網路安全的理論與實務

楊中皇 著

第十一章 Nmap

http://crypto.nknu.edu.tw/textbook/

第十一章 Nmap

- Nmap簡介
- Nmap的安裝方法
- Nmap的使用

Nmap發展歷史

- Nmap 全 名 是 Network Mapper ， 是 由 Fyodor Vaskovich所開發的一套開放原始碼軟體
- 可用於檢測本機或網路遠端主機的安全性弱點
- 可藉由此軟體對本身管理的伺服器主機進行安全性稽核與弱點分析，進而有助於增強系統及網路安全
- 主要功能是針對TCP/IP的TCP埠作掃瞄，不僅可以查出目標主機所開放的TCP埠，還能取得對應的網路服務類型，以及應用軟體名稱與版本
- 此外，還可以偵測出目標主機所使用的作業系統、封包過濾器及防火牆種類等資訊

Nmap操作平台

- 目前已有許多作業系統都提供支援如：
  - Linux
  - Microsoft Windows
  - FreeBSD、OpenBSD、Solaris、IRIX、HP-UX、Mac OS X、NetBSD、Sun OS及Amiga…等
- 有些Unix-like的作業系統會預設安裝Nmap，如：
  - Red Hat Linux、Fedora Core Linux
  - Debian Linux
  - Gentoo、 FreeBSD、OpenBSD

Nmap操作方式

- Nmap操作方式有兩種
  - 命令列模式操作指令
  - 如果在Unix-like系統中有安裝X Window環境，還可使用圖形介面的軟體NmapFE (Nmap Front End)以視窗模式操作

Nmap的安裝方法-Linux

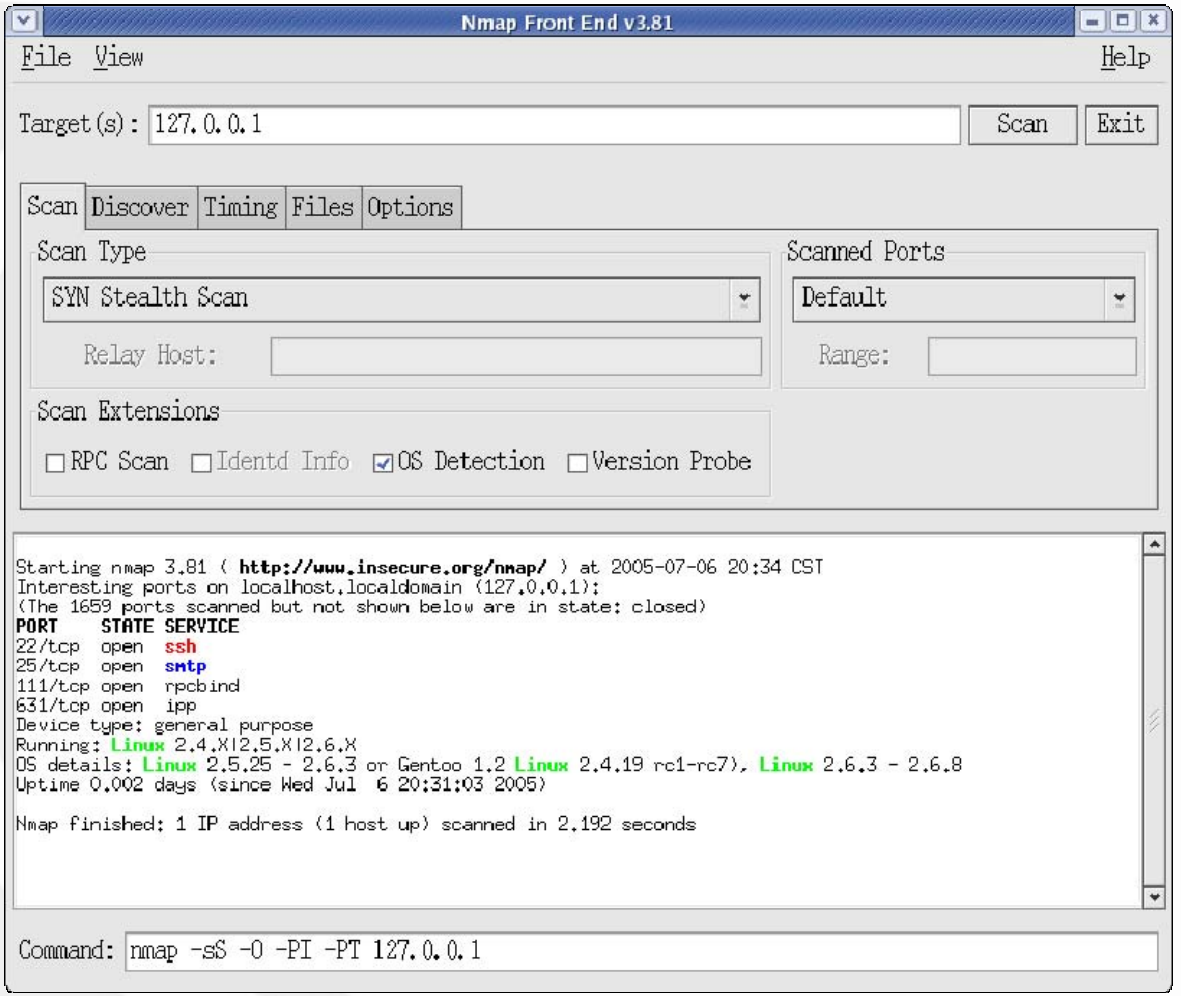
- 在Linux系統下的安裝方式可以採用Tarball原始碼套件安裝，或是以RPM套件安裝，而Tarball套件可安裝在任何的Unix-like系統
- 若以最新穩定版本Nmap 3.81版安裝在Fedora Core 4（FC4）爲例，使用Tarball套件壓縮檔爲nmap-3.81.tar.bz2，安裝指令的操作步驟如下：
  - bzip2 -cd nmap-3.81.tar.bz2 | tar xvf -
  - cd nmap-3.81
  - ./configure
  - make
  - su root （若登入的使用者不具root權限，在make install之前必須切換至root）
  - make install

Nmap的安裝方法-Linux(續)

