Intrusion Detection: a Network View

林鳳銘、吳守豪、李蔡彥

國立政治大學電算中心

l96in@nccu.edu.tw、swu@nccu.edu.tw、li@nccu.edu.tw

摘要

目前 TANet 上許多單位都已經建立網路流量統計資訊，也能夠根據網路上的流量，作為改善網路服務品質的參考。本文中，我們將建立一個進一步的分析這些流量資訊的機制，以萃取出某些異常流量的行為模式並加以分類，使其成為有利於偵測網路入侵的資訊。這些資訊可以提供給網路管理人員作為網路異常現象的參考，同時對伺服器管理者而言，也提供了某些異常連線的資訊。以期能夠在系統入侵的初期，及時防止並減少因入侵所引發的破壞性。

關鍵字：網路流量分析，網路入侵偵測

1. 簡介

在網際網路不斷的發展之下，網路中的流量迅速地增加，入侵與攻擊的事件層出不窮。當發生入侵事件時，經常會影響到某些特定的服務，如：E-mail，World Wide Web 等。為了進行攻擊，入侵者通常會在網路上散播一些掃瞄用的封包，來找出防禦力較弱的主機。因此，雖然已經建立了流量統計的資訊，不過大多是採用 SNMP[1] 的方式，來取得路由器或交換機上流量的相關資訊，如果想要偵測伺服器上的流量，伺服器上就需要安裝 SNMP Daemon，並根據相關的 MIB 資訊來觀察。當伺服器使用不同的平台時，還必須為每一種不同的作業平台，安裝不同的 SNMP Daemon。SNMP 所提供的資訊通常是經過計算後的統計數值，如果想要取得更詳細的資訊，還要進一步分析不同伺服器所產生的 log 檔。

為了入侵某一部伺服器，入侵者可能會採取不同的方法與步驟來嘗試入侵，這裡我們並不討論伺服器上的防護行為，而把重點放在網路端，來觀察入侵行為發生時，網路端是否有些異常現象，可以作為事先防範的基礎。當入侵者不斷傳送少量的偵測封包給一群伺服器，對每一部伺服器而言，只收到少量的封包，這些少量的異常封包很容易被伺服器管理者忽略，而失去找出入侵者的機會。

為了偵測入侵行為，有許多不同的偵測方法被提出，在[2] 偵測了網路架構中路由器上路由表的運作情形，以避免因為某些路由表的項目被更動而影響到許多封包的轉送，而發生入侵的情形。[3] 提出了以不斷偵測網路鍊結的流量情況來達到入侵檢測的功能。有也以分散式的方法來收集網路上封包，並加以分析來找出可能發生入侵的情況[4]。

這裡我們提出了一個偵測機制，可以在網路端建立起同時偵測網路流量與伺服器連線資訊的機制，以方便我們在入侵發生的第一時間，做出必要的保護措施（可以從路由器或是交換器上阻隔攻擊者），並透過一些工具及時地通知伺服器的管理者檢查伺服器的狀態，或進行漏洞修補的動作，來將入侵所造成的影響減到最低。

2. 網路流量資訊的收集

由於所有的封包都必須透過路由器來傳送，因此如果路由器能夠將封包的一些相關資訊如：封包來源端 IP 位址、封包所使用的埠號、封包的接收端 IP 位址與接收端應用程式的埠號、封包的數量與採用的通訊協定等資訊匯出，我們就可以在網路端觀察封包的行為。

對 Cisco 7000 系列路由器而言，可以在每一個需要 export 流量的介面上執行 ip route-cache flow 指令，並且在 global configuration 底下以 ip flow export xx.xx.xx.xx:9999 指令指定一個接收 UDP 封包的伺服器(xx.xx.xx.xx)與埠號(9999)，就可以將需要 export 的封包傳送到某一部伺服器上。在該伺服器上還必須要有一個接收路由器送出流量資訊的 daemon，不斷地接收路由器送出的流量資訊。

