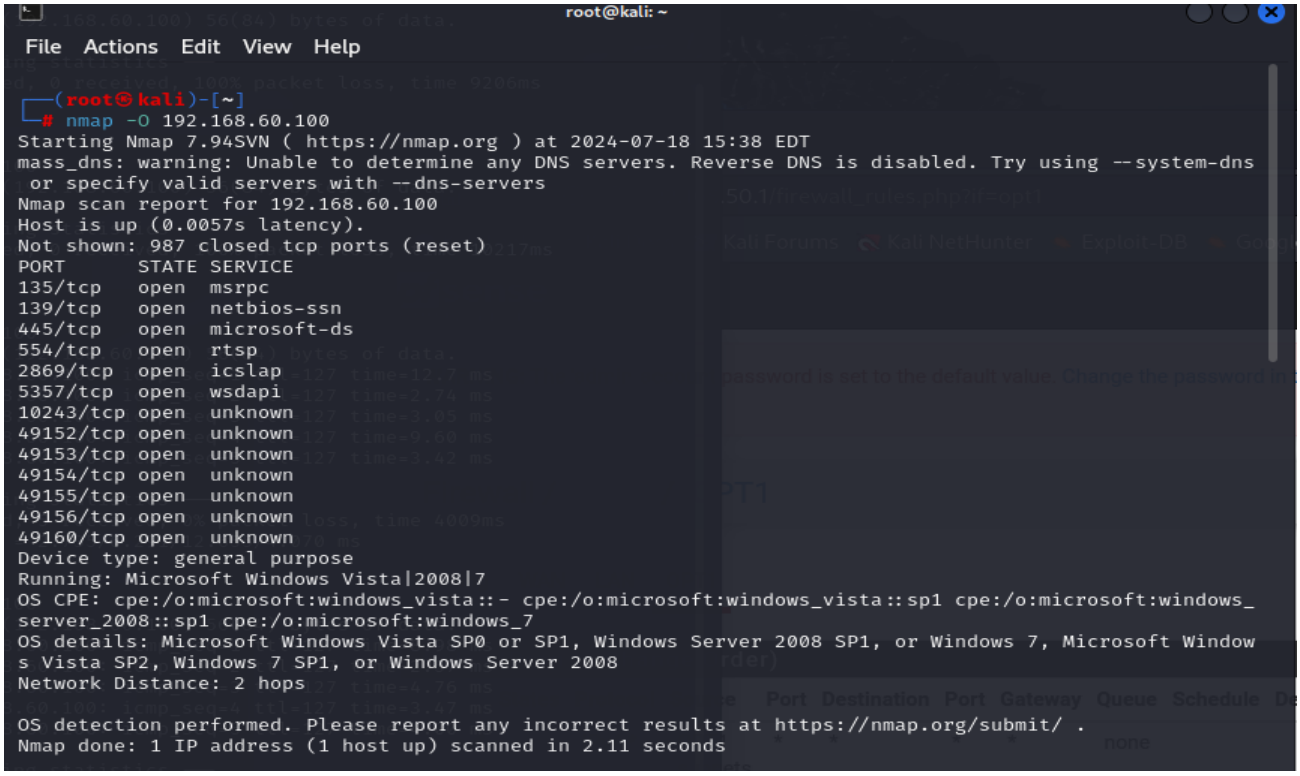
W11D4 – Scansioni di Windows 7 su reti diverse.

