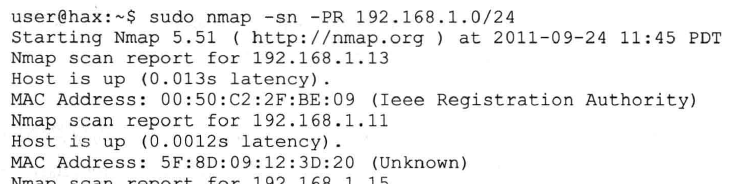
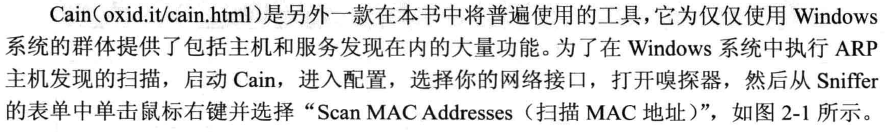
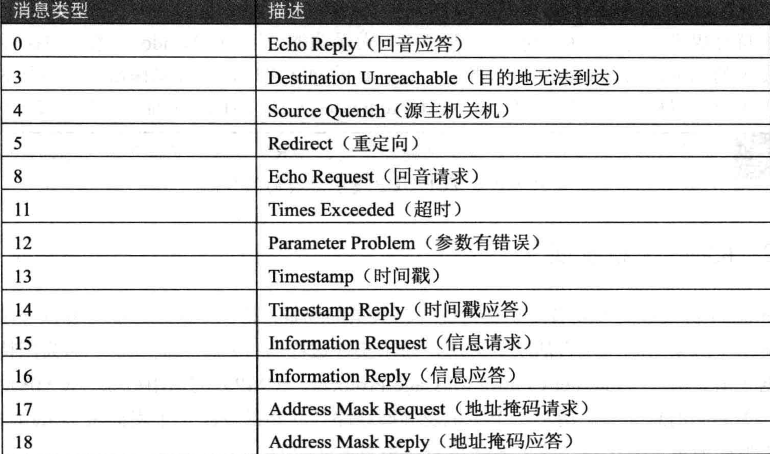
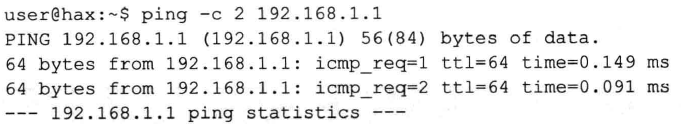
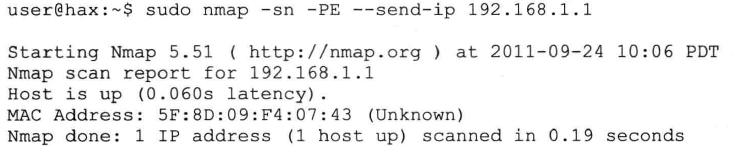
Arp-scan 掃描某網段中主機在線的ip、mac、OUI

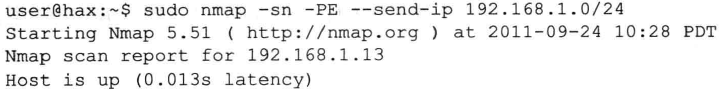
Nmap 功能強大的掃描 (–sn僅掃ip不掃port、-PR執行ARP掃描 加網段)

Cain 掃描arp的程式

ICMP封包的消息類型

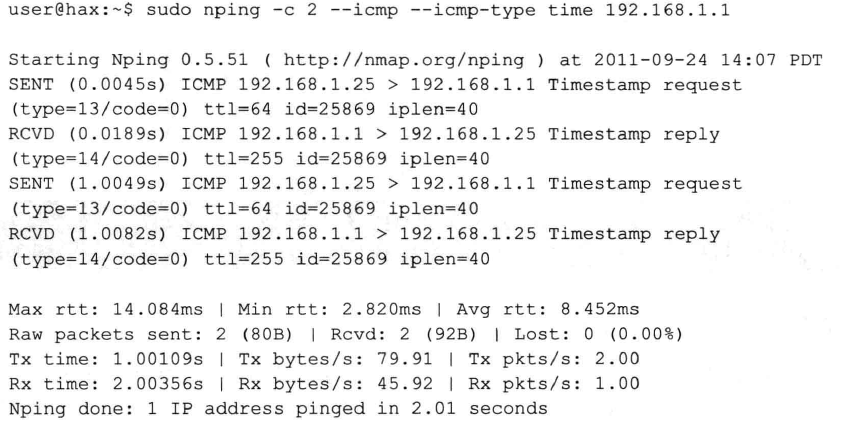
Ping 發送ICMP封包 (-c 2 發送兩個)

