113-1 嵌入式系統 Embedded System (Homework 2)

Class: 資工碩一 Student ID: 113598043 Name: 張育丞

Title: Practice `Nmap (the Network Mapper) ` command

Content: Please refer to the steps and pictures below.

Step:

步驟一：安裝 Nmap 這項套件，使用指令為 sudo apt install nmap。(參考圖一)

步驟二：將整個軟體包清單進行更新，使用指令為 sudo apt-get update。(參考圖二)

步驟三：使用 nmap -h 確認 nmap 具備那些參數可以使用。(參考圖二)

<環境搭建已結束，接下來進入實驗重點。>

Experiment:

實驗一：使用 nmap <目標 IP>進行實驗。

本文使用 iPhone 進行分享獲取<目標 IP>為 **172.20.10.2**，因此指令輸入為 nmap 172.20.10.2，進行目標設備的基礎掃描，確認埠號 (Port)是否開放等。(參考圖四)

實驗二：使用 nmap -sT -p80 <目標 IP>進行實驗。

在 Termainal 中輸入指令為 nmap -sT -p80 172.20.10.2，從參數-sT 可悉知 Scan TCP 的縮寫，在此會進行 SYN 和 ACK 的三方交握流程，這方法相當簡單，沒有太多的特殊權限需要處理。接著，看到 -p，在基礎認知中，網路的埠號 80 就是代表 HTTP 服務，因此得知 nmap 使用 HTTP 的方法進行測試，而測試對象就是<目標 IP>。(參考圖五)

值得一提，如果對應的服務或埠號關閉或啟用過濾的行為，Nmap 套件也能給出相應的訊息給使用者參考。

實驗三：使用 nmap -v <目標 IP>進行實驗。

在 Termainal 中輸入指令為 nmap -v 172.20.10.2，此指令將會對於<目標 IP>進行深度的掃描，因此可以顯示更多的細節，包含 Ping 去測試主機是否在線上，發送 SYN 封包，檢查埠號的開放，還有每項測試之內容與進度的細節紀載。(參考圖六)

該指令適合掃描多個<目標 IP>設備或大量埠號時使用，藉此了解區域網路的結構及狀態，協助管理者更好地去除錯及診斷問題，不過因為檢測量大，帶來需要許多時間的缺點。

實驗四：使用 nmap -sC <目標 IP>進行實驗。

在 Termainal 中輸入指令為 nmap -sC 172.20.10.2，這是一個常見的腳本式掃描行為，-sC 就是內建的預設腳本之參數，屬於 Nmap Scirpting Engine (NSE)的範疇。時常用於檢測網路服務中的版本偵測、漏洞檢測、安全檢查和服務資訊收集等。

圖七中的 Host it up 表示的是樹莓派在線，回應時間為 0.00028 秒，Not shown 998 closed tcp ports (conn-refused)表示 998 個 TCP 埠號正處於關閉，因此被拒絕連線，開放的則有埠號 22 的 SSH 及埠號 5900 的 VNC 連線，在 SSH 連線中提供 ECDSA 和 ED25519 兩種加密類型；VNC 部分可以看見協定為 3.8 版本，支援 VeNCrypt (19)，及 RA2 (5)還有其他安全類型，在 VeNCrypt 中還具備 TLS (262)，此掃描需耗時 21.60 秒。(參考圖七)

實驗五：使用 nmap -sP 系列指令進行實驗。

在 Termainal 中輸入指令為 nmap -sP 172.20.10.2/31，掃描範圍為 172.20.10.2/31，這表示網段 172.20.10.2 以及另一個 IP 位址 (172.20.10.3) 的主機，經掃描有 2 個 IP 位址，但僅有 1 個主機在線，反應時間為 0.00065 秒。(參考圖八)

接著輸入 nmap -sP 172.20.10.2-254，也就是 172.20.10.x 的網路中，從 2~254 進行掃描，經掃描結果僅有 1 個主機在線，回應時間為 0.00014 秒，共 253 個 IP 位址，總耗時 3.33 秒。(參考圖八)

