

多功能 UTM / MS 系列報導

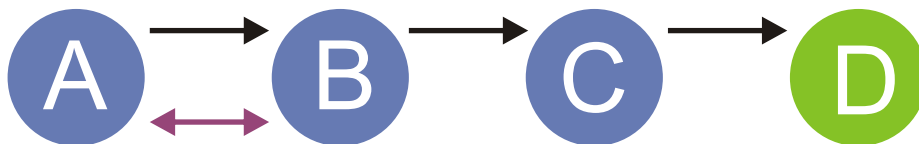
技術淺談與應用 - 入侵偵測防禦特徵名稱的意義說明(二)

『ip record route』

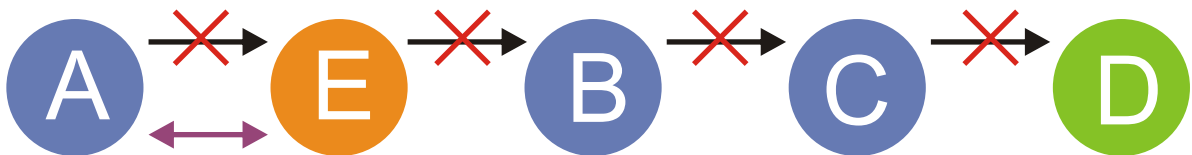
攻擊者可以利用此漏洞製作特殊的來源路由封包，造成系統無條件接收這些惡意封包。

『ip strict src record route』

嚴格的封包路由。簡單來說，嚴格受控來源端路由，意指：發送端給予封包指定路徑，強迫該封包應經過指定的路徑點到達目的端。而使用者可以指定較順暢或是較快速、安全的路徑，將封包送達目的端，而若是指定的路徑發生問題。例如：(圖一)封包要經過 A 點→ B 點→ C 點的路徑，將封包丟到 D 的目的端，則若是在 B 路徑發生路由停止服務，或是路由繁忙時，封包會在 A 到 B 的線路上徘徊，則時間過久 TTL(Time to Live)將會把訊息傳達給 ICMP，而停止該封包的運作。再者若是給予錯誤路徑，例如：(圖二) A 點→ B 點→ C 點，而正常路徑為：A 點→ E 點→ B 點→ C 點，則因沒有給予正確訊息，則封包是不會經過未指定的 E 點，也將會導致無法將封包送達目的端 D 點。對於路徑上的 Segment，會傳達已傳送位址後下一個目的地位址非緊鄰不可的訊息。



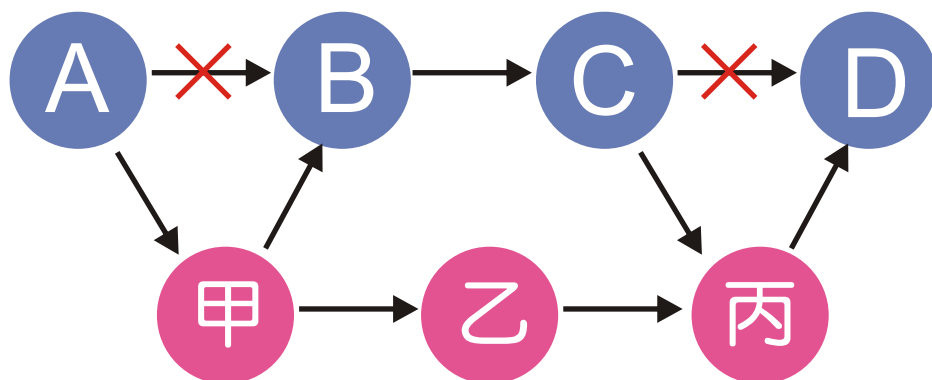
圖一



圖二

『ip loose src record route』

寬鬆的封包路由。意指：發送端給予了封包必須經過的路徑，但如果它需要，也可以經過一些其他的路徑。換句話說，不用考慮封包經過的確切地址，只要它經過這些路徑即可。例如：(圖三)當來源端給予路徑 A、B、C，將封包丟給 D 目的端，而不一定要沿著指定 A → B → C → D 可以選擇經過其他路徑，只需經過指定的路徑即可並非強迫式，若 A 到 B 的點繁忙或是有其他狀況可將其判斷，將封包可以從 A 點到甲點，再由甲點到 B 點一直到送到 D 目的端如此。



