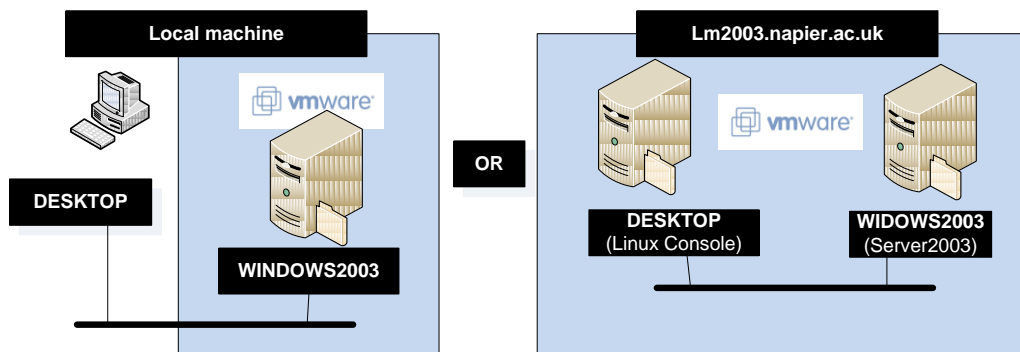


Week	Date	Teaching	Attended
3	24/01/10	Lab 2: Windows Services/Toolkit	

**Aim:** The aim of this lab is to investigate the discovery and configuration of services within Windows. It uses the Windows 2003 VM image (**WINDOWS2003**). You can either run VMWare Workstation on the local machine in the lab, or connect via a web browser to the [www.LM2003.napier.ac.uk](http://www.LM2003.napier.ac.uk) virtualisation server cluster. The Console (**DESKTOP**) on the local machine will be from Windows 7, where in LM2003 it is an Ubuntu console, as outlined below.



**Time to complete:**

4/5 hours (Two supervised hours in lab, and two/three additional hours, unsupervised).

**Activities:**

- Complete Lab 2: Windows Services/Toolkit. pdf from WebCT or <http://www.dcs.napier.ac.uk/~cs342/CSN10102/Lab2.pdf>
- Complete the End Of Unit Test for this chapter at: <http://buchananweb.co.uk/adv01.html>

Note: The module Handbook is available at: <http://buchananweb.co.uk/adv/part1.pdf>

**Learning activities:**

At the end of these activities, you should understand:

- How to define services in Windows.
- How to call-up configuration commands from a toolkit.

**Reflective statements (end-of-exercise):**

- How does the VM image setup itself up so that it can access the Internet, and that the local host can access the services within it?
- What are the key Windows commands used to discover the services which are being run?
- What are the key folder locations for Windows services?

**Source code used:**

<http://buchananweb.co.uk/toolkit.zip>

# Lab 2: Windows Services/Toolkit

## 1.1 Details

**Aim:** To provide a foundation in setup and consuming Windows services, and to continue building a software toolkit.

## 1.2 Windows Services

On-line demo:  
[http://buchananweb.co.uk/adv\\_security\\_and\\_network\\_forensics/threat01/threat01.htm](http://buchananweb.co.uk/adv_security_and_network_forensics/threat01/threat01.htm)

This part of the lab has two elements: the host machine (**DESKTOP**) and the Windows virtual server image (**WINDOWS2003**) as shown in Figure 1. The lab can be completed using VMWare Workstation on the local machine in the lab (shown in **Error! Reference source not found.**), or remotely on our LM2003 virtualisation server cluster, via a web browser (shown in Figure 2).

The local lab architecture is shown below. This requires the Windows2003 Server Virtual Machine to be run using VM Workstation on the local PC.

