

電腦網路實驗實驗報告 < Network Security >

姓名：翁佳煌

學號：409430030

1. 實驗名稱

1. Scan an IP address (IPv4)
 - multiple IP address
 - a range of IP address
2. Read list of hosts from a file
3. Use TCP SYN , TCP connect , UDP protocol scan
4. Find out if a host open firewall
5. Scan a network to find out which servers are up and running

2. 實驗目的

本實驗的目的是使用網絡探測工具 Nmap 對 IPv4 地址或範圍進行各種類型的掃描，以及從文件中讀取主機列表並對它們進行掃描。不同的掃描類型包括 TCP SYN、TCP 連接、UDP 協議掃描和檢查開放防火牆，此外，還能使用 Nmap 工具識別網絡上哪些服務器正在運行。這些實驗的目的是學習如何使用 Nmap，了解如何進行網絡掃描，以收集有關主機及其開放端口的信息。

3. 實驗設備

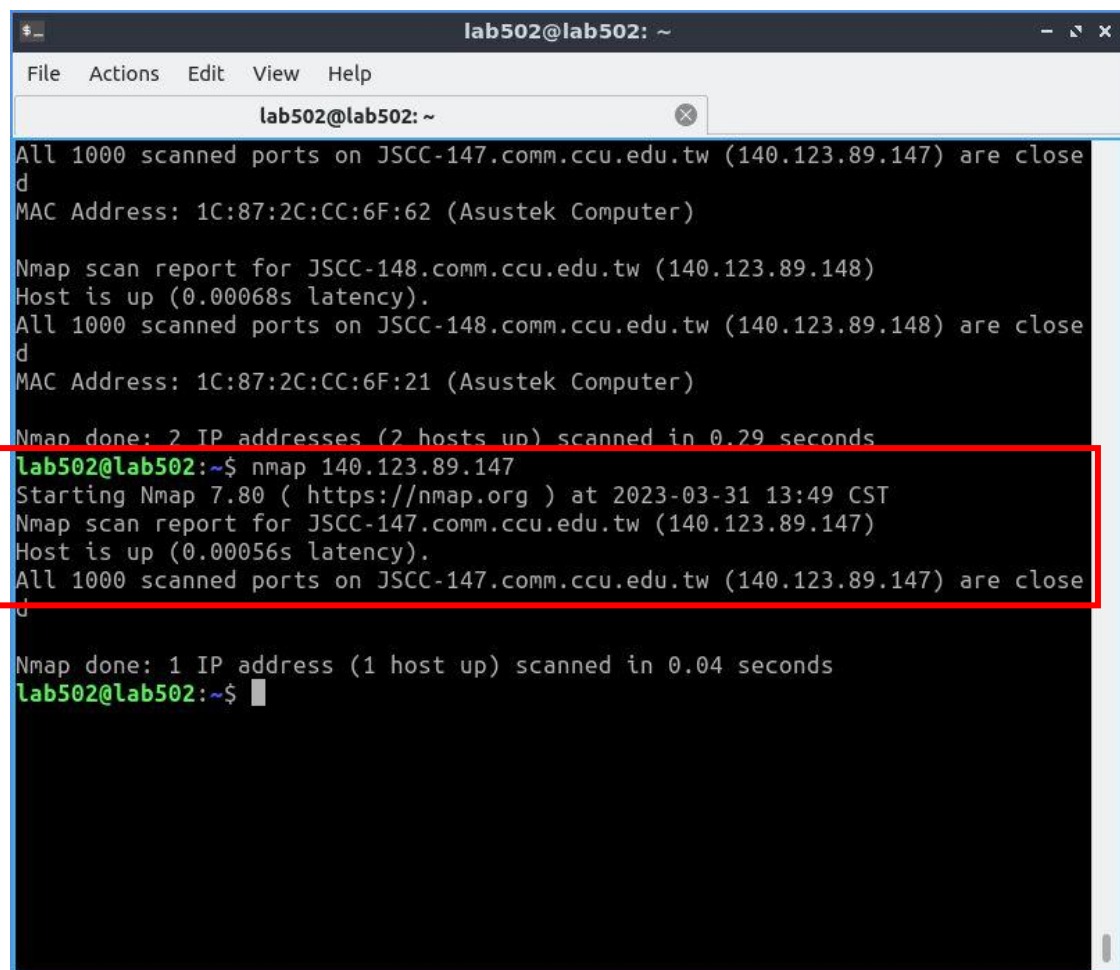
Linux 作業系統之電腦。

Nmap 軟體。

4. 實驗步驟

1-1. Scan an IP address (IPv4)

