常用端口埠對照解析

Port Number	服務	說明
0	Reserved	通常用於分析作業系統。這一方法能夠工作是因在一些系統中“0”是無效埠，當你試圖使用通常的閉合埠連接它時將為生不同的結果。一種典型的掃描，使用 IP 位址為 0.0.0.0，設置 ACK 位元並在乙太網層廣播。
1	tcpmux	這顯示有人在尋找 SGI Irix 機器。Irix 是實現 tcpmux 的主要提供者，默認情況下 tcpmux 在這種系統中被打開。Irix 機器在發佈是含有幾個默認的無密碼的帳戶，如：IP、GUEST UUCP、NUUCP、DEMOS 、TUTOR、DIAG、OUTOFBOX 等。許多管理員在安裝後忘記刪除這些帳戶。因此 HACKER 在 INTERNET 上搜索 tcpmux 並利用這些帳戶。
7	Echo	能看到許多人搜索 Fraggle 放大器時，發送到 X.X.X.0 和 X.X.X.255 的資訊。
19	Character Generator	這是一種僅僅發送字元的服務。UDP 版本將會在收到 UDP 包後回應含有垃圾字元的包。TCP 連接時會發送含有垃圾字元的資料流程直到連接關閉。HACKER 利用 IP 欺騙可以發動 DoS 攻擊。偽造兩個 chargen 伺服器之間的 UDP 包。同樣 Fraggle DoS 攻擊向目標位址的這個埠廣播一個帶有偽造受害者 IP 的資料包，受害者為了回應這些資料而過載。
21	FTP	FTP 伺服器所開放的埠，用於上傳、下載。最常見的攻擊者用於尋找打開 anonymous 的 FTP 伺服器的方法。這些伺服器帶有可讀寫的目錄。木馬 Doly Trojan、Fore、Invisible FTP、WebEx、WinCrash 和 Blade Runner 所開放的埠。
22	Ssh	PcAnywhere 建立的 TCP 和這一埠的連接可能是為了尋找 ssh。這一服務有許多弱點，如果配置成特定的模式，許多使用 RSAREF 庫的版本就會有不少的漏洞存在。
23	Telnet	遠端登錄，入侵者在搜索遠端登錄 UNIX 的服務。大多數情況下掃描這一埠是為了找到機器運行的作業系統。還有使用其他技術，入侵者也會找到密碼。木馬 Tiny Telnet Server 就開放這個埠。
25	SMTP	SMTP 伺服器所開放的埠，用於發送郵件。入侵者尋找 SMTP 伺服器是為了傳遞他們的 SPAM。入侵者的帳戶被關閉，他們需要連接到高帶寬的 E-MAIL 伺服器上，將簡單的資訊傳遞到不同的地址。木馬 Antigen、Email Password Sender、Haebu Coceda、Shtrilitz Stealth、WinPC、WinSpy 都開放這個埠。
31	MSG	木馬 Master Paradise、Hackers Paradise 開放此埠。

	Authentication	
42	WINS Replication	WINS 複製
53	Domain Name Server（DNS）	DNS 伺服器所開放的埠，入侵者可能是試圖進行區域傳遞（TCP），欺騙 DNS（UDP）或隱藏其他的通信。因此防火牆常常過濾或記錄此埠。
67	Bootstrap Protocol Server	通過 DSL 和 Cable modem 的防火牆常會看見大量發送到廣播位址 255.255.255.255 的資料。這些機器在向 DHCP 伺服器請求一個位址。HACKER 常進入它們，分配一個位址把自己作為局部路由器而發起大量中間人（man-in-middle）攻擊。用戶端向 68 埠廣播請求配置，伺服器向 67 埠廣播回應請求。這種回應使用廣播是因為用戶端還不知道可以發送的 IP 位址。
69	Trival File Transfer	許多伺服器與 bootp 一起提供這項服務，便於從系統下載起動代碼。但是它們常常由於錯誤配置而使入侵者能從系統中竊取任何 文件。它們也可用於系統寫入文件。
79	79	入侵者用於獲得用戶資訊，查詢作業系統，探測已知的緩衝區溢出錯誤，回應從自己機器到其他機器 Finger 掃描。
80	HTTP	用於網頁瀏覽。木馬 Executor 開放此埠。
102	Message transfer agent(MTA)-X.400 over TCP/IP	消息傳輸代理。
110	Post Office Protocol -Version3	POP3 伺服器開放此埠，用於接收郵件，用戶端訪問伺服器端的郵件服務。POP3 服務有許多公認的弱點。關於用戶名和密碼交 換緩衝區溢出的弱點至少有 20 個，這意味著入侵者可以在真正登陸前進入系統。成功登陸後還有其他緩衝區溢出錯誤。
113	Authentication Service	這是一個許多電腦上運行的協定，用於鑒別 TCP 連接的用戶。使用標準的這種服務可以獲得許多電腦的資訊。但是它可作為許多服務的記錄器，尤其是 FTP、POP、IMAP、SMTP 和 IRC 等服務。通常如果有許多客戶通過防火牆訪問這些服務，將會看到許多這個埠的連接請求。記住，如果阻斷這個埠用戶端會感覺到在防火牆另一邊與 E-MAIL 伺服器的緩慢連接。許多防火牆支援 TCP 連接的阻斷過程中發回 RST。這將會停止緩慢的連接。
119	Network News Transfer	EWS 新聞組傳輸協定，承載 USENET 通信。這個埠的連接通常是人們在尋找 USENET 伺服器。多數 ISP 限制，只有他們的客戶才能訪問

