**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)

|  |  |
| --- | --- |
| 一張含有 文字, 螢幕擷取畫面, 軟體, 多媒體軟體 的圖片  自動產生的描述 | 一張含有 文字, 螢幕擷取畫面, 軟體, 多媒體軟體 的圖片  自動產生的描述 |
| 圖一：安裝Nmap套件 | 圖二：更新軟體包資訊 |

|  |  |
| --- | --- |
| 一張含有 水, 螢幕擷取畫面, 文字, 數位合成 的圖片  自動產生的描述 |  |
| 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 |
|  |  |
| 圖七：腳本掃描模式 | 圖八：檢查在線主機 |
|  |  |
| 圖九：時間選擇器掃描模式 | 圖十：常見20埠號掃描模式 |