Aim: The aim of this lab is to investigate the discovery and configuration of services within Windows. It uses the Windows2003 VM (WINDOWS2003). You can either run the VM locally using VMWare Workstation, or access via a web browser on the www.vm2003.napier.ac.uk virtualisation server cluster. The lab client machine (DESKTOP) on the local machine will be from Windows 7, or in VM2003 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 Development.
  .pdf from WebCT or http://www.dcs.napier.ac.uk/~cs342/CSN10102/Lab2.pdf

- Complete the End Of Unit Tutorial Questions for this unit, with the NetworkSims Test Engine, and online questions at:
  http://asecuritysite.com/security/tests/tests?sortBy=sfc07

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

Rich Macfarlane, Bill Buchanan 2013

1.1 Details

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

1.2 Windows Services

The following video can be used as a guide to complete the local version of the lab.

On-line video demo:
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 server guest virtual machine (WINDOWS2003) as shown in the figure below. The lab can be completed using VMWare Workstation on the local machine in the lab (shown below in Figure 1), or remotely on our LM2003 virtualisation server cluster (shown in Figure 2).

The local virtualised lab architecture is shown below. This requires the modules 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:

The virtualisation server cluster lab architecture is shown in the figure below. This requires a Linux VM Console and a Linux VM Server to be run in the Virtualisation Cluster (our Private Cloud).

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

---

![Figure 2 - Cluster Lab Architecture](image)

**Setup Windows Server Lab**

**L1.1** Run the Windows 2003 Server virtual machine in the Adv Security Workspace on the VM2003 cluster (or locally run the .vmx file, and power the virtual machine)

Log in to the server using: **CTRL+ALT+INS**, and Username: **Administrator**, Password: **napier**.

Within the WINDOWS2003 virtual server, open a command line window (**Start>Run cmd**, or **WINDOWSKEY+R 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 interface to the virtual network that WINDOWS2003 is connected to.

Complete the IP Addressing diagram in one of the the figures below (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

If your WINDOWS2003 VM does not have an IP Address, check that it is connected to the host via NAT, using the menu VM>Settings, as shown below, and disable/enable your network adapter, to get a new IP Address from the VMWare DHCP server.
L1.2 To check connectivity, from DESKTOP, **ping** WINDOWS2003, and vice-versa.

- Was the ping from DESKTOP to WINDOWS2003 successful? YES/NO
- Was the ping from WINDOWS2003 to DESKTOP successful? YES/NO
- Why might this be?

Use the command **pathping DESKTOPIP** to find out more about the failure.

- Which interface is filtering the packets?

**Windows 7 Firewall**

If DESKTOP is a Windows7 machine it may be that the firewall is blocking virtual networks (connected as type Public), and so we need to either allow ICMP traffic through, or turn the firewall off on this network interface.

On DESKTOP, open the Windows Network and Sharing Center window. This can be accessed by left clicking the **Windows Network Connections Icon**, (⏻ or ⏺) in the notification area, and selecting **Open Network and Sharing Center**. (It can also be accessed via the Windows Control Panel.)
Open **Windows Firewall** to check which services are being blocked on which type of networks. There is a link at the bottom left of the Network and Sharing window.

This **Windows Firewall** application is the basic interface to interact with the built in firewall. **Windows Firewall with Advanced Security** is a newer application which allows more detailed configuration. We will look at this in future labs.

To allow the ICMP packets used by the ping tool, we can simply switch off the firewall for now. Click **Turn Windows Firewall on or off**, as shown below.
Turn off the firewall for the Network Type assigned to the your virtual network (typically Public).

Retest the connectivity test from WINDOWS2003 to DESKTOP.

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Was the ping from WINDOWS2003 to DESKTOP successful?</td>
<td>YES/NO</td>
</tr>
</tbody>
</table>

Retry the command `pathping DESKTOP`.  

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Was the pathping from WINDOWS2003 to DESKTOP successful?</td>
<td>YES/NO</td>
</tr>
</tbody>
</table>

Windows Services

L1.3 In a Windows OS the `netstat` command can be used list the running network services. From WINDOW2003 server use `netstat -h` to check the arguments and options of the command.