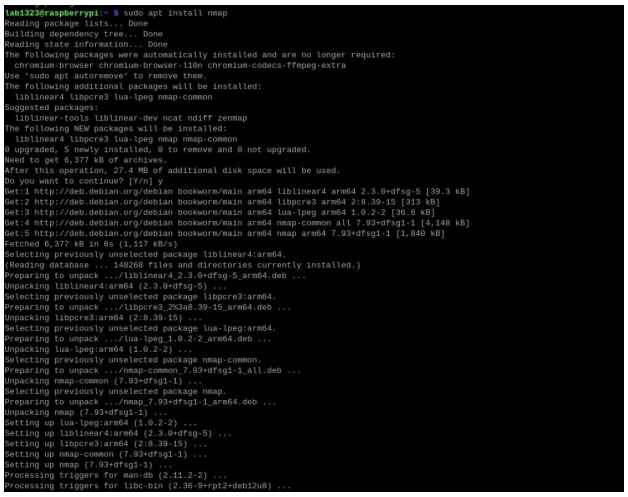
再來使用 nmap -sP 172.20.10.*，此指令會將 172.20.10.x 的網路中，從 0~255 全部掃描，經掃描後 172.20.10.1 的回應時間為 0.026 秒，172.20.10.2 回應時間為 0.00098 秒，256 個位址，僅有 2 個在使用，分為為 iPhone 和 Raspberry Pi，總耗時 15.82。(參考圖八)

實驗六：使用 nmap -sT5 <目標 IP>指令進行實驗。

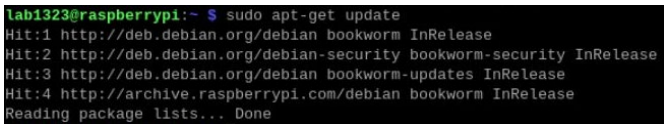
輸入 nmap -T5 172.20.10.2/31，是使用時間選擇器 T，以及最快速掃描之 5 兩個參數合併而成。在此會可以減少等待時間，以便快速完成掃描。經掃描如上面所提及有 998 個 TCP 埠號拒絕連線，僅有 SSH 和 VNC 是開放的。(參考圖九)

實驗七：使用 nmap --top-ports 20 <目標 IP>指令進行實驗。

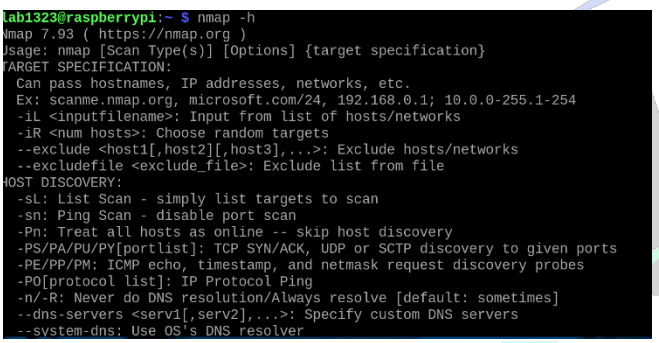
輸入 nmap --top-ports 20 172.20.10.2/31，此參數中告知最常且熱門使用的埠號前 20 個進行掃描，這指令將有效檢查常用埠號的是否開放，其中以 SSH 和 VNC 有開放，未被開放的有 FTP (Port 21)、SMTP (Port 25)、HTTP (Port 80)、HTTPS (Port 443)以及 MySQL (3306)等。(參考圖十)



