網路攻防平台實作：系統入侵之建置

康厚斌[1] 程凱[1]

[1]陸軍軍官學校資訊學系

摘要

本次的研究議題，主要是利用網路攻防平台進行系統入侵之建置，做出相關拓樸，實際了解到系統入侵之前會做些什麼，像是掃描(Scan)、列舉(Enumeration)、執行(Execute)等，最重要的是如何入侵目標主機的系統，入侵後可以做出哪些事情及造成的危害，除此之外，也會將系統入侵建置時可能會發生的問題列出及解決，藉此讓其他使用者在此平台實作時可避免發生相同錯誤，以此提升自我的資訊安全知識與技術。

關鍵詞：網路攻防平台、系統入侵、列舉

一、前言

資訊安全在 21 世紀被認為是亟需關注的議題，電腦、通訊軟體、手機的普及，給予個人生活上的方便，但方便的背後往往有許多安全上沒注意到的問題，例如：在製作軟體時是否有程式碼撰寫不夠完全，造成整個軟體的漏洞，讓他人有機會竄改程式碼使其變成惡意軟體；亦或是在登入軟體或系統時，設定的帳號及密碼不夠複雜，使他人容易隨意猜測而登入獲得資料等等；每個細節都應該去注意，才不枉費前人所創造出來的方便被有心人士加以利用，但要怎麼知道軟體裡是否有疏漏的部分，就要透過實驗研究來做檢查及發覺，因此利用網路攻防平台的環境來做相關的研究，除了能瞭解上述所說之外，也可以增強在未來遇到類似問題時的處置及應對。

二、相關工作

2.1 系統入侵簡介

在這裡的系統是指作業系統(Operating System)，是管理硬體與軟體資源的程式，同時也是系統的核心與基石。作業系統需要處理很多事情，如配置記憶體、決定系統資源供需的優先次序、輸入與輸出裝置、操作網路與管理檔案系統等等，提供一個讓使用者與系統互動的操作介面。作業系統型態有很多樣，不同機器安裝的作業系統可從簡單到複雜。像是有些作業系統整合了圖形化使用者介面，有些僅能使用命令列介面[1]，現在除了電腦有作業系統外，逐漸被應用在平板及手機中，但以電腦發展最為前面，目前也是電腦發展出來的作業系統最多，例如：Windows、Mac、Linux、Unix 等等，每個作業系統都有不同的功能讓各種喜好的使用者來操作；在 Linux 系統，是開放原始碼[2]，提供給程式設計者進行修改，其中有一套專門用來當作駭客的作業系統，叫

做 Kali Linux，Kali Linux 擁有超過 600 個預裝的滲透測試程式，包括:Armitage(圖形化網路攻擊管理工具)、Nmap(服務掃描工具), 、Wireshark(網路掃描工具)、password cracker 等等[3]，資安人員也用此系統做研究。我們在建置此次的系統入侵設計架構裡也會用到此系統進行掃描，得到所需要的資訊進行入侵，入侵的系統是 Windows XP，由於經費問題未在此平台購買 Windows XP 以上版本，因此避免涉及侵權問題，故使用 Windows XP 進行實驗操作，Windows XP 是微軟公司推出供個人電腦使用的作業系統，延伸支援已於 2014 年 4 月 8 日終止服務[4]，基於使用者眾多，所以此系統僅不支援服務，但仍可以使用。

2.2 系統入侵步驟

2.2.1 目標鎖定，資源搜尋

首先駭客想要攻擊一個目標，往往會先蒐集目標公司或網域的相關資訊，其手法不外乎是上目標機構或組織的網站，或是透過搜尋引擎搜查相關的資訊，駭客比較在意的資訊包括:組織坐落的地址、相關的公司或機構、網域名稱、管理聯絡人、登記者、DNS Server 的名稱等等。