- Tarball套件已同時包含命令列模式的nmap及視窗模式的nmapfe等兩種不同類型的執行程式。安裝完畢後，nmap及nmapfe都應位於/usr/local/bin/底下
- FC4預設安裝的RPM套件版本已經是目前最新3.81版（未安裝NmapFE）
- 如果要自行安裝在RPM-based的Linux系統下使用，需要安裝nmap-3.81-1.i386.rpm及nmap-frontend-3.81-1.i386.rpm兩個套件檔，才能選擇使用命令列模式或視窗模式，安裝指令的操作步驟如下：
  - rpm -ivh nmap-3.81-1.i386.rpm
  - rpm -ivh nmap-frontend-3.81-1.i386.rpm

X Window啓動NmapFE，以預設選項掃瞄本機

- 安裝正確無誤後，可以登入Linux的X Window環境，並開啓終端機模式命令視窗，輸入nmapfe即可執行視窗模式
- 以預設值測試掃瞄本機，如右圖

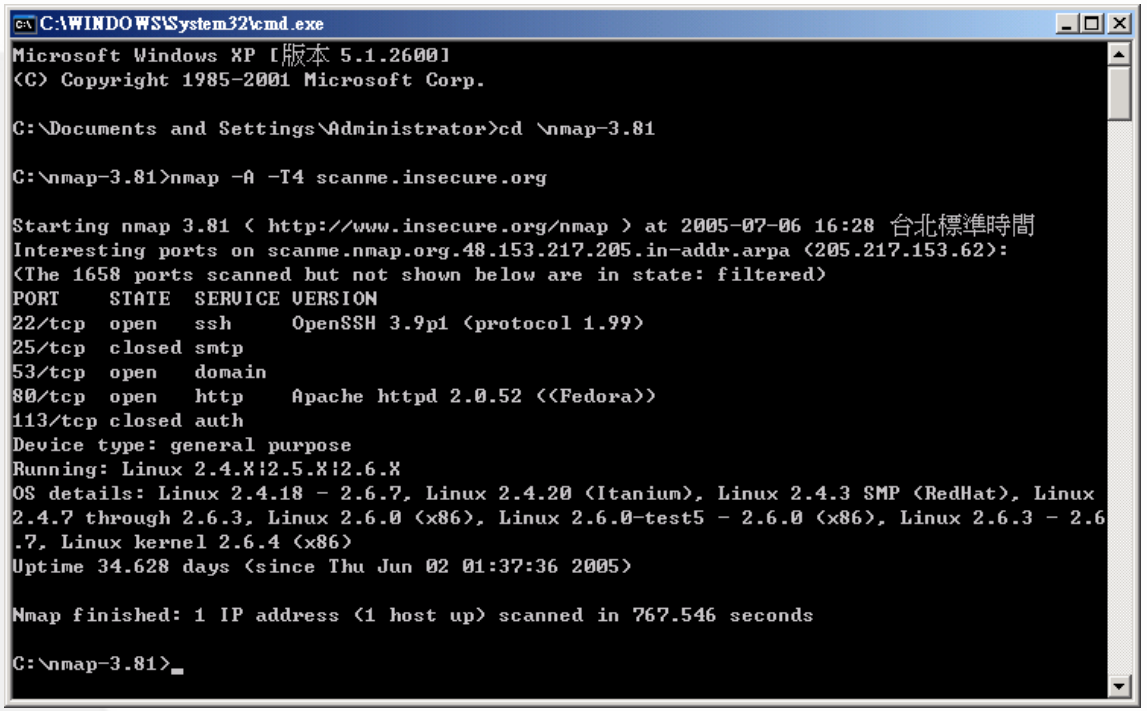


Nmap的安裝方法-Windows

- 目前Nmap對於Microsoft Windows系統所提供之版本，只有命令列的操作模式
- 在安裝Nmap程式之前，必須先行安裝WinPcap 3.1 beta 4或更新的版本
- Nmap的Windows版本在執行掃瞄時，所呈現的效率卻遠不如Unix-like版本。爲了加強Windows版本的掃瞄效率，請檢視解開之後的Nmap資料夾，其中有個登錄檔nmap_performance.reg，直接點選執行將其內容新增到系統登錄檔中

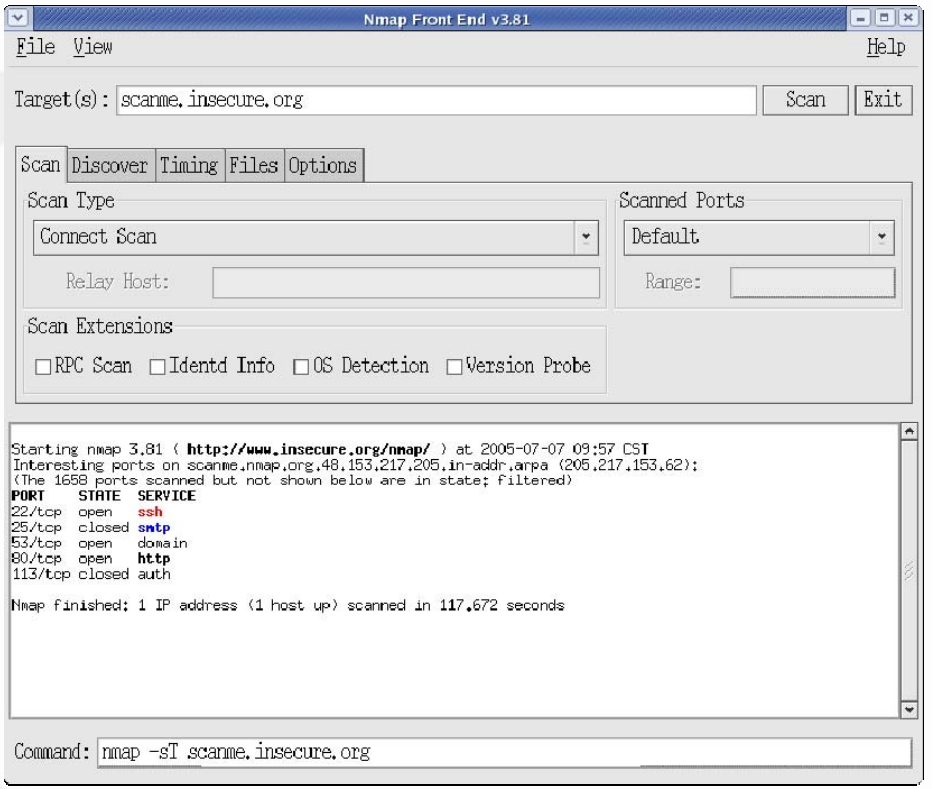
在Windows的MS-DOS環境下測試nmap掃瞄

- Windows系統上只能以命令列操作
- Windows版本尚不能對本機掃瞄，因此安裝完畢後的測試，可針對Nmap官方網站所提供的測試主機（scanme.insecure.org）進行掃瞄測試
- 測試成功的畫面如右圖。要注意的是，Windows系統登入之使用者，必須擁有Administrator權限，才可以使用Nmap