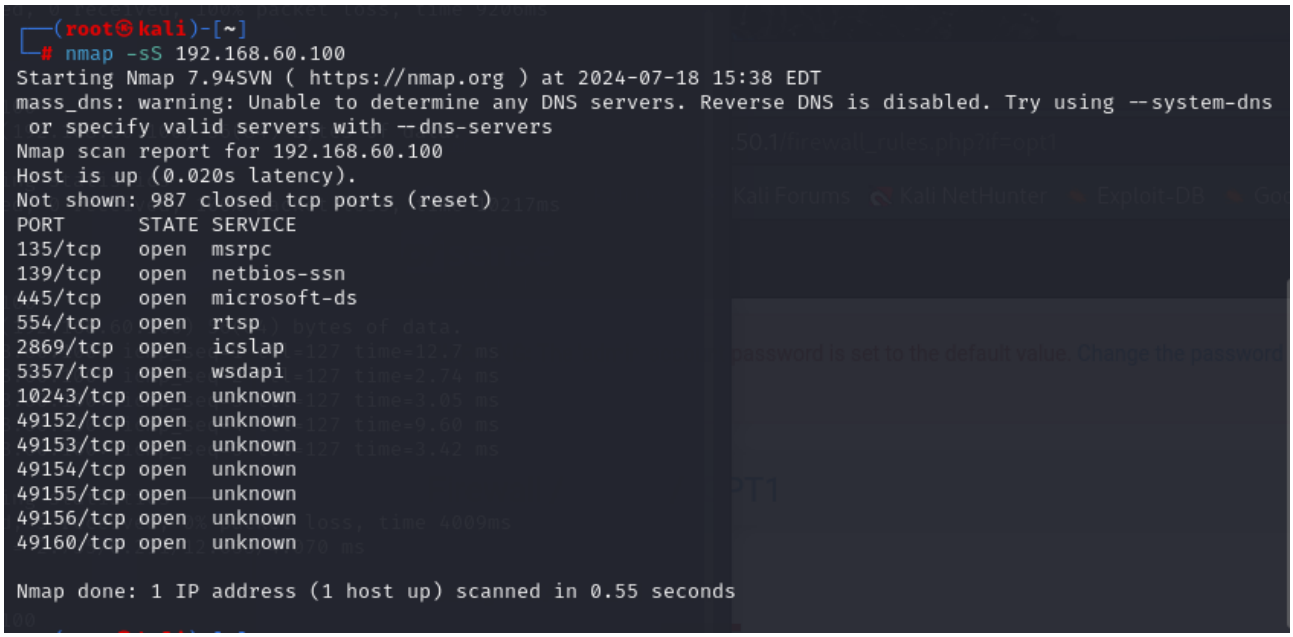
Esercizio obbligatorio ed esercizio facoltativo.

Per prima cosa, ho cambiato l'IP di Windows 7, scegliendo l'IP 192.168.60.100 e spostandolo su una scheda di rete diversa rispetto a Kali Linux, che ha mantenuto l'IP 192.168.50.100. Come router ho utilizzato Pfsense ed ho avviato le diverse scansioni.

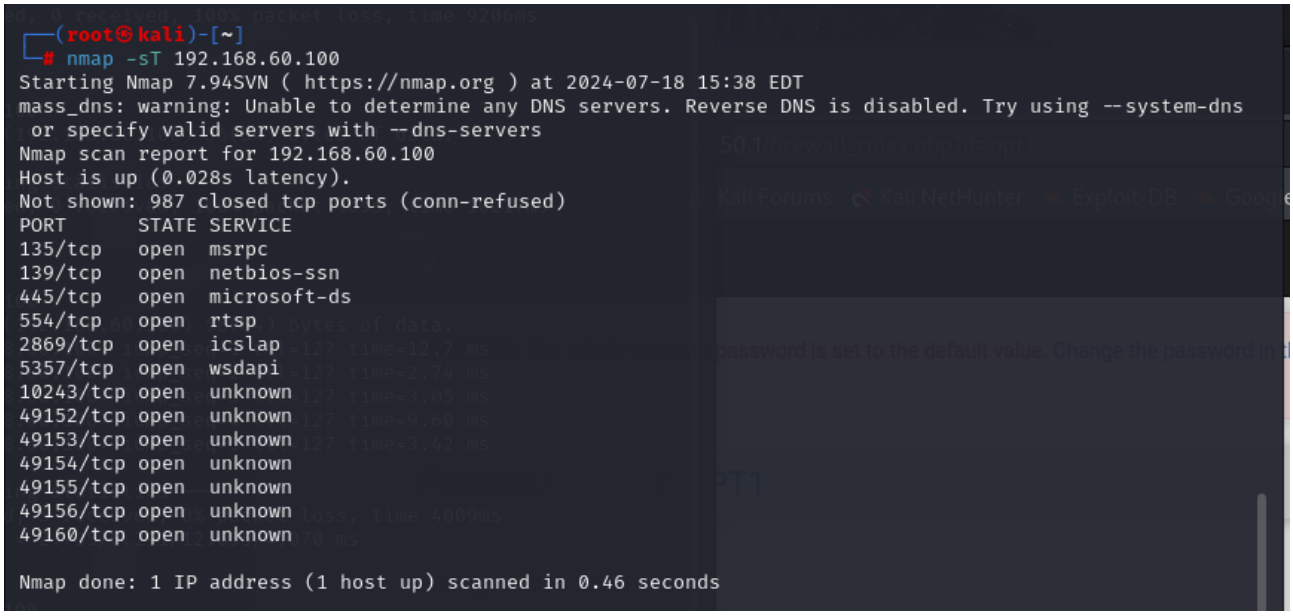
Scansione OS fingerprint con Windows 7 su una rete diversa.



