Intro. to Computer Security Homework 2

Port scanning

1. Nmap 介紹

Nmap 全名為 Network Mapper，他是一個網路掃描工具，他可以用來找到網域中有哪些 hosts，也可以針對 hosts 進行 ports 掃描，找出機器上運行的服務。他是透過傳送特殊封包，並觀察回應來達到此目的。透過觀察目標機器的行為，Nmap 甚至可以分析出對方機器的作業系統、版本、甚至開機時間等等資訊。

管理者可以用來針對旗下網域電腦進行掃描，找出可能存在的弱點進行調整。由於 Nmap 可以用來分析機器的弱點，所以也常被駭客所使用。Nmap 的作者為 Gordon Lyon，在 1997 年代有了第一個公開發行版。Nmap 採 GPL 授權，為開放原始碼軟體，在各大平台上皆可運行。

2. IP 掃描報告

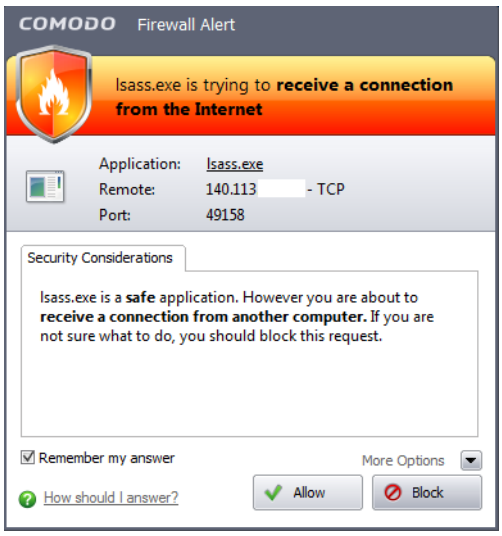
這次掃描主要電腦作業系統為 Windows 7 Enterprise 64-bit SP1，在該電腦上同時有安裝 Comodo Firewall 5。此外，由於平常我使用的作業系統其實為 Ubuntu Linux 64-bit 11.10，配合 Uncomplicated Firewall (ufw)，故我也針對此作業系統做了掃描分析報告。

(以下 IP、MAC 及 ssh key 皆經過隱蔽處理)

A. Windows 7 – Regular scan

```
Starting Nmap 5.61TEST5 ( http://nmap.org ) at 2012-04-14 10:50 Taipei Standard Time
Nmap scan report for 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)
Host is up (0.00074s latency).
Not shown: 993 filtered ports
PORT          STATE SERVICE
135/tcp      open    msrpc
139/tcp      open    netbios-ssn
445/tcp      open    microsoft-ds
49152/tcp open    unknown
49153/tcp open    unknown
49154/tcp open    unknown
49158/tcp open    unknown
MAC Address: xx:xx:xx:xx:xx:xx (Asustek Computer)

Nmap done: 1 IP address (1 host up) scanned in 6.87 seconds
```



從這次掃描中可以發現，有數個 Windows 系統上知名的 ports 被開啟：

135: Microsoft DCE Locator service (aka. end-point mapper)

139: NETBIOS Session Service

445: Microsoft-DS Service (used for resource sharing)

除此之外，也有一些 port 無法辨識出為何項服務，但仍能得知其為開啟狀態。事實上，在進行 port scan 的時候，Comodo 針對每一個建立連線的要求發出了請求授權的提示。由此可見這些 port 其實平常並沒有人會進行連結，而在這次作業中第一次收到連結要求。

令人訝異的是它竟能正確探測出主機板的品牌為 Asustek Computer，推測應該是從 MAC 卡號來判定的。

B. Windows 7 – Intense scan

Starting Nmap 5.61TEST5 (http://nmap.org) at 2012-04-14 11:00 Taipei Standard Time
NSE: Loaded 92 scripts for scanning.
NSE: Script Pre-scanning.

Initiating ARP Ping Scan at 11:01
Scanning 140.113.xxx.xxx [1 port]
Completed ARP Ping Scan at 11:01, 1.40s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 11:01
Completed Parallel DNS resolution of 1 host. at 11:01, 0.00s elapsed

Initiating SYN Stealth Scan at 11:01
Scanning 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx) [1000 ports]
Discovered open port 445/tcp on 140.113.xxx.xxx
Discovered open port 135/tcp on 140.113.xxx.xxx
Discovered open port 139/tcp on 140.113.xxx.xxx
Discovered open port 49153/tcp on 140.113.xxx.xxx
Discovered open port 49154/tcp on 140.113.xxx.xxx
Discovered open port 49158/tcp on 140.113.xxx.xxx
Discovered open port 49152/tcp on 140.113.xxx.xxx
Completed SYN Stealth Scan at 11:01, 4.18s elapsed (1000 total ports)

Initiating Service scan at 11:01
Scanning 7 services on 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)
Service scan Timing: About 57.14% done; ETC: 11:02 (0:00:37 remaining)
Completed Service scan at 11:02, 53.69s elapsed (7 services on 1 host)
Initiating OS detection (try #1) against 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)

NSE: Script scanning 140.113.xxx.xxx.
Initiating NSE at 11:02
Completed NSE at 11:02, 40.06s elapsed

Nmap scan report for 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)
Host is up (0.00048s latency).

