

TRACCIA

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.

INDICE

PARTE 1: STESSA RETE

- OS FINGERPRINTING
 - CON FIREWALL
 - SENZA FIREWALL
- SYN SCAN (-sS)
 - CON FIREWALL
 - SENZA FIREWALL
- TCP SCAN (-sT)
 - CON FIREWALL
 - SENZA FIREWALL
- VERSION SCAN (-sV)
 - CON FIREWALL
 - SENZA FIREWALL

PARTE 2: RETI DIVERSE

- OS FINGERPRINTING
 - CON FIREWALL
 - SENZA FIREWALL
- SYN SCAN (-sS)
 - CON FIREWALL
 - SENZA FIREWALL
- TCP SCAN (-sT)
 - CON FIREWALL
 - SENZA FIREWALL
- VERSION SCAN (-sV)
 - CON FIREWALL
 - SENZA FIREWALL

1. OS FINGERPRINTING (-O)

Con il Firewall Spento Nmap riesce a identificare con precisione la versione Microsoft Windows 10 1507 - 1607 in soli 4.88 secondi, trovando l'esatta versione a partire dalle risposte delle applicazioni in ogni singola porta. Con il firewall spento si noti che sono 981 le porte chiuse, identificate qui come "closed doors" e in stato "reset", mentre sono 19 le porte aperte identificate. Si notino anche i dettagli stessi del sistema operativo, elencati con precisione e senza approssimazioni: il firewall spento ha permesso un'analisi completa di porte e sistema.

Con firewall attivo il tempo di scansione raddoppia a 9.96 secondi, le porte non mostrate aumentano a 990 e l'avviso che riportano ora non è più che sono chiuse, ma che sono "filtered" grazie al firewall, e in stato di "no-response". Come si nota infatti le 19 porte aperte di prima ora sono 10: sappiamo quindi anche quali sono le porte che il firewall chiude quando è attivo. Anche le informazioni sul sistema operativo sono cambiate molto, ora appare l'avviso "Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port": poiché il firewall "zittisce" le porte chiuse rendendole filtrate, Nmap perde il termine di paragone per poter identificare il SO. Così l'identificazione del target diventa meno sicura e basata su probabilità, espresse in percentuale. Questo perché non ci sono più le porte aperte utili per ricevere una risposta dalla quale poter identificare il sistema operativo e le sue versioni. Si noti il nome di questa tecnica, "aggressive os guesses".

SENZA FIREWALL

```
(kali㉿kali)-[~] $ nmap -O 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 11:50 EST
Nmap scan report for 10.0.2.4
Host is up (0.00049s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
5432/tcp   open  postgresql
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
MAC Address: 08:00:27:00:64:D4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 4.88 seconds
```

CON FIREWALL

```
(kali㉿kali)-[~] $ nmap -O 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 11:34 EST
Nmap scan report for 10.0.2.4
Host is up (0.0010s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
5357/tcp   open  wsdapi
8443/tcp   open  https-alt
MAC Address: 08:00:27:00:64:D4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Warning: OSScan results may be unreliable because we could not find at least
        1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1607 (97%), Microsoft Windows Ph
one 7.5 or 8.0 (94%), Microsoft Windows Embedded Standard 7 (93%), Microsoft
Windows 10 1511 - 1607 (92%), Microsoft Windows 10 1511 (91%), Microsoft Wi
ndows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or
Windows 8.1 (91%), Microsoft Windows Server 2016 (91%), Microsoft Windows 7
Professional or Windows 8 (91%), Microsoft Windows Vista SP0 or SP1, Window
s Server 2008 SP1, or Windows 7 (91%)
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 9.96 seconds
```

2. SYN SCAN (-sS)

Con il Firewall Spento, Nmap ha molta libertà e riceve risposte da ogni porta. Il numero di porte non attive rilevate è sempre 981, come closed tcp ports, in stato di reset. Queste porte sono raggiungibili, ma chiuse. Le porte aperte individuate anche qui sono 19. Si noti alla fine il mac address e informazioni su Virtualbox come uniche info di sistema. Inoltre con il firewall spento la scansione dura 13.71 secondi, confermando che Windows risponde anche a tentativi di connessione falliti, e che con firewall spento interroga tutte le porte possibili.