Nmap的使用(NmapFE)

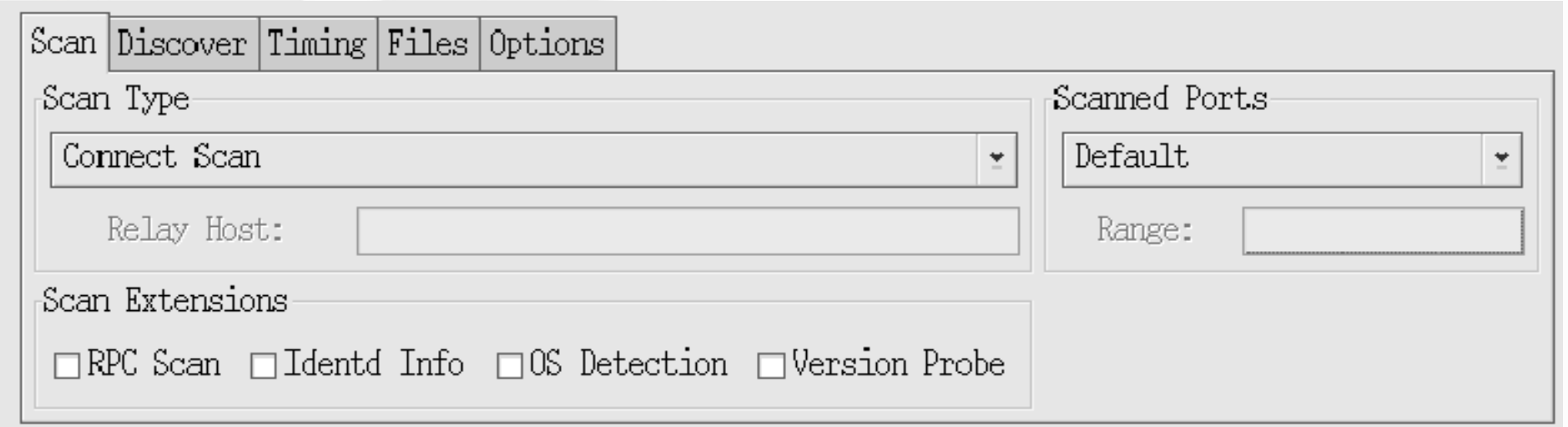
- NmapFE有著與一般視窗軟體的操作特性，只要點選一些簡單選項設定或是輸入所需參數，不需輸入完整指令
- NmapFE執行掃瞄功能時，完整的指令包括設定選項及欲掃瞄主機位址或埠號範圍等，同時也會呈現在最下方的「Command:」欄位，對於指令的學習也很有幫助。
- 右圖是NmapFE的主畫面



NmapFE主畫面說明

- 「View」三項功能：「Black&White」、「Coloured」及「Append log」，前兩項是設定掃瞄結果欄顯示文字的顏色，而「Append log」則是以附加方式將每次設定掃瞄的結果顯示出來，如果不勾選此項設定，則每次執行掃瞄時就會清除前次的掃瞄結果，亦即每次只有顯示當次掃瞄完後的資訊
- 在NmapFE的主畫面中，「Target(s):」欄位是輸入欲掃瞄的主機位址，由於Nmap可以同時掃瞄多部主機，故可設定兩個以上的主機位址，也可以設定一段特定範圍的IP位址，如：192.168.1.10-20
- 選項設定頁是最主要的部分，用來設定掃瞄的特定選項，總共有五個分頁，分別是「Scan」、「Discover」、「Timing」、「Files」及「Options」，會在後續逐一介紹各個分頁的功能。

NmapFE選項設定「Scan」分頁



- NmapFE提供14種掃瞄類型，其中有6種是屬於隱蔽掃瞄（Stealth Scan）
- 使用隱蔽掃瞄的目的，是爲了在掃瞄目標主機時，不在對方的系統上留下日誌記錄

掃瞄類型

- **Connect Scan**：最基本的TCP掃瞄方式，掃瞄時會利用作業系統核心的connect系統呼叫，並嘗試在目標主機探測到每個TCP埠，建立完整的三段式交握連線。如果被探測到的埠正在傾聽連線，connect()系統呼叫就會連線成功；反之，連線則會失敗，這意味著該埠是關閉的。優點是任何使用者都可以使用，並不需要root權限

- **SYN Stealth Scan**：通常稱爲半開式（half-open）掃瞄，因爲在掃瞄目標主機時，若對方開啓TCP埠回應SYN|ACK封包，則Nmap會立即發出RST封包中止連線，而不會建立完整連線，所以會使得目標主機難以偵測，雖然比較不會在對方系統上留下記錄，但還是有可能被某些入侵偵測系統查獲，這種掃瞄必須擁有root權限才能使用

掃瞄類型(續)

- **ACK Stealth Scan**：主要是用來列出目標主機的防火牆配置情況，甚至可觀察出對方防火牆是否Stateful Inspection技術，或只是單純的封包過濾器而已。

- **FIN|ACK Stealth Scan**：類似ACK Stealth Scan，但它多送出FIN封包，掃瞄時對方的TCP埠是開啓著，則會丟棄該封包，若關閉的話，則回應RST封包，因此可判斷並標示出哪些埠是開啓狀態

