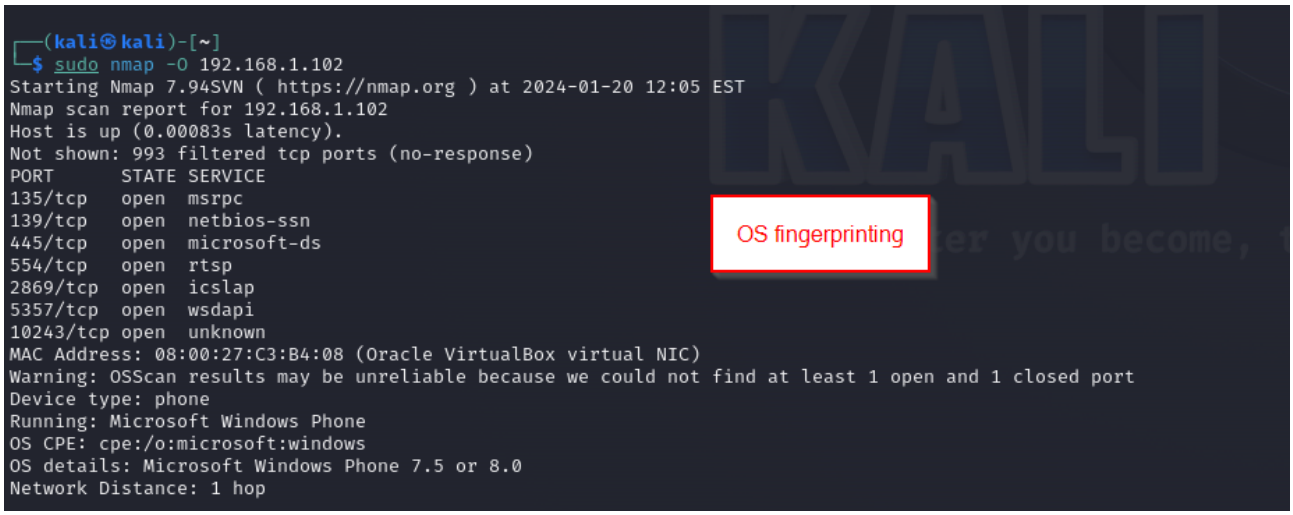


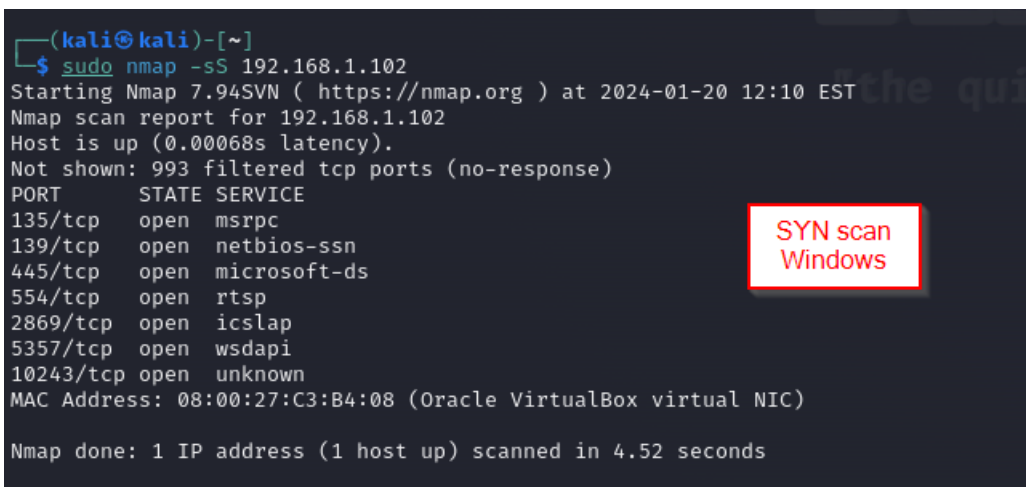

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe53:cba  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:53:0c:ba  txqueuelen 1000  (Ethernet)
        RX packets 1190  bytes 138983 (135.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12696  bytes 792019 (773.4 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 7  bytes 543 (543.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 543 (543.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