Con il Firewall Attivo la situazione cambia molto: la rete diventa più silenziosa, le porte non mostrate aumentano a 990 e l'avviso che riportano cambia: come con la scansione syn le porte ora sono classificate come "filtered tcp ports" e in stato di "no-response". Il firewall intercetta e scarta i pacchetti, senza rispondere. Anche qui le 19 porte aperte di prima sono scese a 10: servizi come echo, daytime e chargen sono spariti, bloccati dal firewall. Si sa quindi con precisione quali servizi protegge il firewall, nascondendoli completamente ad Nmap e lasciando passare solo il traffico strettamente necessario (come HTTP).

Qui il tempo stranamente si riduce a 5.48 secondi. A firewall acceso il tempo si riduce probabilmente perché il firewall stesso blocca direttamente un gran numero di connessioni, scansionando prima tutte le porte disponibili. Le porte non mostrate salgono a 990, ora "filtered" e in stato di "no-response", perché il firewall scarta i pacchetti inviati da Kali sulla maggior parte delle porte, bloccando lo scambio e risparmiando molto tempo. Qui le porte aperte scendono a 10, facendo sparire servizi vulnerabili (come quelli di gestione remota e database), e lasciando visibili solo le porte essenziali.

SENZA FIREWALL

```
└─(kali㉿kali)-[~]
└─$ nmap -sS 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 11:46 EST
Nmap scan report for 10.0.2.4
Host is up (0.00082s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
5432/tcp   open  postgresql
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
MAC Address: 08:00:27:00:64:D4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.71 seconds
```

CON FIREWALL

```
└─(kali㉿kali)-[~]
└─$ nmap -sS 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 11:33 EST
Nmap scan report for 10.0.2.4
Host is up (0.0014s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
5357/tcp   open  wsdapi
8443/tcp   open  https-alt
MAC Address: 08:00:27:00:64:D4 (PCS Systemtechnik/Oracle VirtualBox virtual

Nmap done: 1 IP address (1 host up) scanned in 5.48 seconds
```

3. TCP SCAN (-sT)

Con il Firewall Spento, Nmap riesce a completare l'handshake su tutte le porte. Questo è rapidissimo, in soli 2.38 secondi, e permette di trovare le stesse 19 porte aperte visibili nelle altre modalità. Particolare è il tempo impiegato, che nonostante fosse una scansione completa con scambio completo di syn e ack, ha impiegato molto meno che la scansione solo syn. Troviamo anche il mac address e le info su Virtualbox come nel caso precedente.

Con il Firewall Attivo, l'analisi rallenta a 5.00 secondi e la risposta della rete cambia anche in questo caso. Le 990 porte non attive diventano "filtered" con stato "no-response", dato che il firewall blocca fin da subito quelle connessioni. Il blocco è efficace e lo si nota dalla superficie d'attacco, che scende a 10 porte aperte.

Con firewall spento, Windows risponde subito con un errore (conn-refused), lasciando chiudere a Nmap il tentativo di connessione e passare subito alla porta dopo. Con il firewall attivo, lo stato di no-response sembra obbligare lo scanner ad aspettare un tempo predefinito per ogni porta. In assenza di segnali di risposta Nmap deve quindi aspettare per assicurarsi che la risposta non sia semplicemente in ritardo. Evidente rimane il fatto che con il firewall spento molte porte vengono filtrate così molti dei servizi più a rischio vengono protetti, e di conseguenza il numero di porte disponibili diminuisce di molto. Qui è inoltre confermato che a firewall spento il tempo di scansione diminuisce, passando da 5 a 2.3 secondi.

SENZA FIREWALL

```
(kali㉿kali)-[~]
$ nmap -sT 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 11:49 EST
Nmap scan report for 10.0.2.4
Host is up (0.0014s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
5432/tcp   open  postgresql
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
MAC Address: 08:00:27:00:64:D4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.38 seconds
```

CON FIREWALL

```
(kali㉿kali)-[~]
$ nmap -sT 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 11:33 EST
Nmap scan report for 10.0.2.4
Host is up (0.0021s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
5357/tcp   open  wsdapi
8443/tcp   open  https-alt
MAC Address: 08:00:27:00:64:D4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds
```

4. VERSION SCAN (-sV)

Con il Firewall Spento, la scansione -sV impiega il tempo più lungo in assoluto: 160.94 secondi. Questo perché Nmap ha trovato 19 porte aperte e deve interagire con ognuna per identificare il software e la sua versione. Nmap ha totale libertà e riesce a leggere le informazioni di quasi tutti i servizi, come ad esempio "Microsoft Windows International daytime" sulla porta 13, "Apache Jserv (Protocol v1.3)" sulla porta 8009 e molti altri servizi vulnerabili: il sistema è esposto, lasciando conoscere l'esatta versione di ogni servizio in ascolto, inclusi database (PostgreSQL su 5432) e servizi di terminale.