- **FIN Stealth Scan**：由於SYN Stealth Scan不夠隱蔽，因此Nmap設計出FIN Stealth Scan非起始TCP標準連線模式的掃瞄方式，它是直接送出FIN封包，若目標主機的TCP/IP堆疊符合RFC-793的標準規範，則開啓的TCP埠就會將該FIN封包視爲錯誤封包而丟棄，否則回應RST封包表示關閉。這項掃瞄功能對於Windows作業系統並無作用

掃瞄類型(續)

- **NULL Stealth Scan**：以NULL封包傳送，也就是沒有設定任何控制旗標的封包

- **XMas Tree Stealth Scan**：與FIN Stealth Scan掃瞄方式類似，但傳送的是已經設定FIN、PSH及URG等三個控制旗標的封包

- **TCP Window Scan**：類似ACK Stealth Scan，它有時可偵測出已開啓TCP埠

掃瞄類型(續)

- **UDP Port Scan**：Nmap除了可掃瞄TCP埠，透過此方式還可以掃瞄UDP埠，若想知道目標主機開啓哪些UDP埠服務，便可以使用這種掃瞄方式

- **IP Protocol Scan**：可偵測出目標主機的系統支援哪些IP協定。掃瞄是針對所有協定，逐一發送出沒有指定協定的RAWIP封包，如果對方回應ICMP無法送達的封包，則表示目標主機的系統不支援該項IP協定，否則假設有支援

- **Ping Sweep**：這是單純的Ping掃瞄，可偵測出目標主機是否正處於運行狀態，其實即使不設定這項功能，Nmap也會執行Ping掃瞄

掃瞄類型(續)

- **Host List**：列出欲掃瞄的目標主機IP位址，而不會進行Ping掃瞄或埠掃瞄；如果於「Target(s):」輸入目標主機的DNS名稱，也能轉成IP位址

- **FTP Bounce Attack**：FTP協定有個特性叫做代理FTP連線，或稱爲FTP代理（FTP Proxy），此功能能讓使用者電腦連接到有FTP伺服器的主機，並要該FTP伺服器對網路上其他任何主機發送檔案

- **Idle Scan**：主要是針對僵屍主機；所謂僵屍主機是曾經遭受過入侵攻擊或者是可供間接利用的主機

Scanned Ports（指定掃瞄的埠）

- **Default**：使用預設值進行掃瞄
- **ALL**：掃瞄目標主機所有的埠
- **Most Important[fast]**：只掃瞄最重要的、眾所周知的埠，速度較快
- **Range Given Below**：在下方的空白欄位設定特定的埠範圍值來掃瞄，如1-100

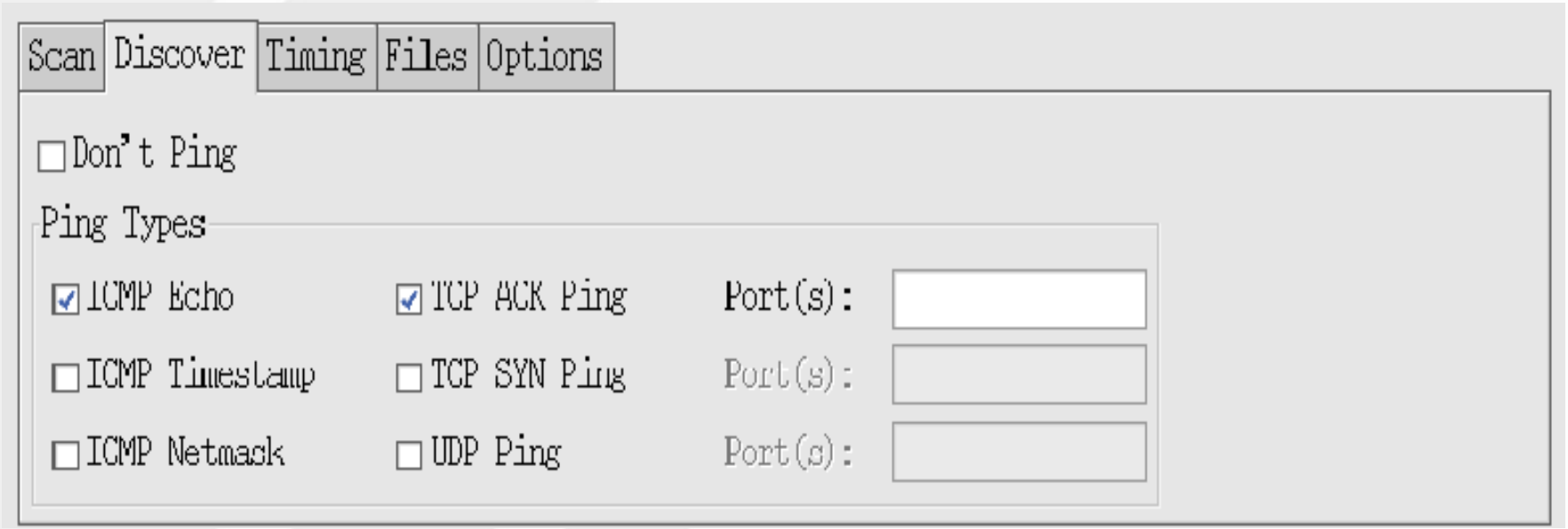
Scan Extensions（掃瞄附加設定）

掃瞄類型\支援附加設定	RPC Scan	Identd Info	OS Detection	Version Probe
Connect Scan	V	V	V	V
SYN Stealth Scan	V		V	V
ACK Stealth Scan	V		V	V
FIN|ACK Stealth Scan	V		V	V
FIN Stealth Scan	V		V	V
NULL Stealth Scan	V		V	V
XMas Tree Stealth Scan	V		V	V
TCP Window Scan	V		V	V
UDP Port Scan	V		V	V
IP Protocol Scan			V	
FTP Bounce Attack	V		V	V
Idle Scan	V		V	V