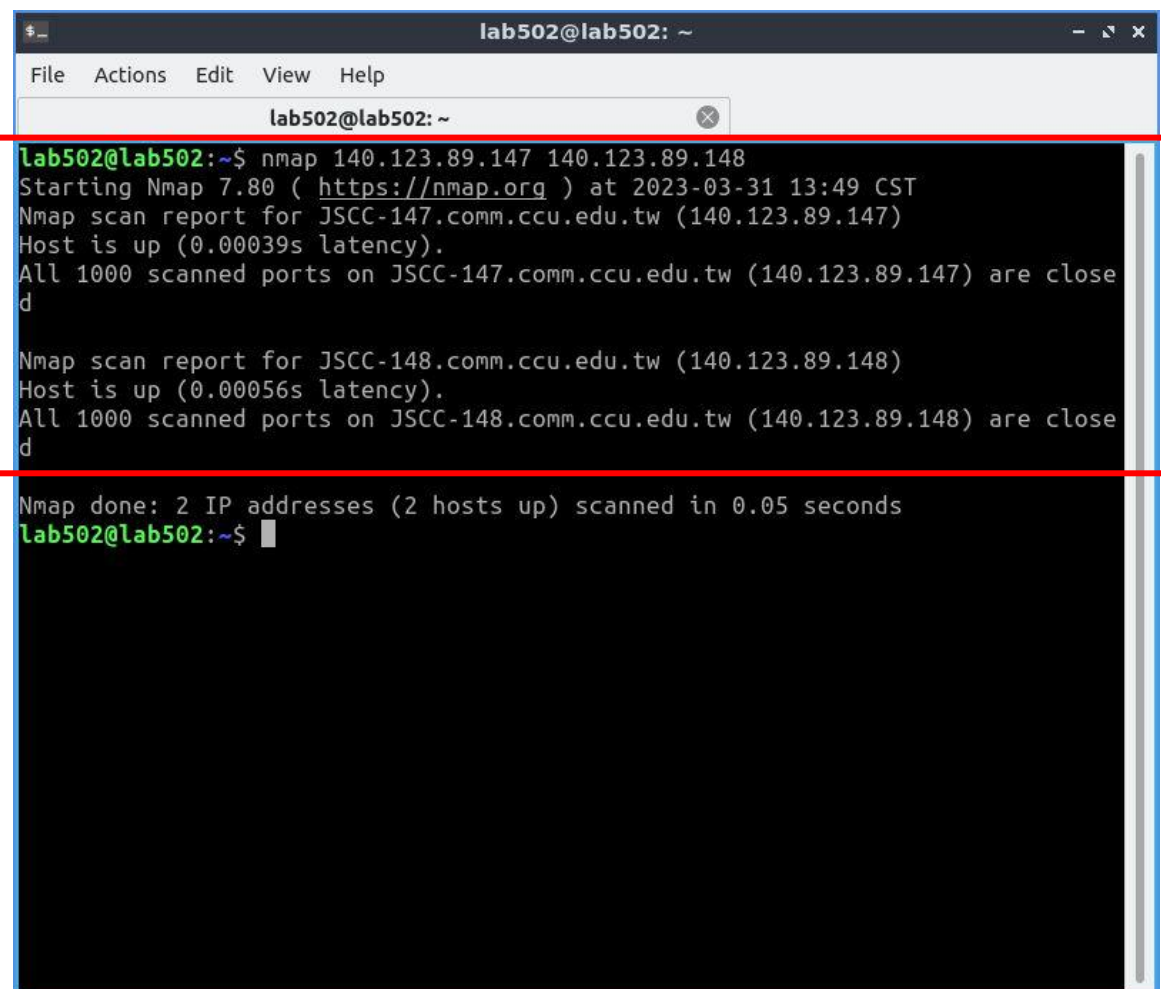
使用 nmap <ip_address> 來完成掃描，需要將<ip_address>替換為要掃描的實際 IPv4 地址。Nmap 將向目標 IP 地址發送探測包，並根據目標的回應確定主機的開放端口和正在運行的服務。此命令適用於需要對單個主機進行深入掃描的場景，例如進行滲透測試或診斷主機網絡問題。



```
lab502@lab502: ~  
File Actions Edit View Help  
lab502@lab502: ~  
All 1000 scanned ports on JSCC-147.comm.ccu.edu.tw (140.123.89.147) are closed  
MAC Address: 1C:87:2C:CC:6F:62 (Asustek Computer)  
  
Nmap scan report for JSCC-148.comm.ccu.edu.tw (140.123.89.148)  
Host is up (0.00068s latency).  
All 1000 scanned ports on JSCC-148.comm.ccu.edu.tw (140.123.89.148) are closed  
MAC Address: 1C:87:2C:CC:6F:21 (Asustek Computer)  
  
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.29 seconds  
lab502@lab502:~$ nmap 140.123.89.147  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-31 13:49 CST  
Nmap scan report for JSCC-147.comm.ccu.edu.tw (140.123.89.147)  
Host is up (0.00056s latency).  
All 1000 scanned ports on JSCC-147.comm.ccu.edu.tw (140.123.89.147) are closed  
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds  
lab502@lab502:~$
```