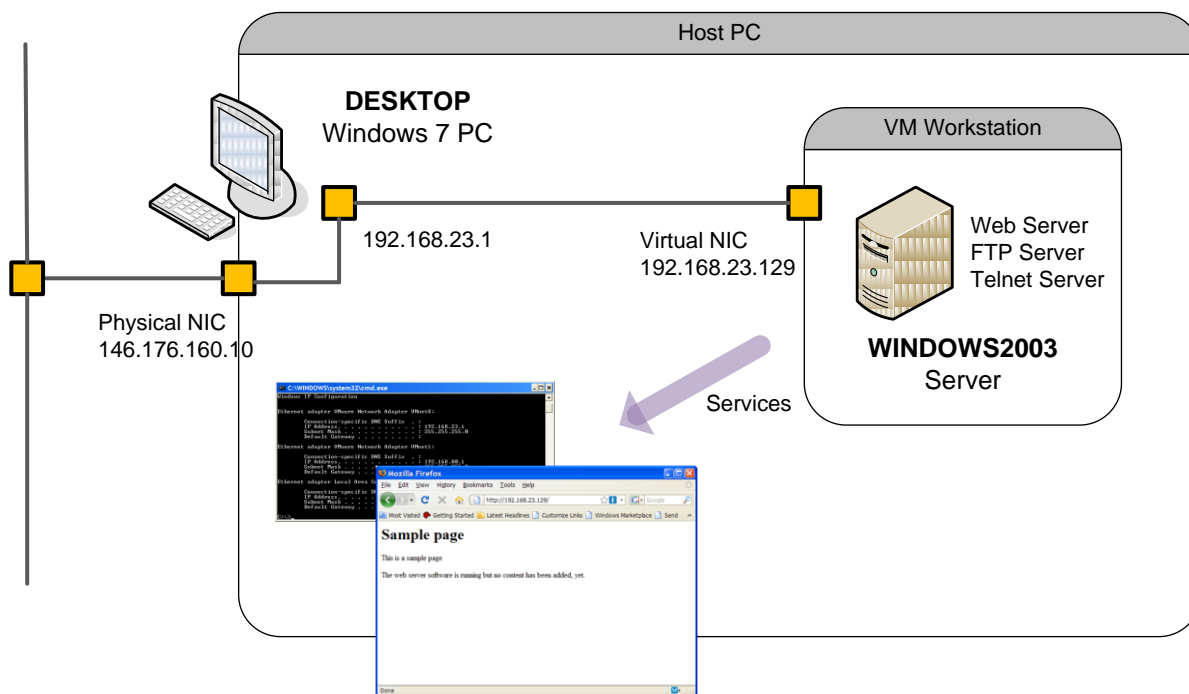


Figure 1 - Lab Architecture

An overview of Windows commands, to assist with the lab, can be found at:  
<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-s/ntcmds.mspx>

An overview of Linux commands, to assist with the lab, can be found at:  
<http://www.computerhope.com/unix/overview.htm>

The virtualisation server cluster lab architecture is shown in **Error! Reference source not found.** below. This requires a Linux VM Console and a Linux VM Server to be run in the Virtualisation Cluster (our Private Cloud).