Scansione SYN con Windows su una rete diversa

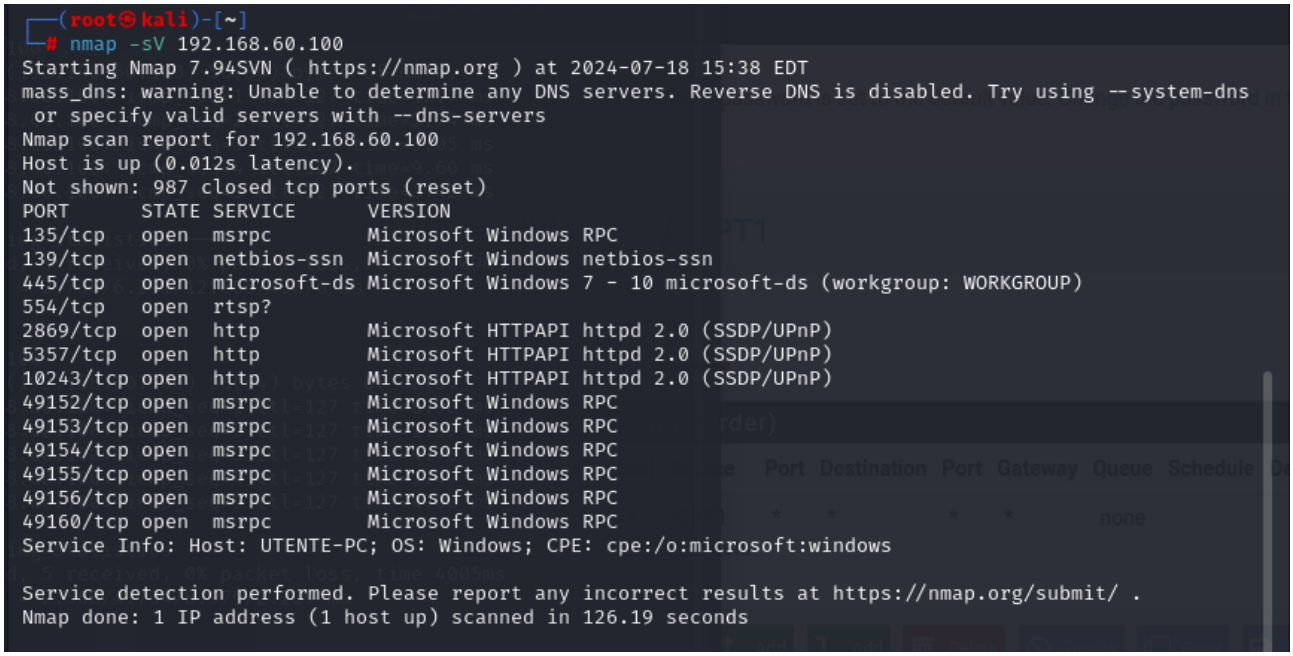


Scansione TCP con Windows su una rete diversa.



```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.60.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-18 15:38 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 192.168.60.100
Host is up (0.028s latency).