1-2. Scan multiple IP address

使用 `nmap <ip_address1> < ip_address2> ...` 掃描多個 IPv4 地址的命令，其中 `<ip_address_1>`、`<ip_address_2>`... 是要掃描的實際 IPv4 地址。在這個命令中，多個 IP 地址之間需要用空格分開，Nmap 將會針對這些 IP 地址進行掃描。當您需要同時掃描多個主機時，這個命令非常有用。例如，您可能需要在網絡上掃描多個關鍵系統的安全狀態，以確保它們是否存在任何潛在的漏洞或安全風險。需要注意的是，大量掃描可能會對網絡帶寬和主機性能產生影響，必須小心使用。

A terminal window titled 'lab502@lab502: ~' with a menu bar (File, Actions, Edit, View, Help) and a tab labeled 'lab502@lab502: ~'. The terminal shows the execution of the command 'nmap 140.123.89.147 140.123.89.148'. The output includes the Nmap version (7.80), the scan time (2023-03-31 13:49 CST), and detailed reports for both IP addresses, stating they are up and all 1000 scanned ports are closed. A summary line at the bottom indicates that 2 IP addresses (2 hosts up) were scanned in 0.05 seconds. The prompt 'lab502@lab502:~\$' is visible at the end of the command line.

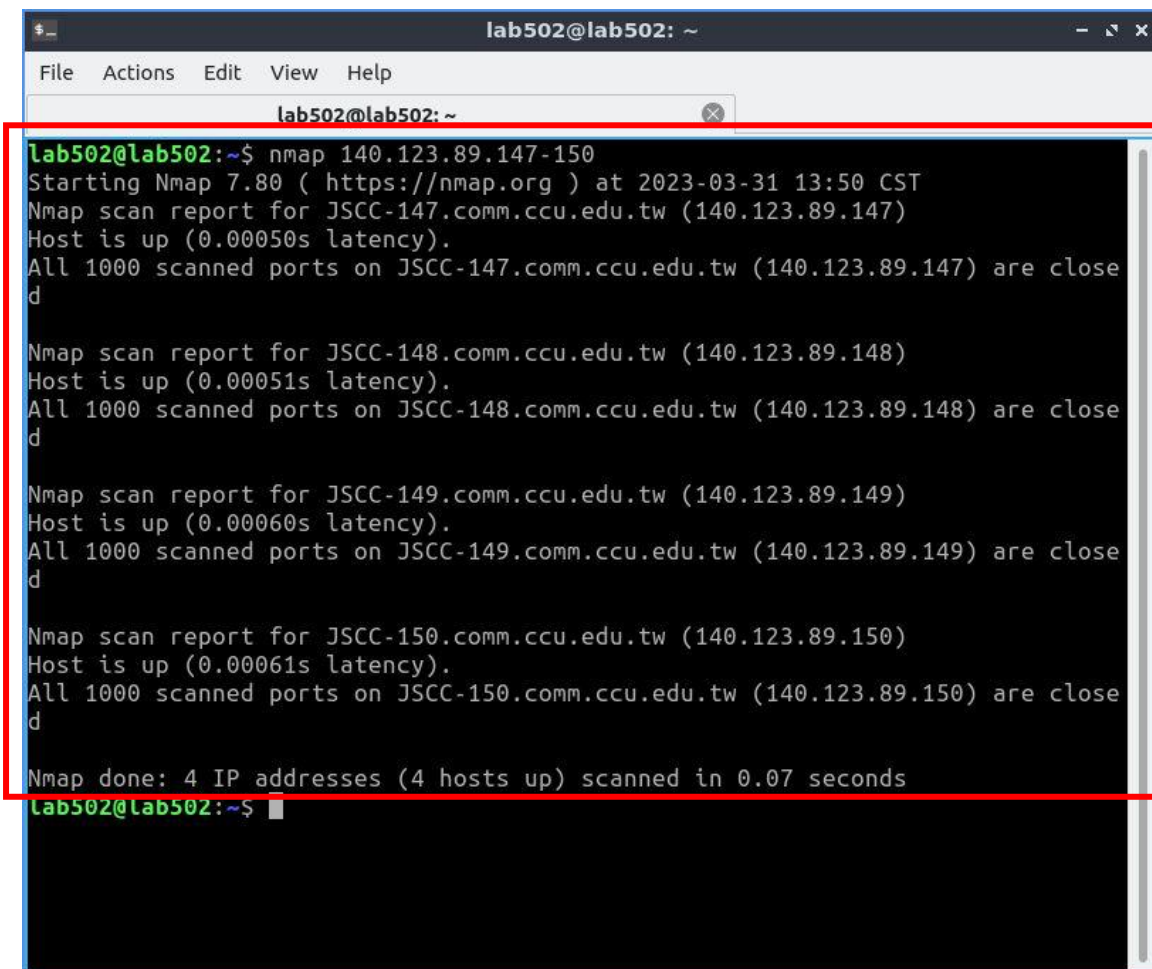
```
lab502@lab502:~$ nmap 140.123.89.147 140.123.89.148
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-31 13:49 CST
Nmap scan report for JSCC-147.comm.ccu.edu.tw (140.123.89.147)
Host is up (0.00039s latency).
All 1000 scanned ports on JSCC-147.comm.ccu.edu.tw (140.123.89.147) are closed

Nmap scan report for JSCC-148.comm.ccu.edu.tw (140.123.89.148)
Host is up (0.00056s latency).
All 1000 scanned ports on JSCC-148.comm.ccu.edu.tw (140.123.89.148) are closed

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.05 seconds
lab502@lab502:~$
```

