**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.

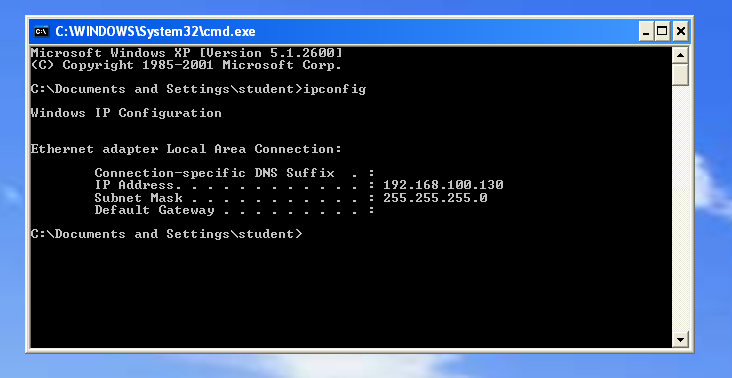
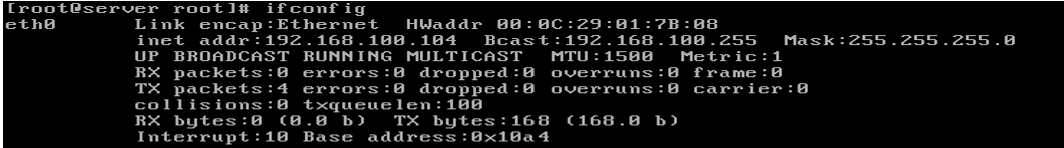
Using Wireshark to monitor and analyse the network protocols and checking the access logs and error logs to confirm the connectivity and communication between the 2 VMs.

**Methodology:**

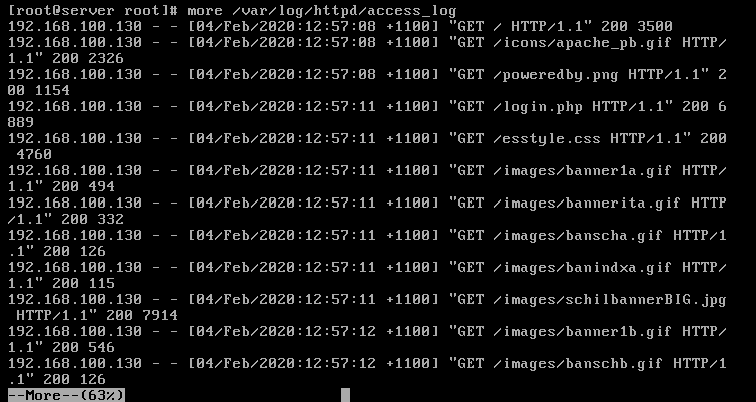
* **Ps -a -** command run to check and observe the different daemon processes.
* **ifconfig -** run on Linux VM to extract its IP address.
* **ipconfig -** run on Windows XP pro VM to get its IP address.
* **192.168.100.104 (Linux VM IP)** searched in the URL of a browser in the Windows VM and http access 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:**