2.2.2 主機掃描

聰明的駭客也知道系統有裝設防火牆，在沒有十全把握之前不會貿然的對目標主機進行掃描的動作，駭客會用 Ping 的手法來看看系統對 Ping 的回應，也會用 Traceroute 這個工具來觀察在目標主機與自己之間有多少主機存在，哪些可能是防火牆，哪些是 router，再依狀況不同來擬定攻擊手法。

2.2.3windows 資源列舉

Windows 系列的作業系統提供的列舉方式將會把你電腦裡面的秘密開放出來讓駭客參考。駭客可以對目標主機建立一個空連線，透過此方式得到目標的主機名稱、網路卡編號、群組、帳號等資訊，如果進一步的猜出系統管理員密碼，它更可以遠端連上主機，擁有一切的權限，這對系統的危害相當的大。

2.2.4 入侵系統

入侵系統的方式有很多種，駭客常用的方式大致為下列幾項：密碼破解、木馬、應用程式漏洞或系統服務漏洞、Sniffer(監聽器)監聽、DoS/DDoS 攻擊等等[5]，本次研究主要是以 Windows XP 的系統漏洞進行入侵，雖然 Windows XP 已經不再被大多數使用者使用，且 Microsoft 也讓此系統停止更新，但可以藉由此系統學習到一般人不會去注意的事情，之後在使用其他電腦時可以去找尋有無相同的漏洞，以確保自己的檔案及個人資料有無遺失，除了查看這些，還會寫上關於在建置此平台發生的問題及解決方案，以供後續研究使用。

三、實作系統入侵之建置

3.1 前置作業

進行系統入侵建置之前，要先建立實驗所需的環境拓樸，此實驗分成兩個部分，第一部分拓樸是設定兩台主機，利用列舉法的方式掃描目標主機獲得相關訊息，作業系統皆為 Windows XP，圖 1 中有一台交換器及兩台主機。

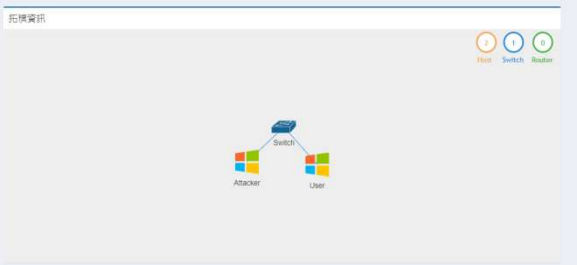

圖 1.前置作業-第一部分

第二部分就要針對上述拓樸所得到的

結果進行系統入侵，所以在此部分從圖 2 可以看到有三台主機，兩台 Windows XP、一台 Kali Linux，在 Kali Linux 中扮演極為重要的角色，用來破解目標主機的帳號及密碼。

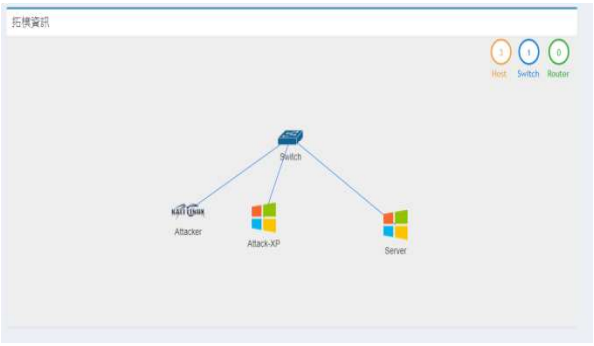

圖 2.前置作業-第二部分

設定完拓樸之後，要設定此實驗的主機 IP，Kali Linux 設定為 192.168.36.129，Windows XP 攻擊主機設定為 192.168.36.130，目標主機為 192.168.36.138，各個主機的子網路遮罩皆設定為 255.255.255.0。

