REPORT DANIELE NIEDDU – ESERCIZIO 15/11/2024

Traccia Esercizio:

Si richiede allo studente di effettuare le scansioni dell'esercizio precedente con Nmap sul target Windows con Windows Firewall abilitato e disabilitato. Elencare tutti i passaggi compiuti ed i tipi di scansione, con i relativi risultati, durante la fase di scrittura report.

Facoltativo: Spostare il target Windows nella stessa rete dell'attaccante e ripetere le scansioni con Windows Firewall abilitato e disabilitato.

Svolgimento Esercizio:

Per lo svolgimento dell'esercizio è stato necessario l'utilizzo della VM Pfsense, così da far comunicare Kali e Windows anche se su reti diverse, simulando una rete WAN.
Kali con IP 192.168.1.100 e Windows 10 con IP 192.168.3.50.
Le scansioni son state svolte 2 volte, come richiesto dall'esercizio la prima volta abbiamo creato una Nuova Regola Firewall su Windows 10 per far sì che Kali potesse comunicare con Windows 10, la seconda volta invece abbiamo disattivato la regola e abbiamo lasciato il Firewall di Windows 10 impostato di Default.

Le scansioni effettuate con nmap son state le seguenti:

OS fingerprinting: Serve per il rilevamento del sistema operativo del target.

SYN Scan: Serve per rilevare e analizzare le porte aperte sul target, ottenendo preziose informazioni di rete senza completare connessioni complete, il che la rende uno strumento di scansione discreto e potente.

TCP Scan: Serve per verificare quali porte su un sistema target sono aperte o in ascolto. È anche conosciuta come "TCP Connect Scan" perché si basa sul completamento del "three-way handshake" di TCP, proprio come farebbe una normale connessione TCP tra due host.

S**ervice Version Detection:** Serve per identificare quali servizi sono in esecuzione su porte aperte di un target e per determinare le loro versioni specifiche. Serve a raccogliere informazioni dettagliate sui servizi attivi e può essere particolarmente utile per la valutazione della sicurezza di un sistema o per ottenere un quadro più completo del target.

Di seguito una breve spiegazione di tutti i comandi usati:

Analizzando i comandi:
-O in Nmap abilita il rilevamento del sistema operativo (OS detection). Utilizzando questa opzione, Nmap cerca di identificare il sistema operativo del target esaminando le risposte a pacchetti di scansione specifici.

--osscan-guess in Nmap attiva la modalità di rilevamento avanzato del sistema operativo e viene utilizzato per fare congetture qualora il rilevamento standard non fornisca risultati precisi.

-A è un'opzione che fornisce un'analisi completa e dettagliata del target, ideale per chi ha bisogno di un quadro molto approfondito durante la scansione.

-T4 in Nmap fa parte della serie di opzioni di timing templates che controllano la velocità della scansione. Il valore -T4 è definito come "Aggressive", e rende la scansione molto più veloce rispetto ai livelli più bassi.

--version-all in Nmap serve a forzare un controllo più approfondito e completo delle versioni dei servizi durante la scansione. Quando si utilizza questa opzione, Nmap tenta di identificare ogni servizio presente sulle porte aperte usando tutti i metodi disponibili per il rilevamento della versione.

-v in Nmap attiva la modalità verbosa. Quando viene utilizzata, Nmap fornisce più dettagli sull'operazione di scansione durante l'esecuzione, mostrando informazioni aggiuntive e aggiornamenti in tempo reale.

-Pn in Nmap disabilita il ping scan, trattando tutti gli host come se fossero attivi (online) senza verificarne la raggiungibilità prima di effettuare la scansione delle porte. In pratica, quando si utilizza -Pn, Nmap non esegue il controllo iniziale tramite ping (ICMP o altri metodi) per determinare se il target è raggiungibile. Questa opzione è utile quando si vuole eseguire una scansione su una rete in cui il ping potrebbe essere bloccato da firewall e quando si vuole forzare la scansione di host che altrimenti verrebbero considerati "offline" in base al ping.

-sS in Nmap esegue una TCP SYN scan, che è una delle modalità di scansione più comuni e veloci utilizzate per individuare porte aperte su un host target. Questa modalità è nota anche come "scansione stealth" perché non stabilisce una connessione TCP completa, rendendola più difficile da rilevare rispetto a una scansione tradizionale.

-p 0-65000 in Nmap specifica un range di porte da scansionare, in questo caso tutte le porte dal numero 0 al 65000

-sV in Nmap attiva il rilevamento delle versioni dei servizi. Quando si utilizza -sV, Nmap cerca di identificare quale servizio (ad esempio, HTTP, FTP, SSH) è in esecuzione su una porta aperta e tenta anche di determinare la versione specifica del software associato a quel servizio.