Not shown: 992 filtered ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	
445/tcp	open	netbios-ssn	
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49156/tcp	closed	unknown	

```
49158/tcp open      msrpc           Microsoft Windows RPC
MAC Address: xx:xx:xx:xx:xx:xx (Asustek Computer)
Device type: general purpose

Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows
Vista SP2 or Windows Server 2008
Uptime guess: 0.010 days (since Sat Apr 14 10:48:14 2012)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| nbstat:
|     NetBIOS name: PC, NetBIOS user: <unknown>, NetBIOS MAC: xx:xx:xx:xx:xx:xx (Asustek Computer)
|     Names
|         PC<00>                  Flags: <unique><active>
|         WORKGROUP<00>           Flags: <group><active>
|         PC<20>                  Flags: <unique><active>
|_        WORKGROUP<1e>           Flags: <group><active>
| smb-security-mode:
|     Account that was used for smb scripts: guest
|     User-level authentication
|     SMB Security: Challenge/response passwords supported
|_    Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
| smb-os-discovery:
|     OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|     NetBIOS computer name: PC
|     Workgroup: WORKGROUP
|_    System time: 2012-04-14 11:02:08 UTC+8

TRACEROUTE
HOP RTT         ADDRESS
1     0.48 ms 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)

NSE: Script Post-scanning.
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 107.37 seconds
                   Raw packets sent: 2034 (92.000KB) | Rcvd: 18 (864B)
```

Intense scan 所增加的參數為 -T4 -A –v，分別設定時間區間，aggressive scan 及列出詳細報告。根據 man page 的說明-A 目前的功能為：Enables OS detection and Version detection, Script scanning and Traceroute，但未來可能改變。

在 Intense scan 的報告中我們可以發現，除了一般的 port scan 外，他確實還會針對 services 進行深度掃描。而之前被列為 Unknown services 的 ports 也因此被測出皆為 msrpc 服務。

透過這樣的掃描，他得以更正確的猜測目標作業系統以及開機時間。此外，他還針對網路芳鄰進行了資訊的截取，而在 smb-os-discovery 的訊息裡也確定了實際的作業系統。

ARP Ping Scan (在 regular scan 即有)

在掃描區網時，Nmap 可能需要掃描大量 IP。由於這些 IP 尚未對應到硬體位置，所以 OS 必須透過 ARP 來找到對應，但由於 OS 沒有預料到需要做如此大的查詢，故他的實作常常比較慢也比較有問題。因此 Nmap 會自己做 ARP scanning。

Parallel DNS resolution (在 regular scan 即有)

針對指定 IP 進行 domain name 反查，為了增加效率所以同步送出多個要求等待結果。

SYN Stealth Scan (在 regular scan 即有)

SYN Steath Scan 是以類似 3-way handshaking 但較不易被發現的掃描方式對 ports 進行掃描。他會先對目標傳送一個 TCP-SYN 訊息，如果對方機器有傾聽該 port 的話就會回應 TCP SYN-ACK 封包；而如果該 port 並未被傾聽的話，對方機器就會回傳一個 TCP RST-ACK 封包。當收到回應後，由於已達成目的，nmap 會立即回應一個 RST 封包，切斷尚未完成 TCP handshaking 的連線。如此對方機器可能較不易發現。

Service scan

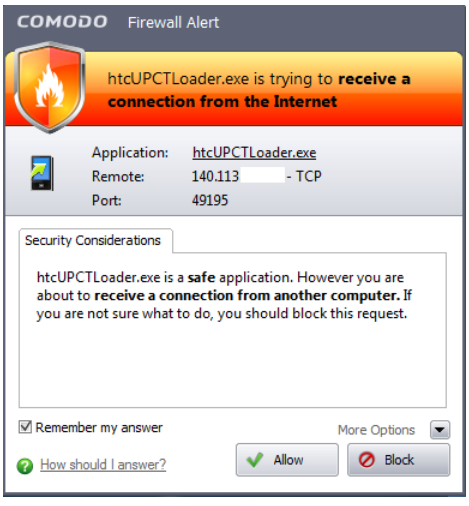
針對有打開的 ports 進行觀察，以找出究竟是何種服務。

NSE Script scanning

進行更複雜的掃描，具有條件判斷的能力。

Traceroute

測試從本端傳封包到目標機器需經過什麼路徑 (因為在同一個區網所以只需一個 hop)。



C. Windows 7 – Intense scan, all TCP ports

基本上和 intense scan 大同小異，只是掃瞄了所有可能的 ports 共 65535 個 (在 intense scan 中只掃瞄了 1000 個 ports)。結果又多掃描出幾個 ports。

49164/tcp open msrpc Microsoft Windows RPC
49166/tcp open msrpc Microsoft Windows RPC
49195/tcp closed unknown

D. Ubuntu 11.10 – Regular scan

Starting Nmap 5.61TEST5 (http://nmap.org) at 2012-04-14 10:46 Taipei Standard Time
Nmap scan report for 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)
Host is up (0.00032s latency).

