Name: _____ **Student ID:**_____

You will need:
RedHat Linux (VM)
Windows XP (VM)
Windows XP Control (VM)
Windows 95 (VM)
A computer with internet access

COS80013 Internet Security

Lab 5 (week 5)

In this lab you will perform **network reconnaissance and a denial of service attack**.

1. Start **Virtual Machine Launcher** and download and run the
   COS80013 / ***RedHat Linux with local network*** image.

Download and run the
   COS80013 / ***Windows XP-Pro with local network*** image.

   Alternatively zipped copies:
Virtual Machines.

Part 1: Network reconnaissance

2. On XP, start **Wireshark**
   start capture:
   select **Capture Options**
   Click "**Start**"

Wait for a minute or two and observe the network traffic initiated by the XP image (NBNS and BROWSER protocols). If there is no traffic, continue through the lab.

Use **Google** to find out about NBNS and BROWSER.
What are the NBNS and BROWSER protocols?

3. On RHLinux, log in as
student
student

password

type
nmap --help
What does the *–sP* option do?

4. **Network Reconnaissance**

To find all PCs on the local subnet, type

nmap –sP 192.168.100.0/24 ***//an IP scan***

Name: _____ Student ID:_____

How many addresses will be scanned?

What IP addresses are found?

Which one is yours (the Linux VM)? Use **ifconfig.** (**`/sbin/ifconfig`**)

5. On XP, have a look at the **nmap** scan in **Wireshark**.
Which protocol does it use?

How would you recognise these packets as a *scan* if you were a firewall?

Back in **Wireshark**, scroll up and look for the start of a 3-way handshake (look for individual packets marked in green). There will be a SYN TCP packet, followed a bit later by a SYN ACK TCP packet. This is how ***nmap*** detects a responding host.

From XP, open a console window and telnet to the Linux VM

```
Start/Run/cmd
telnet 192.168.100.104
```

No need to log in.

Back in **Wireshark**, scroll up and look for the 3-way handshake (first three TCP packets before the TELNET packets) – this is the successful connection of the victim's box to the attacker's Linux box.

If you time-out or end the telnet session, you will terminate the connection. Look for the 4-way tear-down sequence FIN, FIN ACK, FIN ACK, ACK in Wireshark.

6. On Linux, ping the XP box:
```
ping 192.168.100.130
```

On XP, observe the results.

How could you prevent this (and thereby hide your XP box)?

Note: there is no firewall running on XP (no service pack) – you need to turn it on to disable **ping** responses.

In The XP VM, enable the firewall and block ICMP:

Right-click on the small network icon near the click (bottom-right-hand corner) and select ***Open Network Connections***.
Right-click on ***Local Area Connection*** and select ***Properties***
Click on the ***Advanced*** tab and check the ***Protect my computer…*** box
[**OK**]

Observe Wireshark – **What happens to the Ping replies?**

On Linux, you can stop sending the pings typing <**Ctrl**> + **C**

7. On Linux,
enter the command
`man -k traceroute`
What does traceroute do?

Type in
`/usr/sbin/traceroute 192.168.100.130`

You will get a series of * as XP's firewall is now blocking ICMP.

Disable the Windows firewall (Right-click on ***Local Area Connection*** and select ***Properties***
Click on the ***Advanced*** tab and uncheck the ***Protect my computer…*** box
[**OK**])

In Linux, try traceroute again.

The route from Linux to XP is only one hop – no intermediate routers.

On XP, observe the Wireshark traffic caused by **traceroute.**
What is happening during a traceroute? (look at the red-brown and black lines).

Hint: Expand the Internet Protocol layer in the middle Wireshark window to see the IP header. Note the Time To Live.

Name: _____ Student ID:_____

8. In Virtual machine Launcher, download and launch **Windows XP-Control** (the VM).

Start up the XAMPP servers:

On the desktop, double-click on the orange XAMPP icon 

Start up all four services (Filezilla will need to be installed as a service)

On **Red Hat Linux**, enter the command

```
nmap 192.168.100.103
```

What ports and services are running on the XP-control box?

Try logging into a few:
e.g. type

```
telnet 192.168.100.103 88
HEAD / HTTP/1.0
```

(press Enter a few times)

Is this a Kerberos server?

What version of the web server is running?

Name: _____ **Student ID:**_____

```
[student@server student]$ telnet 192.168.100.130 http
Trying 192.168.100.130...
Connected to 192.168.100.130 (192.168.100.130).
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 18 Sep 2012 04:11:56 GMT
Server: Apache/2.2.4 (Win32) DAV/2 mod_ssl/2.2.4 OpenSSL/0.9.8e mod_autoindex_co
lor PHP/5.2.3
X-Powered-By: PHP/5.2.3
Connection: close
Content-Type: text/html
```

On the host, use Google to search for vulnerabilities (exploits) for this version of Apache. **Are there any? Example CVEs?**

Try **`telnet 192.168.100.103 221`**

Is this a fin-spx server (Berkeley rlogind with SPX auth)**?**

What service is there and what version is running?
(Type **quit** to quit)

nmap is getting it wrong, because like most networking software, it looks up the service name in a file called */etc/services* which contains the suggested mapping of services to ports. Windows has one too – in *Windows\System32\Drivers\etc*.

