

Name: _____ Student ID: _____

COS80013 Internet Security

Lab 2 (week 2)

You will need:
RedHat Linux 7.3 (VM)
Windows XP Pro (VM)
KaliLinux(VM)
A computer with internet access

In this lab you will set up a small network using VMWare.

1. Start **Virtual Machine Launcher** and load up the COS80013 / **Redhat Linux with local network** image.

Alternatively zipped copies are on Onedrive here: [Virtual Machines - OneDrive](#)

Observe the startup screen – note which services (servers) are started.
You can use **^S (Control S)** to pause the screen and **^Q (control Q)** to resume.

Pause the screen (Control S) when you see ***fstab***.

1.1 What is the location of ***fstab***?

1.2 What does ***fstab*** do / what is it used for? (use Google)

1.3. View the current `/etc/fstab` settings. Check if any partitions allow execution of unauthorized binaries ***grep -E '(exec/suid)' /etc/fstab*** Check if any partition lacks security options like `noexec`, `nodev`, or `nosuid`. What will be the security impact?

You should see things like

sshd
httpd
MySql
sendmail

starting up.

Once the image has finished booting, log in as

root

security

password

Name: _____ Student ID: _____

and type in
ifconfig

1.3 What is the IP address of the Linux server?

1.4 What is the loopback address?

1.5 How many errors have occurred?

2. Type in the command:

ps -A | more

2.1 List the daemon processes that are running on the server (one of each).

Use Google to identify each one you don't recognise.

-you can skip the ones starting with a k or v. Just list the ones ending in d

2.2 Which of these has vulnerabilities?

Use Google to search for the name of the service and the word: **vulnerability**,
or try searching **CVEdetails.com**

Name: _____ Student ID: _____

3. Use *find* to locate the *path* to the **http access_log**
(*check last-week's lab sheet for how to use find*)

Read the file: **more <path>access_log**

*<path> is the path you
found in 3*

3.1 How many accesses so far?

read the **http error_log** (same procedure).

3.2 Anything unusual?

Ctrl + Alt will release you from the guest VM

4. Go back to Virtual Machine Launcher and load up COS80013 / **Windows XPPro with local network.**

Open a command window (Start/Run/cmd)

Type in
ipconfig

4.1 What is the IP address of the XP machine?

Name: _____ Student ID: _____

type in
netstat

4.2 How many TCP connections are in place?

5. From the XP console window, Ping the Linux box:

ping 192.168.100.y *where the IP address is the one you found in 1.3 above.*

from the Linux box, ping the XP box:

ping -c 3 192.168.100.x *where the IP address is the one you found in 4.1 above.*

Now, check the **access** and **error logs** on the Linux box (using section 3 above)

5.1 Any change? Why?

6. On **XP**, start up the web browser, and go to the Linux box's IP address.

Now check the **logs** on the **Linux** box.

6.1 What is different?

7. Open up **Wireshark** on the **XP** box.

Select *Capture, Options*, and then click *Start*

Using the web browser, open a web page on the server (or refresh the page – F5) and observe the packets resulting from normal traffic. Don't close the browser.

7.1 What colour is normal web traffic?

On XP, open **WS-FTP** and attempt a log in (user: **anonymous**). Check **Wireshark** to see what ftp looks like.

7.2 Can you see the user name and password being sent? *Scroll through the FTP packets in the top*

window and look in the bottom window. The password will be at the end of a packet.

Name: _____ Student ID: _____

You can log in by FTP because both the student and anonymous users are not black-listed.

In Linux you can edit the black-list (vi /etc/ftpusers) to ban users by adding them to the list. Remember how to edit a file?

From the XP VM, try logging in to **Linux** using *telnet* (student:student)
telnet 192.168.100.104

How are the packets different? Look at the Wireshark display. What protocols? Colours?

7.3. Identify **Nmap scan activity** on the network, Start Wireshark on **XP Pro**, on **linux** run, **nmap -sS 192.168.100.103**, Stop capture and filter by **tcp.flags.syn==1 && tcp.flags.ack==0**. How does Nmap send stealth SYN scans? What ports were detected as open?

7.4. Start Wireshark on **XP Pro VM**, From **XP**, run “**ping -t 192.168.100.104**” Will Linux server slows down? Filter by icmp and check response times. What is a Ping flood attack?

7.5. Start Wireshark capture on XP. Open a browser and visit any website. In Wireshark, filter by **tcp.stream eq 1**. How does TCP maintain a stateful connection? What happens when FIN or RST flags are used?

7.6. On XP, try **netstat** again. How many connections?

On Linux, try **netstat -ap**.

7.7 How many connections? Use *more* to see one page at a time.

netstat -ap | more

Name: _____ Student ID: _____

8. On your host PC, open a console window and use **netstat** to look at the connections.

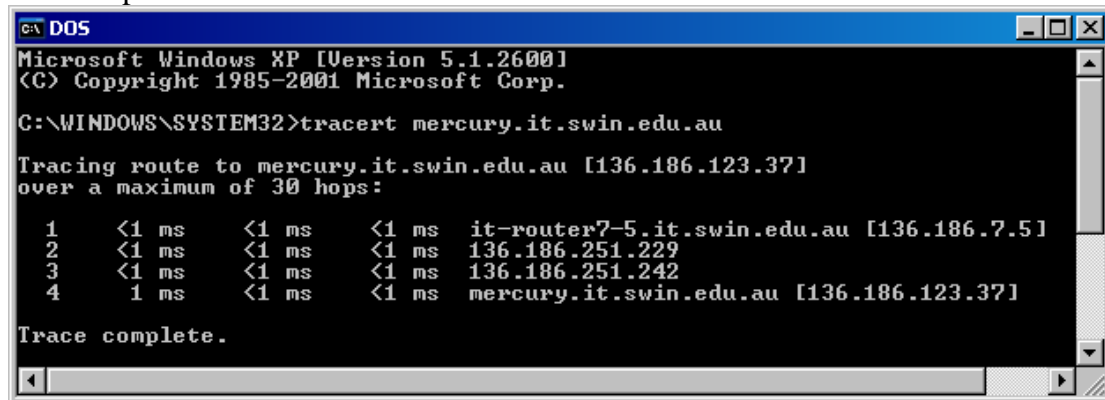
8.1 How many are there?

9. Close all applications on the XP and Linux images and shut the VMs down. Remember *poweroff* ?

10. From your host PC, try this command:

tracert google.com

for example:



```
c:\ DOS
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\SYSTEM32>tracert mercury.it.swin.edu.au

Tracing route to mercury.it.swin.edu.au [136.186.123.37]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    it-router7-5.it.swin.edu.au [136.186.7.5]
  1  <1 ms    <1 ms    <1 ms    136.186.251.229
  2  <1 ms    <1 ms    <1 ms    136.186.251.242
  3  1 ms     <1 ms    <1 ms    mercury.it.swin.edu.au [136.186.123.37]

Trace complete.
```

10.1 What is the IP address of the router between you and the mercury server?

10.2 How many hops?