網路匯集點的 Flooding 訊務偵測與自動通告系統
Flooding Detection and Notification System over Aggregate Network

中央大學 電子計算機中心 資訊工程系
楊素秋 曾黎明
center7@cc.ncu.edu.tw tsenglm@cc.ncu.edu.tw

摘要

依據多年的區網管理經驗,我們發現:絕大部分的 abuse 抱怨事件均源自用戶的忽視電腦安全,致大量主機成為 spammer 持續散播廣告信,發動 DDoS 攻擊的掩護工具.然而,遭誤用的系統會持續,頻繁地建立網路連接到單一或多部主機.所以,不僅源自遭感染主機的 flow 連接與封包量會超量增加,其超量訊務持續時段也明顯拉長.依據這些 Flooding 異常特徵,本研究運用節點 router Netflow 轉送紀錄,實做 Flooding 異常訊務偵測(Flooding Detection System, FDS).

系統首先選定適當的傳訊特徵, 讀取 NetFlow data,累計/排序相關的訊務數值,再據以偵測 flooding 異常訊務,協助管理人員監看 PortScan, Spam,及 UDP Packet flooding 的具體傳訊數據. 此外,系統也萃取 flooding source IP, 連接 RWhois IP 管理資訊 server 查詢對應的管理人員資訊,自動 email 通知網管,協助端點用戶修補遭感染的系統,主動阻截攻擊或廣告信訊務.

Abstract

The rapid growth in DoS attack, spam and mass-mail viruses has increased the need to develop effective approaches for detecting the significant flooding anomaly. As all traffic between the public Internet and the customer's desktop are interconnected through ISP's access router, it might be feasible and effective for adding an extra level flooding filtering over aggregate networks for detecting the source hosts that launch flooding based DoS attack and delivery huge amount of spam.

This work makes use of the transportation traffic log gathered from backbone router to develop flooding detection system (FDS) that measures and detects the extremely anomalous traffic according to the bulk distribution aspect of the obvious anomalies, including: packet flooding attack, portscan, spam distribution, and packet flooding attack.

FDS system has been deployed in one regional network center over a TANet (Taiwan Academic Network) network center for offering an extra level filtering and assisting network users grasping the significantly anomalous traffic.

關鍵字: PortScan, spam, packet flooding, Flooding detection System.

1. 研究背景

隨著網路的快速擴展,駭客也運用 Internet 的開放特性及應用軟體的弱點,發展惡意蠕蟲程式,廣泛搜尋可利用的連網主機,埋入病毒/後門程式.甚至運用騙術 (social engineering) 誘使收信人點選病毒信,感染連網主機,據以建立龐大傀儡軍團 (zombie army),散播廣告信與發動 DDoS 攻擊,浪費大量網路與伺服系統資源[1].正如網路安全專家的評估所示: 全球約有 1/3 的連網主機因遭病毒感染正被誤用.

雖然有愈來愈多的企業、校園網路管理者與網路用戶選購/安裝 Anti-Virus、 Firewall、IDS (Intrusion Detection System),藉以偵測網段(LAN Segment)上發送異常訊務的主機,防止遭感染 PC 被利用作攻擊跳板.然而仍有相當多的家庭連網,校園網路或小型企業網路用戶,受限於短絀的經費,仍暴露於充斥網蟲的環境. 顯然有必要在網路閘門位置增加一層異常訊務偵測機制,提供大範圍的異常訊務監看,偵測遭感染的主機.

由於遭誤用的異常系統會突發地爆出鉅量特殊訊務:頻繁地傳送超量訊務給單一或多部主

機.所以,源自該類主機的連接數與封包數均呈突然的增加,而其持續傳送超量訊務的時段也明顯拉長.本研究乃利用骨幹 router 送出的 flow-based 轉送紀錄[2], 依據各類 flooding 異常的特性,選定適當的傳訊特徵變量,據以累計/突顯異常訊務.並將統計的多個訊務量與選定的臨界值(threshold)比對,偵測遭病毒感染的源端主機,協助管理人員找出 PortScan, Spam 及 UDP Packet flood 訊務,自動 email 通知管理人員協助用戶儘速修補被網蟲感染的系統,主動阻截 DDoS 攻擊或廣告信散播訊務.