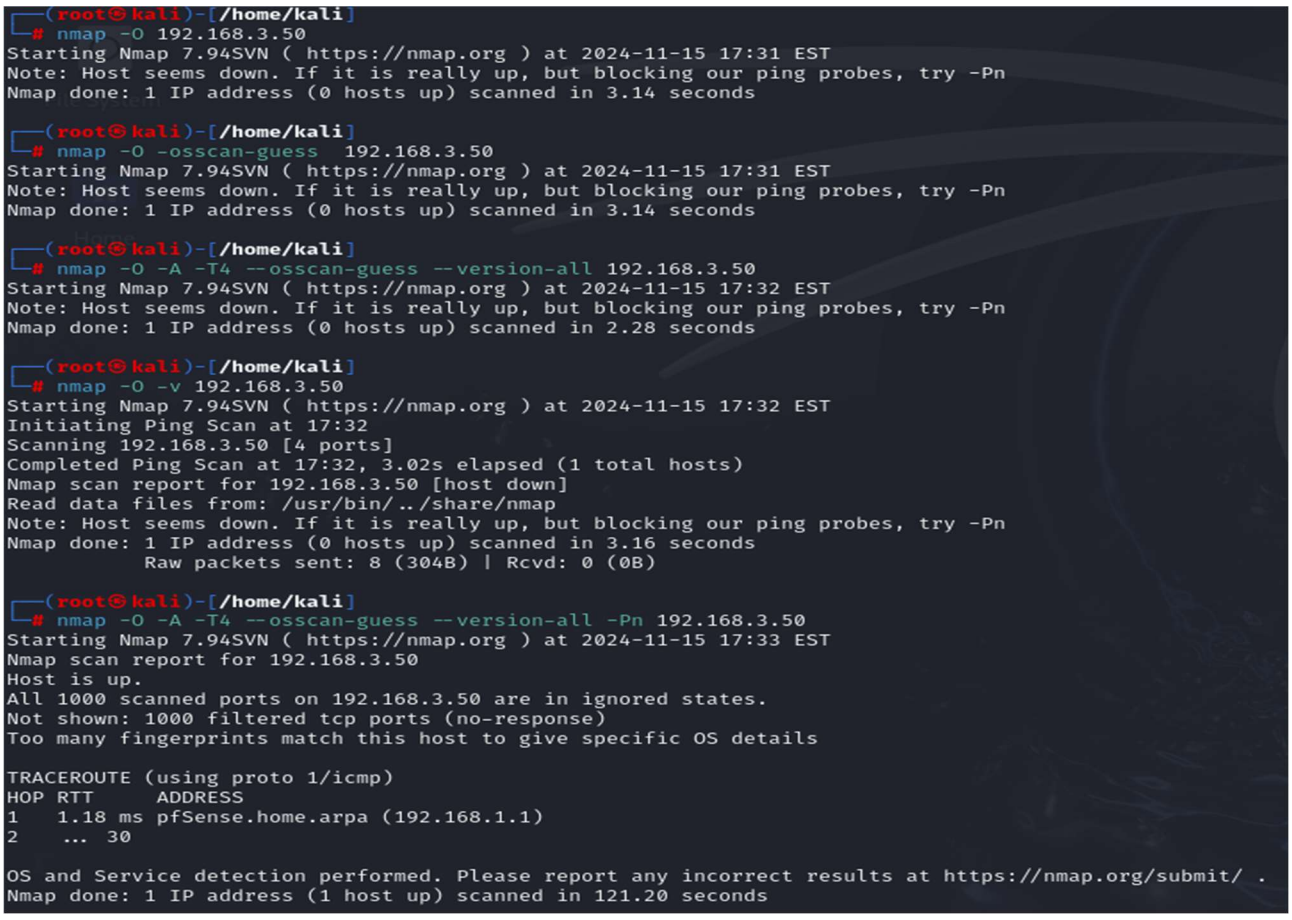
-sT in Nmap esegue una TCP Connect scan, che è il tipo di scansione più semplice e diretta, una scansione TCP Connect stabilisce effettivamente una connessione completa con la porta target.

Per l'**OS Fingerprint** son stati usati i seguenti comandi:

nmap -O <IP> | nmap -O –osscan-guess <IP> | nmap -O -A -T4 –osscan-guess –version-all <IP> | nmap -O -v <IP> | nmap -O -A -T4 –osscan-guess –version-all -Pn <IP> |

Le Immagini sopra fanno riferimento alla scansione effettuata con la regola firewall **ATTIVA,** quindi con kali che può effettuare il ping a Windows.