3.2 實作一-利用 Nbtstat 進行 Enumeration 的資訊收集

3.2.1 Nbtstat 介紹

實作一是為了在系統入侵前使用系統指令 Nbtstat 收集相關訊息，Nbtstat 主要是幫助 NetBIOS 解決問題並分析，當網路是正常運作時，TCP/IP 上的 NetBIOS 將其名稱解析為 IP 位址[6]，Nbtstat 的參數如表一所示。nbtstat 指令：nbtstat -a [RemoteName] [-A IP address] [-c] [-n][-r] [-R] [-RR] [-s] [-S] [interval]，RemoteName 遠端的主機電腦名稱。IP address 以點分隔表示 IP 位址的十進位數。interval 重新顯示選取的統計資料時，每次顯示之間的暫停間隔秒數。例子：nbtstat -A 192.168.36.138(此為 IP address)

表 1. Nbtstat 參數

參數	說明
-a	(介面卡狀態) 列出指定其名稱的遠端電腦名稱表格
-A	(介面卡狀態) 列出指定其 IP 位址的遠端電腦名稱表格
-c	(快取) 列出 NBT 快取的遠端電腦名稱和它們的 IP 位址
-n	(名稱) 列出本機 NetBIOS 名稱
-r	(已解析) 列出由廣播和透過 WINS 解析的名稱
-R	(重新載入) 清除和重新載入遠端快取名稱表格
-S	(工作階段) 列出有目的地 IP 位址的工作階段表格
-s	(階段作業) 列出將目的地 IP 位址轉換成
-RR	(ReleaseRefresh) 傳送名稱釋放封包到 WINS，然後開始重新整理

3.2.2 Null Session 介紹

Null session 通常被稱做"Holy Grail of Windows Hacking"（意指一切 Windows Hacking 的起始源頭）。Null sessions 是利用 CIFS / SMB (Common Internet File System / Server Messaging Block)協定的設計缺失來執行。這表示駭客可以與 Windows 系列作業系統(NT/2000/XP)電腦

主機建立 Null Session 的連線，不需要任何使用者帳號跟密碼。

藉由 Null Session 的連線，駭客可以收集到目標主機裡的許多資訊，在系統入侵簡介有介紹到，除了那些，還有 SIDs(Security Identifiers)。當我們擁有這些資料，那我們可以做出讓人意想不到的事，只要能與一部電腦主機利用 Null Session 建立 NetBIOS 連線，就可以輕易地取得完整的所有使用者名稱、群組名稱、資源共享、權限資料、政策資料、服務資料以及其他許多相關資訊，而且這一切都不需要任何使用者帳號跟密碼即可完成[5]。

3.2.3 實作一-問題

在做此研究時遇到很多問題，實作一的部分從圖 3 可以看到在建立新的網路連線後於狀態欄顯示 OK，但在輸入指令存取目標主機查看共用資源的檔案時發現找不到所設定的 IP 位址。

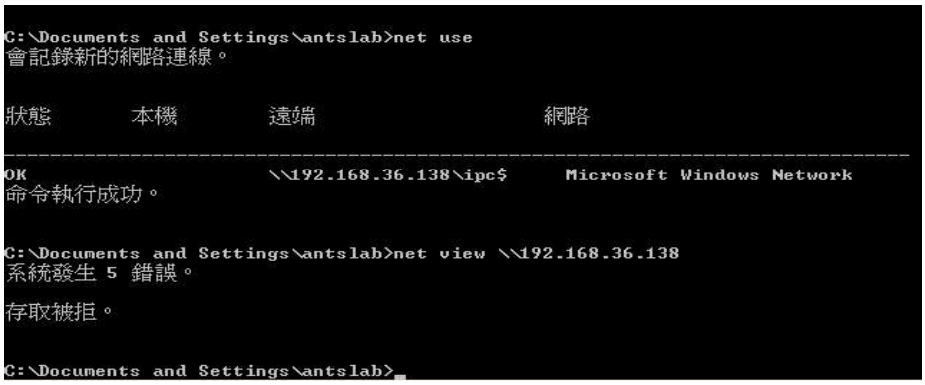

圖 3.實驗一-問題

3.2.4 實作一-解決方案

在經過多次的嘗試後，發現除了輸入目標主機的 IP 方式，還能輸入目標主機的電腦名稱，首先要先查看電腦的名稱，從左下方按「開始」開啟功能表，於「我的電腦」按右鍵選「內容」如圖 4 及圖 5 所示，完整的實驗流程於下一小節。