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there a <code>-l</code> flag to only list the listening servers? (like there is in linux)</td>
<td>YES/NO</td>
</tr>
</tbody>
</table>

Use the `netstat -a -p tcp`, and determine the TCP-based services that are running on the server. Then similarly review the UDP services.

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>List some of the well known services, and their protocol/port number?</td>
<td></td>
</tr>
</tbody>
</table>

**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. The IANA Port Numbers web page lists the official services and their protocol/portnumbers.

Windows IIS Services

Internet Information Services (IIS) is the Microsoft web server application tied closely to Windows OSs. Due to this it is very popular, with only Apache being more popular.
IIS can also provide services other than the web server. IIS is installed via the **Control Panel > Windows Add/Remove programs > Add Remove Windows Components > Application Server**. View the installed services provided under IIS as shown below.

List some of the well known services provided by IIS?

The IIS services can be managed using the IIS Manager. From W2003, run IIS Mgr via Programs>Admin Tools>IIS Mgr as shown below.

**Services: Web Server**

L1.4 From IIS Mgr, open the Web Sites folder and click on the Default web site.
Review the configuration with Right Click>Properties.

Which port is the web server running on?

From the **Home Directory** tab:

Which directory holds the web page files?

From **WINDOWS2003**, navigate to the IIS folder **C:\inetpub**

What are the names of some of the folders?
Go to the IIS Web Server folder C:\inetpub\wwwroot.

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

Use the type command to view the contents of some of the files, such as the command:

type filename | more

What type of files does the folder contain?

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

![Advanced Security Webpage]

On WINDOWS2003, just after loading the page, use the \texttt{netstat -a} command to determine the servers and connectons. (‐a all connections, listening and established)

Can you see the established client/server connection between DESKTOP and WINDOWS2003?

What is the client port?

On WINDOWS2003, in the folder C:\inetpub\wwwroot, use the \texttt{find} command to find files with a string in, such as the command which will find the string advanced in any files:

\texttt{find "advanced" *}

Which file from the wwwroot directory is being served as the default web page?
Which input flag for the find command will ignore case for the string find?

From DESKTOP, open a command window and use the Windows telnet client or Putty to connect to the Web Server on WINDOWS2003. (you may need to activate the Windows telnet client via Control Panel>Programs & Features>Turn Windows Features On & Off).

telnet w.x.y.z 80

and then send the HTTP GET command to the server:

GET /iisstart.htm

What is the response from the web server?

How does this relate to accessing the home page, using the web browser?

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.

From the Solution Explorer pane, add a new web page (HTML Page), using Right Click>Add New Item, saving it as yourname.html.

Create your own home page, with the contents shown below. Use the Split button to display the web page, and now you can add text and format text. Save the page and you should see it in the wwwroot dir. (see the video for guidance if necessary)
Next modify iisstart.htm so that it has a link to your home page.

Can you access this new web page, via a browser, from DESKTOP?  YES/NO

On WINDOWS2003, go to C:\WINDOWS\system32\LogFiles\W3SVC1.

What are the contents of the folder?

What do the files contain?

How might these log files be used to trace malicious activity?
Services: Telnet

L1.5 From DESKTOP, connect to the Telnet Server on WINDOWS2003, using:

```
telnet w.x.y.z
```
(where w.x.y.z is the IP address of WINDOWS2003).

Login in as Administrator (password: napier).

- What is the default home folder for Telnet on WINDOWS2003?
- List the contents of the folder?

On WINDOWS2003 use the `netstat -a` command to determine the servers and connections. (-a all connections, listening and established)

- Can you see the established client/server connection between DESKTOP and WINDOWS2003?
- What is the client port?

Quit the Telnet shell on the remote machine using the `exit` command.

Services: FTP

L1.6 From DESKTOP, connect to the FTP Server using a Web browser and the URL

```
ftp://w.x.y.z - where w.x.y.z is the IP address of WINDOWS2003.
```

- What are the contents of the ftp home directory?
Figure L1.4  FTP connection

Find the *ftproot* directory using the Windows find folders/files dialog (WINDOWSKEY+F)

 Where is the ftproot directory located?