Sotto invece vedremo le stesse scansioni, fatte però con la regola firewall **DISATTIVA**, quindi con **FIREWALL ATTIVO.**



Per il **SYN Scan** son stati usati i seguenti comandi:

nmap -sS <IP> | nmap -sS –p 0-65000 <IP> | nmap -sS -sV <IP> | nmap -sS -O -sV <IP> |

Le Immagini sopra fanno riferimento alla scansione effettuata con la regola firewall **ATTIVA,** quindi con kali che può effettuare il ping a Windows.

Sotto invece vedremo le stesse scansioni, fatte però con la regola firewall **DISATTIVA**, quindi con **FIREWALL ATTIVO.**

Per il **TCP Scan** son stati usati i seguenti comandi:

nmap -sT -O -sV <IP> | nmap -sT -O -sV -Pn <IP> |

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT -O -sV 192.168.3.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 17:24 EST
Nmap scan report for 192.168.3.50
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.3.50 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2
012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.03 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O --script=default 192.168.3.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 17:28 EST
Nmap scan report for 192.168.3.50
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.3.50 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2
012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.28 seconds
```

Le Immagini sopra fanno riferimento alla scansione effettuata con la regola firewall **ATTIVA,** quindi con kali che può effettuare il ping a Windows.

Sotto invece vedremo le stesse scansioni, fatte però con la regola firewall **DISATTIVA**, quindi con **FIREWALL ATTIVO.**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT -O -sV 192.168.3.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 17:44 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.23 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O --script=default 192.168.3.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 17:44 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.26 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sT -O -sV -Pn 192.168.3.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 17:44 EST
Nmap scan report for 192.168.3.50
Host is up.
All 1000 scanned ports on 192.168.3.50 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 211.21 seconds
```

Il **Service Version Detection** è stato inserito nelle altre scansioni col comando **-sV.**

Esercizio Facoltativo :

Per lo svolgimento dell'esercizio facoltativo son state impostate le macchine Kali e Windows sulla stessa rete, simulando una rete LAN, effettuando le stesse scansioni effettuate nell'esercizio precedente, così da confrontare le scansioni effettuate su rete WAN con quelle su rete LAN.
Kali con IP 192.168.1.9 e Windows 10 con IP 192.168.1.10.
Come nell'esercizio precedente le scansioni son state svolte 2 volte, la prima con la Regola Firewall su Windows 10 per far sì che Kali potesse comunicare con Windows 10, la seconda con la regola disattivata e quindi con Firewall di Windows 10 attivo.

Per l'**OS Fingerprint** son stati usati i seguenti comandi:

nmap -O <IP> | nmap -O –osscan-guess <IP> | nmap -O -A -T4 –osscan-guess –version-all <IP> |

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 00:12 CET
Nmap scan report for DESKTOP-QO69ICO.station (192.168.1.10)
Host is up (0.0020s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 08:00:27:BC:17:14 (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: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10|XP (91%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows Server 2019 (91%), Microsoft Windows 10 1909 (90%), Microsoft Windows XP S
P3 (85%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
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 24.77 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -O -osscan-guess 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 00:13 CET
Nmap scan report for DESKTOP-QO69ICO.station (192.168.1.10)
Host is up (0.059s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 08:00:27:BC:17:14 (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: general purpose
Running (JUST GUESSING): Microsoft Windows 10|2019|XP (90%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows 10 1909 (90%), Microsoft Windows Server 2019 (90%), Microsoft Windows XP S
P3 (85%)
No exact OS matches for host (test conditions non-ideal).
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 22.76 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O -A -T4  --osscan-guess --version-all 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 00:15 CET
Nmap scan report for DESKTOP-QO69ICO.station (192.168.1.10)
Host is up (0.0078s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 08:00:27:BC:17:14 (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: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10|XP (90%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows Server 2019 (90%), Microsoft Windows 10 1909 (88%), Microsoft Windows XP S
P3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   7.78 ms DESKTOP-QO69ICO.station (192.168.1.10)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.03 seconds
```

Le Immagini sopra fanno riferimento alla scansione effettuata con la regola firewall **ATTIVA,** quindi con kali che può effettuare il ping a Windows.

Sotto invece vedremo le stesse scansioni, fatte però con la regola firewall **DISATTIVA**, quindi con **FIREWALL ATTIVO.**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 00:26 CET
Nmap scan report for DESKTOP-QO69ICO.station (192.168.1.10)
Host is up (0.00082s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 08:00:27:BC:17:14 (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: general purpose
Running (JUST GUESSING): Microsoft Windows XP (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (87%)
No exact OS matches for host (test conditions non-ideal).
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 24.03 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -O -osscan-guess 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 00:27 CET
Nmap scan report for DESKTOP-QO69ICO.station (192.168.1.10)
Host is up (0.00092s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 08:00:27:BC:17:14 (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: general purpose
Running (JUST GUESSING): Microsoft Windows XP (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%)
No exact OS matches for host (test conditions non-ideal).
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 22.55 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O -A -T4  --osscan-guess --version-all 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 00:28 CET
Nmap scan report for DESKTOP-QO69ICO.station (192.168.1.10)
Host is up (0.00068s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 08:00:27:BC:17:14 (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: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2019 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.68 ms DESKTOP-QO69ICO.station (192.168.1.10)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.93 seconds
```