圖 4.實作一 - 解決方案 1

圖 5.實作一-解決方案 2

3.2.5 實作一-用 Null Session 漏洞做 IPC$ 空連接

實作一在系統入侵之前是很重要的過程，要了解目標主機是否能夠在自己的掌

控範圍，必須去先收集目標主機的資訊以便入侵，圖 6 利用 Nbtstat 的指令獲得重要資訊，在命令提示字元裡 Name 及 Type 內的英文皆會顯示大寫，故圖五級圖六上面所顯示的 user 不同，但皆為相同，紅色方框為用戶名稱，綠色方框為用戶群組，藍色方框為 MAC 位址。

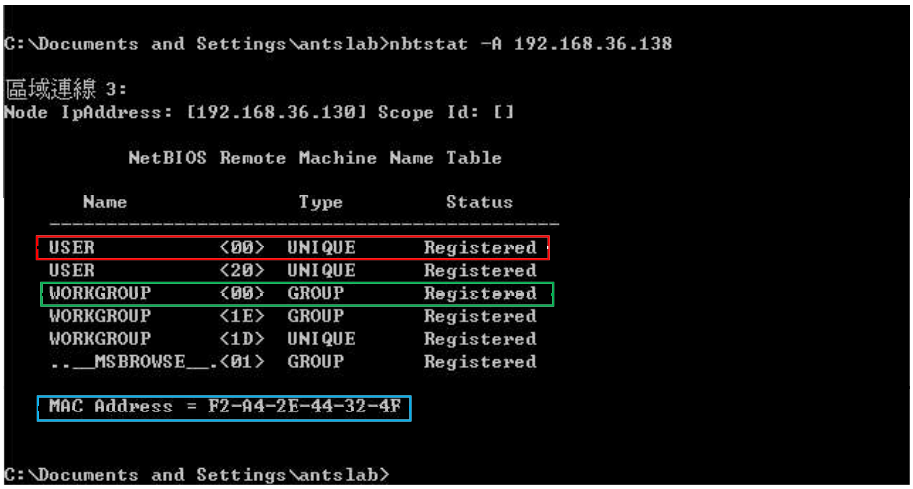

圖 6.實作一-列舉

瞭解上述內容後，接下來就要用列舉法對於 Windows XP 進行 Null session，在圖 7 的部份將使用 Null Session 的指令進行測試，指令：net use \\目標主機 IP\ipc$ "" /user: ""，指令裡面的 ipc$非常有趣，IPC$(Internet Process Connection)是共享"命名管道"的資源，它是為了讓進程間互相通信而開放的命名管道，通過提供可信任的用戶名和指令，連接雙方可以建立安全的通道並以此通道進行加密數據的交換，實現對遠端主機的訪問。

IPC$是 NT/2000 的一項新功能，它有一個特點，即在同一時間內，兩個 IP 之間只允許建立一個連接便可當作通過你的系統帳號和密碼登入。而 IPC$並不算是一個漏洞，但因一般電腦用戶設置系統的密碼為空，這就就成為一個大漏洞了，駭客用管理員權限的帳號和空密碼登入系統後就可以開共享，執行命令、程式、木馬，還可以刪除系統文件，造成極大的危險性。[7]

輸入上述的指令後再輸入 net use 即可查看現在遠端網路的連接狀態，如果狀態欄寫「中斷連線」，就再重新輸入 net use \\目標主機 IP\ipc$ "" /user: ""，便可成功。

圖 7.實作一-Null Session 漏洞

完成 Null Session 的連接後，要在目標主機裡建立一個共用檔案或資料夾，在這裡以資料夾為例，於目標主機的 C 槽建立新資料夾，之後將其設定為共用。如圖 8 所示。