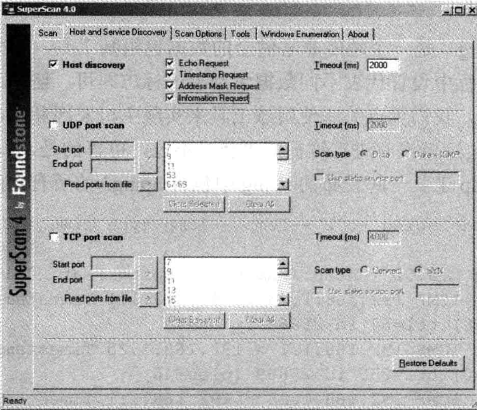
Nmap 發送如Ping的ICMP封包 (-PE ICMP封包)

若要掃描整個網段

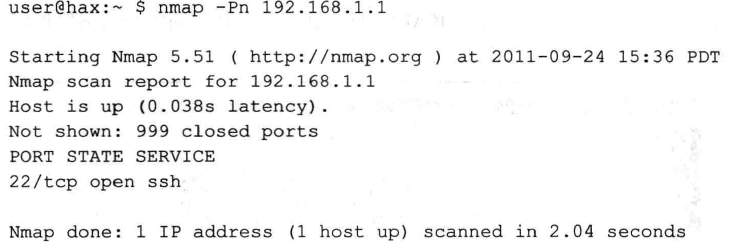
有些主機會忽略某些類型的ICMP封包，因此可使用其他類型如:

Nping 封包的組裝工具，可組合使用多種封包類型，支援偽造ip、mac、etc

以下類型為TIMESTAMP (--icmp-type) 的ICMP封包 (--icmp)

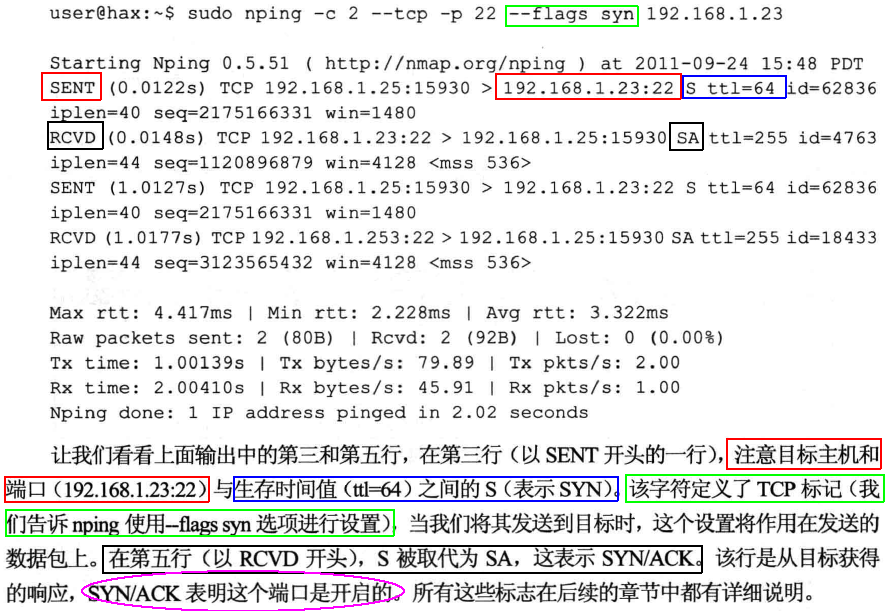
SuperScan 最快的Ping掃描工具之一，並行發送ICMP，主機名稱解析，在HTML中查看內容，使用於WINDOWS