我們以圖 1 來說明流量資訊收集的方式。在圖 1 中，每一個需要將流量 export 出來的介面都會透過網路以 UDP 的方式將封包傳給圖中 Netflow 伺服器上的 daemon[5]，這個 daemon 會收集從 Router 上傳過來的資訊，並以每 10 分鐘對所收集的資料產生一個獨立檔案的方式定期地產生有關網路流量資訊的 log 檔。

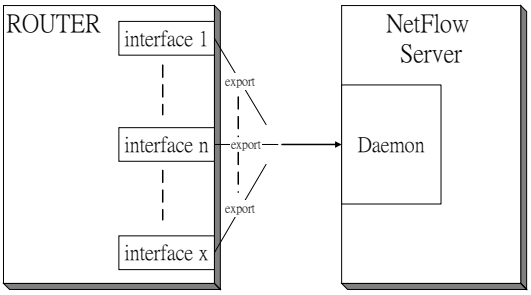

圖 1. 流量資訊的收集。

3. 流量資訊的格式

本文中我們所用到的資料是透過路由器上的介面 export 出來，然後由 Netflow Server 上的 daemon 接收，最後會以檔案的方式儲存在 Netflow Server 上。由於這些資訊是根據 Cisco 所提供的 netflow 技術規格[6]輸出，因此這些資料檔還需要以特殊程式處理，才能成為有意義的資訊。圖 2 就是經過處理之後，路由器上每一個介面所傳送出來的資料格式：

Source Interface	Source IP Address	Destination Interface	Destination IP Address	Protocol	Source Port	Destination Port	Packets	Octets

Source Interface：路由器上資訊流的來源端介面。
Source IP Address：資訊流的來源端 IP 位址。
Destination Interface：路由器上資訊流的接收端介面。
Destination IP Address：資訊流的接收端 IP 位址。
Protocol：資訊流所使用的通訊協定。
Source Port：資訊流發送端所使用的埠號。
Destination Port：資訊流接收端程式所使用的埠號。
Packets：資訊流等於多少個封包。
Ocets：資訊流的大小。

圖 2. 流量資訊的格式。

基本上，由於 Netflow Server 上的接收程式每 10 分鐘會產生一個新的流量檔，所以每一個流量檔是這個路由器每 10 分鐘所處理的資訊總量。流量檔所儲存的每一列都是一個資訊流(flow)，圖 2 就是每一個資訊流內所含有的資訊。

4. 流量資訊的分析

根據圖 2 中有關資訊流的內容，我們可以計算每一個 IP 所傳送與接收的流量大小，並以統計圖表來觀察每一個 IP 所使用的網路資源。不過這不是本文的重點，本文將從這些流量資訊中尋找一些有用的訊息，並透過不同的分析方式，試著歸納出一些與網路入侵相關的行為。

4.1 掃瞄

首先，我們以尋找掃瞄者為例，對掃瞄而言，事實上並沒有對被掃瞄者進行破壞或入侵的動作，而是用來搜尋網路上主機的相關訊息，包含了：網路主機提供了哪些服務、提供服務程式的種類與這些程式是否含有漏洞等。掃瞄者的行為很容易分析，他們會對某些子網路(subnet)循序地加以掃瞄，對流量資訊來說，我們會發現某一個來源端的 IP 在某一段時間內會對某一子網路內的所有的主機傳送少量的封包。