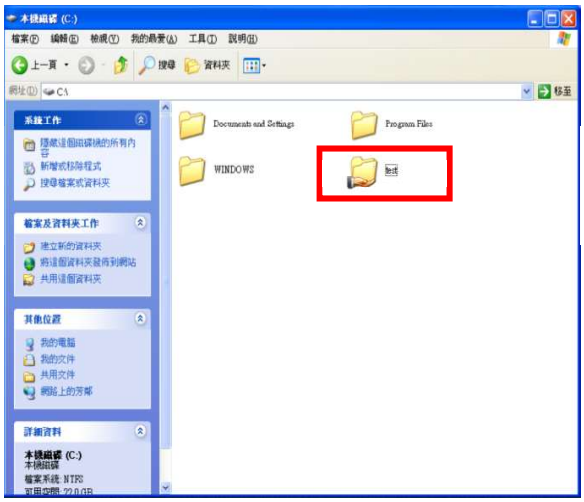

圖 8.實作一-建立共用資料夾

設定好回到攻擊主機的命令提示字元裡輸入指令：net view \\目標主機名稱，完成後如圖 9 所示，解決圖 3 無法查看共用資源問題。

圖 9.實作一-查看共用資源

3.3 實作二-利用 IPC$創造非空連結執行系統入侵

3.3.1 acccheck 介紹

acccheck 是 Kali Linux 作業系統裡的一個工具，他會嘗試連線到 IPC$/ADMIN$預設共用資源，並且利用字典檔進行帳號/密碼猜測攻擊[8]。他的指令為：acccheck –t 目標主機 IP/目標主機名稱 –U 帳號字典檔 –P 密碼字典檔，如果將 U 改成 u，就是指定帳號名稱，將 P 改成 p，就是指定密碼。

3.3.2 建立連結執行入侵

建立連結之前需先破解目標主機之帳號密碼，故會先在 Kali Linux 裡做出帳號字典檔及密碼字典檔，帳號字典檔為 user.txt，密碼字典檔為 password.txt，如圖 10 所示。

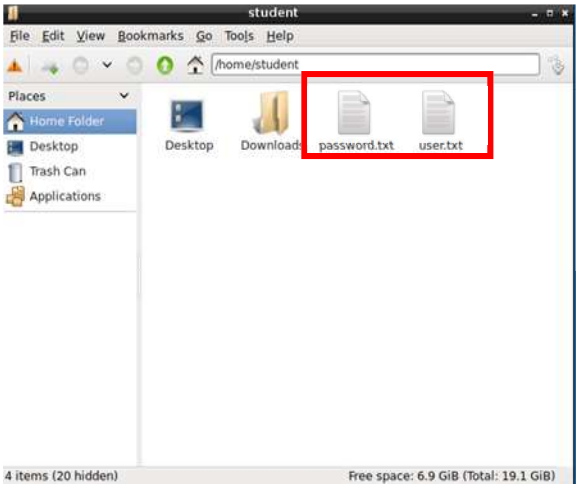

圖 10.實作二-建立字典檔

建立字典檔後便開始執行破解 windows XP 帳號密碼程序，圖 11 便是輸入 acccheck 指令的結果，由此可知帳號為 student，密碼為 student，其中 cat cracked 指令是將目標主機 IP 及破解的帳號密碼列出。

破解完後將此帳號密碼運用在 Null Session 漏洞，建立 IPC$非空連結，指令與 Null Session 沒有太多差別，只差在 Null Session 不用輸入用戶帳密，而非空連結需要，指令為 net use \\目標主機 IP\ipc$ "密碼" /user: "帳號"，從圖 12 可以看到當在輸

