Internet Security – COS80013 Lab - 2 Report

Student ID: 104837257
Student Name: Arun Ragavendhar Arunachalam Palaniyappan
Lab Name: COS80013 Lab 2 – Virtual Network Setup & Network Traffic Monitoring
Lab Date: 21 /03/2025
Tutor: Yasas Akurudda Liyanage Don

Title and Introduction

Setting up a Local Network between 2 VMs one with Redhat Linux and another with Windows XP pro and setting up and testing connectivity between them.

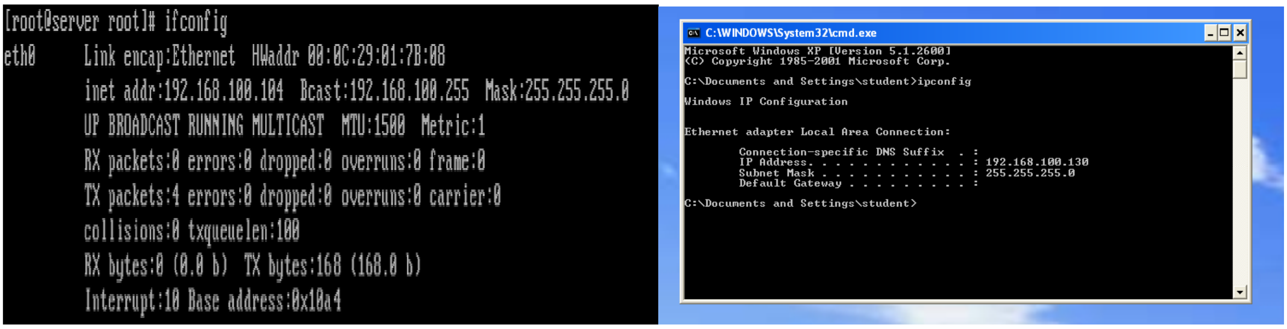
Using Wireshark to monitor and analyse the network protocols and checking the access logs and error logs to confirm the connectivity and communication between the 2 VMs.

Methodology:

- **Ps -a -** command run to check and observe the different daemon processes.
- **ifconfig -** run on Linux VM to extract its IP address.
- **ipconfig -** run on Windows XP pro VM to get its IP address.
- **192.168.100.104 (Linux VM IP)** searched in the URL of a browser in the Windows VM and http access logs viewed from the Linux VM and connectivity was verified.
- **ping 192.168.100.130 (windowsXPpro VM IP)** run from Linux Machine and connectivity was verified.
- A TELNET connection ping was also tried out.
- Simultaneously, the Wireshark tools was used to see the various network packets transferred under different protocols (HTTP, TCP, TELNET, etc).
- Netstat command run from both VMs to confirm the connectivity status.

Data Recording and Screenshots:

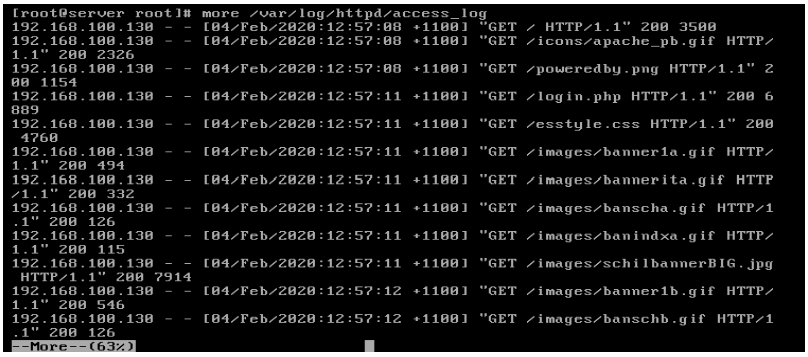
IP details of Linux Box and IP details of windowsXPpro system.



```
[root@server root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:01:7B:08
          inet addr:192.168.100.104  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:168 (168.0 b)
          Interrupt:10 Base address:0x10a4
```