本文於第二節說明 router Netflow 特性,與相關的網路訊務量測研究. 第三節分析 portscan, spam, packet flooding 傳訊特性與其特徵變量的選定,陳述 feature-based 訊務累計與 multi-thresholds 異常偵測程序.說明監看的異常訊務數據.第四節說明 ipRoute SNMP MIB,建置 IP 的管理資訊查詢服務,與異常訊務自動通告系統的程序.最後於第五節做成結論.

2.相關研究

因應網蟲蔓延,spam 與 DDoS 攻擊的不斷成長,許多研究利用 Tcpdump 監聽的封包轉送資訊,或 router NetFlow 網路轉送記錄 實做異常訊務量測,協助掌握問題主機及異常傳訊量.Ntop 訊務監測系統[3]透過訊務統計程式,累計/監看 top-N 連網用戶訊務排行網頁. Wang [4]藉由封包表頭的 TCP SYN-FIN 紀錄,累計網段 SYN 封包數以偵測 SYN flooding 事件.Snort[5]則藉由完整應用封包內容(payload 或 content),歸納病毒入侵與攻擊特徵資料庫,將封包內容與入侵特徵資料比對(signatures matching),偵測具攻擊行為的主機.

Router 位於網路匯集點,其粗略加總的 NetFlow data 將典型的雙向(bi-direction) TCP 傳輸紀錄為兩筆單向的傳輸紀錄: 其一紀錄 source 連接至 destination 的訊務變量,另一則表示由 destination 連接至 source 的傳訊量.Telstra[6]擷取 router NetFlow 轉送紀錄,累計連網用戶的訊務量. FlowScan [7]則利用校園 router NetFlow 資料,加總對應於各 well known Internet 應用 port 的 flow 總數,協助觀察 packet flooding 攻擊.

2.1 PortScan 訊務特徵

PortScan 程式常被駭客用來發掘/感染/集結大量無辜主機,據以發動 flooding DDoS 攻擊與散發大量廣告/色情信.本節依據 PortScan 行為.歸納其傳訊特性,選定適當的 flow 特徵項作為累計與偵測異常訊務的基礎.

網蟲首先利用開放的 TCP three-way handshaking 機制,快速送出 SYN 或 FIN 封包往大量的網路主機, 依據目的主機是否送回 RST 封包,探查具安全弱點的主機群[8].依據圖 2.1 顯示 portscan 通訊的概要模式可發現:portscan 源端主機會同時開啟(forked)多個 process,要求與多個目的主機的弱點 ports 建立連接,再檢視回傳封包 RST Flag,判斷具安全弱點的主機群.我們可以發現其明顯的傳輸特徵:**源端主機要求建立的多個 PortScan flows,集中在特殊的弱點 service ports.** 但由目的主機回應給源端主機的 port number 卻分散於大範圍的 1024 ~ 65535.

本研究 選擇 3 項 NetFlow 辨識特徵:(1)source IP 位址 (src_IP),(2)destination 應用埠(dst_port),與(3)小的 TCP 封包,使 Feature-based 訊務累計程式僅加總超速傳送 SYN|FIN TCP handshaking 封包往大量連網主機特殊弱點 ports 的 source 主機, 為突顯 Portscan 問題主機 (超高速傳送 SYN|FIN 小封包往全球主機的弱點 ports, 企圖發現/集結據弱點主機),

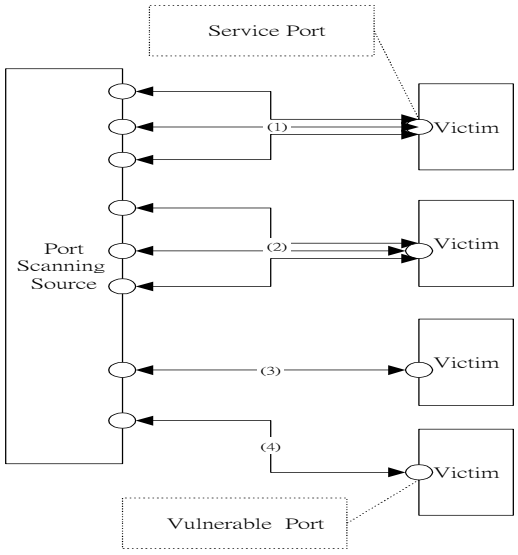


圖 2.1 portscan Communication Model

2.2 SMTP Flooding (Spam) 訊務特徵

為避免回覆大量的 spam complain, Spammer 會藉由自動搜尋程式持續尋找/感染/集結 未設防的網路主機,作為 spam 的 relay 或 sender,重複對龐大的 newsgroup/mailing list 及 mail accounts 傳送廣告信件.甚至透過 mail