入 net use 時上面的狀態寫 OK，表示連結　　順利完成。

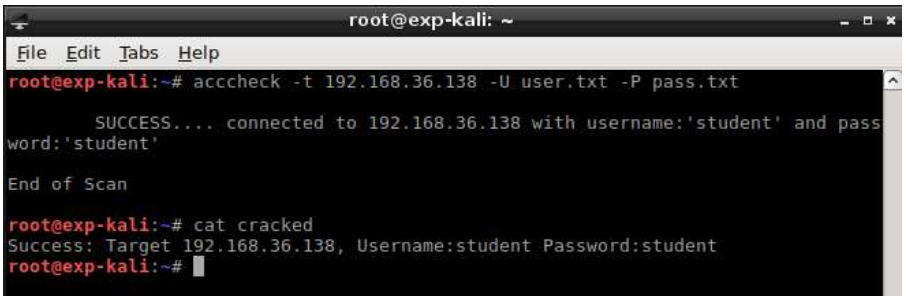

圖 11.實作二-破解 Windows 用戶帳密(一)

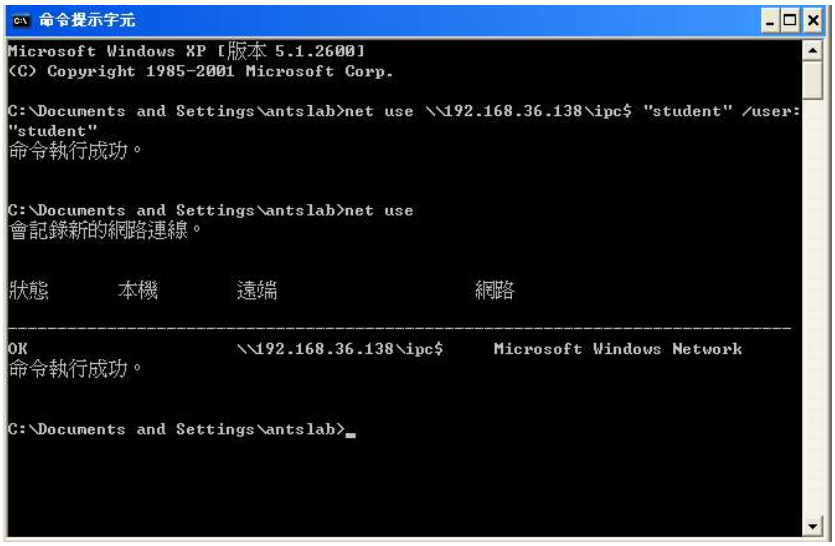

圖 12.實作二-破解 Windows 用戶帳密(二)

3.3.3 實作二-問題

建立完非空連結後，需要複製檔案到目標主機的共用資料夾中，指令為 copy 檔案路徑 \\目標主機 IP\共用資料夾，c$ 代表 C 槽，C 槽為預設共用的資料夾，但傳不進去，如圖 13 所示。

圖 13.實驗二-問題

3.3.4 實作二-解決方案

由於圖 13 顯示出「存取被拒」，因此要先了解共用的資料夾有哪些，藉由其他的資料夾進行傳遞，輸入指令 net share，這個指令只能看到自己本機的共用，但通常使用者不會去改變這些項目，所以可以拿來當作參考，如圖 14 所示。

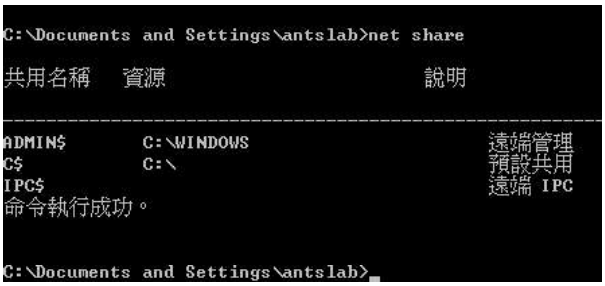

圖 14.實作二-查看共用

從圖 14 得知共用有 3 個，分別為 ADMIN$、C$及 IPC$，這樣可以從 IPC$ 來下手進行檔案的傳遞，傳遞後檔案會出現在目標主機的與攻擊主機同樣的路徑，如圖 15 及圖 16 所示。