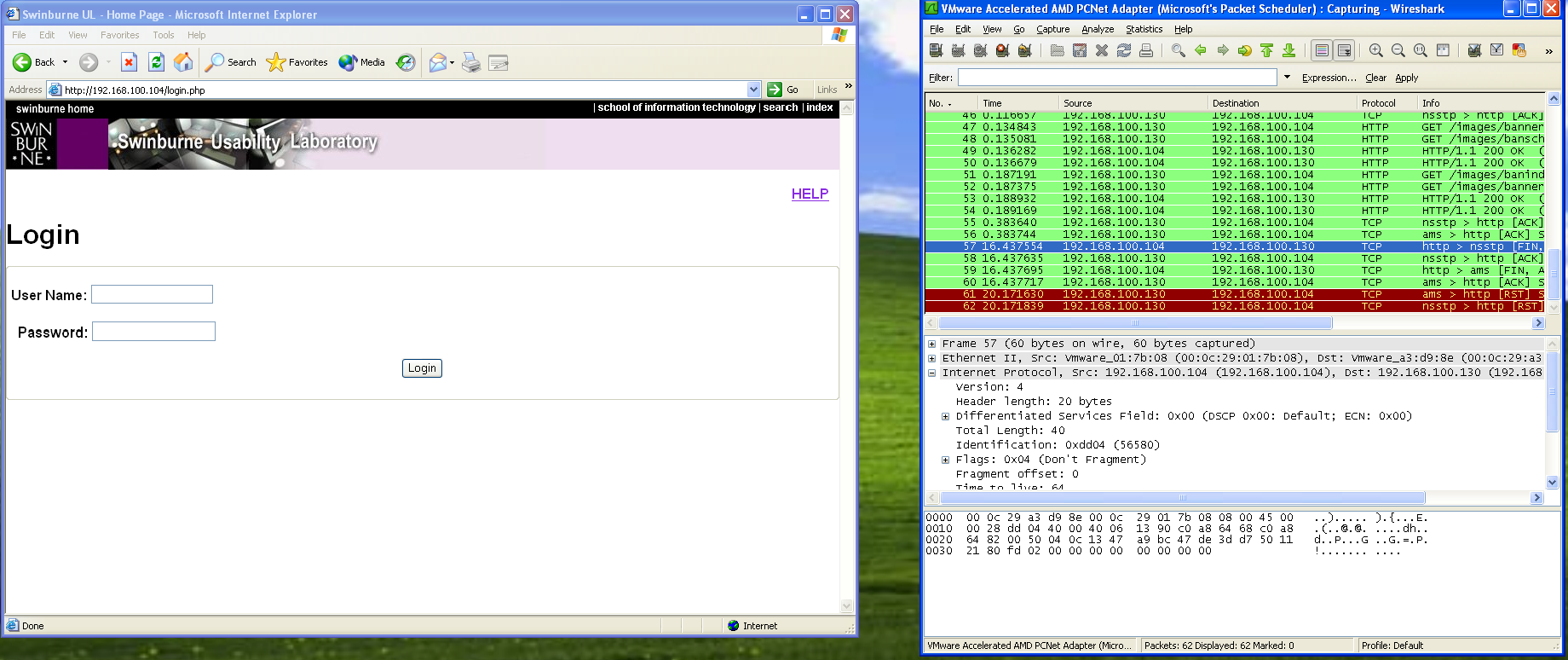
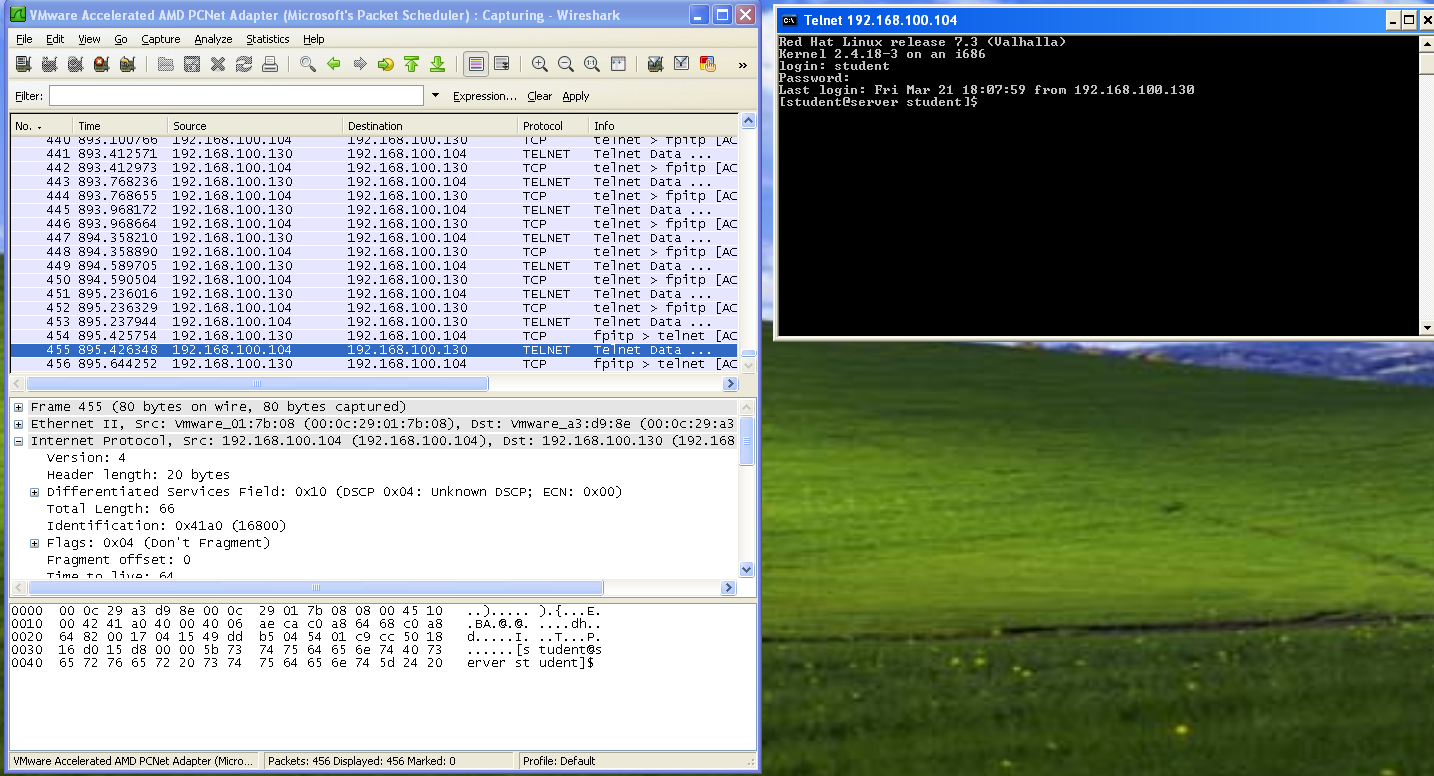
IP details of Linux Box and IP details of windowsXPpro system.



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



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.

**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.