夾檔散播病蟲或攻擊程式,侵入網路主機,集結更大量感染主機,寄發/轉送更大量 spam,不僅使得廣大的 Internet 用戶花費可觀的連線費用,時間與精力下載/收取/刪除 spam. ISP 更須耗費龐大的網路資源,系統硬碟及計算資源,重複傳遞/轉送 junk mails [9].

類似 Portscan 傳訊特徵,spam 源端主機 會持續傳送超量 SMTP (Simple Mail Transfer Ptorocol)訊務往多部主機. 若有量測的 SMTP 訊務數據,網管人員便可發現該主機 outbound 的連接數突然暴增,其超量 SMTP 傳送時段也呈明顯拉長.因此,本研究選擇結合 source 位址 (src_IP) 與 25 tcp destination port, 作為 virtual flow index.限制 flooding 訊務累計程式僅加總 由某 source IP 送出的 email 訊務.

2.3 Packet Flooding 訊務特徵

隨著電腦計算效能的快速提升, 駭客得以利用連網電腦,發動 flooding-based DDoS 攻擊: 產出鉅量的 UDP/ICMP Flooding 封包,據以阻斷選定主機的對外服務,壅塞沿徑 routing 網段. 為防止超量攻擊訊務持續擴散,影響沿徑傳訊效能.本研究選擇 NetFlow data 的 source (src_IP) 特徵項為量測的 virtual flow, 限制累計程式僅統計 source IP 傳送 Packet/Byte/ Flow 訊務變量,偵測送出的 UDP / ICMP 超量非自律性訊務的 source IP.自動阻絕與通告 DDoS 攻擊.

3. Flooding 異常訊務偵測系統

FDS 系統包含兩個主要程式: (A) Feature-based 訊務累計,與(B) Multi-Threshold 異常訊務偵測. 前者持續讀入各時段擷取的 Netflow data, 依據選定的 virtual flow 特徵項累計並排序對應於各時段的 flooding 訊務.偵測程式再據以加總每一 source IP 主機送往各 destination port 的 flow 數,packet 數, byte 數,與 mean packet size 訊務變量, 比對多個訊務變量臨界值,突顯 flooding 發送主機及其具體的傳訊變量.

(A) Feature-based 訊務累計/排序程式

為能快速辨識 Flooding source hosts, **Feature-based** 訊務累計程式會周期地讀入 router 送出的 NetFlow data,分別加總各 virtual flow 相關訊務量.包含: 所建立的連接量, 傳送的封包量,與訊務量($flow_h[vr\_flow_i]$, $pkt_h[vr\_flow_i]$, $byte_h[vr\_flow_i]$). 再依建立的總連接量為主鍵排序各 virtual flow 的訊務量.

圖 4.1(a) 顯示累計對應於各時段的top-N PortScan訊務監測網頁.系統紀錄著各source IP送往各 destination port的: flow連接量, 封包量 (packets), 訊務量(bytes), mean packet size 等變量.依據累計的具體訊務數據,網管與用戶可以大略掌握: 那一個源端主機層針對那一弱點port建立頻繁的連接(flow connections),估計異常的訊務臨界值.