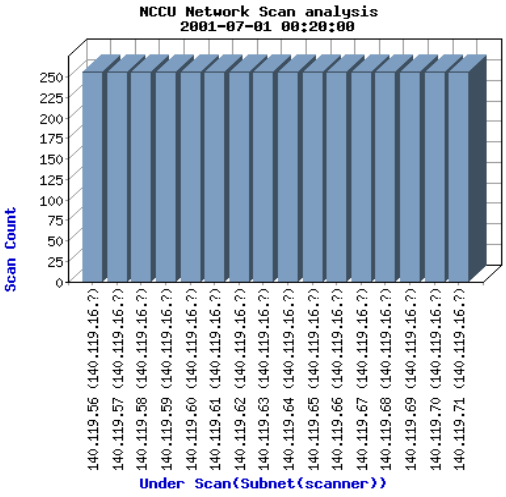

圖 3. 被掃瞄的子網路。

根據網路流量資訊，我們找出了在 2001-07-01 AM 00:20:00 這段時間內，對 NCCU 校內的某些子網路進行掃瞄的資訊，在圖 3 中的 X 軸列出了被掃瞄的子網路與掃瞄者 IP（為了保密原則，IP 的最後一碼我們用？表示），Y 軸則是該子網路被掃瞄的次數。在這裡我們發現掃瞄者通常會對一段連續的網路（如圖 3 中的 140.119.56～140.119.71）內所有可能存在的主機進行掃瞄，所以圖中的掃瞄次數幾乎都相同。當我們藉由分析路由器送出的流量資訊而找到掃瞄他人機器的機器管理者後，我們發現到一個現象是，有許多掃瞄他人機器的主機並非是入侵者所使用的機器，而是這些機器已經被入侵者控制，並用來作為入侵其它機器的跳板。

4.2 針對特定 IP 的攻擊

如果入侵者分析掃瞄後所的到的資訊，找到了可以被攻擊的主機後，下一步就是進一步的攻擊行動。就網路的觀點而言，這裡指的是某一部或某一群主機針對某一台主機的攻擊行為，這種攻擊方式很像阻斷服務（DOS）或是分散式阻斷服務攻擊（DDOS）。經過我們分析網路流量資訊檔後，會發現某一部主機 10 分鐘內會接到數千甚至數萬個資訊流。就一台正常服務的主機而言，我們可以發現它正處於被資訊流淹沒的狀況。圖 4 列出了 NCCU 校內，八月四日當天每個 10 分鐘內，疑似遭到攻擊的主機（10 分鐘內的資訊流超過 1000 次）。

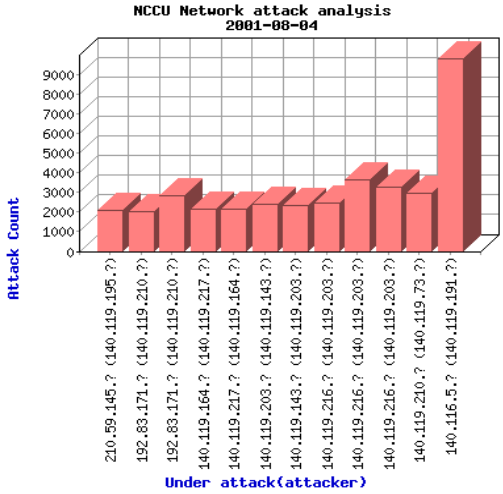

圖 4. 疑似遭到攻擊的主機。

圖 4 中的 X 軸中的 Under attack (attacker) 前面的資訊是被攻擊者的 IP，大括號中的數值則是攻擊者的 IP。Y 軸 attack count 是以 10 分鐘為單位來計算的資訊流數量。舉例來說，140.119.216.?(140.119.203.?) 表示 10 分鐘內 140.119.203.? 這部機器對 140.119.216.? 共傳送了約 2000 多個資訊流，經過換算也就是每秒要求傳送 3.3 個資訊流，除非這兩部機器因為特殊要求不斷進行一些測試動作，除此之外，很有可能 140.119.203.? 正在對 140.119.216.? 進行攻擊。

4.3 針對特定埠號的攻擊

本文我們所謂的針對特定埠號的攻擊是指某一部主機利用網路，攻擊不同主機或相同主機特定埠號的行為。這種攻擊方式與最近很流行的 Code Red Worm [7]病毒的攻擊方式很相似。