1-3. Scan a range of IP address

使用 `nmap <starting_ip_address>-<ending_ip_address>`，其中 `<starting_ip_address>` 和 `<ending_ip_address>` 是您要掃描的起始 IP 地址和結束 IP 地址。這個命令將掃描從起始 IP 地址到結束 IP 地址之間的所有 IP 地址，包括這兩個 IP 地址。這個命令非常適用於在一個特定的 IP 地址範圍內查找主機，例如在公司內部網絡上查找所有已連接到網絡的主機。使用這個命令可以有效地節省時間和工作量，並提高網絡管理的效率。當然，大量掃描可能會對網絡帶寬和主機性能產生影響，也必須小心使用。

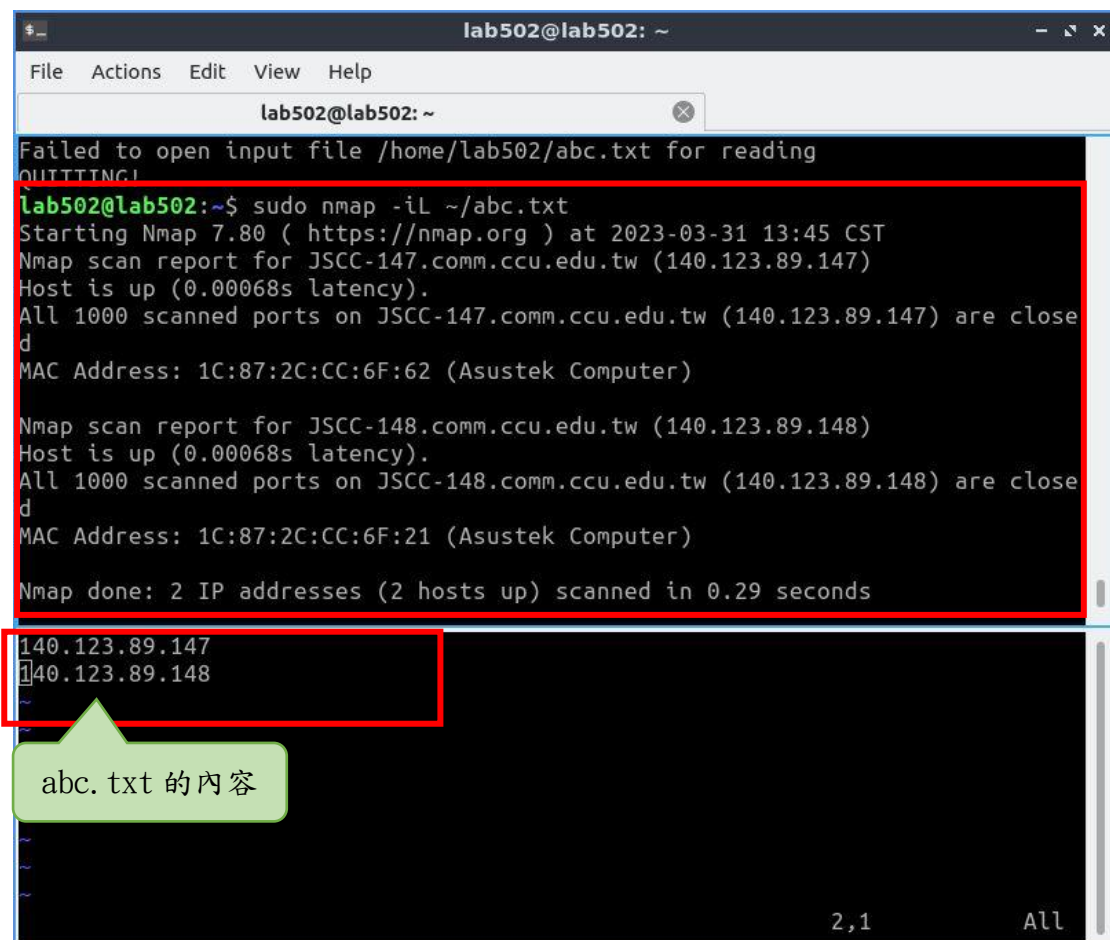
A screenshot of a terminal window titled 'lab502@lab502: ~'. The terminal shows the execution of the command 'nmap 140.123.89.147-150'. The output displays four individual scan reports for IP addresses 140.123.89.147, 140.123.89.148, 140.123.89.149, and 140.123.89.150. Each report indicates that the host is up and that all 1000 scanned ports are closed. The terminal concludes with 'Nmap done: 4 IP addresses (4 hosts up) scanned in 0.07 seconds'. The entire terminal output is enclosed in a red rectangular box.

```
lab502@lab502: ~  
File Actions Edit View Help  
lab502@lab502: ~  
lab502@lab502:~$ nmap 140.123.89.147-150  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-31 13:50 CST  
Nmap scan report for JSCC-147.comm.ccu.edu.tw (140.123.89.147)  
Host is up (0.00050s latency).  
All 1000 scanned ports on JSCC-147.comm.ccu.edu.tw (140.123.89.147) are closed  
  
Nmap scan report for JSCC-148.comm.ccu.edu.tw (140.123.89.148)  
Host is up (0.00051s latency).  
All 1000 scanned ports on JSCC-148.comm.ccu.edu.tw (140.123.89.148) are closed  
  
Nmap scan report for JSCC-149.comm.ccu.edu.tw (140.123.89.149)  
Host is up (0.00060s latency).  
All 1000 scanned ports on JSCC-149.comm.ccu.edu.tw (140.123.89.149) are closed  
  
Nmap scan report for JSCC-150.comm.ccu.edu.tw (140.123.89.150)  
Host is up (0.00061s latency).  
All 1000 scanned ports on JSCC-150.comm.ccu.edu.tw (140.123.89.150) are closed  
  
Nmap done: 4 IP addresses (4 hosts up) scanned in 0.07 seconds  
lab502@lab502:~$
```

2. Read list of hosts from a file

首先在該目錄下創建了一個文檔，名叫 abc.txt，內容寫入想要掃描的 ip address，之後回到終端機輸入 nmap -iL <filename>，<filename>是包含主機列表的文件名，在這裡為 abc.txt。