圖三

『invalid url』

傳送一個格式有問題的 URL 到正在運行的驗證服務 TCP 端口，以達到系統關閉並且重新啟動，進一步要求重新啟動的 WatchGuard 為它工作。

『winnuke』

利用 Windows 的系統漏洞，通過 TCP/IP 協議向遠程機器發送一段可導致 OOB 錯誤的信息，使電腦屏幕上出現一個藍屏及提示：「系統出現異常錯誤」，或者當機，而目前的 WinNuke 系列工具已經從最初的簡單選擇 IP 攻擊某個埠發展到可以攻擊一個 IP 區間範圍的電腦，並且可以進行連續攻擊，還能夠驗證攻擊的效果，還可以對檢測和選擇埠，所以使用它可以造成某一個 IP 位址區間的電腦全部藍屏及當機。

『bad ip protocol』

偵測非標準的 IP 通訊協定

『Portscan』

掃 port，一次完整的網路安全掃描分為 3 個階段：

- (1) 第 1 階段：發現目標主機或網路。
- (2) 第 2 階段：發現目標後進一步搜集目標資訊，包括作業系統類型、運行的服務以及服務軟體的版本等。如果目標是一個網路，還可以進一步發現該網路的拓撲結構、路由設備以及各主機的資訊。
- (3) 第 3 階段：根據搜集到的資訊判斷或者進一步測試系統是否存在安全漏洞。原本用來檢測自己的電腦，但是常被人拿來做為刺探它人所用。

『http inspect』

檢測 http 的封包內容是否包含惡意程式碼。缺少或不正確的通訊協定宣告、缺少欲連結的主機名稱、不合法的網站連結路徑、不合法的字元存在於欲連結的主機名稱中。

文  陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 利用多功能 UTM 的垃圾郵件防護機制，能為企業帶來什麼樣的好處？

電子郵件系統是最常也是最容易遭受攻擊的一項管道，同時也是目前最為嚴重的問題，如垃圾郵件、病毒、間諜軟體、釣魚詐騙攻擊等等，這些不請自來的種種問題，進而可能對企業機密資料和業務管理造成相當的危害，相信也都是大家瞭解的一件事。因此，在企業中部署一個郵件安全閘道，以保護所有進出的電子郵件，已經成為企業網路安全策略中不可或缺的環節。

新軟系統多功能 UTM 眾多功能中，其中就包含了針對垃圾郵件這領域的防護功能，而新軟系統多功能 UTM 裡，垃圾郵件防護機制所能夠為公司帶來什麼樣的好處？

多功能 UTM 中所附屬的垃圾郵件防護機制擁有多項功能，垃圾郵件過濾、郵件病毒偵測、郵件通知、郵件稽核備份。這些強大的功能不但能夠避免公司內部遭受外部網路層出不窮泛濫的病毒攻擊而造成電子郵件服務中斷之外，還可準確有效的防範如洪水般的垃圾郵件以及釣魚信件、病毒郵件的攻擊，並且還擁有 Web Mail 的管制功能，讓防護更全面、更加的完善，為公司在郵件方面創造乾淨穩定的環境。

而如此的環境下，連帶所產生的另一項更大的價值就是能夠有效的提高員工工作效率，讓公司在內對外、外對內溝通的管道順利、穩定情況下，進而可提升公司的生產力及競爭力，並且可降低郵件系統管理負擔、節省郵件伺服器之數量與儲存空間。

多功能 UTM 另一項優點則是多種設備的功能整合後，網管人員不再需要管理眾多的 UI 介面，透過新軟系統多功能 UTM，只需使用同一個 UI 介面即可管理及控制所有的功能，簡單易懂，而且容易操作，即使是初學者也可輕鬆上手，如此人性化的設計，成功的簡化了公司內部安全部署與管理，同時也大大的減輕管理人員的負擔，讓管理人員有更多的心力去處理其他公司內部相關的事務。

新軟系統多功能 UTM - MS 系列產品，針對公司規模大小的不同，而特別設計不同的機型，適用人數從 30 人到超過 300 人，公司可依照本身的規模來選購最合適的設備機型。新軟系統多功能 UTM - MS 系列產品擁有最完善的功能設計，加上其他強大功能，所能為公司帶來的好處絕對不僅於此，相信新軟系統多功能 UTM - MS 系列產品一定是公司、企業最佳的選擇。

- 如欲瞭解更詳細、完整的機型內容說明，歡迎至 <http://www.nusoft.com.tw>

文  陳殿鴻 kim@nusoft.com.tw