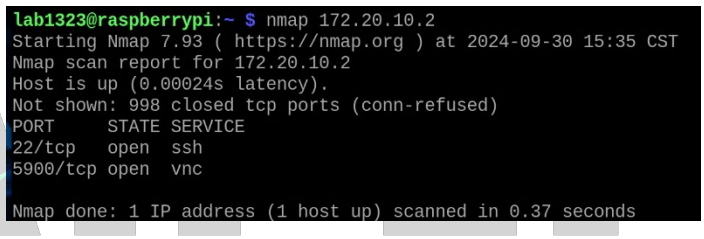
圖一：安裝 Nmap 套件



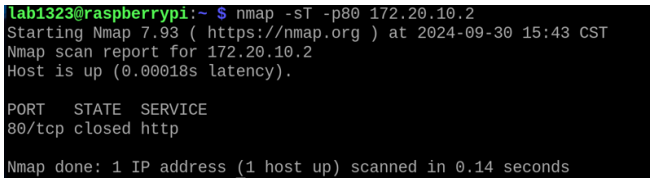
圖二：更新軟體包資訊



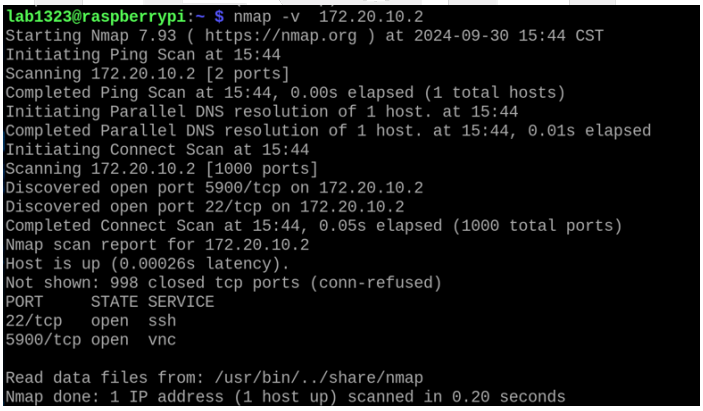
圖三：Nmap 的幫助訊息



圖四：簡易掃描服務服務



圖五：全連接掃描模式



圖六：詳細掃描模式

```
lab1323@raspberrypi:~ $ nmap -sC 172.20.10.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-30 15:44 CST
Nmap scan report for 172.20.10.2
Host is up (0.00028s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   256 e7dde146bfa90059786cfb7beaf0b321 (ECDSA)
|_  256 eed060a07c85a0166de9e556eb6d688d (ED25519)
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VeNCrypt (19)
|     Unknown security type (129)
|     RA2 (5)
|   VeNCrypt auth subtypes:
|_    Plain, Server-authenticated TLS (262)

Nmap done: 1 IP address (1 host up) scanned in 21.60 seconds
```

圖七：腳本掃描模式

```
lab1323@raspberrypi:~ $ nmap -sP 172.20.10.2/31
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-30 15:35 CST
Nmap scan report for 172.20.10.2
Host is up (0.00056s latency).
Nmap done: 2 IP addresses (1 host up) scanned in 1.21 seconds
lab1323@raspberrypi:~ $ nmap -sP 172.20.10.2-254
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-30 15:35 CST
Nmap scan report for 172.20.10.2
Host is up (0.00014s latency).
Nmap done: 253 IP addresses (1 host up) scanned in 3.33 seconds
lab1323@raspberrypi:~ $ nmap -sP 172.20.10.*
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-30 15:40 CST
Nmap scan report for 172.20.10.1
Host is up (0.026s latency).
Nmap scan report for 172.20.10.2
Host is up (0.00098s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 15.82 seconds
```

圖八：檢查在線主機

```
lab1323@raspberrypi:~ $ nmap -T5  172.20.10.2/31
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-30 15:42 CST
Nmap scan report for 172.20.10.2
Host is up (0.00025s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
5900/tcp open  vnc

Nmap done: 2 IP addresses (1 host up) scanned in 1.30 seconds
```

圖九：時間選擇器掃描模式

```
lab1323@raspberrypi:~ $ nmap -top-ports 20 172.20.10.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-30 15:42 CST
Nmap scan report for 172.20.10.2
Host is up (0.00019s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
53/tcp   closed domain
80/tcp   closed http
110/tcp  closed pop3
111/tcp  closed rpcbind
135/tcp  closed msrpc
139/tcp  closed netbios-ssn
143/tcp  closed imap
443/tcp  closed https
445/tcp  closed microsoft-ds
993/tcp  closed imaps
995/tcp  closed pop3s
1723/tcp closed pptp
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
5900/tcp open   vnc
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

圖十：常見 20 埠號掃描模式