(B) multi-thresholds 異常偵測程式

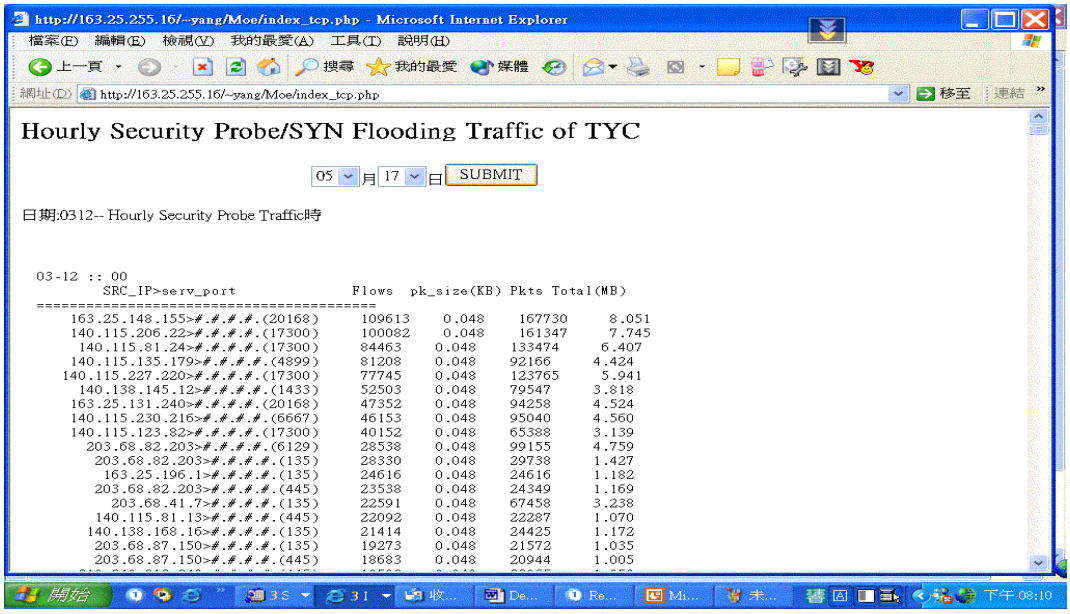
multi-thresholds 異常偵測程式依據各時段累計的 PortScan 訊務變量,再藉由: (1) flow 連接數, (2) flood 持續時數,(3) mean flow rate, (4)packet size,多個訊務變量的比對, 找出持續/快速送出超大量短 TCP 封包訊務的源端主機.

偵測程式首先讀入先前累計的 PortScan 訊務變量,並以 source IP 作為 index,累計該時段 source 主機所建立的 flow 總數(flow[$source_i$]), 所送出的封包總量(packet[$source_i$]),訊務總量(byte[$source_i$]),與平均封包大小(pkt_size[$source_i$]) 等變量.再加總其發送超量 TCP 封包的持續時段(duration[$source_i$] ,推計其每小時建立的平均連接數 (flow_rate[$source_i$].最後,程式將各源端主機的 flow_rate[$source_i$], mean_pkt_size [$source_i$], duration[$source_i$] 等變量,與估定臨界質比對,篩選得 PortScan sources.