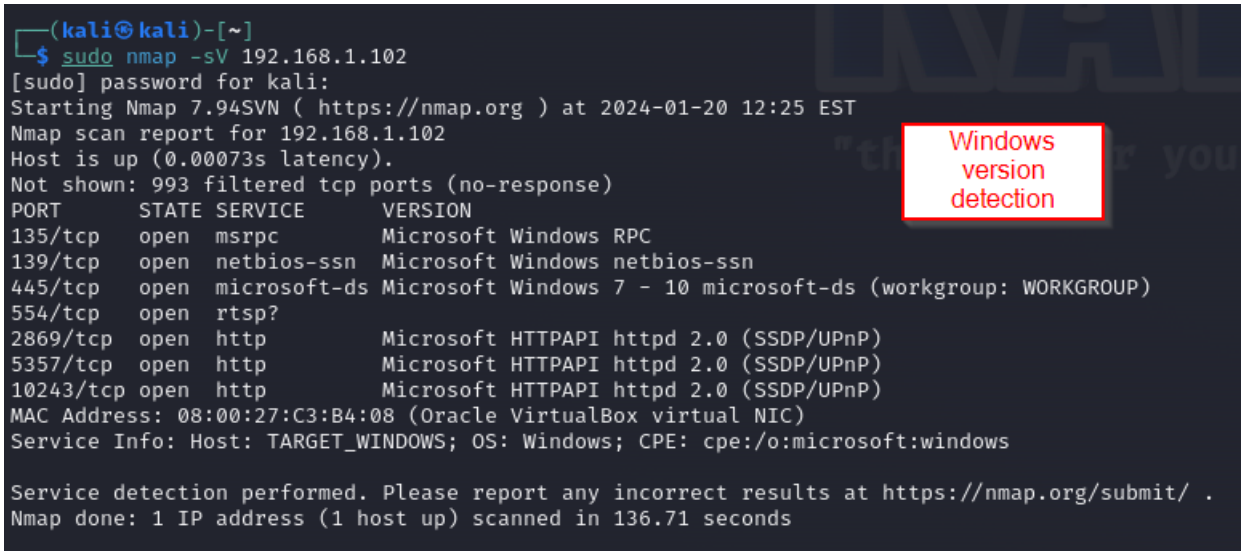

Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
Windows configuration


Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : home.arpa
Link-local IPv6 Address . . . . . : fe80::dcc:15c5:507e:4298%11
IPv4 Address. . . . . : 192.168.1.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Tunnel adapter isatap.home.arpa:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : home.arpa
C:\Users\Target>
Windows configuration same network

Scan nmap


(kali㉿kali)-[~]
$ sudo nmap -O 192.168.1.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-20 12:05 EST
Nmap scan report for 192.168.1.102
Host is up (0.00083s 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 icslap
5357/tcp open wsdapi
10243/tcp open unknown
MAC Address: 08:00:27:C3:B4:08 (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: phone
Running: Microsoft Windows Phone
OS CPE: cpe:/o:microsoft:windows
OS details: Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop
OS fingerprinting


(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.1.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-20 12:10 EST
Nmap scan report for 192.168.1.102
Host is up (0.00068s 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 icslap
5357/tcp open wsdapi
10243/tcp open unknown
MAC Address: 08:00:27:C3:B4:08 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 4.52 seconds
SYN scan Windows



Risultati

Troviamo 993 porte filtrate e solo 7 porte attive con i loro servizi. Una scena più vicina ad un contesto reale ci appare, perché il firewall di Windows va a proteggere le altre porte.

IP	SISTEMA	PORTE APERTE	SERVIZI IN ASCOLTO	DESCRIZIONE SERVIZI
192.168.1.102	Microsoft Windows phone 7.5 or 8.0	135, 139, 445, 554, 2869, 5357, 10243	Microsft Windows RPC, Microsoft Windows netbios-ssn, Microsft Windows 7-10 microsoft-ds, Microsft HTTPAPI httpd 2.0 (SSDP/UPnP)	(Descrizioni in basso)

Descrizione servizi

Microsoft Windows RPC: Consente la comunicazione tra processi. Rende possibile l'esecuzione di una procedura di un programma su un indirizzo di memoria remoto.

Microsoft Windows netbios-ssn: Consente la comunicazione dei computer tramite rete locale. Tale protocollo è utilizzato per la condivisione di file e stampanti.

Microsft Windows 7-10 microsoft-ds: Consente la comunicazione dei computer tramite rete locale. Tale protocollo è utilizzato per la condivisione di file e stampanti.

Microsft HTTPAPI httpd 2.0 (SSDP/UPnP): Consente la comunicazione dei computer tramite rete locale. Questo servizio è anch'esso è utilizzato per la condivisione di file e stampanti. Il protocolo UPnP(Universal Plug and Play) è un estensione del protocollo SSDP(Simple Service Discovery Protocol)