Per il **SYN Scan** son stati usati i seguenti comandi:

nmap -sS <IP> | nmap -sS -O -sV <IP> |

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 00:20 CET
Nmap scan report for DESKTOP-QO69ICO.station (192.168.1.10)
Host is up (0.00080s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 08:00:27:BC:17:14 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.14 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -O -sV 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 00:21 CET
Nmap scan report for DESKTOP-QO69ICO.station (192.168.1.10)
Host is up (0.00094s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:BC:17:14 (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: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10|XP (91%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows Server 2019 (91%), Microsoft Windows 10 1909 (90%), Microsoft Windows XP S
P3 (85%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.33 seconds
```

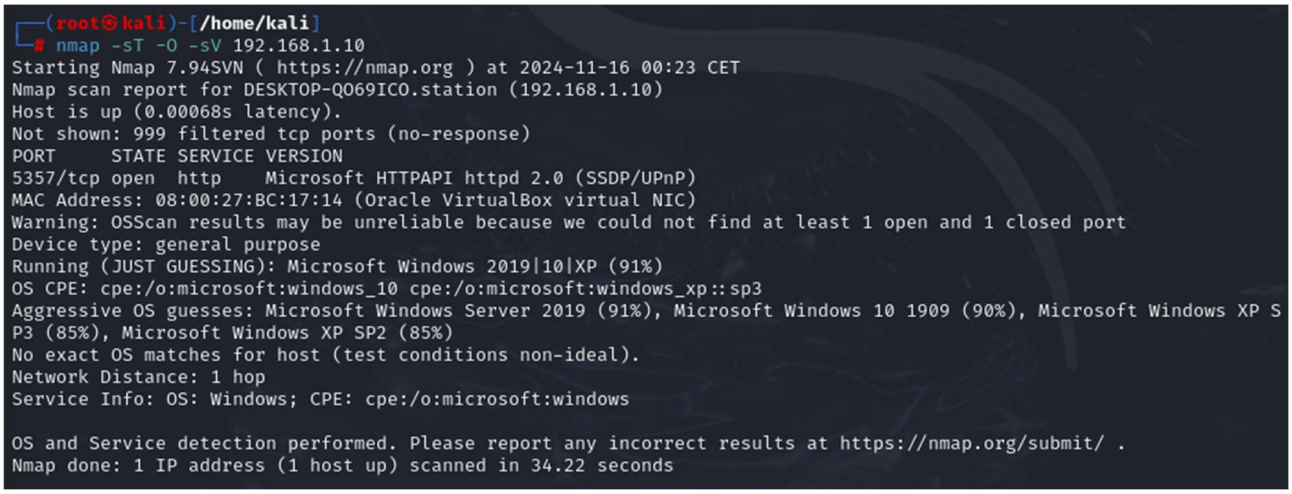
Le Immagini sopra fanno riferimento alla scansione effettuata con la regola firewall **ATTIVA,** quindi con kali che può effettuare il ping a Windows.

Sotto invece vedremo le stesse scansioni, fatte però con la regola firewall **DISATTIVA**, quindi con **FIREWALL ATTIVO.**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 00:33 CET
Nmap scan report for DESKTOP-QO69ICO.station (192.168.1.10)
Host is up (0.00065s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 08:00:27:BC:17:14 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.67 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -O -sV 192.168.1.10

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 00:33 CET
Nmap scan report for DESKTOP-QO69ICO.station (192.168.1.10)
Host is up (0.00084s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:BC:17:14 (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: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2019 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.63 seconds
```