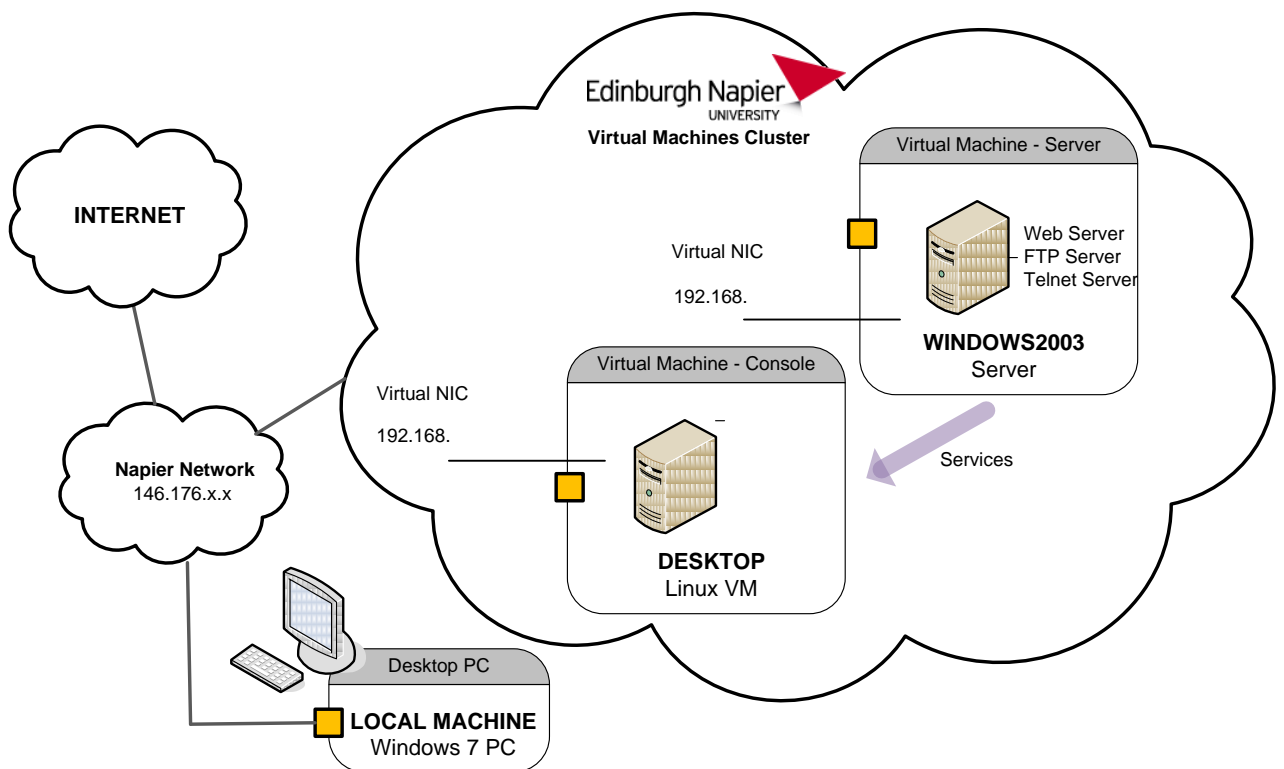


Figure 2 - Cluster Lab Architecture

**L1.1** Run the Windows 2003 Server virtual machine in the **Adv Security Workspace** on the LM2003 cluster (or locally run the .vmx file, and power the virtual machine)

Log in to the server using: Username: **Administrator**, Password: **napier**).

Within the WINDOVS2003 virtual server, open a command line window (Start>Run>cmd) and determine the virtual servers IP address using the Windows command **ipconfig**.

Similarly, from DESKTOP open a command line window and determine the IP Address of the DESKTOP.

☞ Complete the IP Addressing diagram in **Error! Reference source not found.** or 5, depending on which architecture you are using. Fill in the IP addresses(s) of the DESKTOP machine, and the WINDOWS2003 virtual server.

