**Internet Security – COS80013 Lab - 5 Report**

**Student ID:** 104837257  
**Student Name:** Arun Ragavendhar Arunachalam Palaniyappan  
**Lab Name:** COS80013 Lab 5 – Network Reconnaissance and a Denial-of-service attack.  
**Lab Date:** 04 /04/2025  
**Tutor:** Yasas Akurudda Liyanage Don

**Title and Introduction**

This lab was about simulating basic network attacks in a safe environment using virtual machines. The tasks included scanning the local network, tracing routes, blocking pings using a firewall, capturing credentials with a packet sniffer, and launching a denial-of-service (DoS) attack. The idea was to understand how attackers perform reconnaissance and disrupt systems, and how simple defences like firewalls can reduce exposure. Tools like nmap, Wireshark, snort, and a C-based exploit (jolt.c) were used.

**Methodology**

First the RedHat Linux and Windows XP virtual machines were started. Wireshark was started on XP to monitor background traffic.On Linux, the nmap –sP 192.168.100.0/24 command was used to scan the subnet. This listed other active machines. The Linux machine’s IP was found using ifconfig, and responses to the scan showed SYN and ACK handshake packets in Wireshark.The Linux VM then sent ICMP pings to the XP machine. To block them, the XP firewall was enabled via **Network Connections > Advanced**, which stopped ping replies. Wireshark confirmed that the echo replies were no longer received.

Traceroute from Linux to XP was run using /usr/sbin/traceroute. With the firewall on, no reply came through. After turning the firewall off, it showed one direct hop between the machines, and TTL values were visible in the IP header.

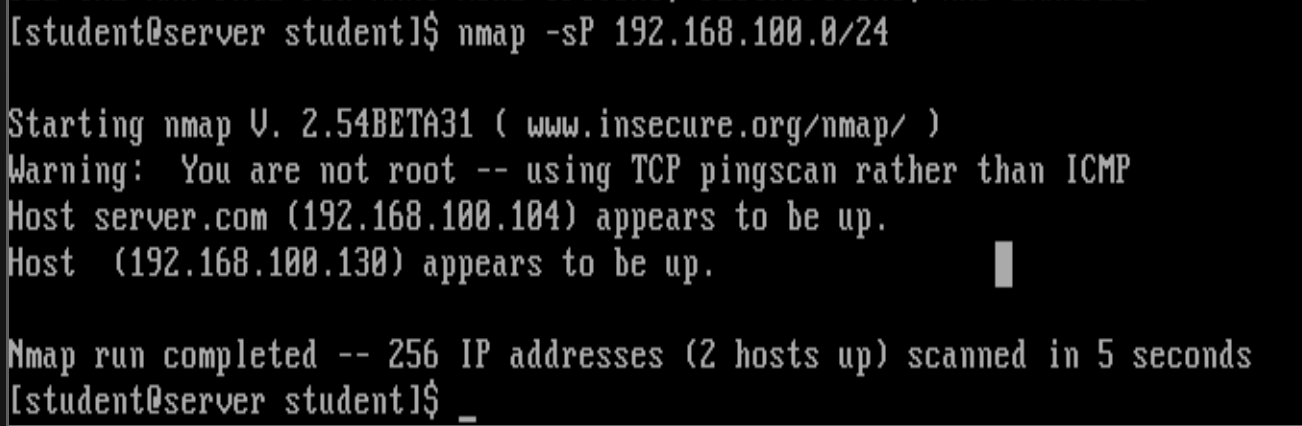
Windows XP-Control VM was scanned using nmap, revealing ports like 80 (HTTP), 88 (Kerberos), and 221. Telnet was used to connect to port 88, and by typing a basic HTTP request, the Apache version was identified. A quick online search showed known vulnerabilities linked to that version.

Snort command was run on Linux with /usr/sbin/snort –vd –l ./snortlog, and from the XP VM, telnet was used to log in with a given username and password. Once snort was stopped, the log files were checked, and the captured packets showed the credentials being sent in plain text.

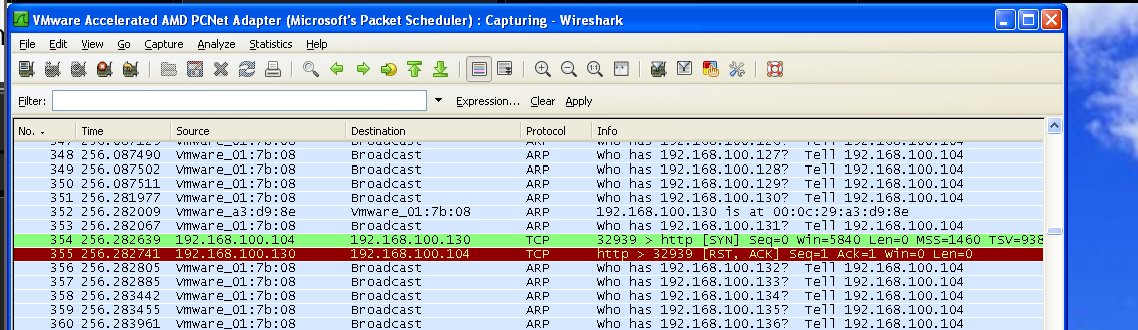
Lastly, the DoS part was carried out. The jolt.c file was compiled and made executable. The command ./jolt 192.168.100.104 192.168.100.130 100 was run to send spoofed traffic to the XP machine. Task Manager on XP showed CPU usage spikes. When the packet count was increased to 10000, the system became sluggish, confirming the attack's impact.