La maggior parte dei servizi sono di Microsoft, servizi integrati del computer per il suo funzionamento di base.

Con il Firewall Attivo, il tempo di scansione scende fino a 82.41 secondi, praticamente la metà. Questo è dovuto al carico di lavoro molto diminuito: il firewall ha bloccato in partenza l'accesso a molte delle porte, come negli altri casi. Di conseguenza il modulo -sV di Nmap ha dovuto interrogare 9 servizi in meno, risparmiando tutto il tempo che prima perdeva nel ricavare informazioni con le porte ora "filtered". Anche qui lla protezione dei servizi più sensibili è evidente: sono scomparsi i servizi più critici e vulnerabili come PostgreSQL, Tomcat e il Desktop Remoto, lasciando visibili solo i servizi più di base.

Sia con firewall spento che attivo, Nmap riesce a trovare il nome esatto della macchina target, ossia "DESKTOP-9K1O4BT" come anche la famiglia del sistema operativo Windows.

Dato che le porte base sono rimaste aperte in entrambi i casi, il sistema continua a presentarsi a chiunque. Quindi anche nello scenario con firewall, l'attaccante ottiene comunque informazioni utili per attacchi verso quell'host.

Si noti che anche senza il firewall attivo, alcuni servizi non ricevono lo stesso una versione: ad esempio le porte 7 (echo), 9 (discard) e 19 (chargen), così come msmq (1801) e postgresql (5432). Molte di queste hanno un punto interrogativo a fianco, come se nmap non fosse riuscito a leggerne la versione.

SENZA FIREWALL

```
(kali㉿kali)-[~]
$ nmap -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 11:36 EST
Nmap scan report for 10.0.2.4
Host is up (0.00046s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime      Microsoft Windows International daytime
17/tcp     open  qotd        Windows qotd (English)
19/tcp     open  chargen
80/tcp     open  http         Microsoft IIS httpd 10.0
135/tcp    open  msrpc
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp   open  msmq?
2103/tcp   open  msrpc
2105/tcp   open  msrpc
2107/tcp   open  msrpc
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
5357/tcp   open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5432/tcp   open  postgresql?
8009/tcp   open  ajp13
8080/tcp   open  http        Apache Tomcat/Coyote JSP engine 1.1
8443/tcp   open  ssl/https-alt
MAC Address: 08:00:27:00:64:D4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; 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 160.94 seconds
```

CON FIREWALL

```
(kali㉿kali)-[~]  Trash  Visual Studio  Google Ch...  burgsuite
$ nmap -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 11:28 EST
Nmap scan report for 10.0.2.4
Host is up (0.0018s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp     open  http        Microsoft IIS httpd 10.0
135/tcp    open  msrpc
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp   open  msmq?
2103/tcp   open  msrpc
2105/tcp   open  msrpc
2107/tcp   open  msrpc
5357/tcp   open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8443/tcp   open  ssl/https-alt
MAC Address: 08:00:27:00:64:D4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; 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 82.41 seconds
```

OS FINGERPRINTING

Con il Firewall Spento, anche se siamo su una rete diversa (infatti si legge "Network Distance: 2 hops"), Nmap riesce comunque a capire che è Windows 10 in 9.72 secondi. La grande differenza rispetto all'esercizio prima in locale è che qui non vediamo più il MAC Address. Passando attraverso un router, l'indirizzo fisico viene perso, quindi Nmap deve basarsi solo sui pacchetti TCP/IP e non più sull'ARP. E da qui anche la distanza aumentata di 1 hop.

Si nota un piccolo cambiamento rispetto all'esercizio in rete locale: le porte aperte sono scese da 19 a 18. Manca all'appello la porta 5357 (WSDAPI).