Scan Extensions說明

- **RPC Scan**：可以辨別哪一個埠有開啓執行RPC的服務，以及服務類型及版本編號
- **Identd Info**：用來開啓Nmap的反向旗標掃瞄功能，主要是有關RFC-1413標準所制定的Identification協定，該協定允許透過TCP連線提供系統中任何行程的擁有者資訊，然後使用identd確認HTTP伺服器行程是否由root執行，這種掃瞄方式必須是經由完整TCP連線，亦即掃瞄類型只能設定爲Connect Scan。此外，如果目標主機並沒有執行identd程式，這種掃瞄就會無效
- **OS Detection**：用以偵測目標主機的作業系統
- **Version Probe**：能辨別出開啓的埠所提供的網路服務類型及其軟體版本編號

NmapFE選項設定「Discover」分頁



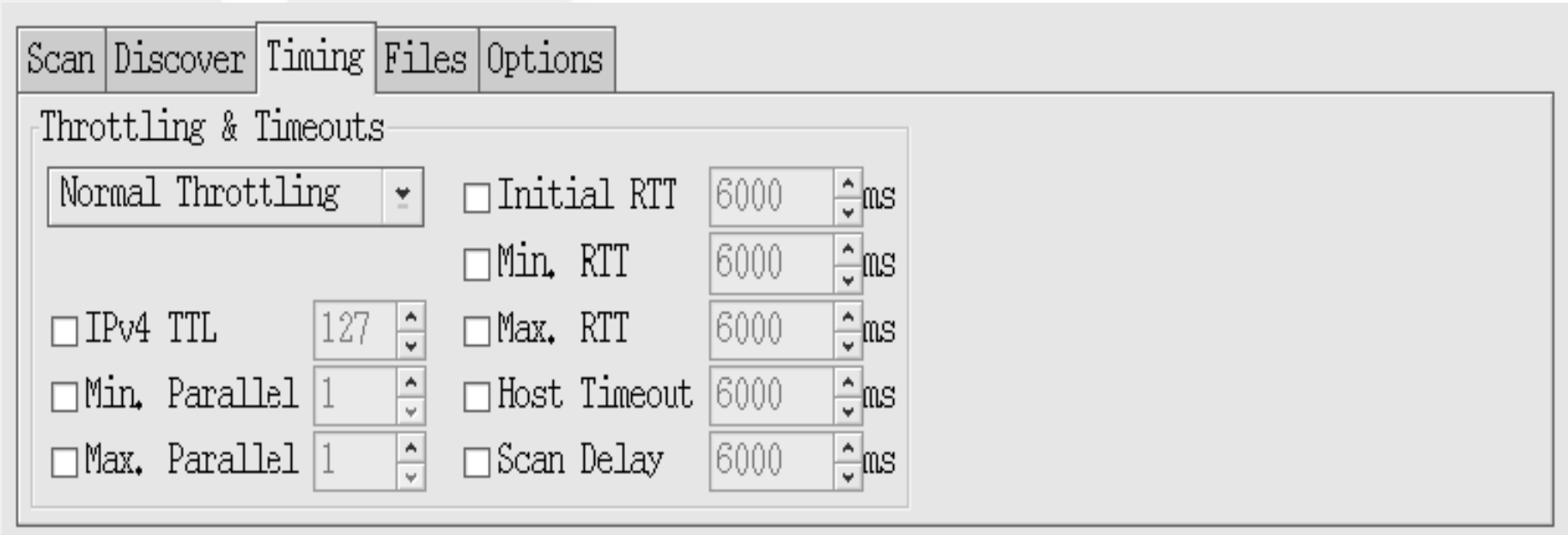
NmapFE選項設定「Discover」說明

- **Don‘t Ping**：在執行埠掃瞄之前，不需要先Ping目標主機
- **Ping Types（Ping類型）**：可提供6種方式用來Ping目標主機，且使用的封包種類涵蓋ICMP封包、TCP封包及UDP封包
- **ICMP Echo**：可發出ICMP Echo請求封包，查詢目標主機是否正在運行
- **ICMP Timestamp**：發出ICMP時，則請求封包探查正在傾聽的主機
- **ICMP Netmask**：發出ICMP網路遮罩請求封包探查正在傾聽的主機

NmapFE選項設定「Discover」說明(續)

- **TCP ACK Ping**：發出TCP ACK封包而非ICMP Echo請求封包，如果目標主機正在運行則會回應RST封包，但只有在目標主機阻絕ICMP Echo請求封包，且允許Nmap對其掃瞄的情況下，這個選項才有效。如果使用時不是以root權限，則必須搭配Connect Scan才能夠使用；另外還需要輸入某個目標埠號，預設是80埠，通常80埠不會被過濾
- **TCP SYN Ping**：發出TCP SYN封包來Ping目標主機，如果對方正在運行則回應RST封包或SYN|ACK封包，但需要指定目標埠號
- **UDP Ping**：發出UDP封包Ping目標主機，需要指定目標埠號

NmapFE選項設定「Timing」分頁



NmapFE選項設定「Timing」說明

- **Paranoid Throttling**：爲了避開入侵偵測系統，Nmap串列所有的掃瞄動作，至少每隔5分鐘才發送一個封包
- **Sneaky Throttling**：與Paranoid Throttling類似，但間隔時間爲15秒。
- **Polite Throttling**：爲了避免掃瞄動作導致目標主機當機，採用的方式是串列每個探測動作，發送間隔時間爲0.4秒，這樣較不會增加太多的網路負擔