Not shown: 987 closed tcp ports (conn-refused)
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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

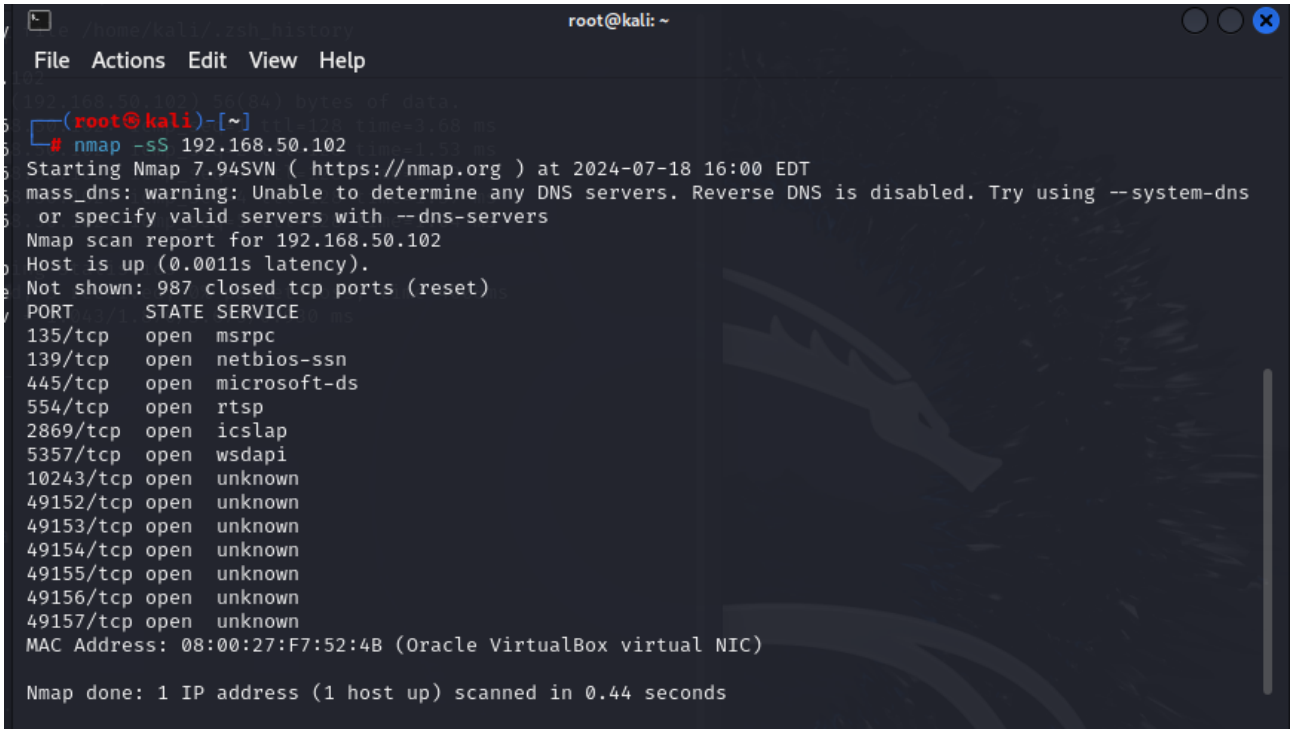
Scansione version detection con Windows su una rete diversa.



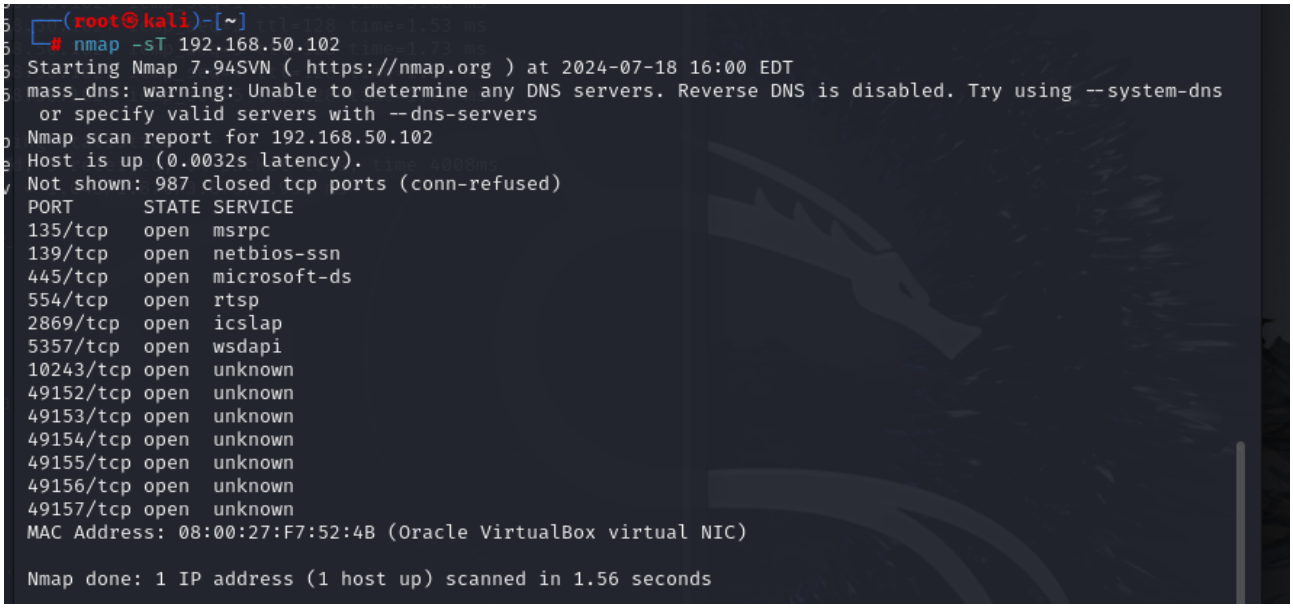
```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.60.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-18 15:38 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
 or specify valid servers with --dns-servers
Nmap scan report for 192.168.60.100
Host is up (0.012s latency).
