新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2008/9/1-2008/9/14 第75期

多功能 UTM / MS 系列報導

技術淺談與應用 - 入侵偵測防禦特徵名稱的意義說明(一)

在多功能 UTM 中，位於“入侵偵測防禦 > 特徵設定 > 異常偵測”，下所存在的內建特徵名稱有許多種，但這些名稱是代表著什麼意思？用來做什麼用的？相信也有不少管理人員抱有著相同的疑問。其實這些讓人會產生疑問的名詞指的是駭客常用來攻擊的方式，而這些名詞大多是都沒有正式的中文名稱。

位於系統中的特徵名稱所代表的意思，以下將一一的來作介紹說明：

『syn flood』

此種攻擊主要是利用 TCP 連結時的三向交握訊息（three way handshake）來造成的。當攻擊者惡意地送出許多 TCP SYN 封包給被攻擊端，在被攻擊端回覆接受訊息(SYN + ACK)後，而攻擊端後續沒有再返回一個確認報訊息給被攻擊端時，這種情況下被攻擊端伺服器會將攻擊端的位置暫時做儲存，過段時間後再重試（再次發送接受訊息給攻擊者）。此種攻擊就是利用這方式，以數以萬計的半連接來消耗被攻擊端非常多的 CPU 時間和記憶體，讓被攻擊端不斷對暫存於記憶體列表中的 IP 進行回覆訊息(SYN + ACK)的重試，因而導致暫停服務。

『udp flood』

又稱為 Fragile 攻擊，它是透過 UDP protocol 送出假造來源的 UDP broadcast 封包至目標網路，以產生放大的資料流程，當目的網域中的眾多主機回應之後，便可以造成網路的壅塞。即使某些 IP 位址沒有回應，但產生的 ICMP 封包（type 3，Destination Unreachable）仍然可以達到 DoS 攻擊的效果。

『icmp flood』

此種攻擊方式是發送 ICMP 者假造來源 IP 之後，再將 ICMP 封包大量的送至被害者主機，則伺服器主機會回應等量的 ICMP 封包到所假造的來源 IP 網路上，直接造成被害者與被假造來源的 IP 兩個網路之間的網路流量大量增加。造成沒有多餘的頻寬可以讓一般正常使用者使用，以達到 Denial-of-Service 的攻擊。

『syn fin』

過濾不合規範的 IP 封包，利用 tcp 連接的建立到終止都跟蹤檢測的方式，來做詳細過濾。在同一個 tcp 連接中，封包的關系是相互關聯的，先是 syn 封包→數據封包→fin 封包。但如果分割這些關系，單獨的只過濾數據封包的話，很容易被精心所構造的攻擊數

據封包欺騙，有心的駭客可利用 syn 封包、fin 封包，來探測防火牆後面的網路，也就是所謂的後門，事後來進行入侵。

『tcp no flag』

丟棄不含或含不合規範標誌位元的 TCP 封包。蠕蟲通常會嘗試透過內建的名單或是隨機產生感染的目標，但並不是每一次都能順利的連結成功。由於 NetFlow 會將每個 session 中所有傳輸時的 TCP 控制旗標全部儲存在封包控制旗標（TCP Flag）這個欄位中，因此透過這個欄位中的資訊來協助我們推測特定主機連線的特性。在一個 Flow 正常的建立 TCP 連結後，其封包控制旗標（TCP Flag）欄位會記錄的包含 ACK、SYN、FIN 等控制旗標，但是如果蠕蟲進行感染的動作時，由於隨機選取的主機並不一定存在，或是即使存在但目標主機沒有開放蠕蟲所要感染的 TCP port，在這種情況下，NetFlow 資訊中由受感染主機對外連線所產生的 Flow 封包控制旗標（TCP Flag）欄位會只存在 SYN 這個 TCP 控制旗標，所以可根據這種特性來過濾不合規範的封包。

『fin no ack』

通常，在設置了 FIN 標誌的 TCP 封包，同時也會配置了 ACK 標誌（以確認接收到的前一個封包）。所以設置了 FIN 標誌但未設置 ACK 標誌的 TCP 封包是異常的 TCP 行為。一般作業系統可能會通過發送設置了 RST 標誌的 TCP 封包來做出回應，而受害者的回應則會給攻擊者提供有關其作業系統的線索，讓攻擊者有入侵的管道。

『tcp land』

此種手法是利用特殊的 TCP 封包傳送至目標主機，使被攻擊端因為無法判別而當機或被迫重新啟動，攻擊者所利用的就是 TCP 通訊協定中，定義規則與作業系統之間漏洞所造成的攻擊手法。攻擊者利用 IP 偽裝的技術修改即將送出的封包，將其來源與目的 IP 位址均改成是目標機器的 IP 位址，以及將來源與目標連接埠也改為一樣，來使得某些作業系統或網路設備當機無法正常運作。