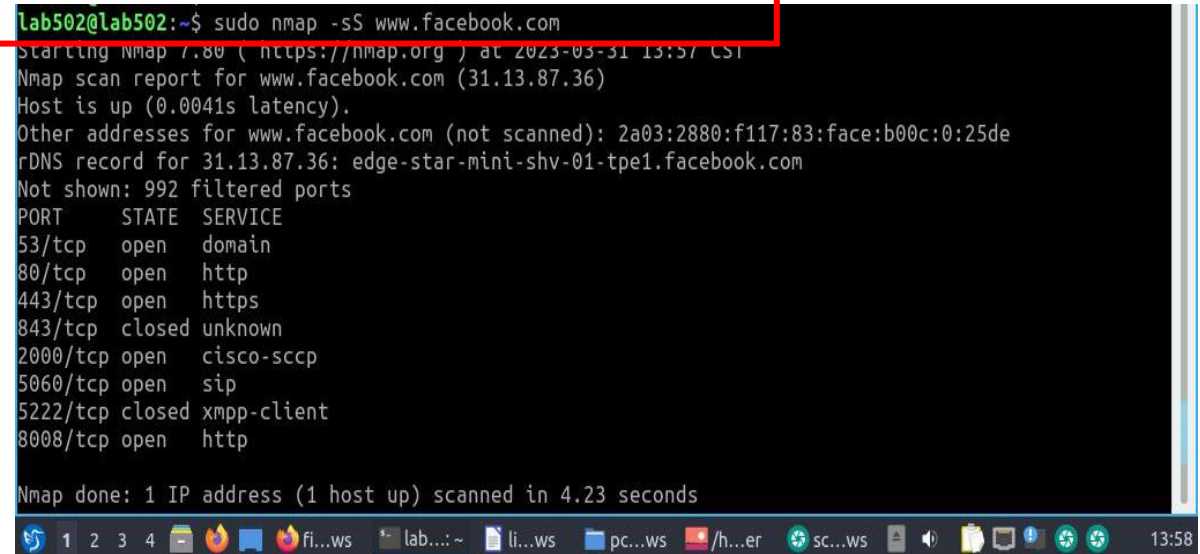
這個命令可以讓您從文件中輕鬆讀取主機列表，而不必手動輸入每個主機的 IP 地址。在命令中，-iL 選項指定要使用文件作為主機列表的輸入來源。可以在文件中列出多個 IP 地址，每個地址佔一行。Nmap 將依次掃描文件中列出的所有 IP 地址。這個命令非常適用於大規模網絡中的主機掃描，例如在整個公司網絡中查找特定服務的所有主機。



```
lab502@lab502: ~  
File Actions Edit View Help  
lab502@lab502: ~  
Failed to open input file /home/lab502/abc.txt for reading  
QUITTING!  
lab502@lab502:~$ sudo nmap -iL ~/abc.txt  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-31 13:45 CST  
Nmap scan report for JSCC-147.comm.ccu.edu.tw (140.123.89.147)  
Host is up (0.00068s latency).  
All 1000 scanned ports on JSCC-147.comm.ccu.edu.tw (140.123.89.147) are closed  
MAC Address: 1C:87:2C:CC:6F:62 (Asustek Computer)  
  
Nmap scan report for JSCC-148.comm.ccu.edu.tw (140.123.89.148)  
Host is up (0.00068s latency).  
All 1000 scanned ports on JSCC-148.comm.ccu.edu.tw (140.123.89.148) are closed  
MAC Address: 1C:87:2C:CC:6F:21 (Asustek Computer)  
  
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.29 seconds  
  