Not shown: 987 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)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
49160/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: UTENTE-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 126.19 seconds
```

Scansione OS fingerprint con Windows 7 sulla stessa rete, con IP 192.168.50.102.

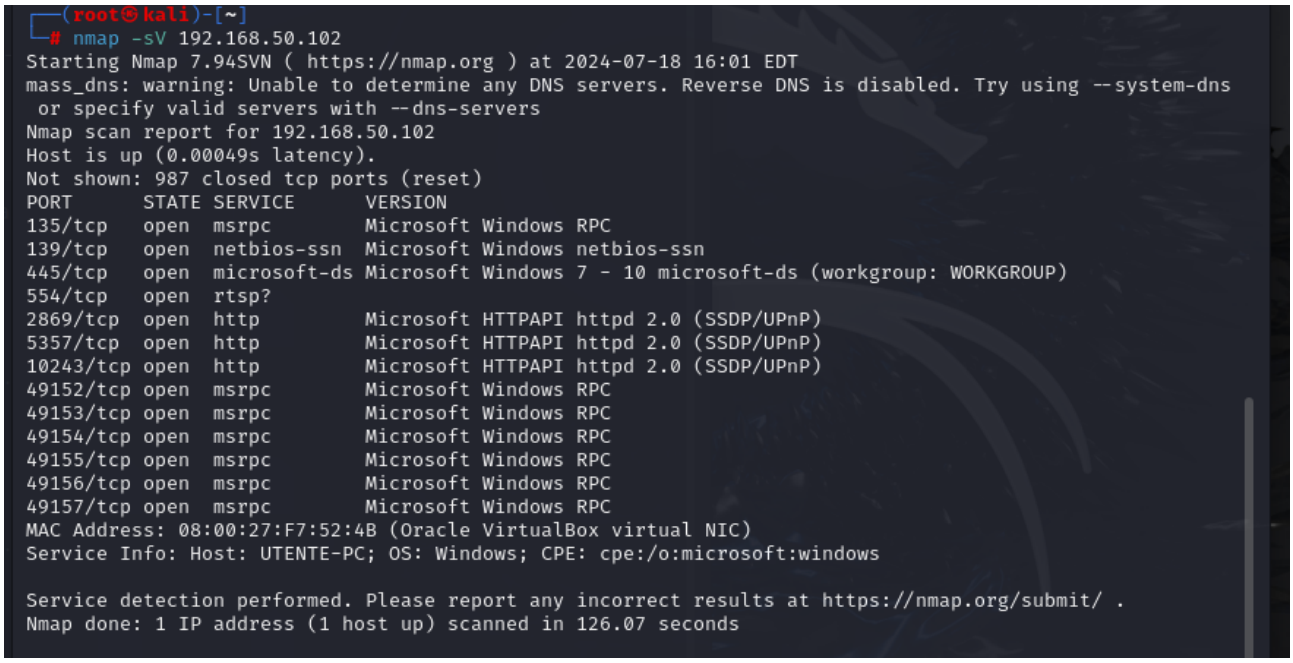
Scansione SYN con Windows sulla stessa rete



Scansione TCP con Windows sulla stessa rete



Scansione version detection con Windows sulla stessa rete.