圖 15.實作二-傳送檔案

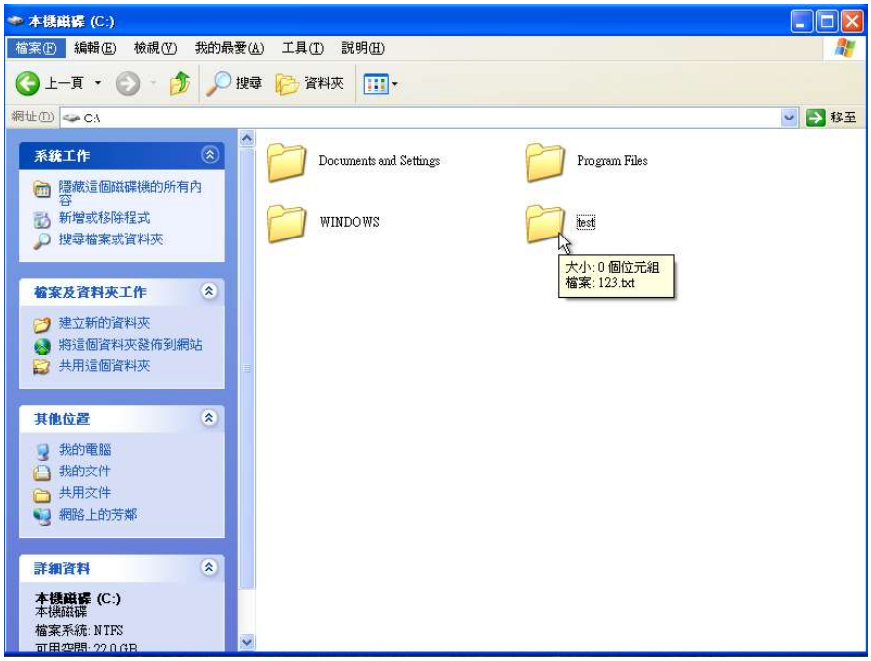

圖 16.實作二-檔案存放位置

如果可以利用這樣的方式傳送檔案，那駭客只要自己做出蠕蟲、木馬、後門程式檔案傳上來，把檔名設定成與日常息息相關的字語，引誘使用者開啟，那很多使用者就會因此讓電腦進入惡意軟體的陷阱裡。

3.3.5 實作一與實作二之分析

實作一是使用 Null Session 製造出共用空間，實作二是使用非 Null Session 來製作，兩個所使用的語法相近，差別就在於 Null Session 是一個匿名(anonymous)連接的網路通信[9]，而非 Null Session 則是再加上目標主機的使用者名稱及密碼，相較之下，實作一的作法比實作二簡單許多，只要輸入指令連接到目標主機形成共用後就可以傳遞檔案，但限制於匿名的方式，現在的許多使用者使用電腦不會去設定密碼，讓駭客可以使用實作一的方式就可以達成目的，而實作二的方式較為繁雜，但卻可以用在有設定帳號及密碼的使用者身上，其傳遞的方式都是使用原本 Windows 所設定的指令，駭客也不用特別花心思去思考指令輸入問題，不論是使用

實作一及實作二的方法，其重點都是在於使用 Windows 系統就有可能會有這方面的疑慮，當然要預防是可以的，但往往使用者只會用，不會去預防，致使駭客可以趁虛而入將使用者的資料竊取。

