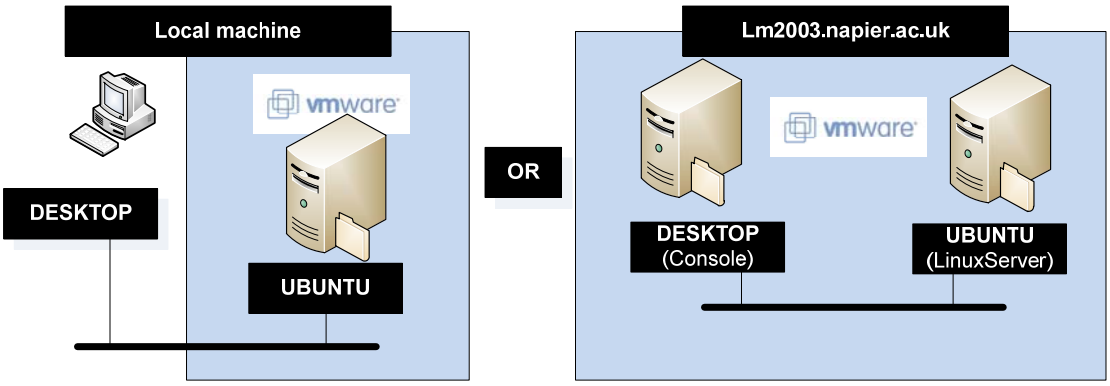
Labs

Contact: Prof Bill Buchanan/Richard Macfarlane
Email: w.buchanan@napier.ac.uk/r.macfarlane@napier.ac.uk
Room: C.63/C.43

Week	Date	Teaching	Attended
2	**19/01/11**	Lab 1: Linux Services/Toolkit 1	

Aim: The aim of this lab is to investigate the discovery and configuration of services within Linux. It uses the Ubuntu VM image (UBUNTU). You can either use the local machine or connect to the LM2003 server. The Console on the local machine will be from Windows 7, where in LM2003 it is a Ubuntu console.



Time to complete:
4/5 hours (Two supervised hours in C.27, and two/three additional hours, unsupervised).

Activities:
- Complete Lab 1.

Learning activities:
At the end of these activities, you should understand:

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

Reflective statements (end-of-exercise):
What are the key Linux commands used to discover the services which are being run?

What is the key folder location for the Web server in Linux?

Why does Linux need the VNC Client, when Windows uses the Remote Desktop Client?

Source code used:

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

1 Lab 1: Linux Services/Toolkit

1.1 Details

Aim: To provide a foundation in setup and consuming Linux services, and to start creating a toolkit which will be built-up over the next series of labs.

1.2 Activities

On-line demo: http://buchananweb.co.uk/adv_security_and_network_forensics/unix/unix.htm (VMware) or: http://buchananweb.co.uk/e_presentations/vmware_lab01/vmware_lab01.html (for cluster)

This part of the lab has two elements: the console machine (**DESKTOP**) and the Linux virtual image (**UBUNTU**).

L1.1 Run the Linux virtual image (User name: Administrator, Password: napier123). Within the virtual image, run a Terminal and determine its IP address using **if-config**.

What are the IP and MAC addresses of the server and the network address which will be used to connect to the virtual image: What is the name of the interface (such as eth6):

L1.2 From **DESKTOP**, ping **UBUNTU**, and vice-versa.

SERVICE: Web

L1.3 In **UBUNTU**, go to the folder /var/www.

What are the names of the files in this folder:

L1.4 From **UBUNTU**, run `netstat -l`, and determine the services that are running.

List some of the services:

L1.5 Connect to the Web Server from **DESKTOP** using http://w.x.y.z, where w.x.y.z

is the IP address of **UBUNTU** (Figure L1.1). Repeat this using:

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

and then enter:

GET /index.html

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

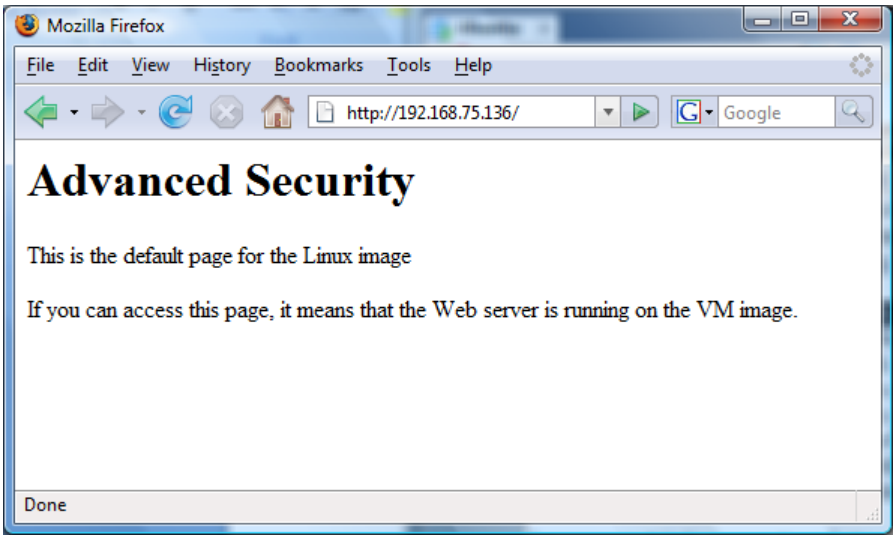


Figure L1.1 HTTP connection

L1.6 On UBUNTU, using Screem HTML/XML Editor, open up the /var/www and create a new page, such as:

My Home Page

This is a sample ASP.NET page. Click [here] to return to the default home file.

☞ Can you access this page from the host (DESKTOP)?

☞ On UBUNTU, go to /var/log/apache2. What is the contents of the folder, and what do the files contain?

☞ How might these log files be used to trace malicious activity?

SERVICE: Telnet

L1.7 From your host, connect to the Telnet Server from DESKTOP using telnet x.y.y.z, where w.x.y.z is the IP address of UBUNTU. Login in with napier (password: napier123).

☞	What is the default home folder for Telnet on UBUNTU (use pwd to determine the current directory):

Quit from Telnet, using the "exit" command.

SERVICE: FTP

L1.8 From your host, connect to the FTP Server from DESKTOP using ftp://w.x.y.z where w.x.y.z is the IP address of UBUNTU (Figure L1.2). 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):

USER napier
331 Password required for napier.
PASS napier123
230- Linux ubuntu 2.6.31-14-generic #48-Ubuntu SMP Fri Oct 16 14:04:26 UTC 2009 i686
230-
230- To access official Ubuntu documentation, please visit:
230- http://help.ubuntu.com/
230-
230 User napier logged in.
PWD
257 "/home/napier" is current directory.
TYPE I
200 Type set to I.
PASV
227 Entering Passive Mode (192,168,75,136,146,31)
LIST

Now FTP opens up a port for the data transfer. This is calculated from the last two digits of the Passive Mode response (227 response). It is calculated as 146 times the second last digital plus the last digital (31). So, in this case, it is:

Port = 146*256+31 = 37397

Next open up the data transfer by creating a new Telnet connection, such as:

telnet w.x.y.z 37397

- ☞ Can you access this page from the host?
- ☞ On UBUNTU, go to /var/log. View the syslog file (such as with **cat syslog**). What is its contents?
- ☞ How might these log files be used to trace malicious activity?
- ☞ View the contents of /etc/inetd.conf file. How is this used to enable services?

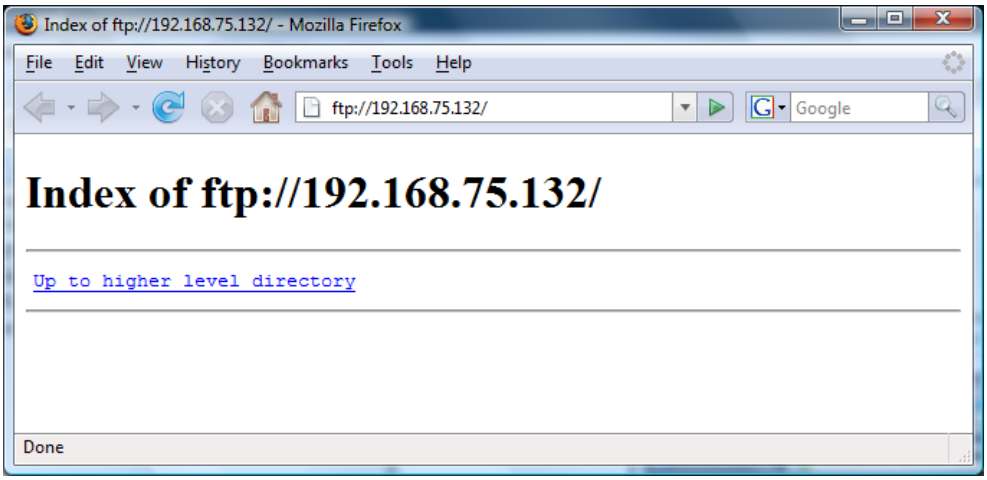


Figure L1.2 FTP connection

SERVICE: Remote Desktop

L1.9 Download the VNC Client from:
http://www.realvnc.com/cgi-bin/download.cgi

then from the host, connect to UBUNTU using the Remote Desktop (Figure L1.3).

- ☞ Which is the service which is running on UBUNTU that allows the remote connection to happen?