Report della scansione e differenze tra la scansione con le macchine su reti diverse e la scansione con le macchine sulla stessa rete.

Il target di entrambe le scansioni è la macchina Metasploitable 2, con IP 192.168.60.100 con le macchine su due reti diverse, mentre l'IP 192.168.50.102 è l'IP della macchina Metasploitable sulla stessa rete di Kali Linux. La scansione di Metasploitable su una rete diversa da quella di Kali Linux ha rilevato come sistema operativo Microsoft Windows Vista versione 7 del 2008, che non è il sistema operativo corretto della macchina analizzata, essendo Windows 7. Tra i dettagli del sistema operativo rilevato, vengono proposte varie opzioni, tra cui figura anche la versione corretta del sistema operativo, ossia Windows 7. Le versioni ipotizzate sono Microsoft Windows Vista SP0 o SP1, Microsoft Windows Vista SP2, Windows Server 2008 e Windows server 2008 SP1, oppure Windows 7 e Windows 7 SP1. Il sistema operativo viene rilevato in modo molto più preciso con la scansione sulla macchina nella stessa rete, perché viene subito rilevato il sistema operativo Microsoft Windows 7, versione 8.1 del 2008. Vedendo nei dettagli, il sistema operativo ipotizzato è Microsoft Windows 7 SP0 – SP1, Windows Server 2008 SP1, Windows server 2008 R2 e tra le ipotesi figurano anche Windows 8 o Windows 8.1. Si può dunque affermare che il rilevamento del sistema operativo è più preciso con entrambe le macchine sulla stessa rete, perché con la scansione sulla macchina con IP 192.168.50.102 il sistema operativo rilevato è stato subito Windows 7, mentre per l'altra macchina si è ipotizzato principalmente Windows Vista. Osservando queste due scansioni, si nota che la network distance è di 2 hop quando le macchine sono su due reti diverse, perché c'è il passaggio aggiuntivo con il router Pfsense, mentre con le macchine sulla stessa rete la network distance si riduce e diventa di un solo hop. Sia la scansione SYN che la scansione TCP sulla macchina con IP 192.168.60.100 hanno rilevato 987 porte chiuse e 13 porte aperte. Le porte aperte sono le porte numero 135, 139, 445, 554, 2869, 5357, 10243, 49152, 49153, 49154, 49155, 49156, 49160. I servizi attivi su queste porte sono, rispettivamente, msrpc, netbios-ssn, microsoft-ds, rtsp, icslap, wsdapi e 7 servizi sconosciuti. Nella scansione sulla macchina sulla stessa rete, è stata rilevata la porta 49157 aperta, mentre non è stata rilevata la porta 49160 come una porta aperta ed anche sulla porta 49157 è in ascolto un servizio sconosciuto. Per il resto non c'è nessuna differenza tra le scansioni sia SYN che TCP tra la macchina con IP 192.168.60.100 e la macchina con IP 192.168.50.102. Per quanto riguarda la versione dei servizi rilevati, sulla macchina su reti diverse 192.168.60.100 le versioni dei servizi trovati sono, rispettivamente, Microsoft Windows RPC, Microsoft Windows netbios-ssn, Microsoft Windows 7 – 10 Microsoft-ds (workgroup:WORKGROUP), non è stata rilevata la versione del servizio rtsp, mentre nelle tre porte successive è presente come servizio http con la versione Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) e nelle ultime 6 porte è presente un servizio msrpc con versione Microsoft Windows RPC. Non vi è alcuna differenza con quanto registrato durante la scansione sulla macchina con IP 192.168.50.102 sulla stessa rete. Il servizio msrpc, ossia Microsoft remote procedure call, è un protocollo di comunicazione interprocesso che consente a processi diversi di comunicare tra loro, netbios-ssn permette a due netbios di stabilire una connessione e mantenere una sessione e microsoft-ds è un servizio di registrazione di dispositivi di rete. RTSP, real time streaming protocol, fornisce contenuti in

live streaming, icslap serve per la comunicazione di rete ed infine wsdapi estende il modello di plug and play locale per poter accedere ad un dispositivo da remoto e ai servizi associati in una rete.