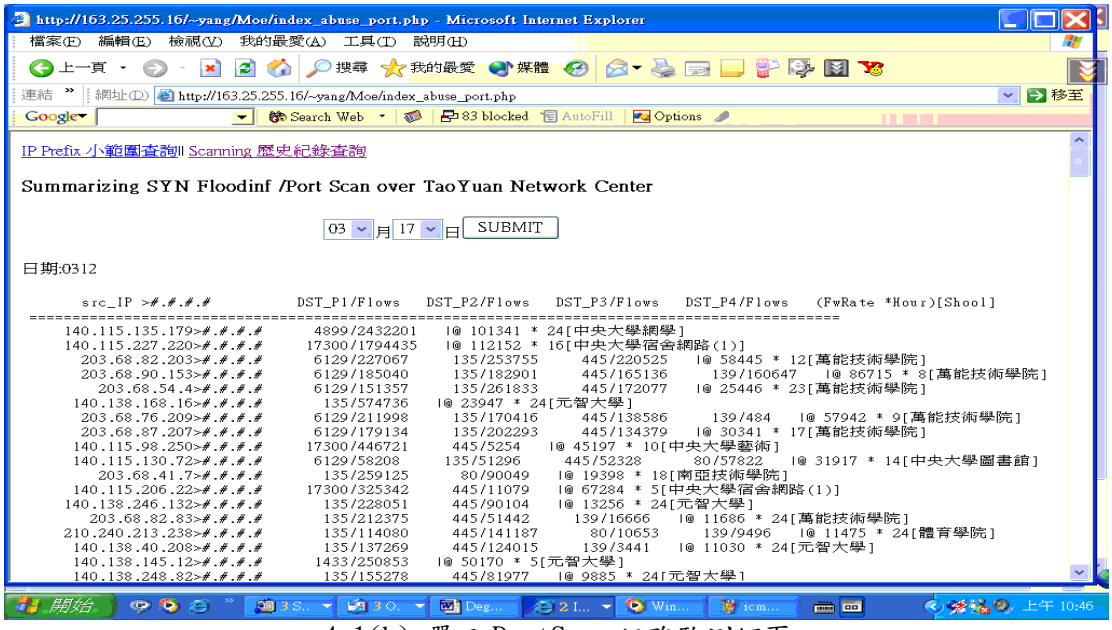
(C) Flooding 訊務的監看

依據偵測的 portscan 具體訊務數據,管理人員能有效地與使用者溝通/解釋其系統可能遭遇的問題,進而修補遭感染的系統. 依據偵測的 PortScan 異常訊務,網管可以掌握: 哪些源端主機針對哪些弱點 port 建立的頻繁連接(flow connection), 及其 PortScan 持續時段,據以判斷/找出遭感染的主機及其送出的超大量 probe 訊務.

以圖 4.1(b) 的單日 PortScan 訊務為例. 某單一 source PC 同時以每小時高達: $O(10^5)$ 至 $O(10^6)$的速率,掃描 17300/TCP port (Kuang2 病毒預留後門), 20168/TCP.(W32.Lovegate 網蟲後門, 135,445/TCP ports (RPC/DCOM), 6129/TCP port (Dameware 弱點). 由於遭感染系統的超量訊務為突然出現, 且持續數小時, 甚至數日之久, 可以清楚判定遭感染的大量網路主機. 圖 4.2 與 4.3 為單日的 spam 與 packet flooding 訊務監測網頁.