Not shown: 998 filtered ports
PORT STATE SERVICE
22/tcp open ssh
2121/tcp closed ccproxy-ftp
MAC Address: xx:xx:xx:xx:xx:xx (Asustek Computer)

Nmap done: 1 IP address (1 host up) scanned in 6.70 seconds

我們看到，跟掃描 Windows 的結果大同小異，只是打開的 open 只有一個：22，是用來做 ssh 遠端登入的，而 2121 是我用來 port forward 到虛擬機器客戶端電腦的 ssh 用，因為沒開虛擬機器，故 port 成關閉狀態。

E. Ubuntu 11.10 – Intense scan

Starting Nmap 5.61TEST5 (http://nmap.org) at 2012-04-14 10:38 Taipei Standard Time
NSE: Loaded 92 scripts for scanning.
NSE: Script Pre-scanning.

Initiating ARP Ping Scan at 10:38
Scanning 140.113.xxx.xxx [1 port]
Completed ARP Ping Scan at 10:38, 1.45s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 10:38
Completed Parallel DNS resolution of 1 host. at 10:38, 5.33s elapsed

Initiating SYN Stealth Scan at 10:38
Scanning 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx) [1000 ports]
Discovered open port 22/tcp on 140.113.xxx.xxx
Completed SYN Stealth Scan at 10:39, 4.86s elapsed (1000 total ports)

Initiating Service scan at 10:39
Scanning 1 service on 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)
Completed Service scan at 10:39, 0.19s elapsed (1 service on 1 host)

Initiating OS detection (try #1) against 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)
Retrying OS detection (try #2) against 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)

NSE: Script scanning 140.113.xxx.xxx.
Initiating NSE at 10:39
Completed NSE at 10:39, 0.23s elapsed

Nmap scan report for 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)
Host is up (0.00011s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.8p1 Debian 7ubuntu1 (protocol 2.0)

| ssh-hostkey: 1024 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx (DSA)
|_2048 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx (RSA)
2121/tcp closed ccproxy-ftp
MAC Address: xx:xx:xx:xx:xx:xx (Asustek Computer)
Device type: general purpose|**firewall**

Running (JUST GUESSING): Linux 2.6.X|3.X (97%), IPFire Linux 2.6.X (88%)

OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3 cpe:/o:ipfire:linux:2.6
Aggressive OS guesses: Linux 2.6.32 - 2.6.38 (97%), Linux 3.0 (94%), Linux 2.6.38 (93%), Linux 2.6.32 (92%), IPFire firewall 2.11 (Linux 2.6) (88%), Linux 2.6.31 - 2.6.32 (88%), Linux 2.6.32 - 2.6.39 (87%), Linux 2.6.15 - 2.6.26 (87%), Linux 2.6.32 - 2.6.33 (87%), Linux 2.6.32 - 2.6.35 (87%)
No exact OS matches for host (test conditions non-ideal).

Uptime guess: 0.174 days (since Sat Apr 14 06:28:53 2012)
Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=265 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.11 ms 140-113-xxx-xxx.Dorm8.NCTU.edu.tw (140.113.xxx.xxx)

NSE: Script Post-scanning.

Initiating NSE at 10:39
Completed NSE at 10:39, 0.00s elapsed

Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 29.14 seconds
Raw packets sent: 2069 (94.632KB) | Rcvd: 25 (1.744KB)

在 Intense scan 中，我們發現他對 Linux 核心的猜測雖然頗為相近，然而也無法像 smb-os-discovery 一樣完全準確(系統上實際跑的核心為 3.X)。

Running (JUST GUESSING): Linux 2.6.X|3.X (97%), IPFire Linux 2.6.X (88%)

有趣的地方在於它發現了系統上有防火牆的存在，可是對 Windows 的掃描卻無法測出(也或許是因為我都選擇放行的緣故)。此外，Linux 和 Windows 在 IP ID Sequence Generation 的處理方式是不同的，Windows 為 Incremental，Linux 則為 All zeros。

另外一個值得注意的現象是掃描 Ubuntu 只花了 29.14 秒，可是對 Windows 7 進行 Intense scan 卻需要 107.37 秒。

F. Ubuntu 11.10 – Intense scan, all TCP ports

和 Intense scan 得到一樣的結果，確實，ufw 放行的 port 其實就只有那兩個。