140.123.89.147  
140.123.89.148  
  
abc.txt 的內容  
  
2,1 All
```

3-1. Use TCP SYN

對於命令 `nmap -sS www.facebook.com`，它的目的是對 Facebook 的網站進行 TCP SYN 掃描，以檢查其開放的 TCP 端口。由於該命令沒有指定端口範圍，因此 Nmap 將會掃描 `www.facebook.com` 的所有已知端口。與 TCP connect 掃描不同，TCP SYN 掃描是一種隱蔽的掃描方式，因為它不會完整地建立 TCP 連接，而是只發送一個 TCP SYN 段。因此，TCP SYN 掃描可能比 TCP connect 掃描更難被檢測到，但也可能被防火牆規則所過濾。



```
lab502@lab502:~$ sudo nmap -sS www.facebook.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-31 13:57 CST
Nmap scan report for www.facebook.com (31.13.87.36)
Host is up (0.0041s latency).
Other addresses for www.facebook.com (not scanned): 2a03:2880:f117:83:face:b00c:0:25de
rDNS record for 31.13.87.36: edge-star-mini-shv-01-tpe1.facebook.com
Not shown: 992 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
843/tcp   closed unknown
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
5222/tcp  closed xmpp-client
8008/tcp  open  http

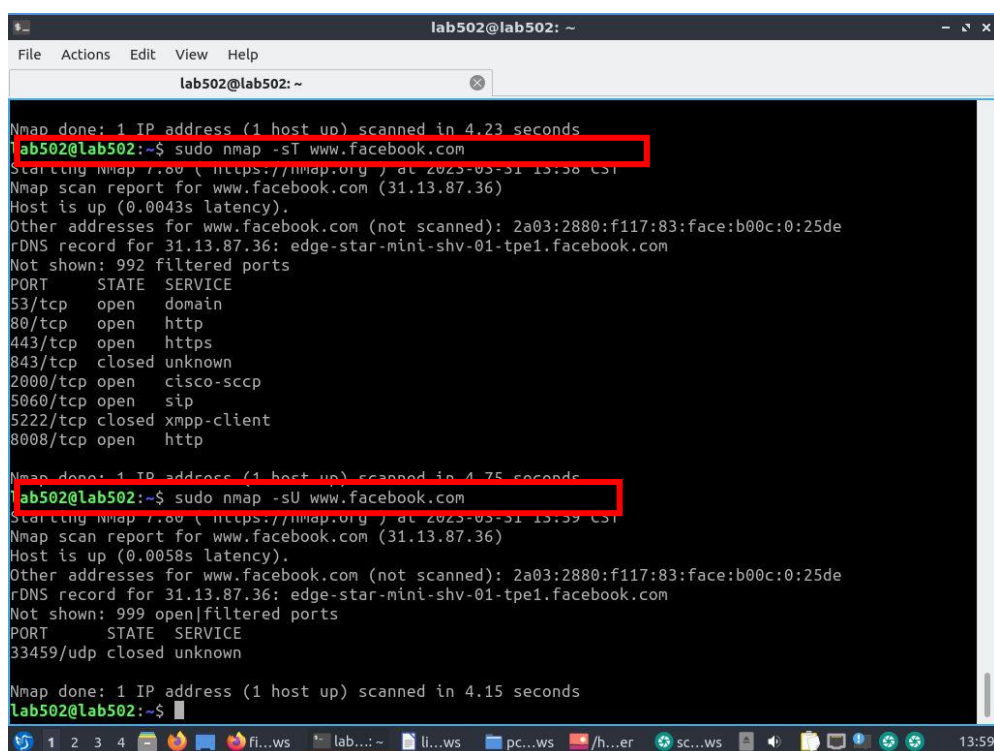
Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
```