四、 結論

系統入侵從以上的操作可以知道，如果只需要這些指令就可以達成，那駭客想要滲透非常輕而易舉，我們現在必須做的，除了不要讓駭客入侵之外，更重要的是定時的系統更新，沒有作業系統設計出來就是完美的，密密麻麻的程式碼中總是有疏忽的地方，畢竟做出軟體只需要經過編譯、連結、載入、執行四個步驟，語法正確就可過編譯的關卡，後續的只是將軟體正常的操作就能發行使用，所以事後的維護是每個工程師會再繼續測試，直到該軟體沒有人將其破解為止，除了定期更新系統與應用程式外，還要備份資料，作業系統不是使用者可以自行更改，也沒有每個使用者都懂程式的指令，備份資料便是使用者在使用電腦時可以運用的一個方法；不定期更換密碼，不定期的原因是如果定期更換密碼，駭客如果知道這台機器的密碼會實施週期性更換，那被破解也只是時間上的問題，不定期更改可以不讓駭客抓住節奏，還需要將密碼的複雜度變高，在實作二中可以知道 acccheck 使用的是字典攻擊，現在的密碼大多都會設定生日、電話等等，這些純數字密碼或是簡單的英文單字都是駭客早已加入字典檔裡面的一部份，加入英數以外的字元增加密碼的複雜度，讓駭客想輕易破解也很難，最後就是定期掃描系統查看有無異狀，如果出現一些非系統之檔案須提高警覺，將此檔案名稱或路徑至網路上搜尋查看是否有人遭遇相似的困境以便處理。

誌謝

本論文感謝科技部計畫(MOST 106-2221-E-145-002-)提供經費支持本研究的進行。

參考文獻:

[1] 作業系統 – 維基百科,自由的百科全書(2018/3/18) https://zh.wikipedia.org/wiki/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F

[2] Linux – 維基百科，自由的百科全書(2018/3/18) https://zh.wikipedia.org/wiki/Linux

[3] Kali Linux – 維基百科，自由的百科全書(2018/3/20) https://zh.wikipedia.org/wiki/Kali_Linux

[4] Windows XP – 維基百科，自由的百科全書(2018/3/20) https://zh.wikipedia.org/wiki/Windows_XP

[5] 電腦駭客如何入侵電腦？ @ 有間.格:: 隨意窩 Xuite 日誌(2018/3/21) http://blog.xuite.net/ann12342/twblog/98949029-%E9%9B%BB%E8%85%A6%E9%A7%AD%E5%AE%A2%E5%A6%82%E4%BD%95%E5%85%A5%E4%BE%B5%E9%9B%BB%E8%85%A6%EF%BC%9F

[6] Nbtstat - TechNet - Microsoft(2018/3/23) https://technet.microsoft.com/en-us/library/cc940106.aspx

[7] IPC$ 掃瞄和 IPC$漏洞的防範@ I'n Blog 之萬象真藏:: 痞客邦:: (2018/3/30) http://ivan0914.pixnet.net/blog/post/54

49098-ipc%24-%E6%8E%83%E7%9E%84%E5%92%8Cipc%24%E6%BC%8F%E6%B4%9E%E7%9A%84%E9%98%B2%E7%AF%84

[8] Kali Linux 滲透測試工具第二版(電子書): - 第 6-45 頁 - Google 圖書結果(2018/3/31) https://books.google.com.tw/books?id=GAe9CwAAQBAJ&pg=SA6-PA45&lpg=SA6-PA45&dq=acccheck&source=bl&ots=jyOnJClGxR&sig=ktyCNxWKYBF6TM-DNEfBZE55Zsk&hl=zh-TW&sa=X&ved=0ahUKEwjihoHBsf3ZAhXI2LwKHYw2Aek4ChDoAQgtMAE#v=onepage&q=acccheck&f=false

[9] Null Session – 維基百科，自由的百科全書(2018/4/2) https://en.wikipedia.org/wiki/Null_session

Network Attack and Defense Platform – Building of System Hacking

Hou-Bin Kang[1], Kai Chain[1]

[1]Department of Computer Information Science, R.O.C Military Academy

Abstract

The research topic of this study is mainly to use the network attack and defense platform to build system intrusions, make related topologies, and actually understand what to do before the system hacking, such as scanning, enumeration, and execution etc. The most important thing is how to hack the system of the target host and what hazards will be done after the hacking. In addition, the problems that may occur when the system is built will also be listed and resolved. In this way, other users can avoid the same mistakes when working on this platform. This will enhance related information security knowledge and technology.

Key words: Network Attack and Defense Platform, System Hacking, Enumeration