

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

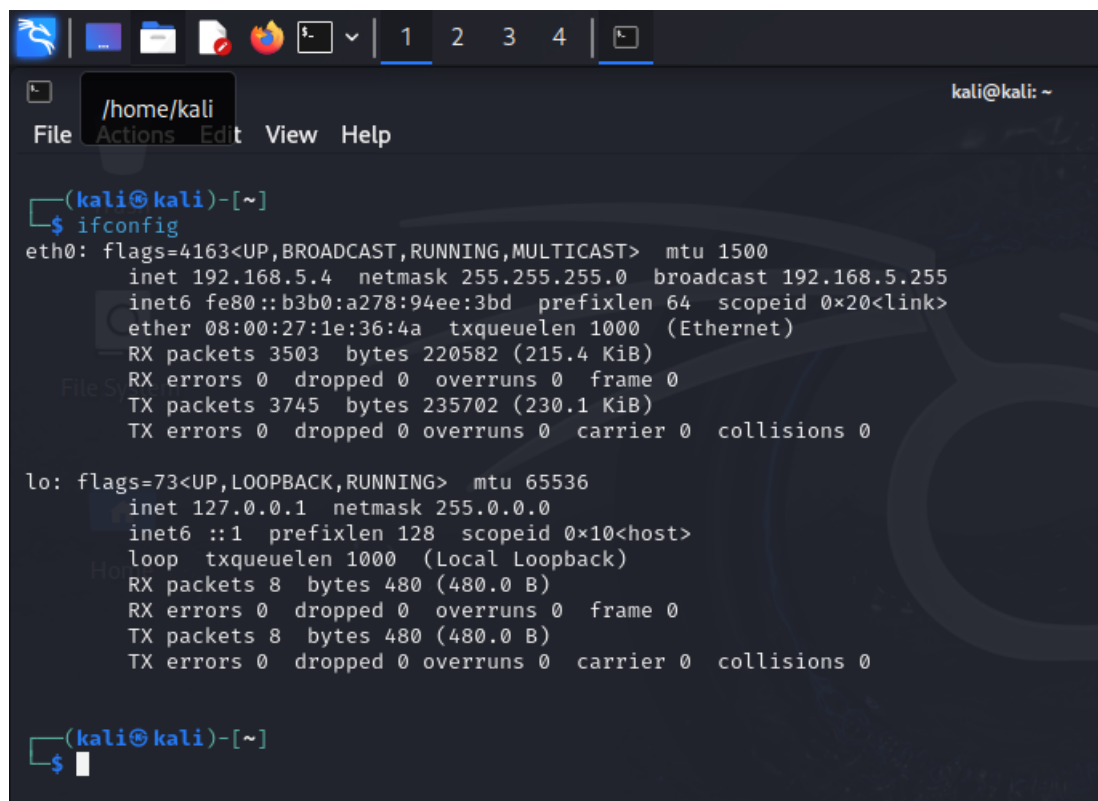
**Quesito extra (al completamento dei quesiti sopra):**

Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?



per lo svolgimento dell'esercizio dobbiamo impostare le 2 macchine sulla stessa rete e cambiare gli indirizzi ip in modo che riescano a comunicare:

Kali linux :



```

(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.5.4  netmask 255.255.255.0  broadcast 192.168.5.255
    inet6 fe80::b3b0:a278:94ee:3bd  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:1e:36:4a  txqueuelen 1000  (Ethernet)
    RX packets 3503  bytes 220582 (215.4 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 3745  bytes 235702 (230.1 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 8  bytes 480 (480.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 8  bytes 480 (480.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali@kali)~$
  
```

Windows 7 :

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.

C:\Users\ vboxuser>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::7d96:a01c:9bed:5040%
11
    Indirizzo IPv4. . . . . : 192.168.5.6
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.5.1

Scheda Tunnel isatap.{7CBA0DD8-ED0F-455D-8317-28E1828335F2}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\ vboxuser>
```

Dopo aver configurato le macchine procediamo con la scansione di windows 7 tramite kali linux

- Scansione del sistema operativo di windows 7:

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)~$ sudo nmap -O 192.168.5.6
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-02 17:04 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.5.6
Host is up (0.00078s latency).
Not shown: 991 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
49157/tcp  open  unknown
MAC Address: 08:00:27:0B:B9:BE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
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 2.78 seconds

(kali@kali)~$
```

- Scansione syn :

```

kali@kali: ~
File Edit View Help

(kali@kali)-[~]
$ sudo nmap -sS 192.168.5.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-02 17:06 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.5.6
Host is up (0.00054s latency).
Not shown: 991 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
49157/tcp  open  unknown
MAC Address: 08:00:27:0B:B9:BE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.74 seconds

(kali@kali)-[~]
$

```

- Scansione della versione dei servizi:

```

/home/kali
File Actions Edit View Help

(kali@kali)-[~]
$ sudo nmap -sV 192.168.5.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-02 17:09 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.5.6
Host is up (0.00079s 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: 08:00:27:0B:B9:BE (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; 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 60.68 seconds

(kali@kali)-[~]
$

```

Di seguito elenchiamo una tabella con i dettagli ottenuti dagli scann effettuati su windows 7 :

IP	Kali linux : 192.168.5.4 - Windows 7 : 192.168.5.6
SISTEMA OPERATIVO	Windows 7 SP0 – SP1 / Mac address : 08:00:07:0B:B9:BE
PORTE APERTE	135/TCP – 139/TCP – 445/TCP – 49152/TCP – 49153/TCP – 49154/TCP – 49155/TCP- 49156/TCP – 49157/TCP
SERVIZI IN ASCOLTO CON VERSIONE	135/TCP – servizi in ascolto : msrpc 139/TCP – servizi in ascolto : netbios-ssn 445/tcp – servizi in ascolto : microsoft -ds 49152/TCP- servizi in ascolto : msrpc 49153/TCP – servizi in ascolto : msrpc 49154/TCP – servizi in ascolto : msrpc 49155/TCP – servizi in ascolto : msrpc 49156/TCP – servizi in ascolto : msrpc 49157/TCP – servizi in ascolto : msrpc

DESCRIZIONE DEI SERVIZI	135/TCP – versione dei servizi : Microsoft Windows RPC 139/TCP – versione dei servizi: Microsoft Windows netbios-ssn 445/tcp – versione dei servizi: Microsoft Windows 7 – 10 microsoft-ds (workgroup : WORKGROUP) 49152/TCP - versione dei servizi : Microsoft Windows RPC 49153/TCP – versione dei servizi: Microsoft Windows RPC 49154/TCP – versione dei servizi: Microsoft Windows RPC 49155/TCP – versione dei servizi: Microsoft Windows RPC 49156/TCP – versione dei servizi: Microsoft Windows RPC 49157/TCP – versione dei servizi: Microsoft Windows RPC

#### Quesito extra :

durante l'esercizio abbiamo rilevato il sistema operativo , le porte aperte, i servizi , le versioni di quest'ultime.

Possiamo dire che rilevati le versioni dei vari servizi potremmo condurre un test su questi servizi per verificare la loro vulnerabilità , inoltre possiamo continuare con altri tipi di scann come **nmap -A** , per andare a testare gli script di default e quindi ottenere più informazioni. Possiamo utilizzare altri switch come per esempio **nmap -f mtu512**. Questo switch è molto interessante perché ci permette di bypassare eventuali sistemi difensivi come firewall.