3-2、3-3. TCP connect ,UDP protocol scan

`nmap -sT <ip_address>` 是使用 TCP connect()掃描技術對目標主機進行掃描。該命令將使用 TCP 協議與目標主機建立連接，並在連接成功後向主機發送一系列探測消息，以確定端口的狀態。使用 TCP connect()掃描技術的優點是其穩定性和可靠性高，但其缺點是可能會被目標主機的防火牆或其他安全設備檢測到。

`nmap -sT www.facebook.com` 該命令將使用 TCP connect()掃描技術對 `www.facebook.com` 進行掃描，並顯示該主機的開放端口和相應的服務信息。

`nmap -sU <ip_address>` 是使用 UDP 掃描技術對目標主機進行掃描。該命令將向目標主機的 UDP 端口發送一系列的探測消息，以確定該端口的狀態。使用 UDP 掃描技術的優點是可以檢測到 TCP 掃描無法檢測到的開放 UDP 端口，但其缺點是由於 UDP 是無連接的協議，因此無法檢測到 TCP connect()掃描技術那樣的詳細信息。
`nmap -sU www.facebook.com` 該命令將使用 UDP 掃描技術對 `www.facebook.com` 進行掃描，並顯示該主機的開放 UDP 端口和相應的服務信息。



```
lab502@lab502: ~  
File Actions Edit View Help  
lab502@lab502: ~  
Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds  
lab502@lab502:~$ sudo nmap -sT www.facebook.com  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-31 13:38 CST  
Nmap scan report for www.facebook.com (31.13.87.36)  
Host is up (0.0043s latency).  
Other addresses for www.facebook.com (not scanned): 2a03:2880:f117:83:face:b00c:0:25de  
rDNS record for 31.13.87.36: edge-star-mini-shv-01-tpe1.facebook.com  
Not shown: 992 filtered ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
843/tcp   closed unknown  
2000/tcp  open  cisco-sccp  
5060/tcp  open  sip  
5222/tcp  closed xmpp-client  
8008/tcp  open  http  
Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds  
lab502@lab502:~$ sudo nmap -sU www.facebook.com  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-31 13:39 CST  
Nmap scan report for www.facebook.com (31.13.87.36)  
Host is up (0.0058s latency).  
Other addresses for www.facebook.com (not scanned): 2a03:2880:f117:83:face:b00c:0:25de  
rDNS record for 31.13.87.36: edge-star-mini-shv-01-tpe1.facebook.com  
Not shown: 999 open|filtered ports  
PORT      STATE SERVICE  
33459/udp closed unknown  
Nmap done: 1 IP address (1 host up) scanned in 4.15 seconds  
lab502@lab502:~$
```


4. Find out if a host open firewall

`nmap -sA` 是用來探測主機是否有防火牆或是防火牆規則。當使用這個指令時，Nmap 會嘗試進行 TCP ACK 掃描，也就是向目標主機發送 TCP ACK 封包。如果主機收到了封包並回應了 TCP RST 封包，這代表目標主機沒有開啟防火牆，但是如果主機收到了封包並回應了 TCP ACK 封包，這代表目標主機有開啟防火牆。Nmap 掃描了 `www.facebook.com` 這個主機的 1000 個 TCP port，並且顯示主機是活著的，延遲為 0.00024 秒。同時顯示所有的掃描端口都是 `unfiltered`，這代表在這個掃描中沒有發現任何防火牆規則將封包擋下，也就是目標主機沒有開啟防火牆。因此，結果顯示 `www.facebook.com` 主機並沒有封鎖 Nmap 發送的 TCP ACK 封包，可能是因為 Facebook 需要讓人們能夠方便地訪問他們的網站，所以他們沒有啟用 TCP ACK 封包的過濾。

```
alan@alan-VirtualBox:~$ sudo nmap -sA www.facebook.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-01 14:10 CST
Nmap scan report for www.facebook.com (31.13.87.36)
Host is up (0.00024s latency).
Other addresses for www.facebook.com (not scanned): 2a03:2880:f117:83:face:b00c:0:25d
e
rDNS record for 31.13.87.36: edge-star-mini-shv-01-tpe1.facebook.com
All 1000 scanned ports on www.facebook.com (31.13.87.36) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
```


