

Dopo aver verificato l'IP della macchina Win7 tramite ipconfig vediamo che è sulla stessa rete di kali 1.0/24, con IP 192.168.1.105, quindi dopo aver settato il gateway affinché le due macchine possano comunicare posso eseguire le varie scansioni. Con il comando **nmap -O** vediamo che nmap non riesce ad identificare precisamente che tipo di OS ha scansionato ma ci dà delle indicazioni su probabili sistemi.

```
(kali@kali)-[~]
└─$ sudo nmap -O 192.168.1.105
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-01 05:23 EDT
Nmap scan report for 192.168.1.105
Host is up (0.0011s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2869/tcp  open  iclslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
MAC Address: 08:00:27:CE:5B:66 (Oracle VirtualBox virtual NIC)
Warning: OS detection results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP2 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
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 19.45 seconds
```

Con la scansione SYN possiamo vedere le eventuali porte aperte sul sistema senza farci notare perché la connessione non viene portata a termine e non si aspetta il termine della connessione.

```
(kali@kali)-[~]
└─$ sudo nmap -sS 192.168.1.105
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-01 05:44 EDT
Nmap scan report for 192.168.1.105
Host is up (0.0011s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2869/tcp  open  iclslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
MAC Address: 08:00:27:CE:5B:66 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 87.23 seconds
```

Infine la scansione della versione dei servizi attivi eseguita tramite comando **nmap -sV <ip_target>** ci dà informazioni sulla versione dei servizi in questo caso eseguita con il comando T5 per velocizzare la scansione.

```
(kali@kali)-[~]
└─$ sudo nmap -T5 -sV 192.168.1.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-01 06:06 EDT
Nmap scan report for 192.168.1.105
Host is up (0.0014s latency).
Not shown: 994 filtered tcp ports (no-response)
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)
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  tcpwrapped
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:CE:5B:66 (Oracle VirtualBox virtual NIC)
Service Info: Host: DAVIDE-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 55.26 seconds
```

La scansione del SO non è andata a buon fine poiché essendo presente un firewall sulla macchina bersaglio nmap non riesce a stabilire una connessione, infatti nel risultato della scansione ci dice che potrebbe essere irrealizzabile perché non è stata trovata almeno una porta aperta o chiusa, per questo ci può essere utile eseguire una scansione dei servizi che potrebbe darci più indicazioni sul SO della macchina o se si potesse aggirare il firewall per accedere liberamente alla macchina.

```
MAC Address: 08:00:27:CE:58:00 (Oracle VM VirtualBox Virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows server 2008:r2 cpe:/o:microsoft:windows 8.1 cpe:/o:microsoft:windows 7::-:professional cpe:/
```