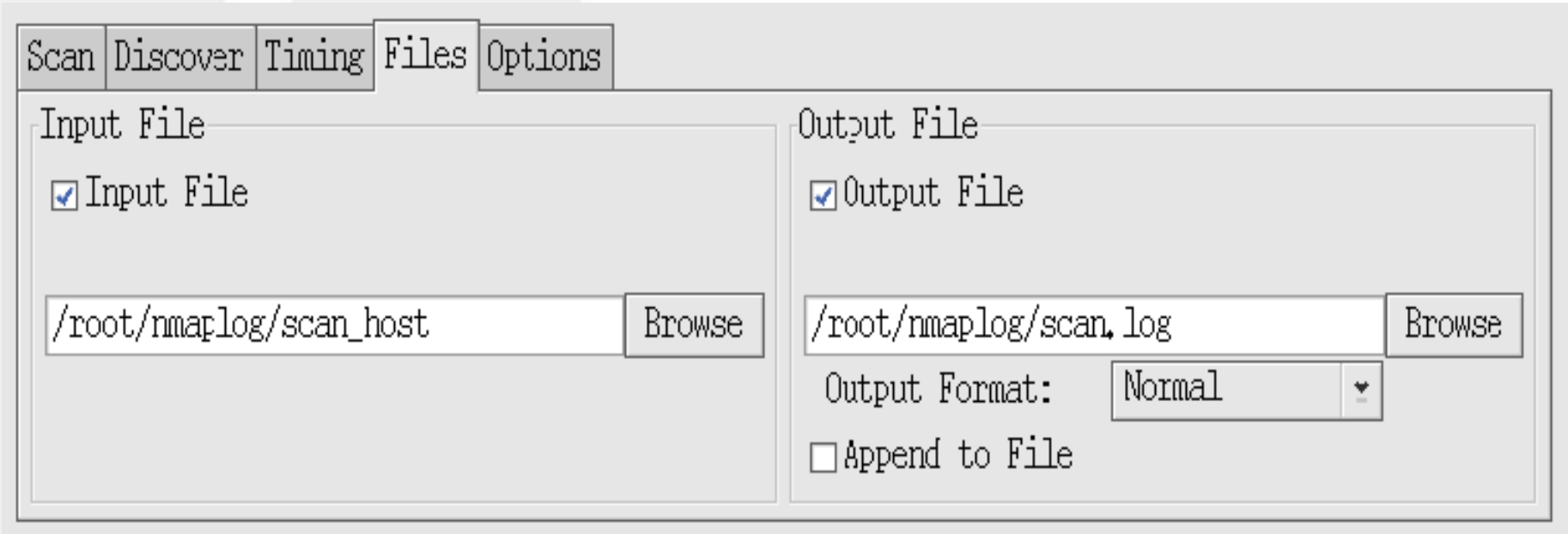
NmapFE選項設定「Timing」說明(續)

- **Normal Throttling**：預設的調時掃瞄方式
- **Aggressive Throttling**：設定5分鐘的超時限制，若同時對多部主機進行掃描，採用這種方式會讓Nmap對每部主機的掃瞄時間最多不超過5分鐘，並使每次探測動作等待回應時間在1.5秒以內
- **Insane Throttling**：與Aggressive Throttling類似，但超時限制僅有75秒，探測等待回應時間只有0.3秒，這較適用在高速網路的環境中，或者使用者本身不在乎會漏失部分掃瞄資訊的情況下

其他逾時控制相關的設定

- **IPv4 TTL**：設定IPv4的封包存活時間（Time To Live）
- **Min. Parallel**：設定最小的平行掃瞄數量，單位是埠
- **Max. Parallel**：設定最大的平行掃瞄數量，單位是埠
- **Initial RTT**：設定初始化探測的逾時值，要搭配勾選「Discover」分頁的「Don‘t Ping」使用
- **Min. RTT**：設定每次探測動作至少等待時間，沒有設定的話，Nmap會自行視目標主機回應的時間縮短每次探測的等待時間，雖然有助於提升掃瞄速度，但可能會漏失掉某些回應時間較長的封包
- **Max. RTT**：每次探測動作的逾時值，如果超過時間就會重新探測
- **Host Timeout**：掃瞄一部目標主機的時間，以毫秒爲單位
- **Scan Delay**：在兩次探測動作之間必須等待的時間，可降低網路負擔

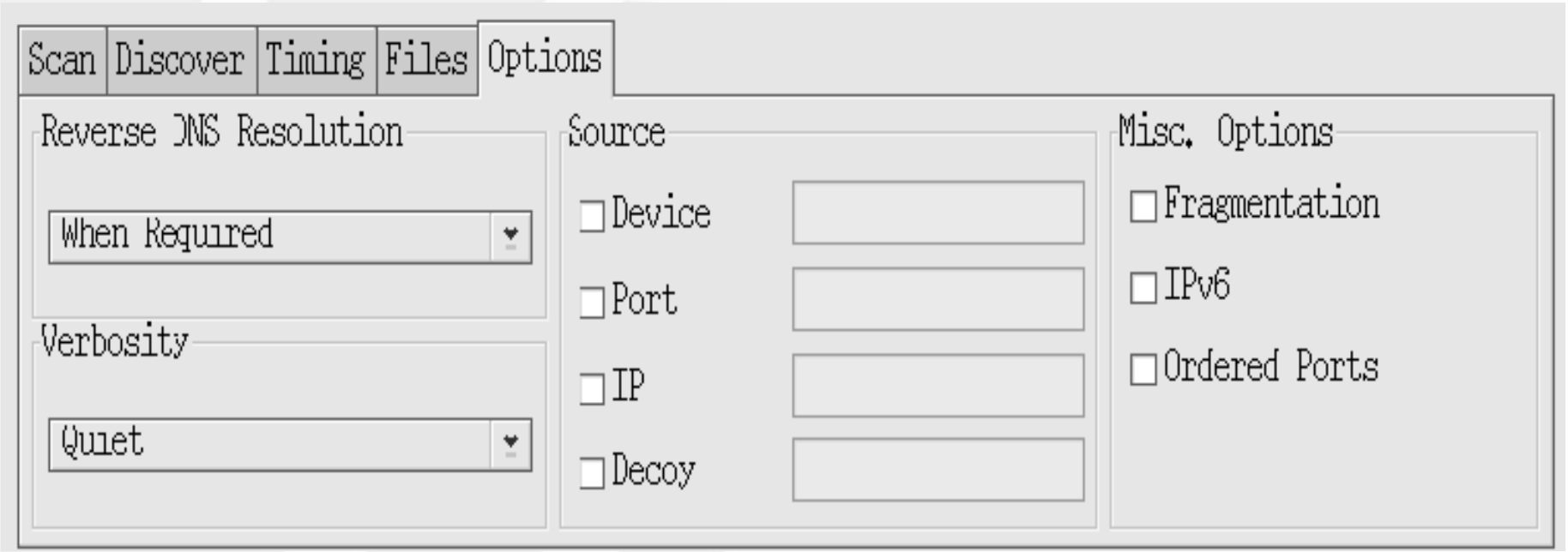
NmapFE選項設定「Files」分頁



NmapFE選項設定「Files」說明

- **Input File**（匯入檔案）：通常這功能可利用來輸入大量目標主機位址，無論是DNS名稱或是IP位址都可以
- **Output File**：此選項是將掃瞄結果儲存到使用者所設定的檔案，其儲存方式有：
  - **Normal**：以使用者設定的檔名存成純文字檔。
  - **grep-able**：存成grep格式檔。
  - **XML**：存成XML檔。
  - **All**：依據設定的檔名，一次存成純文字檔、grep格式檔及XML檔等三種檔案格式，並附加副檔名以資識別
  - **ScriptKiddie**：存成ScriptKiddie檔
- 在「Output File」設定下方還有個「Append to File」選項，如果勾選此選項且設定的檔名已有相同檔案存在，則會將目前的掃瞄結果內容附加儲存檔案原有內容之後