某些主機防火牆會擋ICMP封包，所以可以送TCP封包去掃所有PORT

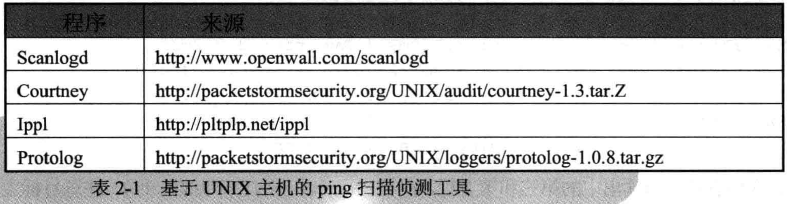
Nmap 掃描某ip的port，預設掃1-1000 (-Pn)

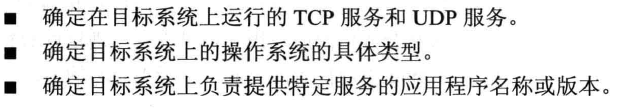
掃描某網段中IP的特定PORT，忽略Pn (-Ss –p 22 --open)，有哪些host開22

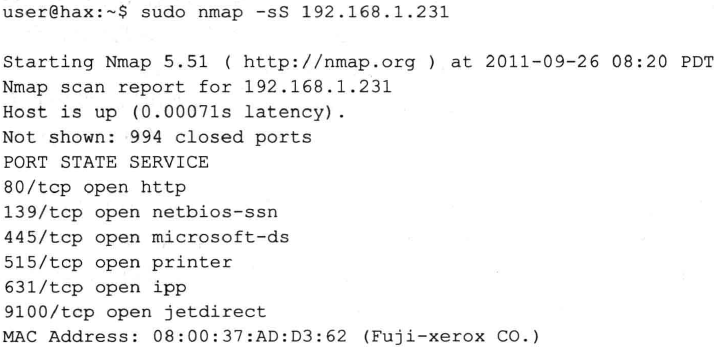
SuperScan 也可以用TCP/UDP掃描ip、port

Nping 使用TCP掃描IP、PORT，測試主機、埠是否開啟

Snort 偵測用ping掃描攻擊的入侵掃瞄系統IDS(Intrusion Detection System)

其他監控PING的工具

ICMP有很多類型，ECHO和ECHO\_REPLY只是其中兩種，不需要全部都開，開越多越危險，最簡單方法可以只允許ECHO\_REPLY、HOST\_UNREACHABLE、TIME\_EXCEEDED這幾種進入DMZ網路，亦可通過存取控制表（Access Control List，ACL）把ICMP限制在屬於某些ISP的IP，這樣更安全。