4.1(a) 單時段的 PortScan 訊務監測網頁



4.1(b) 單日 PortScan 訊務監測網頁

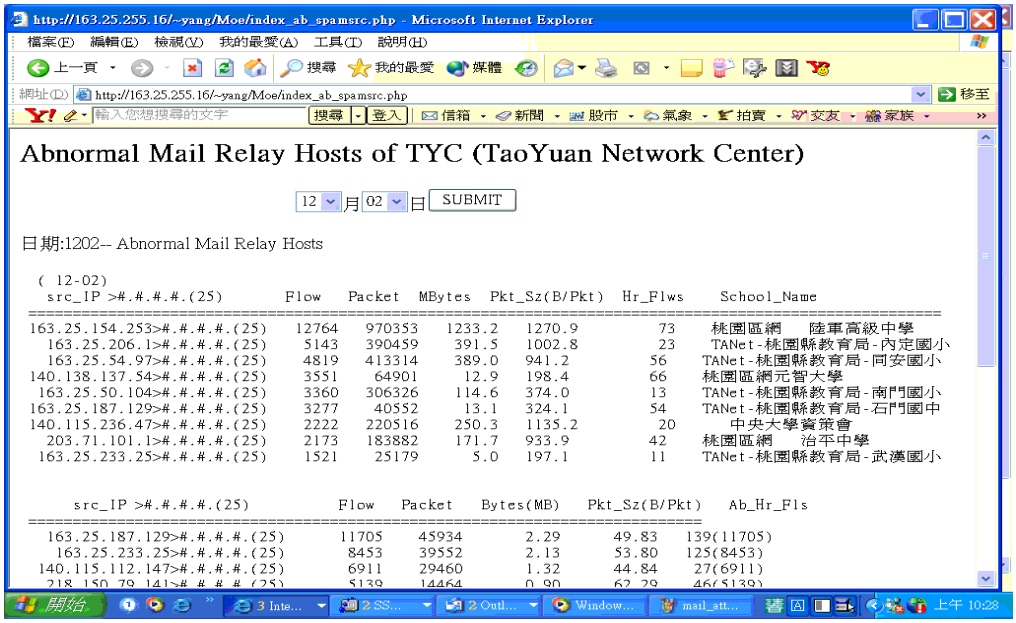
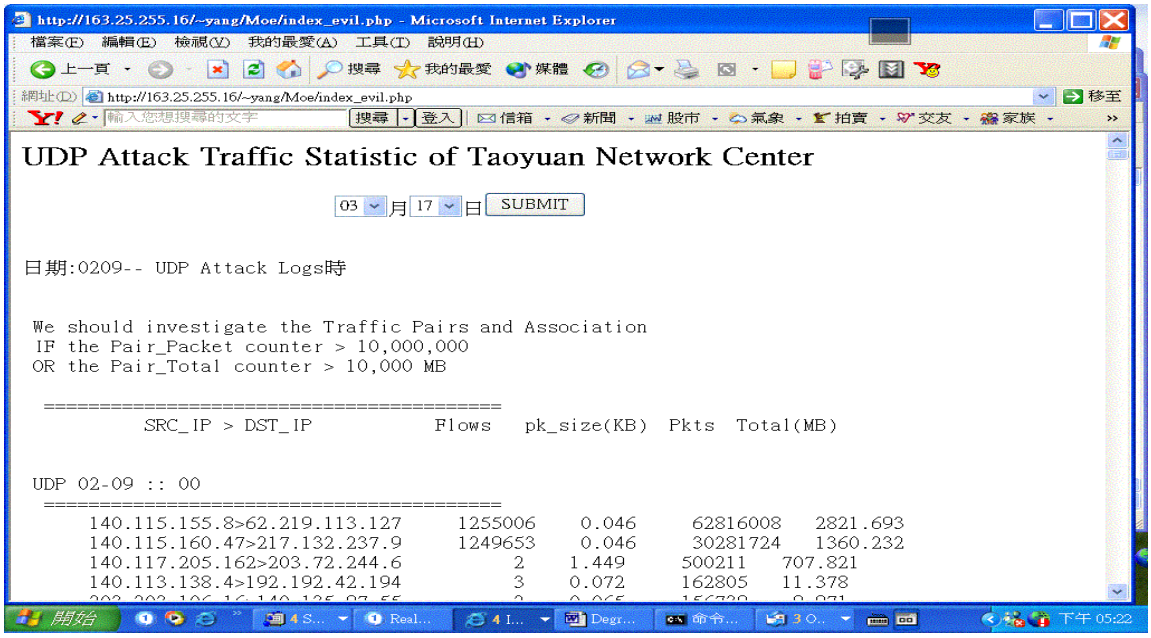


圖 4.2 單日的 spam 訊務監測網頁



4.3 單日的 packet flooding 訊務監測網頁

4. Flooding 異常訊務的自動通告

Simple Network Management Protocol [SNMP, 10] 定義的管理資訊儲存結構,不僅提供網路設備間方便的資訊交換管道;也允許網管人員藉由 SNMP pulling 應用程式擷取連網介面 (Interface) 訊務量、傳訊錯誤,ipRoute 等 MIB,發現與排除網路問題.

本研究藉由 University of California David (UCD)的 snmpwalk 程式,擷取骨幹 router 的數萬筆 ipRouteMask 與 ipRouteNextHop MIB,據以萃取/重建龐大 ip_routing 紀錄 [11].並參照連線單位的聯絡紀錄檔完成 IP 管理資訊查詢系統,實做異常訊務自動通告機制.

4.1 ipRoute SNMP MIB

IP 邏輯位址並不包含任何管理資訊據.為自動通告 flooding 源端主機用戶,提升 flooding 事件處理效率,系統需結合 routing table 與網路管理人員聯絡紀錄,建立 RWhois 資料庫 [12], 提供 IP 管理資訊查詢服務,方便管理人員依據 IP 位址查詢對應的 Admin-Contact (管理人員), Email address, Tel(聯絡電話), Updated-By(資料建立者),Updated (資料建立日期) 等資料.

系統首先藉由 snmpwalk 程式擷取 router ipRoute MIB 分支下的 ipRouteMask (1.3.6.1.4.21.2.1.11)與 ipRouteNextHop MIB (1.3.6.1.4. 21.2.1.7) 紀錄,儲存於 **NetMask** 佇列與 **NextHop** 佇列 (以 IP 網段位址為 index).最後,整合 NetMask, NextHop 佇列資訊,獲取 ip_routing 紀錄並存檔. 其次,系統再重複讀取各筆區網 routing 紀錄,並依據 NextHop 紀錄比對/萃取對應的管理聯絡資訊,構建符合 RWhois network schema 關聯紀錄檔,建立資料庫 indexing,建置與啟動 RWhois IP 管理資料查詢系統,作為自動通告機制的基礎.