『large icmp』

可稱為 ICMP 大封包，這種情況多屬於異常流量的行為。通常 ICMP 封包都不會太大，但如果封包過大，則表式正處於被攻擊，或者有人在測試使用大封包 ping 被攻擊端的主機。由於在早期的路由器方面對封包的最大尺寸都有限制，許多操作系統對 ICMP 封包上都是有大小上的規定，而攻擊方則利用聲稱自己的尺寸大小超過 ICMP 上限的封包，也就是所加載的尺寸大小超過所規定的上限時，就會使被攻擊方出現內存上分配的錯誤，因而導致 TCP/IP 堆棧崩潰，致使被攻擊方(接受方)當機。

新軟系統多功能 UTM 所提供的入侵偵測防禦特徵碼，當然不會僅只有上述的 8 種而已，其餘的特徵碼我們將會於下一期－第 76 期的新軟週報中繼續為您來做完整的說明。

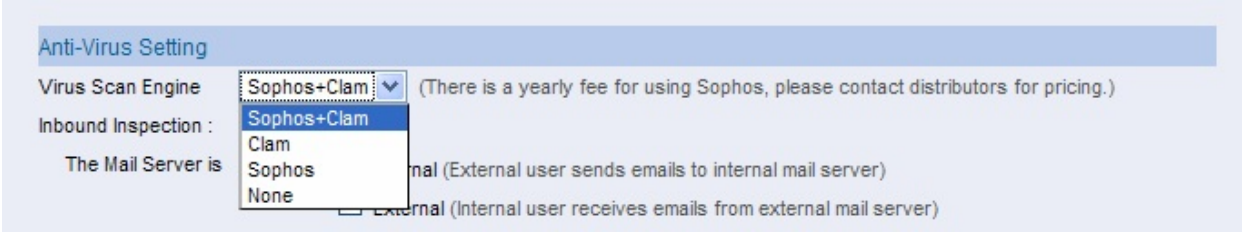
文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 拒絕公司被殭屍病毒入侵

相信前陣子所發生於七夕情人節的新聞報導，有關於電子告白信內含有病毒的事件，大家都還記憶猶新，只要開啟信件連結的收件者，就會立即的被所謂的『殭屍病毒』所感染。散播者利用特殊節日的影響下，加上讓人心動的標題來降低收件者防備的心態，讓收件者開啟含有『殭屍病毒』的信件，以達到入侵的目的，一旦收件者因為好奇，按下郵件中所附的連結，那可能會是一場夢魘。根據趨勢科技最新發現指出，含有「Stand by my side」、「I want to be with you」以及「Lucky to have you」等告白訊息的電子郵件，都有可能是殭屍網路所散播含有惡意連結的垃圾郵件，當然中文標題也不例外，利用「我愛你」之類聳動人心的標題也是讓收件者踏入圈套的一個陷阱。

台灣目前僵屍病毒十分泛濫，每個人於每天所收的郵件當中，經常會發現 10 封信中可能 10 封都是莫名奇妙的垃圾信，面對那些正規的信件，總是被垃圾信所掩蓋，而這些令人厭煩的垃圾信則大多是經由已被僵屍病毒侵的僵屍電腦所發送，由於使用者依舊可以正常使用電腦，因此很難察覺自己的電腦其實已經被入侵，甚至已被當作跳板在對外發送垃圾信。若公司成為病毒郵件或垃圾郵件的轉送點，不僅會將網路資源消耗殆盡，還會嚴重的影響公司形象。

針對此問題，新軟系統『多功能-UTM』對各式各樣的網路服務建置了數種病毒掃描機制，其中就有包含了郵件病毒的過濾。而『多功能-UTM』所採用的掃毒引擎為 Clam、Sophos。



防毒設定畫面截圖

當郵件傳遞時，『多功能-UTM』會先行將其信件存放於暫存區內，並針對信件的內容、所夾帶的檔案掃毒（壓縮檔解壓掃毒）。若郵件判斷為異常（病毒郵件、釣魚郵件…），『多功能-UTM』會將該郵件依照管理人員所設定的處置方式處理（隔離儲存、刪除…）剩下的郵件再交由垃圾郵件過濾機制處理。

垃圾郵件過濾畫面截圖

除此之外『多功能-UTM』同時也包含了 HTTP / Web Mail、FTP 病毒過濾及 IDP 病毒過濾，並且內建的自動線上更新系統，可自動更新病毒碼，完全不需管理人員手動更新，即可輕鬆的享受到在『多功能-UTM』保護下乾淨的網路環境。

文 陳殿鴻 kim@nusoft.com.tw