ICMP 模糊測試攻擊

系所／資訊工程學系

指導老師／徐武孝

組員／張力仁、楊承榆

　　模糊測試(fuzz testing)是一種檢測安全性的自動化或半自動化軟體測試技術，透過發送「隨機性」、「無效」、「預期外」的測試數據給予目的端，並監測目的端是否有出現任何的例外狀況發生。假設我們更改了某個顏色的數值並發送，我們收到的圖片顯示可能會與原本的情況不相同(如圖 1)，此時我們便可以藉此來檢測出可能會發生的錯誤情況，來達到漏洞的安全預防。

圖 1：本來預期的數值以及更改後回應的數值差別

　　本專題旨在於藉由模糊測試對ICMP(Internet Control Message Protocol)協定進行攻擊，並尋找出 ICMP 協定中可能存在的漏洞。ICMP 位於網際網路OSI(Open System Interconnection Reference Model)七層架構中的網路層（Network Layer），為網際網路協定套組的核心協定之一(定義於 RFC792)，主要作為輔助 IP 協定所欠缺的錯誤偵測及錯誤回報的機制，使管理者可尋找出問題並做出解決方法。在 ICMP 協定諸多功能中屬 Ping 與 Traceroute 最常被使用到，Ping 是用來檢測兩台主機是否能連通以及偵測連線錯誤，可由一台主機對目標主機的 IP 位址進行 Ping 的動作，若成功連通，則目的端主機會接受封包並回傳封包給來源端主機(如圖 2)，Traceroute 是用來尋找傳送端與目的端之間會經過的路由器(Router)，每當經過一個路由器會回傳一個封包並計算該路由器與傳送端之間的往返時間(如圖 3)。

圖 2：在 CMD 中執行 PING 結果

圖 3：在 CMD 中執行 TRACEROUTE
結果

　　本專題的研究目的希望能夠在
ICMP 協定上找出可能存在的缺漏，我
們使用 Fuzz 作為測試工具，以手動方
式去更改 ICMP 協定中的欄位數值，將
資料由客戶端(Client)送出給伺服端
(Server)，在送出資料的同時使用
Wireshark 進行封包監測，並確認在封包
回傳時是否有異樣的數值產生，藉此去
尋找可能存在的協定漏洞。