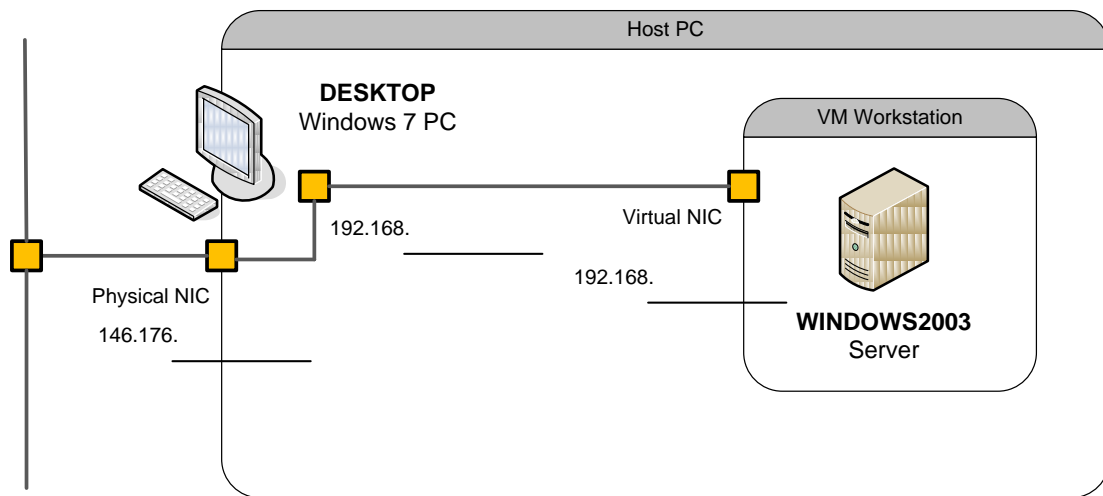


Figure 3 -Lab1 Local IP Addressing

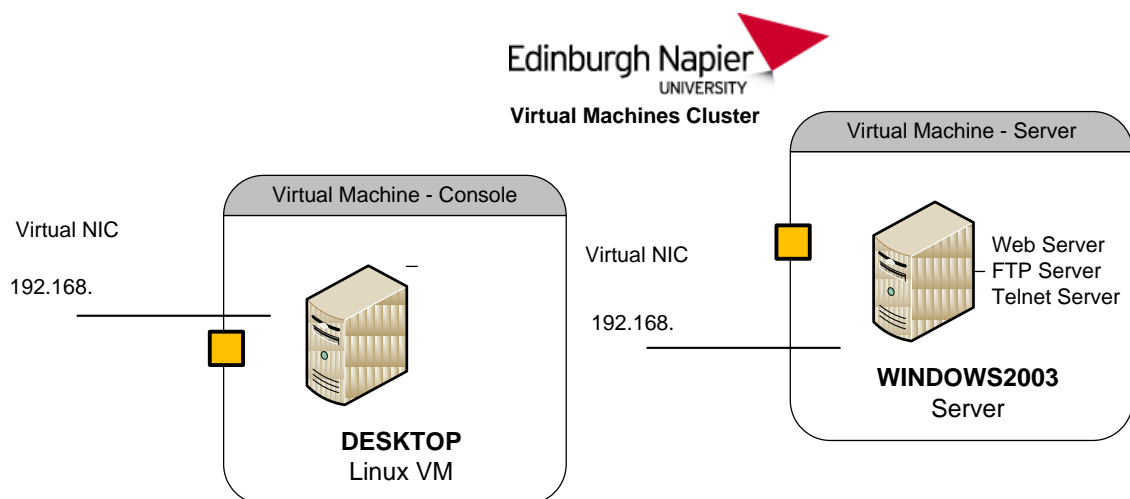


Figure 4 - Cluster IP Addressing

L1.2 To check connectivity, from DESKTOP, ping WINDOWS2003, and vice-versa.

☞ Were the pings successful? YES/NO

L1.3 From WINDOW2003, run **netstat -a**, and determine the services that are running on the server.

☞ List some of the services, and their protocol/port number?

**Note:** Use the `-h` flag to get help for the command. The `-n` flag can be used to find the numeric port numbers of the listening servers, and the IANA Port Numbers web page lists the official services and their protocol/portnumbers.

## SERVICE: Web

**L1.4** In WINDOWS2003, navigate to the IIS folder `C:\inetpub`

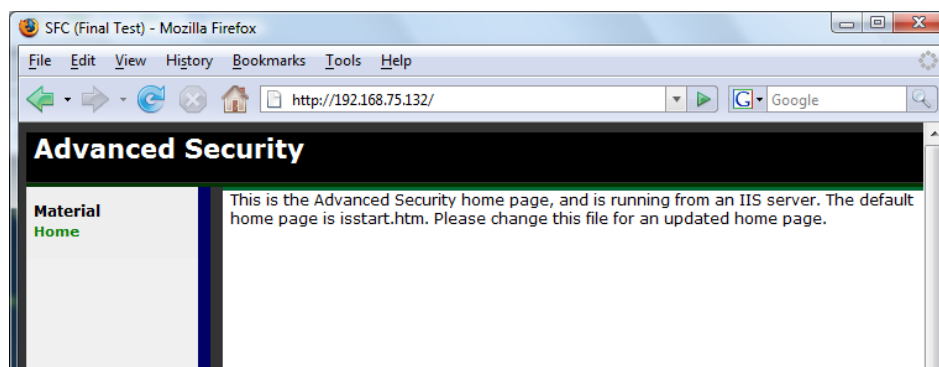
☞ What are the names of some of the folders?

In WINDOWS2003, go to the IIS Web Server folder `C:\inetpub\wwwroot`.

☞ What are the names of some of the files in this folder?

☞ What type of files does the folder contain?