4.2 異常訊務數據的自動通告

藉由 FDS 偵測的具體數據與 Rwhois IP 管理資訊查詢服務, 自動通告程式得以讀取偵測的 flooding source IP 紀錄,呼叫 Net::Rwhois.pm Perl 模組程式,遠端連接 RWhoisd server,比對/回應相對的 IP routing 與管理資訊後, 再呼叫 Mail::Sendmail.pm 模組程式,將偵測的異常訊務紀錄 email 通告該網段管理人員或用戶. 簡述 FDS 異常**通告**程序如下:

Step_1: 讀取偵測的異常訊務紀錄檔, 萃取各 source IP 位址.

Step_2: 呼叫 Net::Rwhois.pm,遠端連線 RWhois server,查詢 source IP 對應管理資訊,萃取管理人員 email 位址.

Step_3:萃取/暫存各異常發送源的 flooding 訊務數據,呼叫 Mail::Sendmail.pm,將具體的 flooding 訊務通告管理人員,請求儘速修補遭誤用的系統.

5. 總結

本研究利用 aggregate router 的 NetFlow 轉送訊務紀錄,實做 Flooding 異常訊務偵測系統(FDS).自動偵測 PortScan, spam 與 packet flooding 攻擊訊務,並透過 Rwhoisd IP 管理資訊的查詢,自動將具體的異常訊務通告該網路用戶,促使其補強系統安全,阻截 flooding 攻擊.

依據幾年來的使用經驗,我們確定建置於網路匯集點的異常偵測系統, 不僅能偵測多變的 portscan 訊務 (不斷翻新的弱點 ports), spam 與 packet flooding 事件,累計的多個具體 flooding 訊務數據,更能協助網管人員掌握異常源端主機,聯絡用戶並分析其主機 flooding 現象.

然而,網路匯集點的 FDS 系統也與一般網段或端點主機的 IDS 系統一樣: 存在著誤判的問題.雖然拉高 thresholds 值可以改善,但會有"漏網之魚"的顧慮. 誤判問題將是研究的下一項改進重點.

參考文獻

(1) Bellovin S.M., Security Problems in TCP/IP Protocol Suit, Computer Communication Review, vol. 19, No. 2, pp. 32-48. April 1989.

(2) Cisco IOS Netflow Technology, http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/ iosnf_ds.htm.

(3) Luca D.; Finsiel S.A., Effective Traffic Measurement Using Ntop, IEEE Communications Magazine, May 2000, Pages: 138-143.

(4) Wang H.; Zhang D.; Shin K. G.; Detecting SYN flooding attacks, twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002), Volume: 3, Jun 2002, Pages: 1530 - 1539.

(5) Roesch M., Snort - Lightweight Intrusion Detection for Networks, Proceedings of 13th Systems Administration Conference (LISA '99), Nov 1999, Pages: 229 - 235.

(6) Telstra G.; Measuring IP Network Performance, Internet Product Journal, March 2003, Pages: 2-19.

(7) Plonka D., FlowScan: A network traffic flow reporting and visualization tool, Proceedings of 14th Systems Administration Conference (LISA 2000), Dec 2000, Pages: 305 - 317

(8) Urupoj K.; Surasak S.; Wipa J., A Rule-based Approach for Port Scanning Detection, Electrical Engineering Conference (EECON-23), Nov 2000.

(9) Levy, E.; The making of a spam zombie army. Dissecting the Sobig worms, Security & Privacy Magazine, IEEE, Volume: 1, Issue: 4, July-Aug. 2003, Pages: 58 - 59.

(10)Request for Comments: 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II, 1991.

(11)Request for Comments: 1354, IP Forwarding Table MIB, July 1992.

(12) Request for Comments 2167; Referral Whois (RWhois) Protocol V1.5. S. Williamson, M. Kosters, D. Blacka, J. Singh, K. Zeilstra. June 1997.