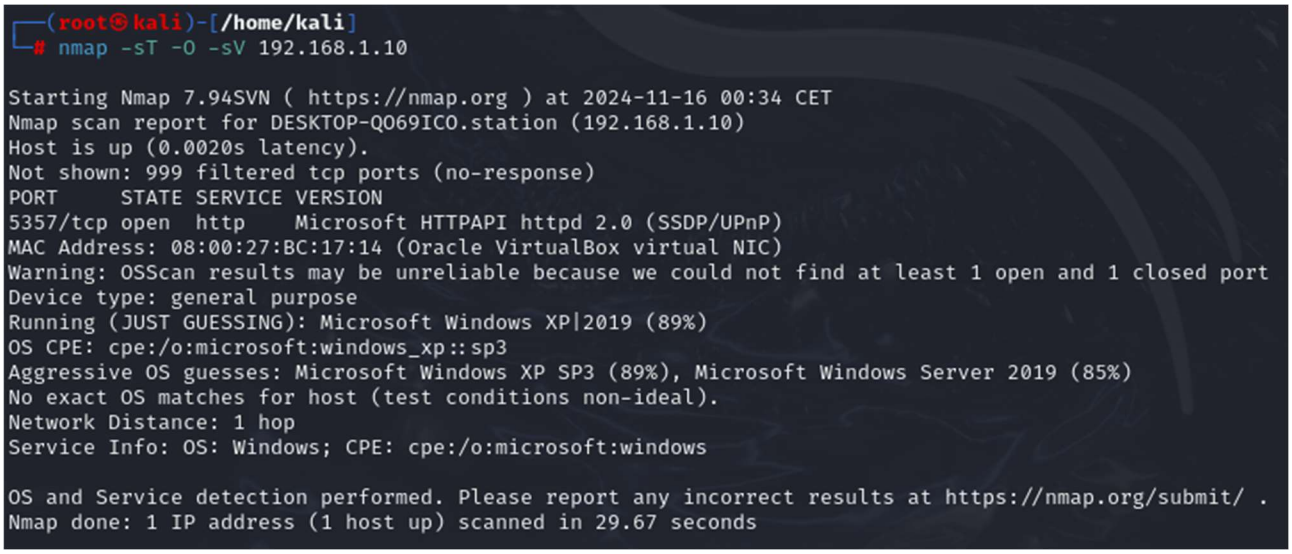
Per il **TCP Scan** son stati usati i seguenti comandi:

nmap -sT -O -sV <IP> |



Le Immagini sopra fanno riferimento alla scansione effettuata con la regola firewall **ATTIVA,** quindi con kali che può effettuare il ping a Windows.

Sotto invece vedremo le stesse scansioni, fatte però con la regola firewall **DISATTIVA**, quindi con **FIREWALL ATTIVO.**



Conclusioni :

In conclusione, le differenze tra una scansione in rete locale e una rete esterna sono significative e devono essere comprese per valutare correttamente i risultati di una scansione di rete. In una rete locale, infatti, l'indirizzo MAC della macchina target è visibile, permettendo di ottenere informazioni più precise sui dispositivi presenti sulla rete.
Al contrario, in una rete esterna, l'indirizzo MAC non è disponibile, poiché i pacchetti passano attraverso vari dispositivi intermedi, come router e firewall, che ne impediscono la visualizzazione.

Effettuando la scansione in locale, abbiamo ottenuto un'informazione che su WAN non avevamo ottenuto, l'informazione che è emersa è la porta TCP 5357 aperta, comunemente utilizzata dal servizio Web Services for Devices (WSD) su sistemi Windows. Questo protocollo è progettato per facilitare la scoperta e la gestione di dispositivi in rete, come stampanti, scanner e altri dispositivi. Sebbene utile in ambienti locali, la porta 5357 può rappresentare un rischio di sicurezza se esposta su reti pubbliche o non adeguatamente protetta. Se non correttamente gestita, potrebbe consentire a malintenzionati di rilevare dispositivi di rete o sfruttare vulnerabilità nel protocollo. Pertanto, è fondamentale limitare l'accesso a questa porta alle sole reti interne fidate per evitare potenziali minacce.

In sintesi, una scansione di rete in un ambiente locale offre risultati più precisi grazie alla visibilità degli indirizzi MAC e alla bassa latenza, mentre le scansioni in rete esterna sono essenziali per valutare la sicurezza dei servizi esposti, considerando le sfide legate alla visibilità e ai tempi di risposta. È cruciale, quindi, prestare attenzione ai rischi associati ai servizi esposti, come nel caso del WSD (Web Services for Devices), per garantire che le reti siano protette da vulnerabilità sfruttabili.