	Protocol	他們的新聞組伺服器。打開新聞組伺服器將允許發/讀任何人的帖子，訪問被限制的新聞組伺服器，匿名發帖或發送 SPAM。
135	Location Service	Microsoft 在這個埠運行 DCE RPC end-point mapper 為它的 DCOM 服務。這與 UNIX 111 埠的功能很相似。使用 DCOM 和 RPC 的服務利用電腦上的 end-point mapper 註冊它們的位置。遠端客戶連接到電腦時，它們查找 end-point mapper 找到服務的位置。HACKER 掃描電腦的這個埠是為了找到這個電腦上運行 Exchange Server 嗎？什麼版本？還有些 DOS 攻擊直接針對這個埠。
137、138、139	NETBIOS Name Service	其中 137、138 是 UDP 埠，當通過網上鄰居傳輸文件時用這個埠。而 139 埠：通過這個埠進入的連接試圖獲得 NetBIOS/SMB 服務。這個協定被用於 windows 文件和印表機共用和 SAMBA。還有 WINS Regisrtation 也用它。
143	Interim Mail Access Protocol v2	和 POP3 的安全問題一樣，許多 IMAP 伺服器存在有緩衝區溢出漏洞。記住：一種 LINUX 蠕蟲（admv0rm）會通過這個埠繁殖，因此許多這個埠的掃描來自不知情的已經被感染的用戶。當 REDHAT 在他們的 LINUX 發佈版本中默認允許 IMAP 後，這些漏洞變的很流行。這一埠還被用於 IMAP2，但並不流行。
161	SNMP	SNMP 允許遠端管理設備。所有配置和運行資訊的儲存在資料庫中，通過 SNMP 可獲得這些資訊。許多管理員的錯誤配置將被暴露在 Internet。Cackers 將試圖使用默認的密碼 public、private 訪問系統。他們可能會試驗所有可能的組合。SNMP 包可能會被錯誤的指向用戶的網路。
162	SNMP Trap	SNMP 陷阱。
177	X Display Manager Control Protocol	許多入侵者通過它訪問 X-windows 操作臺，它同時需要打開 6000 埠。
389	LDAP、ILS	輕型目錄訪問協定和 NetMeeting Internet Locator Server 共用這一埠。
443	Https	網頁瀏覽埠，能提供加密和通過安全埠傳輸的另一種 HTTP。
636	LDAP	SSL（Secure Sockets layer）
993	IMAP	SSL（Secure Sockets layer）
1024	Reserved	它是動態埠的開始，許多程式並不在乎用哪個埠連接網路，它們請求系統為它們分配下一個閒置埠。基於這一點分配從埠 1024 開始。這就是說第一個向系統發出請求的會分配到 1024 埠。你可以重啟機器，打開 Telnet，再打開一個窗口運行 natstat -a 將會看到 Telnet 被

		分配 1024 埠。還有 SQL session 也用此埠和 5000 埠。
1080	SOCKS	這一協定以通道方式穿過防火牆，允許防火牆後面的人通過一個 IP 地址訪問 INTERNET。理論上它應該只允許內部的通信向外到達 INTERNET。但是由於錯誤的配置，它會允許位於防火牆外部的攻擊穿過防火牆。WinGate 常會發生這種錯誤，在加入 IRC 聊天室時常會看到這種情況。
1433	SQL	Microsoft 的 SQL 服務開放的埠。
1500	RPC client fixed port session queries	RPC 客戶固定埠會話查詢
1503	NetMeeting T.120	NetMeeting T.120
1720	NetMeeting	NetMeeting H.233 call Setup。
1731	NetMeeting Audio Call Control	NetMeeting 音頻調用控制。
2049	NFS	NFS 程式常運行於這個埠。通常需要訪問 Portmapper 查詢這個服務運行於哪個埠。
2500	RPC client using a fixed port session replication	應用固定埠會話複製的 RPC 客戶
3128	squid	這是 squid HTTP 代理伺服器的默認埠。攻擊者掃描這個埠是為了搜尋一個代理伺服器而匿名訪問 Internet。也會看到搜索其他代理伺服器的埠 8000、8001、8080、8888。掃描這個埠的另一個原因是用戶正在進入聊天室。其他用戶也會檢驗這個埠以確定用戶的機器是否支援代理。
3389	超級終端	WINDOWS 2000/XP/2003 終端(遠端桌面)開放此埠。
4000	QQ 用戶端	騰訊 QQ 用戶端開放此埠。
5632	pcAnywere	有時會看到很多這個埠的掃描，這依賴於用戶所在的位置。當用戶打開 pcAnywere 時，它會自動掃描局域網 C 類網以尋找可能的代理（這裏的代理是指 agent 而不是 proxy）。入侵者也會尋找開放這種服務的電腦。，所以應該查看這種掃描的源地址。一些搜尋 pcAnywere

		的掃描包常含埠 22 的 UDP 資料包。
6970	RealAudio	RealAudio 客戶將從伺服器的 6970-7170 的 UDP 埠接收音頻資料流程。這是由 TCP-7070 埠外向控制連接設置的。
8000	OICQ	騰訊 QQ 伺服器端開放此埠。
8080	代理埠	WWW 代理開放此埠。
445	Common Internet File System(CIFS)	公共 Internet 文件系統
500	Internet Key Exchange(IKE)	Internet 密鑰交換
1645、1812	Remot Authentication Dial-In User Service(RADIUS)authentication(Routing and Remote Access)	遠端認證撥號用戶服務
1646、1813	RADIUS accounting(Routing and Remote Access)	RADIUS 記帳（路由和遠端存取）
1701	Layer Two Tunneling Protocol(L2TP)	第 2 層隧道協定
1801、3527	Microsoft Message Queue Server	Microsoft 消息佇列伺服器。還有 TCP 的 135、1801、2101、2103、2105 也是同樣的用途。
2504	Network Load Balancing 網路平衡負荷	網路平衡負荷