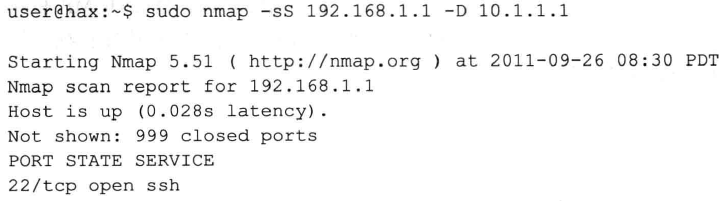
Nmap 掃描某主機上的TCP Port

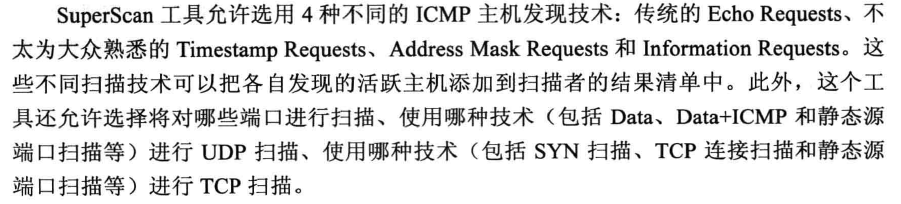
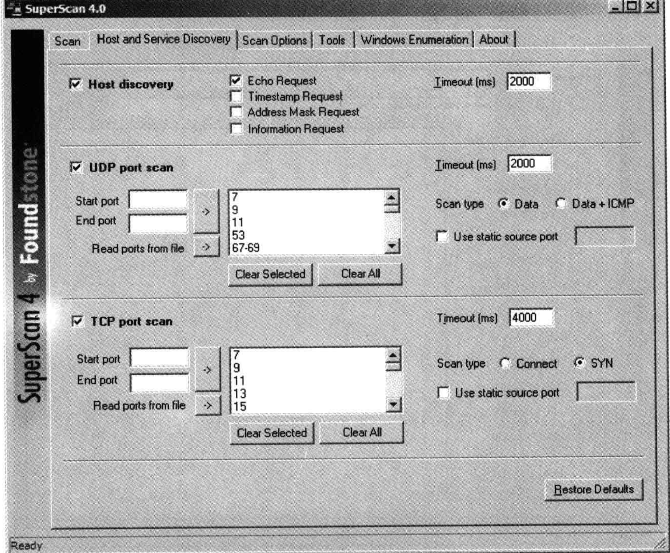
Nmap 加上

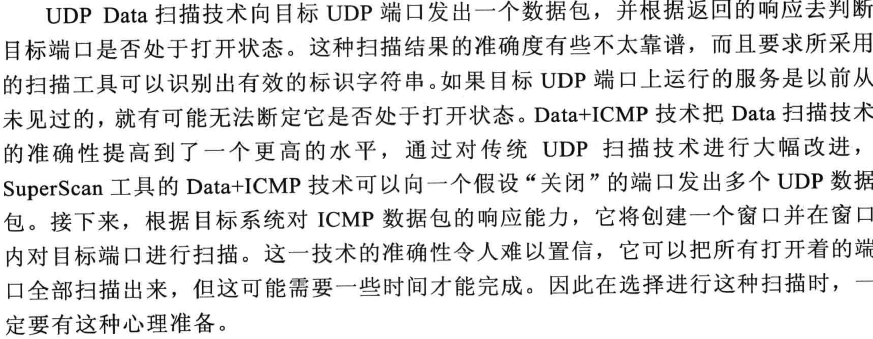
–oN 可以將資訊存成檔案 -oG 存成用tab隔開的檔案

-oX 存成xml檔案 -oA 所有格式

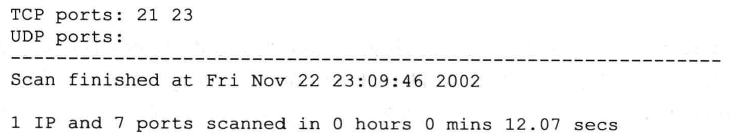
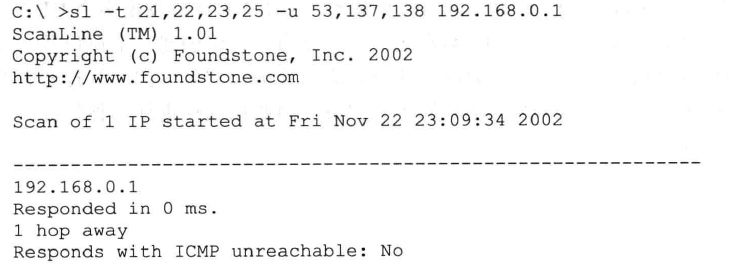
Nmap 可用 –f 將封包分割，有些主機不會組合就直接放行