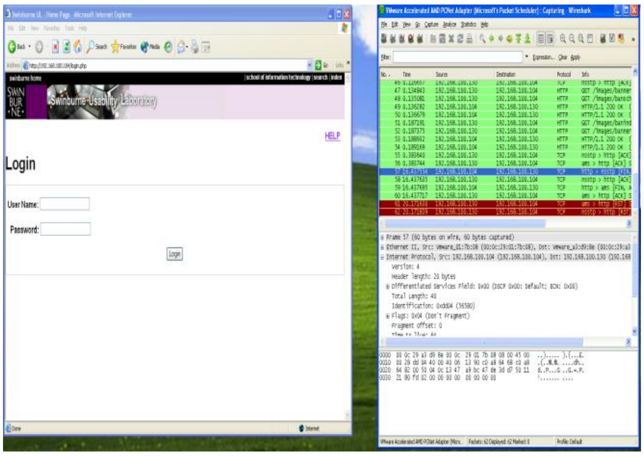
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\student>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.100.130
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\student>
```

Access logs from the Linux VM showing HTTP GET requests from the windows XP VM



```
[root@server root]# more /var/log/httpd/access_log
192.168.100.130 - - [04/Feb/2020:12:57:08 +1100] "GET / HTTP/1.1" 200 3500
192.168.100.130 - - [04/Feb/2020:12:57:08 +1100] "GET /icons/apache_pb.gif HTTP/
1.1" 200 2326
192.168.100.130 - - [04/Feb/2020:12:57:08 +1100] "GET /poweredby.png HTTP/1.1" 2
00 1154
192.168.100.130 - - [04/Feb/2020:12:57:11 +1100] "GET /login.php HTTP/1.1" 200 6
889
192.168.100.130 - - [04/Feb/2020:12:57:11 +1100] "GET /esstyle.css HTTP/1.1" 200
 4760
192.168.100.130 - - [04/Feb/2020:12:57:11 +1100] "GET /images/banner1a.gif HTTP/
1.1" 200 494
192.168.100.130 - - [04/Feb/2020:12:57:11 +1100] "GET /images/bannerita.gif HTTP
/1.1" 200 332
192.168.100.130 - - [04/Feb/2020:12:57:11 +1100] "GET /images/banscha.gif HTTP/1
.1" 200 126
192.168.100.130 - - [04/Feb/2020:12:57:11 +1100] "GET /images/banindxa.gif HTTP/
1.1" 200 115
192.168.100.130 - - [04/Feb/2020:12:57:11 +1100] "GET /images/schilbannerBIG.jpg
 HTTP/1.1" 200 7914
192.168.100.130 - - [04/Feb/2020:12:57:12 +1100] "GET /images/banner1b.gif HTTP/
1.1" 200 546
192.168.100.130 - - [04/Feb/2020:12:57:12 +1100] "GET /images/banschb.gif HTTP/1
.1" 200 126
--More--(63%)
```

Wireshark network protocol monitoring when the windows machine is used to connect and view the Linux machine’s web pages. Telnet Connection from WindowsXPpro to Linux.



Swinburne IA - Home Page - Microsoft Internet Explorer

Address: http://192.168.100.104/login.php

swinburne home | school of information technology | search | index

Swinburne Usability Laboratory

HELP

Login

User Name:

Password:

Login

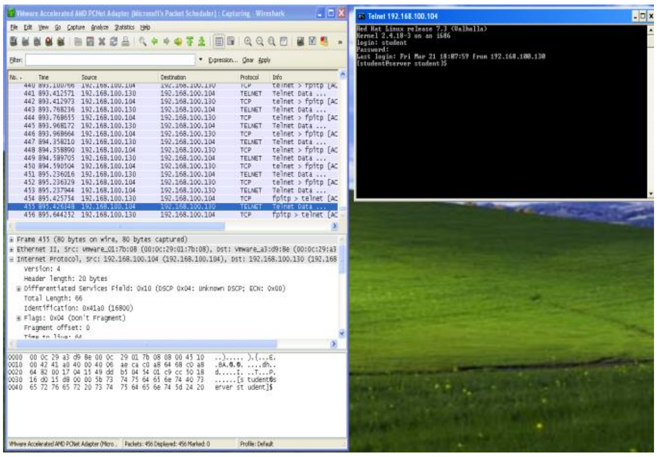
VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark

```
No. .  Time       Source           Destination      Protocol  Info
46 0.13?657       192.168.100.130  192.168.100.104  TCP       nsstp > http [ACK]
47 0.134843       192.168.100.130  192.168.100.104  HTTP      GET /images/banner
48 0.135082       192.168.100.130  192.168.100.104  HTTP      GET /images/banech
49 0.136282       192.168.100.104  192.168.100.130  HTTP      HTTP/1.1 200 OK  (
50 0.136679       192.168.100.104  192.168.100.130  HTTP      HTTP/1.1 200 OK  (
51 0.187181       192.168.100.130  192.168.100.104  HTTP      GET /images/banind
52 0.187375       192.168.100.130  192.168.100.104  HTTP      GET /images/banner
53 0.188892       192.168.100.104  192.168.100.130  HTTP      HTTP/1.1 200 OK  (
54 0.189168       192.168.100.104  192.168.100.130  HTTP      HTTP/1.1 200 OK  (
55 0.383640       192.168.100.130  192.168.100.104  TCP       nsstp > http [ACK]
56 0.383744       192.168.100.130  192.168.100.104  TCP       ams > http [ACK] S
57 16.437554      192.168.100.104  192.168.100.130  TCP       http > nsstp [FIN,
58 16.437635      192.168.100.130  192.168.100.104  TCP       nsstp > http [ACK]
59 16.437685      192.168.100.104  192.168.100.130  TCP       http > ams [FIN, A
60 16.437717      192.168.100.130  192.168.100.104  TCP       ams > http [ACK] S
61 20.171688      192.168.100.130  192.168.100.104  TCP       ams > http [RST] S
62 20.171819      192.168.100.130  192.168.100.104  TCP       nsstp > http [RST]
```

```
⊞ Frame 57 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Vmware_01:7b:08 (00:0c:29:01:7b:08), Dst: Vmware_a3:d9:8e (00:0c:29:a3
⊟ Internet Protocol, Src: 192.168.100.104 (192.168.100.104), Dst: 192.168.100.130 (192.168
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 40
    Identification: 0xdd04 (56580)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
```

```
0000  00 0c 29 a3 d9 8e 00 0c  29 01 7b 08 08 00 45 00   ..)..... ).{...E.
0010  00 28 dd 04 40 00 40 06  13 90 c0 a8 64 68 c0 a8   .(..@.@. ....dh..
0020  64 82 00 50 04 0c 13 47  a9 bc 47 de 3d d7 50 11   d..P...G ..G.=.P.
0030  21 80 fd 02 00 00 00 00  00 00 00 00               !....... ....
```

VMware Accelerated AMD PCNet Adapter (Micro... | Packets: 62 Displayed: 62 Marked: 0 | Profile: Default



VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark

```
No. .  Time         Source           Destination      Protocol  Info
440 893.100766      192.168.100.104  192.168.100.130  TCP       telnet > fpitp [AC
441 893.412571      192.168.100.130  192.168.100.104  TELNET    Telnet Data ...
442 893.412973      192.168.100.104  192.168.100.130  TCP       telnet > fpitp [AC
443 893.768236      192.168.100.130  192.168.100.104  TELNET    Telnet Data ...
444 893.768655      192.168.100.104  192.168.100.130  TCP       telnet > fpitp [AC
445 893.968172      192.168.100.130  192.168.100.104  TELNET    Telnet Data ...
446 893.968664      192.168.100.104  192.168.100.130  TCP       telnet > fpitp [AC
447 894.358210      192.168.100.130  192.168.100.104  TELNET    Telnet Data ...
448 894.358890      192.168.100.104  192.168.100.130  TCP       telnet > fpitp [AC
449 894.589705      192.168.100.130  192.168.100.104  TELNET    Telnet Data ...
450 894.590504      192.168.100.104  192.168.100.130  TCP       telnet > fpitp [AC
451 895.236016      192.168.100.130  192.168.100.104  TELNET    Telnet Data ...
452 895.236329      192.168.100.104  192.168.100.130  TCP       telnet > fpitp [AC
453 895.237944      192.168.100.104  192.168.100.130  TELNET    Telnet Data ...
454 895.425754      192.168.100.130  192.168.100.104  TCP       fpitp > telnet [AC
455 895.426348      192.168.100.104  192.168.100.130  TELNET    Telnet Data ...
456 895.644252      192.168.100.130  192.168.100.104  TCP       fpitp > telnet [AC
```

```
⊞ Frame 455 (80 bytes on wire, 80 bytes captured)
⊞ Ethernet II, Src: Vmware_01:7b:08 (00:0c:29:01:7b:08), Dst: Vmware_a3:d9:8e (00:0c:29:a3
⊟ Internet Protocol, Src: 192.168.100.104 (192.168.100.104), Dst: 192.168.100.130 (192.168
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00)
    Total Length: 66
    Identification: 0x41a0 (16800)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
```

```
0000  00 0c 29 a3 d9 8e 00 0c  29 01 7b 08 08 00 45 10   ..)..... ).{...E.
0010  00 42 41 a0 40 00 40 06  ae ca c0 a8 64 68 c0 a8   .BA.@.@. ....dh..
0020  64 82 00 17 04 15 49 dd  b5 04 54 01 c9 cc 50 18   d.....I. ..T...P.
0030  16 d0 15 d8 00 00 5b 73  74 75 64 65 6e 74 40 73   ......[s tudent@s
0040  65 72 76 65 72 20 73 74  75 64 65 6e 74 5d 24 20   erver st udent]$
```

VMware Accelerated AMD PCNet Adapter (Micro... | Packets: 456 Displayed: 456 Marked: 0 | Profile: Default

Telnet 192.168.100.104

```
Red Hat Linux release 7.3 (Valhalla)
Kernel 2.4.18-3 on an i686
login: student
Password:
Last login: Fri Mar 21 18:07:59 from 192.168.100.130
[student@server student]$
```

Discussion and application of Learnings:

Learning 1:

- The method/procedure and CLI commands to make connections between different Virtual Machines and setting up a local network and verifying the connection were learnt in this lab.

Real World Application in cyber security Industry:

- This learning can be used to set up a virtual test environment for simulating attacks. For example, an analyst can connect a Linux VM (acting as a web server) and a Windows XP VM (as a client) to test how malware spreads across the network and identify weak points in system communication.

Learning 2:

- Usage of Wireshark monitoring tool to monitor and analyse the packets and the different network protocols through which the 2 VMs are communicating.

Real World Application in cyber security Industry:

- This learning can be used to detect data breaches using Wireshark. For instance, if a Windows XP machine sends suspicious HTTP traffic to an unknown IP, an analyst can capture and analyze the packets to confirm data exfiltration and take immediate action.

Limitation

One key limitation observed in this lab is the use of TELNET and HTTP protocols for communication. TELNET transmits data, including login credentials, in plain text, making it highly vulnerable to interception and man-in-the-middle attacks. Similarly, HTTP lacks encryption, exposing all data exchanged between client and server. In real-world scenarios, secure alternatives like SSH (for remote access) and HTTPS (which uses SSL/TLS encryption) should be used to ensure data confidentiality and integrity during transmission.