ANY SERVICE CAN RUN ON ANY PORT

9. On Linux, change to the *root* user:
su — ***su* means substitute user – log in as another user (*root* by default)**
security — **password**

try this command:
`nmap -O 192.168.100.103`

What version of Windows does nmap think is running?

Name: _____ **Student ID:**_____

10. On the XP desktop, run ***Superscan*** – try to find the IP address of the Linux box.
    enter **192.168.100.1** as the start address
    enter **192.168.100.254** as the end address
    click on the arrow button 

Note: RHLinux is running a **honeypot** which walks up after the first scan. You may find many other hosts on the subnet, but only one is real.
When you get a chance, look up what a *honeypot (computer science)* is.

What is the IP address of the Linux box?

Did you find any other IP addresses? Try running ***superscan*** again

TOOLS GET IT WRONG

From the Linux box, use **`nmap 192.168.100.yyy`** (where yyy is the final octet of your Linux box), scan the ports open on Linux.

Which ports are open on the Linux box?

11. On Linux, create a directory called "snortlog"

```
mkdir snortlog
```

run snort :

```
/usr/sbin/snort -vd -l ./snortlog
```

On XP, open a command window (Start / Run / command / enter) and log into Linux:

Name: _____ **Student ID:**_____

`telnet 192.168.100.104` (or **`telnet www.server.com`**)
(user: `sucker`, password: `briantoldme`)

You can watch the packets live on the Linux box as you log in

do an **`ls`**, and exit

On Linux, type *Control+C* to stop **snort**
type:
`cd snortlog`

`cd` 192.168.100.130
`ls`
What files are present?

Type a file:
`more TCP:nnnn-23`
(nnnn will be a port number allocated at the time of the connection – use **`ls`** to see what it is.)

Press the space bar while watching the packet contents on the right of the screen – when you see the word "login", note down the single letter at the start of each packet (followed by space).

Continue looking through the file until you find the word "password"-
note down the single letter at the start of each packet.

What is the user name and password?

Part 2: Denial of Service

On XP, return to **Wireshark**

12. On XP, start (or return to) the web browser and go to
http://192.168.100.104 or http://www.server.com

13. On XP, start Task Manager (Right-click on an unused part of the lower toolbar, and select
Task Manager

Name: _____ **Student ID:**_____

Change to the ***"Performance"*** Tab.

14. On Linux, log in as
hacker
warezwarez (password)

cd to the ***exploits*** directory

Have a look at the contents of *jolt.c*

more jolt.c

What does jolt do?

Compile it:

gcc –o jolt jolt.c

What operating system was it intended for?

Permit it to execute:

chmod +x jolt

Run it:

./jolt

Need an IP address of the target?
use nmap to scan for a Windows victim:

nmap –sT 192.168.100.0/24

What is the target IP address?

Now try again:

./jolt 192.168.100.130 192.168.100.130 10

number of packets

spoofed source IP

destination IP

"Operation not permitted"?
Change to **root**:

su (substitute user)
security (the root password)

Try **./jolt** again.

On XP check the Performance and Networking graphs. ***Did XP get a spike?***

Name: _____ **Student ID:**_____

What information does Wireshark display about the packets sent by jolt?

Try:

```
./jolt 192.168.100.130 192.168.100.130 100
```

How bad is it this time?

What was the max CPU load?

What would happen if 10,000 computers sent a jolt at the same time to one computer?

15. Download and run the ***Windows95 with local network*** virtual machine.

Double-click on the clock so that you can see the clock face with the second hand (moving).

Use ***nmap*** to find the IP address of the win95 machine:

```
nmap –sP 192.168.100.0/24
```

What is the target IP address?

To confirm that it is *win95*,

```
nmap –O 192.168.100.x
```

x is the final octet of the IP address.

Try using jolt:

```
./jolt 192.168.100.x 192.168.100.x 100
```

You can monitor the network traffic using wireshark running on the XP machine, even though XP is not being attacked.

Is Win95 running?

15. On XP, close Wireshark (Continue without saving),
16. Shut down all guest OSs (**`poweroff`**, ***Start/Turn off computer***, close VMWare, the browser, etc.) and log out.

Name: _____ Student ID:_____

Homework:

In your spare time look up the *Low Orbit Ion Cannon*.

What is it?

How many versions are there?

Why is it so popular with script kiddies?

What about the High Orbit Ion Cannon?

What techniques mitigate or stop DDOS attacks?

End of Lab.