Seminar3 — 資安事件防護與處理簡介

演講者: 資策會 南資處 辜國隆 處長

2003.10.13

報告撰寫者： 政大資科所碩一 謝淳達 92753008

1 演講主題及摘要

近年來電腦科技一日千里, 電腦網路也慢慢融入人類的生活, 不論是工作或是日常生活, 網路都帶給我們相當大的便利。然而網路的進步也帶來電腦安全新的危機。越來越多的怪客利用網路無所不在的特性, 在虛擬世界中對其他電腦發動「網路攻擊」, 企圖透過網路癱瘓其他電腦, 造成企業的損失或是竊取他人的資料等等。因此, 我們必須加強對「資訊安全」的認識, 並了解怪客們的攻擊手法, 進而研究因應之道, 以確保我們的資料能夠不被破壞或竊取。

2 要點整理

「資訊安全」的主題非常廣泛, 但主要可以分成「怪客入侵」、「電腦病毒」、「實體安全」等等議題。

怪客們的網路攻擊手法可說是花招百出, 防不勝防。DoS (阻斷式攻擊,Denial of Service) 是最近常見也是最好的一種網路攻擊手法。主要是在網路上丟一大堆封包給想要攻擊的電腦, 然後該電腦會爲了一一回應這些惡意的封包, 而負載過重導致程式當掉。但目前由於沒有一個有效的辦法讓電腦本身判斷一個符合規定的封包是否由一般使用者傳來的, 所以幾乎可以說是束手無策。

爲了避免被查出是誰惡意攻擊他人電腦, 怪客們都會先入侵其他不是攻擊目標的電腦來當作「跳板」, 然後再由這些「跳板」對眞正的目標發動攻擊。找到的「跳板」越多, 封包就越多, 而使得攻擊效果更顯著。

然而一般電腦使用者, 甚至是一般公家機關或學術單位理的電腦管理者, 由於不熟悉電腦, 沒有作好應有的安全防護, 所以常常會被怪客拿來當做跳板攻擊其他電腦。前一陣子台灣的政府網站被大陸的怪客入侵就是利用這一點, 由於台灣政府的網路都有設定大陸網路無法直接連通, 所以大陸的怪客都利用民間的電腦當作跳板, 進而攻擊台灣政府的網站。爲了避免這類事件再次發生, 所有電腦使用者都必須更重視資訊安全的重要性, 及時做好防護措施。

「電腦病毒」也是怪客常用的攻擊手法。例如前一陣子很熱門的 MSBlast (疾風病毒) 便是利用 Microsoft Windows 上的 RPC (遠端存取服務) 的漏洞, 使全世界許多公司的電腦系統立即癱瘓。

此外, 電腦設備的「實體安全」也是不容忽視的一環。有許多公司常常會致力於電腦管理上的保護, 卻往往忽略了電腦硬體「本身」的安全。例如去年底有某家公司發生火災, 幸好該公司經常作「異地備援」的工作, 所幸資料沒有遺失。

3 評論

有許多網路攻擊手法都屬於DoS 攻擊. 其中一種方法就是 SYN Flood 攻擊法。我們在網路概論都有學過, 在建立 TCP 封包前必須有 handshaking 的動作, 而這個動作的第一步就是要由客戶端送出 SYN packet。如果怪客故意只丟 SYN Packet 假裝要跟伺服端連線, 就會造成伺服端負荷過大而癱瘓。

還有一種更厲害的 DoS 攻擊手法是利用 UDP 封包。跟一般我們常用的 TCP 不同之處在於, 這種封包不需要在伺服器端跟客戶端之間確立連線, 所以駭客們可以利用這種特性送出揑造的 UDP 封包給某台電腦 (將封包內的來源 IP 改成欲攻擊的電腦), 一但該電腦收到這些封包, 就會自動傳更多的封包「回應」給揑造的來源 IP, 進而使其癱瘓。

很多 Linux 的書籍都會提到, 爲了避免系統被入侵, 系統管理者最好定時更新系統及

其應用軟體, 因爲世界上沒有一套軟體是絕對安全無漏洞的, 所以軟體作者都會每過一段時間就釋出 bug fix 的版本。此外, 由於軟體多多少少都會有漏洞, 所以如非必要, 也盡量少開一些網路上不必要的服務, 例如 sendmail(mail server)、bind(dns) 等等。此外, 架設防火牆也是非常有幫助的, 我們可以透過防火牆設定允許的來源 ip 和 port , 不但可以防止某些 DoS 攻擊 (因爲可以透過防火牆將這些封包直接丟棄不予理會, 就不會造成系統癱瘓), 也可以避免某些後門程式將私人資料透過網路傳送到其他地方。像是企業網路就常常透過防火牆或是建立 NAT 來保護企業內部的電腦資訊安全。某些作業系統, 如 FreeBSD , 甚至可以設定 ICMP(一種可利用來作 DoS 攻擊的封包格式) 數量上限, 避免系統因爲忙於回應此種封包而癱瘓。

電腦系統的權限設定也是很重要的一環。電腦系統必須有支援權限的設定, 網管人員也有義務將重要的機密資料設定存取限制。

之前曾經看過一本雜誌, 上面寫說國外有一家公司, 他們的電腦控管的非常嚴謹, 權限設定以及入侵防護也都作的相當的好。然而, 不幸的是有一天他們的重要機密資料仍然外洩了。而外洩的方法卻是有公司內部的職員「透過列表機將資料印成紙本」然後竊取。由此看來, 資訊安全的確有許多漏洞, 除了電腦管理上的問題之外,「制度」的重要性也是不容忽視的。

除了網路攻擊以外,「密碼」也是最常見的資訊安全問題。像是最近最重大的資訊安全事件大概就是密碼搞的鬼了。約一個月前有個集團開始在南部某些 ATM 櫃員機裝上密碼「側錄」裝置側錄提款人的金融卡密碼, 在收集了一個月之後, 前幾天該集團陸陸續續盜領了五十幾位民衆的存款, 目前盜領金額高達五百萬元, 並且持續增加中。爲了避免這類事情發生, 除了存款人必須要經常更新自己的密碼以外, 盡速將金融卡「晶片化」更是刻不容緩。

另外就是, 許多人常常都把「駭客 (haker)」以及「怪客 (cracker)」混爲一談。其實這兩個名詞的意義是有明顯的區別的。「駭客」其實是用來形容那些電腦高手, 他們樂於研究電腦, 並且將自己所學與人分享。然而, 後來有一些「自稱」「駭客」的年輕人, 專門用電腦侵入其他電腦系統甚至破壞, 這些人被稱爲「怪客」。很不幸地, 許多作家以及記者均稱這些人爲「駭客」, 以致於大家以訛傳訛誤用這兩個名詞。

4 相關資料

駭客跟怪客的定義：http://www.angelfire.com/ok/leekawo/hacker.htm
鳥哥的 Linux 私房菜：http://www.vbird.org/