NmapFE選項設定「Options」分頁



NmapFE選項設定「Options」說明

- **Reverse DNS Resolution**：將目標主機的DNS名稱反解析成IP位址，這個選項可以設定爲Always、When Required及Never

- **Verbosity**：設定掃瞄結果列出資訊的詳細程度，Quiet是呈現最普通的資訊，而其他選項會顯示不同程度且更爲詳細的掃瞄資訊

NmapFE選項設定「Options」說明(續)

- **Source**4個子選項：
  - **Device**：告知系統使用何種裝置發送與接收封包，則系統對該裝置進行測試，若該裝置無效就會通知使用者
  - **Port**（設定掃瞄使用的來源埠）：只有在對目標主機也能掃瞄到相對應的埠號時，這個設定才有效；否則Nmap還是會自行更改爲其他的埠號作爲來源埠
  - **IP**：有時會發生Nmap無法確認本機位址的情況，此時使用者可在此設定本機的IP位址且這個選項還有欺騙掃瞄的作用，如果掃瞄時將其內容設定爲其他IP位址，可能會讓目標主機誤認爲是別部主機在對它掃瞄
  - **Decoy**（誘餌掃瞄功能）：使用者可以設定多個IP位址，每個IP位址之間用逗號隔開，當使用者在執行掃瞄動作時，主機位址則會以隨機方式夾雜其中，使用者可以用ME這個代碼將實際IP位址放在特定的位置。假設目標主機有安裝入侵檢測系統，仍無法辨別出哪個是真正發起掃瞄的位址，這種掃瞄方式能夠將本機位址隱藏的很好而不易被目標主機發現

NmapFE選項設定「Options」說明(續)

- **Misc.Option**3個子選項：
  - **Fragmentation**（發送碎片封包）：碎片封包能增加封包過濾器、防火牆或是入侵偵測系統的檢查難度。不過，有些網路基於效能的考量，並不允許發送碎片封包，這個選項不能在所有作業系統上使用，但多數的Unix-like系統是可以使用
  - **IPv6**：支援系統掃瞄IPv6的位址
  - **Ordered Ports**：強制讓系統依照被掃瞄埠之順序進行掃瞄。

使用指令

- 了解使用指令才是最根本且正確的學習方式，尤其是在Unix-like系統
- 一個優良的系統管理員，應熟悉如何使用指令
- 初學者如果先學會如何使用NmapFE，應該能很快體會到Nmap的強大功能
- Nmap「掃瞄類型」、「選項及參數」、「目標主機的位址或範圍」，其中掃瞄類型及選項的設定請參考後續各表所列說明

Scan Type（掃瞄類型）選項

功能名稱	對應選項	備註
Connect Scan	-sT	利用作業系統核心的connect()系統呼叫，建立完整的三段式交握連線之後再進行掃瞄，但容易遭目標主機截獲並記錄。
SYN Stealth Scan	-sS	又稱為半開式掃瞄，掃瞄目標主機時，若對方開啟的TCP埠回應SYN|ACK封包，則立即發出RST封包中止連線。
ACK Stealth Scan	-sA	可用來列出目標主機的防火牆配置情況，但掃瞄結果並不會標示出哪些TCP埠是開啟的。
FIN|ACK Stealth Scan	-sM	類似-sA，但多送出一個FIN封包，可以判別哪些埠是開啟狀態。
FIN Stealth Scan	-sF	較隱蔽的掃瞄方式，送出FIN封包探測，目標主機的系統需支援RFC-793標準才能使用。
NULL Stealth Scan	-sN	較隱蔽的掃瞄方式，送出NULL封包探測，但目標主機的系統需支援RFC-793標準。
XMas Tree Stealth Scan	-sX	較隱蔽的掃瞄方式，送出已經設定FIN、PSH及URG等三個控制旗標的封包，但目標主機的系統需支援RFC-793標準。
TCP Window Scan	-sW	類似-sA，然而有時可以偵測出開啟的TCP埠。
UDP Port Scan	-sU	掃瞄UDP埠。
IP Protocol Scan	-sO	偵測目標主機的系統支援哪些IP協定，最多只能掃瞄256種協定。
Ping Sweep	-sP	單純的Ping掃瞄。
Host List	-sL	只列出欲掃瞄的目標主機IP位址，不會進行真正的Ping掃瞄或埠掃瞄。
FTP Bounce Attack	-b	利用FTP代理伺服器掃瞄TCP埠。選項設定參數如下： -b username:password@server:port
Idle Scan	-sI	掃瞄曾經遭受過入侵攻擊或者是可供間接利用的僵屍主機

Scan Extensions（掃瞄附加設定）選項

功能名稱	對應選項	備註
RPC Scan	-sR	辨別哪一個埠有開啟執行RPC的服務，以及其服務的類型及版本編號。
Identd Info	-I	使目標主機經由完整的TCP連線，提供系統中任何行程的擁有者資訊，須搭配-sT使用。
OS Detection	-O	用以偵測目標主機的作業系統。
Version Probe	-sV	辨別出開啟的埠所提供的網路服務類型，及其軟體版本編號。

Scanned Ports（設定欲掃瞄的埠）選項

功能名稱	對應選項	備註
All	-p-	掃瞄目標主機所有的埠
Most Important[fast]	-F	只掃瞄最重要的埠，速度較快。
Range	-p	設定特定的埠範圍值來掃瞄，如1-100。