**L1.3** From DESKTOP, connect to the Web Server using a Web Browser, and the URL `http://w.x.y.z`, where `w.x.y.z` is the IP address of WINDOWS2003, as shown below.



**Figure L1.1** Web server HTTP connection

Now connect to the Web Server, but this time using telnet:

```
telnet w.x.y.z 80
```

and then use the HTTP GET command:

```
GET /iisstart.htm
```

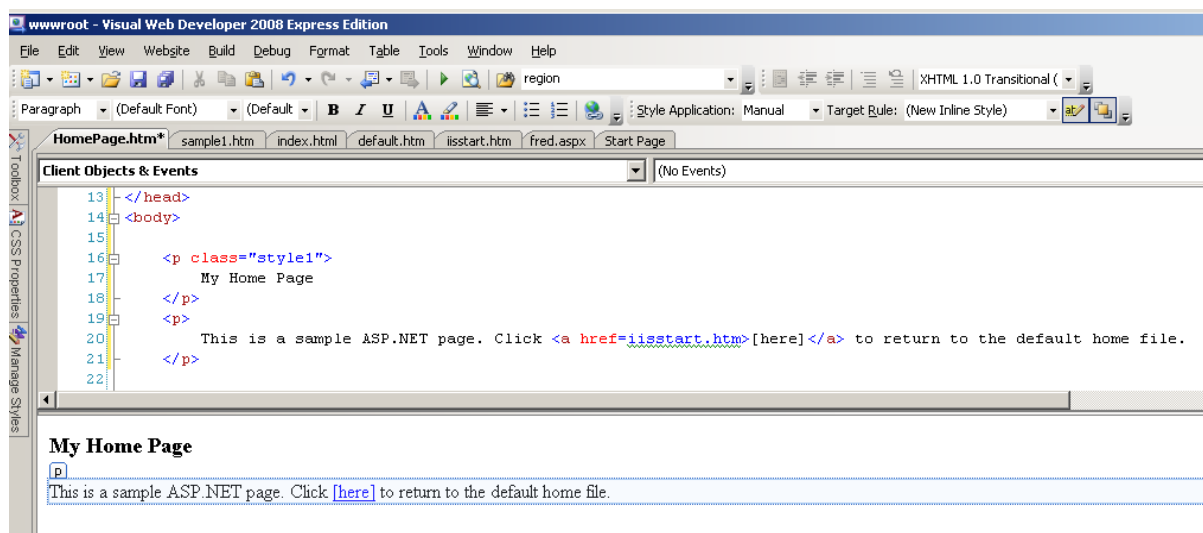
☞ What is the result, and how does it relate to accessing the home page of the Web server?

**L1.4** On WINDOWS2003, using **Microsoft Web Developer Express** (register with your live email account if necessary), open up the C:\inetpub\wwwroot Web folder, and Add a New Item to create your own home page, as shown below. (see the video for guidance if necessary)

Next modify `iisstart.htm` so that it has a link to your home page. The home page contain the following,:

## My Home Page

This is a sample page. Click [here](#) to return to the default home file.



**Figure L1.2** Create a new Web page

- ☞ Can you access this page, via a browser, from DESKTOP?  
YES/NO
- ☞ On WINDOWS2003, go to C:\WINDOWS\system32\LogFiles\W3SVC1. What are the contents of the folder, and using a text viewer/editor, what do the files contain?
- ☞ How might these log files be used to trace malicious activity?