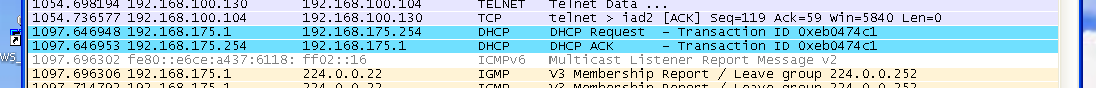
**Data Recording and Screenshots**

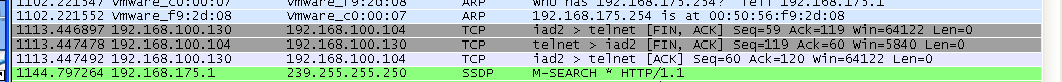
* **Nmap Scan** – Detected active IPs in subnet



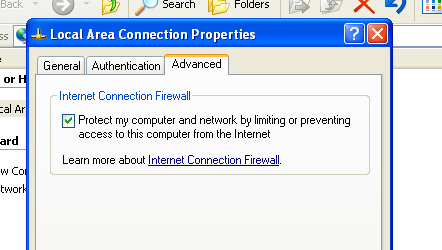
* **Wireshark** – Showed TCP handshakes and ping traffic

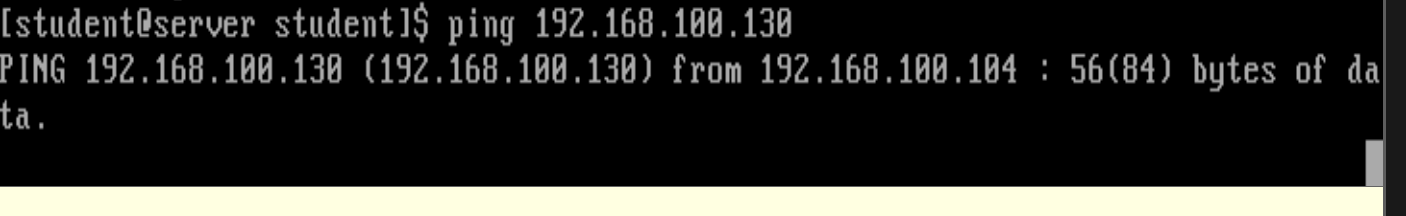




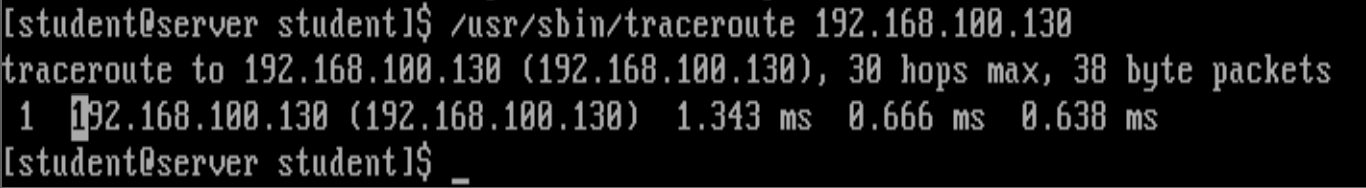


* **Firewall Enabled** – Ping replies from XP stopped

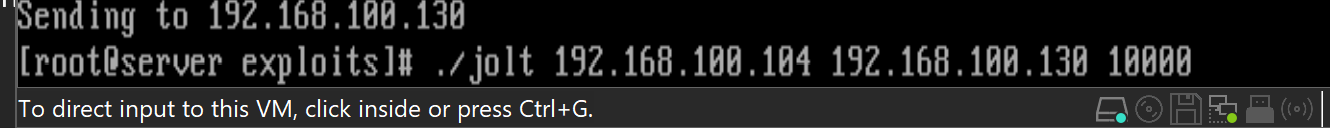


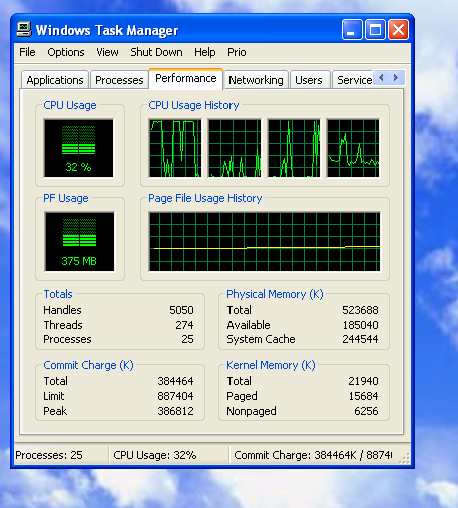


* **Traceroute** – Confirmed one-hop route to XP



* **Jolt DoS Attack** – CPU usage spike visible in Task Manager





**Discussion and Learnings**

**Learning 1**  
The main learning was about how attackers use tools like nmap and Wireshark to scan a network and find targets. The scan traffic was clearly visible, showing how network monitoring can help detect intrusions early.

**Real-World Link**  
This is how real-world attackers identify vulnerable systems. Network admins use the same tools to monitor and block unusual activity.

**Learning 2**  
Turning on the firewall stopped pings and blocked traceroute. This showed how even a basic firewall can hide a machine from attackers doing reconnaissance.

**Real-World Link**  
This technique is often used to protect important systems from being found during network scans.

**Learning 3**  
Running jolt showed how easily a system can be overloaded with fake traffic. The packet flood caused the XP VM to slow down significantly.

**Real-World Link**  
Modern DoS attacks are more powerful, often distributed (DDoS), and can bring down websites or services. Security systems must be in place to stop or reduce their effects.

**Limitations**

* The lab used old operating systems like windows XP which behave differently to modern systems.
* The jolt.c attack is outdated, but it still helped show how packet floods work.
* Only basic credential capture was done. In real life, encryption and secure protocols make this harder.