Ping相關選項

功能名稱	對應選項	備註
Don't Ping	-P0	執行掃瞄之前，不需要先Ping目標主機。
ICMP Echo	-PI	發出ICMP Echo請求封包，查詢目標主機是否正在運行。
ICMP Timestamp	-PP	發出ICMP時戳請求封包探查正在傾聽的主機。
ICMP Netmask	-PM	發出ICMP網路遮罩請求封包探查正在傾聽的主機。
TCP ACK Ping	-PT	發出TCP ACK封包Ping目標主機。使用的時候不是以root權限，則必須搭配-sT才能使用。另外還需輸入目標埠號，預設值是80埠。
TCP SYN Ping	-PS	發出TCP SYN封包Ping目標主機，需要指定目標埠號。
UDP Ping	-PU	發出UDP封包Ping目標主機，需要指定目標埠號。

Throttling（設定調時掃瞄方式）選項

功能名稱	對應選項	備註
Paranoid Throttling	-T 0	串列所有的掃瞄動作，至少每隔5分鐘才發送一個封包。
Sneaky Throttling	-T 1	與-T 0類似，但間隔時間是15秒。
Polite Throttling	-T 2	串列每個探測動作，發送間隔時間是0.4秒。
Normal Throttling	不用設定	預設的調時掃瞄方式。
Agressive Throttling	-T 4	對每部主機的超時限制不超過5分鐘，且每次探測等待回應的時間在1.5秒以內。
Insane Throttling	-T 5	超時限制僅75秒，等待回應時間僅0.3秒。

Timeouts（逾時控制相關設定）選項

功能名稱	對應選項	備註
IPv4 TTL	--ttl	設定IPv4的封包存活時間。
Min. Parallel	--min_parallelism	設定最小的平行掃瞄數量，單位是埠。
Max. Parallel	--max_parallelism	設定最大的平行掃瞄數量，單位是埠。
Initial RTT	--initial_rtt_timeout	初始化探測的逾時值，這個選項要搭配勾選-P0使用，預設值是6000毫秒。
Min. RTT	--min_rtt_timeout	每次探測動作的至少等待時間。
Max. RTT	--max_rtt_timeout	每次探測動作的逾時值，如果超過這個時間，就再重新探測，預設值是9000毫秒。
Host Timeout	--host_timeout	掃瞄一部目標主機的時間，單位是毫秒。
Scan Delay	--scan_delay	在兩次探測動作之間必須要等待的時間，可降低網路負擔。

檔案處理選項

功能名稱	對應選項	備註
Input File	-iL	匯入某個含有目標主機位址資料的檔案，並依據其他設定好的選項逐一對其中所有主機位址進行掃瞄。
Output File(Normal)	-oN	以設定的檔名存成純文字檔。
Output File(grep-able)	-oG	以設定的檔名存成grep格式檔。
Output File(XML)	-oX	以設定的檔名存成XML格式檔。
Output File(ScriptKiddie)	-oS	以設定的檔名存成ScriptKiddie檔。
ALL	-oA	依據設定的檔名，一次存成純文字檔、grep格式檔及XML檔等三種檔案格式，並分別附加.nmap、.gnmap及.xml等副檔名以資識別。

Reverse DNS Resolution選項

功能名稱	對應選項	備註
Always	-R	反解析每一個設定的DNS名稱為IP位址。
When Required	不用設定	視需要而決定是否反解析。
Never	-n	不予解析。

Verbosity（掃瞄資訊的詳細程度）選項

功能名稱	對應選項	備註
Quiet	不用設定	預設只列出簡單扼要的掃瞄資訊。
Verbose	-v	列出詳細的掃瞄資訊。
Very Verbose	-vv	列出更多詳細的掃瞄資訊。
Debug	-d	以偵錯模式列出詳細的掃瞄資訊。
Verbose Debug	-d2	以偵錯模式列出更多詳細的掃瞄資訊。

其他常用選項

功能名稱	對應選項	備註
Source Device	-e	告知Nmap使用哪個裝置發送和接收封包，如果該裝置無效Nmap就會通知使用者。
Source Port	-g	設定掃瞄使用的來源埠，只有在對目標主機也能掃瞄到對應埠號時，此設定才有效。
Source IP	-S	當Nmap無法確認本機位址時，可在此設定本機IP位。此外選項還有欺騙掃瞄的作用，設定別的IP位址可使目標主機誤認為是別部主機在對它進行掃瞄。
Source Decoy	-D	可以做到誘餌掃瞄的功能，以設定多個IP位址，每個位址用逗號隔開，可使目標主機無法辨別出哪個是真正發起掃瞄的位址。
Fragmentation	-f	發送碎片封包，增加封包過濾器、防火牆或是入侵偵測系統的檢查難度。
IPv6	-6	支援掃瞄IPv6的位址。
Ordered Ports	-r	強制依照被掃瞄埠的順序執行掃瞄。

偵測測試與分析

- 本書提供以下五種測試範例，測試結果及分析請詳見書本內容
  - 測試一：Connect Scan掃瞄
  - 測試二：XMas Tree Stealth Scan掃瞄
  - 測試三：FIN|ACK Stealth Scan掃瞄
  - 測試四：偵測目標主機作業系統
  - 測試五：以偵錯模式列出偵測目標主機作業系統的詳細資訊

參考資料

- Fyodor Vaskovich, ”Remote OS detection via TCP/IP Stack FingerPrinting,” June 11, 2002, http://www.insecure.org/nmap/nmap-fingerprinting-article.txt
  中文見http://www.insecure.org/nmap/nmap-fingerprinting-article-tw.html
- Fyodor Vaskovich, ”The Art of Port Scanning,” September 6, 1997, http://www.insecure.org/nmap/nmap_doc.html
- Mark Wolfgang, ”Host Discovery with nmap,” November 2002, http://www.megasecurity.org/papers/discovery.pdf
- Michael D. Bauer, *Building Secure Servers with Linux*, O’Reilly, 2002
- Nmap指令, http://www.insecure.org/nmap/data/nmap_manpage.html