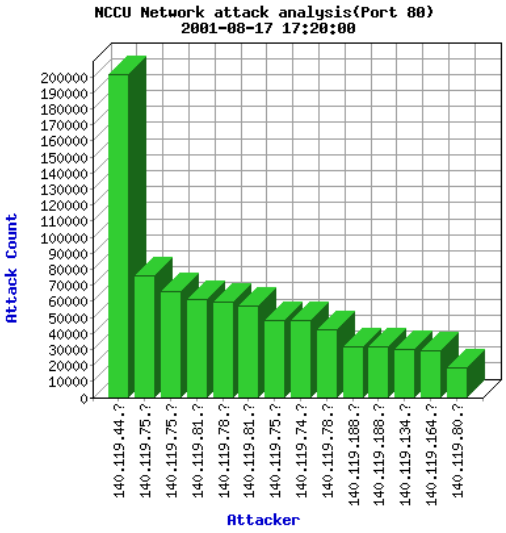

圖 5. 攻擊某些特定埠號的主機。

圖 5 我們列出了在 2001-08-17 17:20:00 經過分析所得到向外攻擊 port 80 的資料，圖中我們發現有許多主機不斷利用 port 80 企圖與其它主機建立連線，以 140.119.44.? 為例，在 10 分鐘內這部主機一共對外建立了約 200000 次 port 80 的連結，也就是大約每秒對外 333.33 個資訊流。這就是目前 Code Red Worm 針對 www port(80) 的攻擊模式。

5. 及時偵測與預防

就網路端的入侵偵測系統而言，其中最重要的一件事是：當發現伺服器出現異常狀況時，系統的處理方式。對我們所設計的機制來說，由於 netflow 伺服器不斷地接收來自路由器所送出的流量資訊，並且在每次產生一個新的流量資訊檔時（每十分鐘），就立刻進行上一個流量資訊檔的分析工作。我們可以及時地將發生異常現象機器的 IP 位址公告於網頁上。對個別被入侵的機器而言，我們則即時透過 e-mail 來通知管理者，伺服器目前所遭遇到的危機。在一段時間內，如果我們所認定的疑似被入侵系統並沒有加以處理，我們還可以在相關的路由器或交換器上執行阻隔該伺服器封包的動作，而將該伺服器孤立，以避免因為被入侵的伺服器管理者無法及時處理而造成更嚴重的破壞行為。

6. 結論

在網路端執行安全性流量偵測的優點是可以在網路入侵的初期，就能發覺異常的現象，也可以避免因為伺服器管理人員的疏忽而造成更嚴重的破壞。如果網路管理人員與伺服器管理者能相互合作與支援，將可以更有效地預防入侵行為的發生。

除了安全外，在網路端分析網路流量資訊不但可以幫助網路管理者瞭解網路的流量情形，找出網路流量的異常點，使網路管理人員能夠提早發現問題所在而提出有效的改善方案。

本文中所建立的網路流量分析機制，是根據來源端與目的地端的 IP 來分析異常流量，如果來源端的 IP 是假造的，就無法正確地找出真正的攻擊者，這是本文的限制所在。

7. 參考文獻

[1] Paul Simoneau, SNMP Network Management, *McGraw-Hill*, May 1999.

[2] Y. Frank Jou, Fengmin Gong, Chandru Sargor, Shyhtsun Felix Wu, and Cleaveland W. Rance Architecture design of a scalable intrusion detection system for the emerging network infrastructure. Technical Report CDRL A005 Dept. of Computer Science, North Carolina State University, Releigh, N.C, USA April 1997.

[3]Vern Paxon. Bro:A system for detecting intruders in real-time. In proceedings of the 7th USENIX security symposium, San Antonio,TX, USA Jan 1998.

[4]H. S. Tavitz and A. Valdes. The SRI IDES

Statistical Anomaly Detector. In Proceedings of the IEEE Symposium of Security and Privacy, May 1991.

[5]ftp://ftp.net.ohio-state.edu

[6]http://www.cisco.com

[7]http://www.eeye.com/html/Research/Advisories/AL20010717.html