Con il Firewall Attivo, invece, il tempo sale a 10.17 secondi e, proprio come succedeva in rete locale, Nmap ci avvisa che i risultati sono inaffidabili ("Aggressive OS guesses"). Il motivo è sempre che il firewall nasconde le porte chiuse, togliendo a Nmap i punti di riferimento per capire la versione di Windows. Quindi, da remoto con firewall attivo, è quasi impossibile avere una certezza sul sistema operativo.

Anche qui il numero di porte trovate è cambiato. Rispetto alla rete locale, con 10 porte aperte, ne vediamo solo 7. Sono sparite le porte 139 (NetBIOS) e 445 (SMB/Microsoft-DS). Erano quelle per la condivisione file, dimostrando che anche se la condivisione file è attiva, il firewall la permette in automatico solo nella rete locale, proteggendosi così da attacchi esterni.

SENZA FIREWALL

```
└─(kali㉿kali)-[~]
  $ nmap -O 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 08:44 EST
Nmap scan report for 192.168.51.101
Host is up (0.0018s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
3389/tcp   open  ms-wbt-server
5432/tcp   open  postgresql
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1607
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.72 seconds
```

CON FIREWALL

```
└─(kali㉿kali)-[~]
  $ nmap -O 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 08:46 EST
Nmap scan report for 192.168.51.101
Host is up (0.0016s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp     open  http
135/tcp    open  msrpc
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
8443/tcp   open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1607 (97%), Microsoft Windows Phone 7.5 or 8.0 (94%), Microsoft Windows Embedded Standard 7 (93%), Microsoft Windows 10 1511 - 1607 (92%), Microsoft Windows 10 1511 (91%), Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2016 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.17 seconds
```

SYN SCAN

Passando alla scansione SYN, con il Firewall Spento è velocissima: ci mette solo 1.60 secondi per trovare le 18 porte aperte. È strano, perché nell'esercizio in rete locale ci aveva messo quasi 13 secondi. Probabilmente stando su una rete diversa qualcosa ha reso tutto più fluido. Vediamo 982 porte chiuse che rispondono con "reset".

Con il Firewall Attivo, il tempo si alza a 4.95 secondi e le porte aperte scendono drasticamente a 7 (sono spariti tutti i servizi vulnerabili visti prima). Le porte non mostrate salgono a 993 e sono tutte "filtered" e "no-response", per cui il firewall costringe Nmap ad aspettare i timeout per ogni porta filtrata. In generale i tempi sembrano molto ridotti rispetto alla rete locale.

SENZA FIREWALL

```
(kali㉿kali)-[~] $ nmap -sS 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 08:57 EST
Nmap scan report for 192.168.51.101
Host is up (0.010s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
3389/tcp   open  ms-wbt-server
5432/tcp   open  postgresql
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

CON FIREWALL

```
(kali㉿kali)-[~] $ nmap -sS 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 08:46 EST
Nmap scan report for 192.168.51.101
Host is up (0.0039s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp     open  http
135/tcp    open  msrpc
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds
```

TCP SCAN

Con il Firewall Spento, si ottiene lo stesso risultato della SYN scan: 1.60 secondi e 18 porte aperte. Ma qui il "Three-way Handshake" è completo su ogni porta, creando connessioni reali complete, molto più facili da intercettare rispetto alla scansione precedente. Il fatto che il tempo sia identico alla SYN scan ci dice che la rete è molto veloce e stabile, annullando il vantaggio di velocità che solitamente ha la SYN scan.

Con il Firewall Attivo, invece la scansione impiega di più, diventando la più lenta del gruppo con 5.70 secondi. Mentre nella SYN scan Nmap gestisce tutto da solo, qui Nmap deve chiedere di aprire una connessione vera e propria. Come già visto il firewall scarta i pacchetti ("no-response" su 993 porte), il sistema operativo di Kali impiega un attimo in più a gestire l'errore per ogni porta prima di tornare a Nmap. Anche qui, la superficie d'attacco si conferma ridotta alle sole 7 porte essenziali.

SENZA FIREWALL

```
(kali㉿kali)-[~]
└─$ nmap -ST 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 08:57 EST
Nmap scan report for 192.168.51.101
Host is up (0.0093s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT      STATE SERVICE
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
80/tcp     open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
3389/tcp   open  ms-wbt-server
5432/tcp   open  postgresql
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