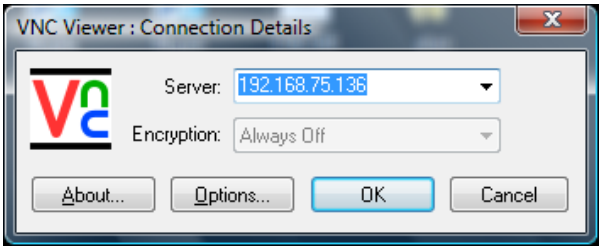


Figure L1.3 VNC Viewer

1.3 Toolkit 1

On-line demo:
http://buchananweb.co.uk/adv_security_and_network_forensics/toolkit01/toolkit01.htm

The objective of this series of labs is to build an integrated toolkit. Open up the following

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

and extract to a local folder. Next open up toolkit.sln, and double click on client.cs.

L1.10 Select the [Network] table, and double click on the "netstat –a" button, and add the code:

```
runProgram("netstat", "-a");
```

and test the program.

L1.11 Select the [Network] table, and complete the rest of the buttons (netstat –a, "arp –a", "nbstat –n", "systeminfo", "ipconfig", "ipconfig /all", "route print" and "net view|). See Figure L1.4.

For Audit Policy add:

```
runProgram("Auditpol", "/get /category:*");
```

For Clear ARP add:

```
runProgram("netsh", "interface ip delete arpcache");
```

For Add Firewall Rule:

```
runProgram("netsh", "advfirewall firewall add rule name=\"NetworkSims Rule\"
dir=in action=allow  protocol=TCP localport=65000");
```

For Add ICMP Rule:

```
runProgram("netsh", "advfirewall firewall add rule name=\"NetworkSims Rule\"
protocol=icmpv4:8,any dir=in action=allow");
```

For Delete Rule:

```
runProgram("netsh", "advfirewall firewall delete rule name=\"NetworkSims
Rule\" dir=in");
```

For Show Rules:

```
runProgram("netsh", "advfirewall firewall show rule name=\"NetworkSims
     Rule\"");
```

L1.12 Now add three buttons, and three text boxes (tbPing, tbTracert and tbTracert) and add a ping, tracert and nslookup button. Next add the code to each of the buttons:

```
runProgram("ping", tbPing.Text);
runProgram("tracert", tbTracert.Text);
runProgram("nslookup", tbTracert.Text);
```

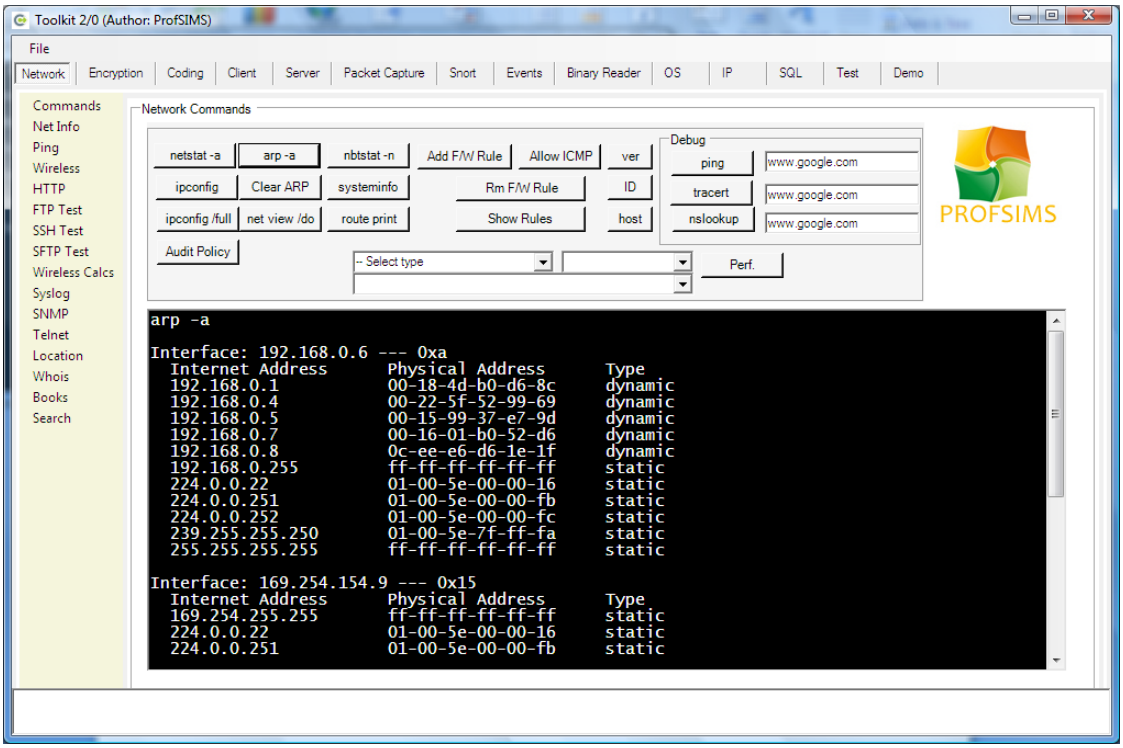


Figure L1.4 Buttons to add