5. Scan a network to find out which servers are up and running

使用 `-sn` 選項指定掃描模式為 ping 掃描。指定網絡地址為 `140.123.89.0/24`，表示要掃描這個網段中的所有 IP 位址。

Nmap 掃描了 256 個 IP 位址，發現其中有 8 台主機處於啟動和運行狀態。對於每台主機，Nmap 提供了主機名稱（如果有的話）、IP 位址和 ping 延遲時間（以秒為單位）。

```
alan@alan-VirtualBox:~$ nmap -sn 140.123.89.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-01 14:20 CST
Nmap scan report for Unregistered.comm.ccu.edu.tw (140.123.89.18)
Host is up (0.048s latency).
Nmap scan report for vpn.comm.ccu.edu.tw (140.123.89.21)
Host is up (0.062s latency).
Nmap scan report for bbs.comm.ccu.edu.tw (140.123.89.93)
Host is up (0.057s latency).
Nmap scan report for 140.123.89.95
Host is up (0.057s latency).
Nmap scan report for srv03.comm.ccu.edu.tw (140.123.89.103)
Host is up (0.052s latency).
Nmap scan report for srv04.comm.ccu.edu.tw (140.123.89.104)
Host is up (0.052s latency).
Nmap scan report for Unregistered.comm.ccu.edu.tw (140.123.89.248)
Host is up (0.052s latency).
Nmap scan report for gateway-115.comm.ccu.edu.tw (140.123.89.249)
Host is up (0.052s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 24.12 seconds
```

5. 問題與討論

1. 為什麼要掃描一個 IP 地址？

掃描一個 IP 地址可以確定該主機是否正在運行，以及哪些端口是開放的。這對於評估安全性、診斷網絡問題和掃描潛在目標非常有用。

2. 如何處理多個 IP 地址和 IP 地址範圍？

掃描多個 IP 地址或 IP 地址範圍可以使用 Nmap 的 `-iL` 選項和 `-n` 選項。使用 `-iL` 選項可以指定包含要掃描的 IP 地址列表的文本文件，而使用 `-n` 選項可以避免 DNS 查詢，以加快掃描速度。

3. TCP SYN、TCP 連接和 UDP 協議掃描有什麼區別？

TCP SYN 掃描是 Nmap 的默認掃描模式，它通過發送 SYN 封包測試每個端口的狀態。TCP 連接掃描通過嘗試建立 TCP 連接來測試端口的狀態。UDP 掃描通過向 UDP 端口發送數據包來測試端口的狀態。每種掃描方式都有其優點和缺點，具體使用哪種方式取決於特定的情況。

4. 如何找出主機是否開放防火牆？

可以使用 Nmap 的 `-sA` 選項執行 ACK 掃描來測試主機是否開放防火牆。如果主機返回 RST，則表示防火牆是開放的。如果主機沒有返回 RST，則表示防火牆是關閉的或存在其他問題。

5. 為什麼要掃描網絡以查找運行中的伺服器？

掃描網絡以查找運行中的伺服器可以幫助管理員評估網絡拓撲和識別設備。這對於維護網絡安全、發現問題並尋找解決方案非常有用。

6. 心得與感想

這次的實驗讓我學到了如何使用 nmap 工具進行網路掃描。透過實驗，我學習了如何指定掃描的 IP 地址，包括掃描單個 IP、多個 IP 以及 IP 範圍等；學習了不同的掃描模式，如 TCP SYN、TCP connect、UDP 等；還學習了如何從掃描結果中找出哪些主機開啟了防火牆，以及如何查找哪些主機在運行特定的服務。這些技巧對於網路安全和系統管理等方面都非常有用，讓我在以後的工作中能更加有效地管理和保護網路系統。

7. 參考文獻

<https://nmap.org/>

<https://blog.gtwang.org/linux/nmap-command-examples-tutorials/>

<https://zh.wikipedia.org/zh-tw/Nmap>

<https://ithelp.ithome.com.tw/articles/10213539>

<https://medium.com/%E7%92%BF%E7%9A%84%E7%AD%86%E8%A8%98%E6%9C%AC/nmap-%E5%85%A5%E9%96%80%E6%95%99%E5%AD%B8-36ed094d6ef8>