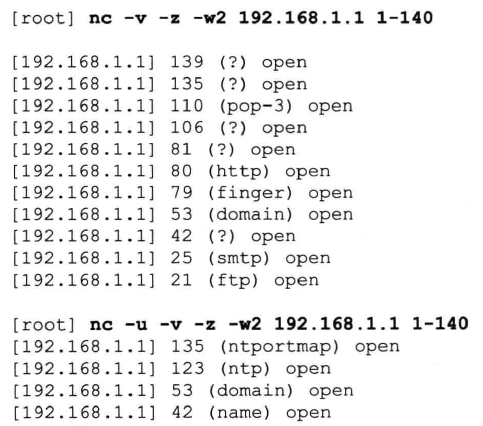
可用-D來灌輸多餘訊息，以此來欺騙目標主機

SuperScan幾乎是包裝了Nmap的功能強大GNU版本

UDP Data掃描技術

ScanLine 使用在windows中對一個ip的port進行TCP or UDP掃描



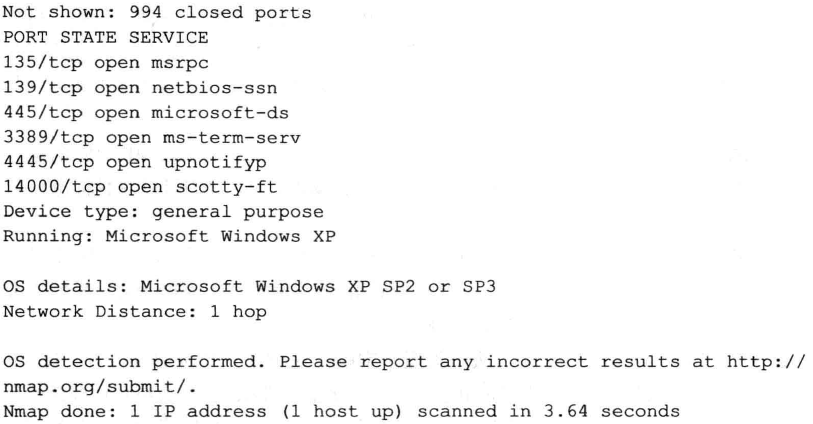
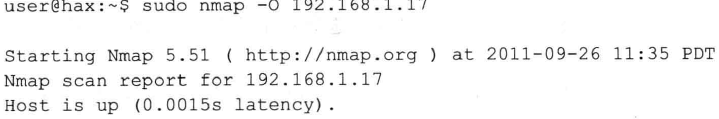
nc 掃描port (-v生成詳細檔案 –vv生成非常詳細檔案 –u使用UDP –z零模式)

各系統技術探查

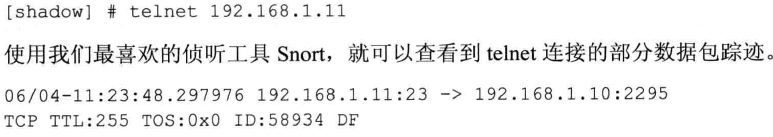
|  |  |  |
| --- | --- | --- |
| FIN探查 | 無效標誌探查 | ISN初始序列號 |
| DF標誌位監控 | TCP初始數據長度 | ACK值 |
| ICMP出錯消息抑制 | ICMP消息內容 | ICMP出錯消息-回應完整性 |
| TOS服務類型 | 封包拆分處理 | TCP選項 |

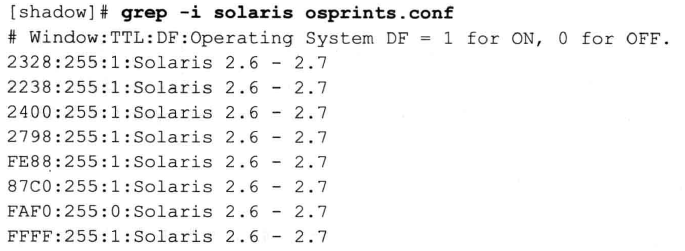
Nmap 使用-O可同時使用以上技術(除了封包拆分處理& ICMP出錯消息)

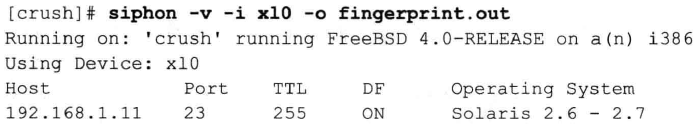
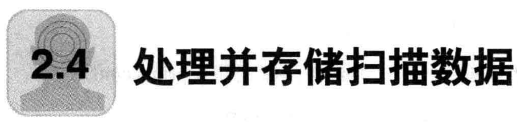
也可以抓到OS的資訊存放在nmap-os-fingerprints檔案裏面