On WINDOWS2003, in a command window, navigate to the *ftproot* directory.

 What are the contents of the directory?

On the server, in *ftproot* create a directory files, and add some test files to it. Now from DESKTOP, refresh the web browser (CTRL+F5) connected to the FTP Server.

 What are the contents of the ftp home directory now?

From DESKTOP, connect to the FTP server using telnet (Windows Client or using Putty)

\[(\text{telnet w.x.y.z 21})\]

Then enter the commands in **bold** below (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
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 (4) plus the last digital (65).

So, in this case, it is:

\[
\text{Data Channel Port} = 4 \times 256 + 65 = 1089
\]

Next open up the data transfer by creating a new Telnet connection, in a 2nd command window such as the command (1089 for our example):

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

Now try the **LIST** command again, in the 1st command window.

Did the **LIST** command succeed? YES/NO

How might type of FTP cause a security problem?

**Services: SMTP Mail Server**

**L1.1 Sending mail via a mail server, using telnet.**

From DESKTOP, connect to the SMTP mail server on WINDOWS2003, using the following command:

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

Next enter the SMTP commands below 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 <NAPIERMp7lvxrMVHFb00000001@napier> Queued mail for delivery

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

 acquaintance Was the mail successfully queued? If not, which mail folder has the file in?
 acquaintance Outline the format of the EML file?

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

Services: Find the service?

L1.8 From DESKTOP connect to the service on Port 7 on WINDOWS2003 using telnet.

 acquaintance What is the service being connected to, and what protocol/port number pair does it
use? (try the IANA web site for confirmation of service)
Windows Audit Logging

L1.9 Auditing and logging are important in terms of tracing activities. The Windows Event Viewer application can be used to view/manage logs from running applications and services (Start>Programs>Administrative Tools>Event Viewer)

Application, Security, Setup and System logs are available to browser.

In WINDOW2003, check the Event Viewer – System Log Records. The log records are listed in reverse chronological order, so the most recent events are at the top and as you scroll down you’ll move back in time.

Can you identify a Windows Update log record? When was the last Update log record?

Double click the record to check the details of the Windows Update.

Check in the Event Viewer – Security Logs, and that the Logon event has been added.

Which User logged on most recently?

How might this be used to trace activity?
A Windows Local Security Policy can be used to control Authentication (who has access), Authorisation (what resources can be accessed), and Auditing (logging actions) on the Windows machine.

On WINDOWS2003 run the Local Security Policy Manager either via the control panel or with \WINDSSTART>Programs>Admin Tools> Local Security Policy

**Figure L1.1** Windows Event viewer

In the Local Security Policy>Audit Policy, find the option which audits Logons. What is the option? What is its current setting?

What would be an issue with this?

In the Local Security Policy>Audit Policy, find the option to change so that any Privileged Access is audited. What is the option? What is its current setting?
From **Local Security Policy**, find the option to change option so that the Guest Account cannot login. What is the option?

### 1.3 Security Toolkit Development 2 – WinDump

The objective of this series of labs is to build an integrated toolkit. This toolkit software development lab has an associated video demo.

- **Video demo of part 2 of the toolkit software development:**
  
  http://buchananweb.co.uk/adv_security_and_network_forensics/toolkit02/toolkit02.htm

This toolkit lab shows how to integrate the **WinDump** command line network sniffer/packet analyser into the toolkit software. 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

For this lab, download the partially finished toolkit application source code (a Visual Studio C# Solution) from the link below:

- **Toolkit source code:**
  
  http://buchananweb.co.uk/toolkit.zip

Extract the source code for the C# Windows Application to a local folder. Next open the toolkit application with Visual Studio (VS) (double click the VS solution file toolkit.sln). You should see the **Solution Explorer panel** on the right of the VS Window.

- **For reference, the finished toolkit application can be downloaded from:**
  
  http://buchananweb.co.uk/dotnetclientserver.zip

#### L2.1 Select the **[WinDump]** tab, and double click on the drop down Combo Box (cbInterfacesWin).

Next add the following code: (the code can be cut & pasted from the .pdf)

```csharp
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
    {

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

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

Test the program, as shown below.

Figure L1.2  WinDump running from the Toolkit