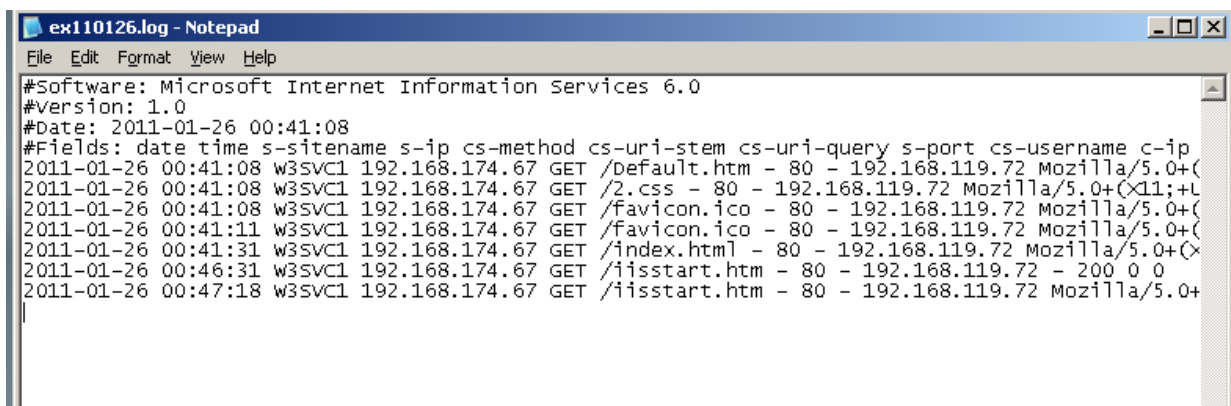


Figure L1.3 IIS Web Server Log File

## SERVICE: Telnet

**L1.5** Connect to the Telnet Server on WINDOWS2003 from DESKTOP, using **telnet w.x.y.z**, (where w.x.y.z is the IP address of WINDOWS2003). Login in as Administrator user (password: napier).

- ☞ What is the default home folder for Telnet on WINDOWS2003?
- ☞ List the contents of the folder?
- ☞ Which command did you use?

Quit from Telnet, using the **exit** command.

## SERVICE: FTP

L1.6 From your host, connect to the FTP Server from DESKTOP using your Web browser and the URL `ftp://w.x.y.z` where w.x.y.z is the IP address of WINDOWS2003.

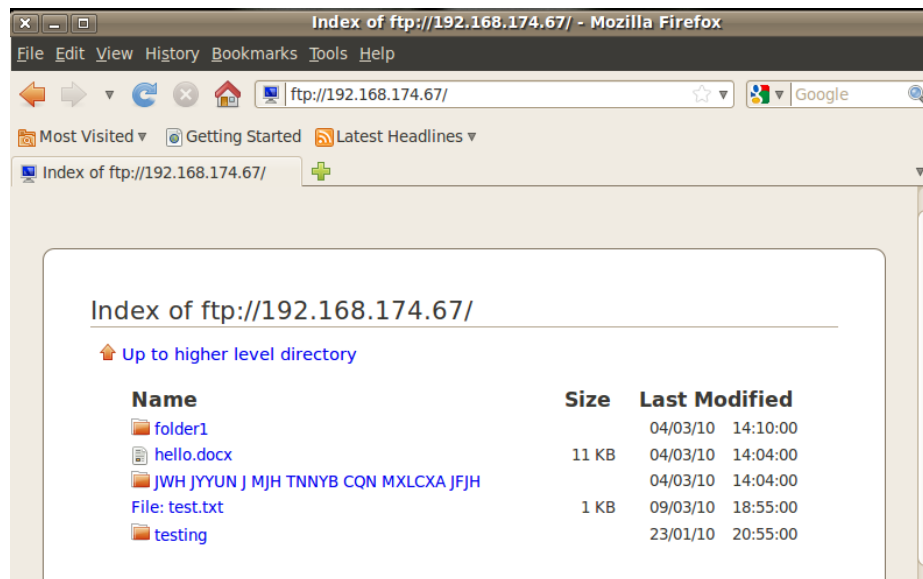


Figure L1.4 FTP connection

Repeat this using:

**telnet w.x.y.z 21**

and then enter the commands in bold (and note the commands that you get beside the sample return ones):

```
220 Microsoft FTP Service
HELP
214 The following commands are recognised ...
ABOR
ACCT
...
USER Administrator
331 Password required for Administrator.
PASS napier
230 User Administrator logged in.
SYST
215 Windows_NT
TYPE I
200 Type set to I.
PASV
227 Entering Passive Mode (192,168,75,132,4,65).
LIST
☞ Did you see the output of the LIST command?
YES/NO
```

The **PASV** FTP command opens up a second channel, using a high (above 1024) port number, for the data transfer. This is calculated from the last two digits of the Passive Mode response (227 response). It is calculated as 256 times the second last digital plus the last digital. So, in this case, it is:

Port =  $4 * 256 + 65 = 1089$

Next open up the data transfer by creating a new Telnet connection, in a 2nd command window such as:

```
telnet w.x.y.z 1089
```

Now try the **LIST** command again, in the 1<sup>st</sup> command window.