使用Snort可以看到telnet的封包蹤跡

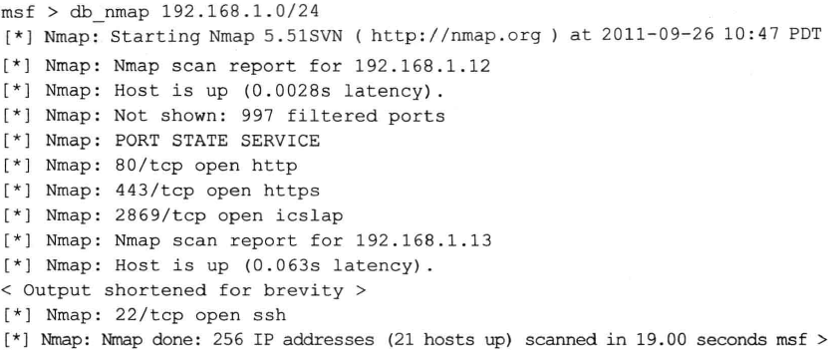


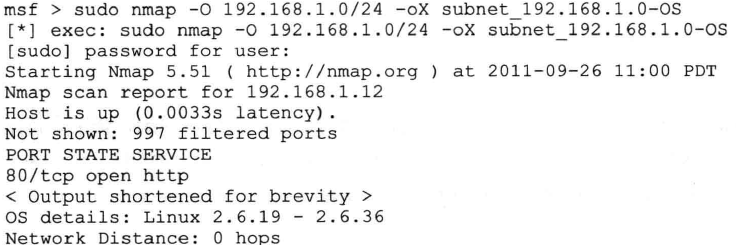
查看osprints.conf發現第四條與Snort一樣

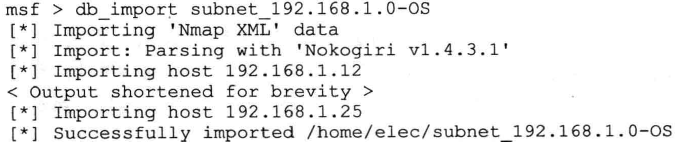
使用siphon看到TTL跟長度都跟Snort一樣

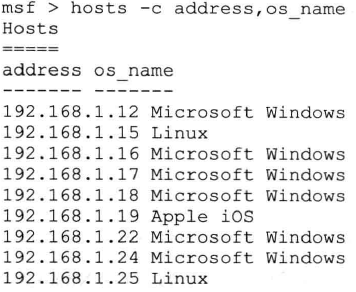
MetaSploit 通用的漏洞偵測軟體包，模組化探勘與載荷攻擊

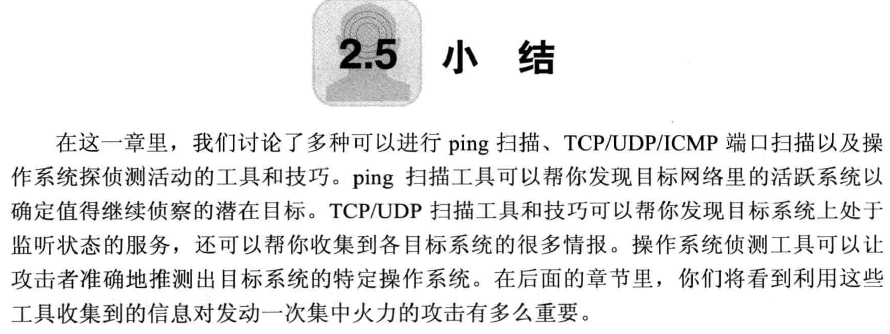
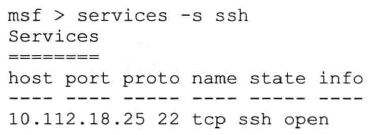
安裝MetaSploit會建立一個PostgreSQL，設定連接資料庫可在mfsconsole輸入

 mfs的db\_nmap就像nmap

mfs中使用sudo nmap 得到操作系統的資訊

將nmap得到的資訊存到資料庫裏

用hosts –c 列出資料庫裡的所有主機

Services -s查看所有有開啟一service的主機 (如10.112.18.25這台主機有開ssh)