CON FIREWALL

```
(kali㉿kali)-[~]
└─$ nmap -ST 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 08:47 EST
Nmap scan report for 192.168.51.101
Host is up (0.0088s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp     open  http
135/tcp    open  msrpc
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 5.70 seconds
```

4 VERSION SCAN (-sV)

Infine la scansione delle versioni. Con il Firewall Spento, ci mette 161.00 secondi. Questo tempo è praticamente identico a quello della scansione in rete locale. Il motivo è che Nmap deve comunicare con ben 18 servizi diversi attraverso la rete, e la distanza di 2 hops non aiuta.

Con il Firewall Attivo, succede di nuovo che la scansione scende, a 82.50 secondi, quasi la metà. Non perché Nmap sia diventato più veloce, ma perché il firewall gli ha risparmiato il lavoro bloccando 11 porte. Dovendo analizzare solo 7 servizi invece di 18, finisce molto prima. Anche qui come nel caso locale, le versioni dei servizi critici (come database o RDP) sono nascoste, e le porte sono filtrate.

Si noti che a firewall attivo sul nome dell'host non sappiamo nulla ma solo che è un OS windows, mentre con firewall spento riceviamo anche il nome. Probabilmente una delle porte filtrate dal firewall dava l'accesso a quelle informazioni.

SENZA FIREWALL

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 08:58 EST
Nmap scan report for 192.168.51.101
Host is up (0.0090s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime      Microsoft Windows International daytime
17/tcp     open  qotd        Windows qotd (English)
19/tcp     open  chargen
80/tcp     open  http         Microsoft IIS httpd 10.0
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)
1801/tcp   open  msmq?
2103/tcp   open  msrpc        Microsoft Windows RPC
2105/tcp   open  msrpc        Microsoft Windows RPC
2107/tcp   open  msrpc        Microsoft Windows RPC
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
5432/tcp   open  postgresql?
8009/tcp   open  ajp13       Apache Jserv (Protocol v1.3)
8080/tcp   open  http        Apache Tomcat/Coyote JSP engine 1.1
8443/tcp   open  ssl/https-alt
Service Info: Host: DESKTOP-9K104BT; 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 161.00 seconds
```

CON FIREWALL

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 08:48 EST
Nmap scan report for 192.168.51.101
Host is up (0.0054s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp     open  http         Microsoft IIS httpd 10.0
135/tcp    open  msrpc        Microsoft Windows RPC
1801/tcp   open  msmq?
2103/tcp   open  msrpc        Microsoft Windows RPC
2105/tcp   open  msrpc        Microsoft Windows RPC
2107/tcp   open  msrpc        Microsoft Windows RPC
8443/tcp   open  ssl/https-alt
Service Info: 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 82.50 seconds
```

CONCLUSIONI FINALI

Confrontando le scansioni fatte sulla stessa rete con quelle su reti diverse, si notano alcune differenze principali.

La prima è che nel report "remoto" è sparito il MAC Address e la distanza è passata da 1 a "2 hops". Essendoci un router di mezzo, si è perso il contatto diretto con la parte fisica del target, che si aveva prima grazie all'ARP e che faceva mostrare il MAC address. Da una rete esterna non si vede più il MAC Address del target e la scoperta dell'host non è più tramite ARP (livello 2) ma tramite Ping (livello 3), che è molto più facile da bloccare per un firewall.

A livello di sicurezza, che sia con firewall acceso o spento, da remoto si vedono meno porte aperte. A firewall attivo si scende da 10 a 7 porte, e a firewall spento da 19 a 18. A firewall spento ovviamente ogni porta dovrebbe passare: quella bloccata, la 5357, si "nasconde" in automatico quando capisce che la scansione viene da un'altra rete che non le appartiene. Questo perché viene permesso il traffico dei software di condivisione file solo nella stessa sottorete.

Infine, l'accuratezza dell'identificazione del sistema operativo è legata al firewall, che la scansione sia locale o remota. L'unico scenario in cui Nmap fornisce un risultato certo quando il firewall è completamente spento. Invece, in entrambi i casi in cui il firewall è attivo, sia in locale che remota, l'identificazione fallisce, dando risultati basati su probabilità. (Aggressive OS guesses).