☞ Did the LIST command succeed?

YES/NO

☞ How might type of FTP cause a security problem?

## SERVICE: SMTP

L1.1 From your host, use the following command:

```
telnet w.x.y.z 25
```

and connect to the SMTP server. Next enter the commands in bold:

```
220 napier Microsoft ESMTP MAIL Service, Version: 6.0.3790.3959 ready at Sun,
0 Dec 2009 21:56:01 +0000
help
214-This server supports the following commands:
214 HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN
BDAT VRFY
helo me
250 napier Hello [192.168.75.1]
mail from: email@domain.com
250 2.1.0 email@domain.com....Sender OK
rcpt to: fred@mydomain.com
250 2.1.5 fred@mydomain.com
Data
354 Start mail input; end with <CRLF>.<CRLF>
From: Bob <bob@test.org>
```

**To:** Alice <alice@ test.org >  
**Date:** Sun, 20 Dec 2009  
**Subject:** Test message

**Hello Alice.**

**This is an email to say hello**

.

250 2.6.0 <NAPIERMp7lzvxrMVHfB00000001@napier> Queued mail for delivery

**L1.7** Go to WINDOWS2003, and go into the C:\inetpub\mailroot\queue folder, and view the queued email message.

☞ Outline the format of the EML file?

☞ How might this type of programmable sending of mail messages be abused?

## **SERVICE: Find the service?**

**L1.8** From your host connect to Port 7 using telnet.

☞ What is the service being connected to, and what protocol/port number pair does it use?

## **AUDIT LOGGING**

**L1.9** Auditing and logging are important in terms of tracing activities.

☞ Check in the Event Viewer in WINDOW2003 (Figure L1.5), that the logon event has been added. How might this be used to trace activity?

☞ From Local Security Policy, find the option to change option so that Privileged Access is audited. What is the option:

☞ From Local Security Policy, find the option to change option so that the Guest Account cannot login. What is the option:

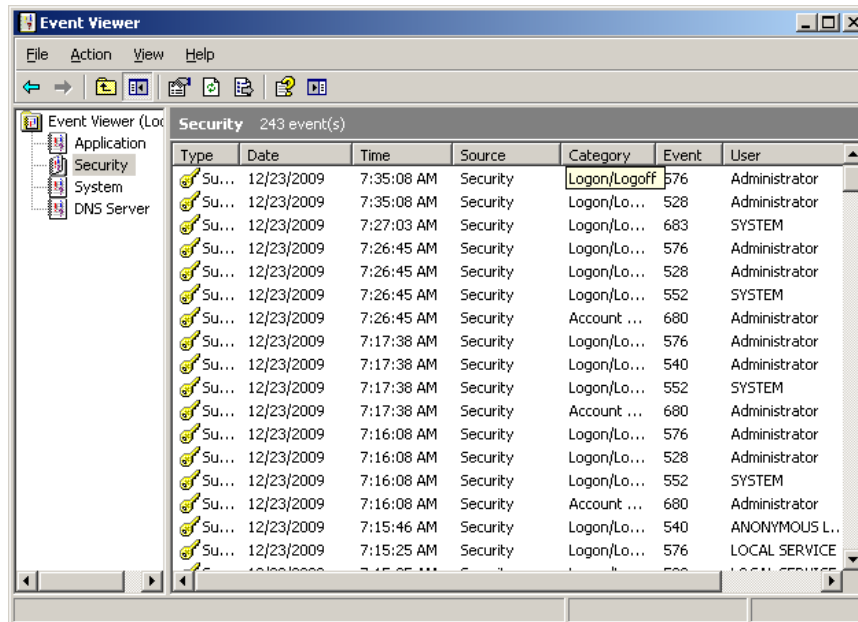


Figure L1.5 Windows Event viewer

## 1.3 Toolkit Development 2 – WinDump

☞ Video demo of part 2 of the toolkit software development:  
[http://buchananweb.co.uk/adv\\_security\\_and\\_network\\_forensics/toolkit02/toolkit02.htm](http://buchananweb.co.uk/adv_security_and_network_forensics/toolkit02/toolkit02.htm)

The objective of this series of labs is to build an integrated toolkit. Today we add the **WinDump** command line network packet analyser. WinDump is the Windows version of the UNIX tcpdump network analyser.

☞ For more on WinDump see the home page:  
<http://www.winpcap.org/windump/default.htm>

Download:

☞ <http://buchananweb.co.uk/toolkit.zip>

and extract to a local folder. Next open up **toolkit.sln**, and double click on **client.cs**. (Refer to <http://buchananweb.co.uk/dotnetclientserver.zip> for a completed version).

**L2.1** Select the [**WinDump**] tab, and double click on the Combo Box (cbInterfacesWin). Next add the following code: (cut & paste the code from the .pdf)

```
stopProcess ("windump");
```

```

if (processCaller2 != null) processCaller2.Cancel();

processCaller2 = null;
int ind = cbInterfacesWin.SelectedIndex+1;
string args="-q -i "+ind;
if (this.cbVerbose.Checked) args += " -v ";
if (tbOption.Text.Length > 0) args += " " + tbOption.Text;

runProgram2("WinDump.exe",args );

```

Next add the method:

```

public void stopProcess(string name)
{
    try
    {
        Process[] pArray = Process.GetProcesses();

        foreach (Process p1 in pArray)
        {
            string s = p1.ProcessName;
            s = s.ToLower();

            if (s.CompareTo(name) == 0)
            {
                p1.Kill();
            }
        }
    }
    catch (Exception ex)
    { }
}

```

Test the program, as shown below.

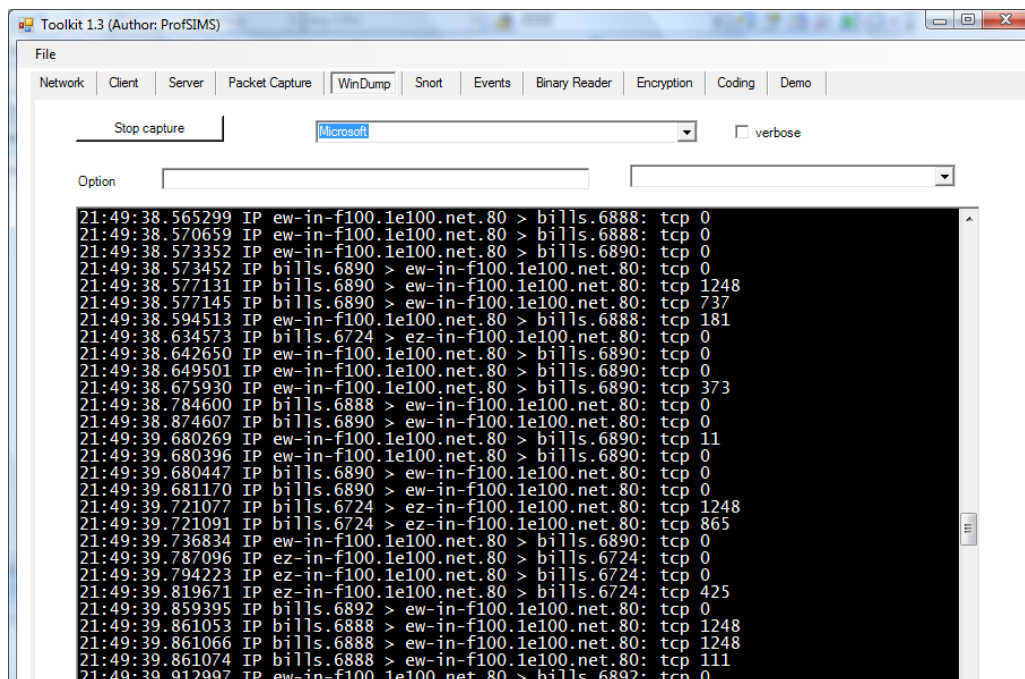


Figure L1.6 WinDump running from the Toolkit