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.

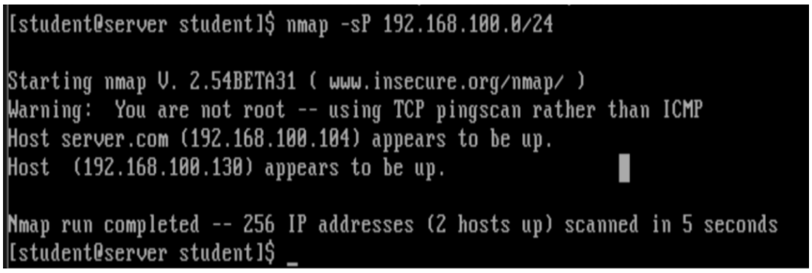
Windows XP-Control VM was scanned using nmap, revealing ports like 80 (HTTP), 88 (Kerberos), and 221. Telnet was used to connect to port 88, and by typing a basic HTTP request, the Apache version was identified. A quick online search showed known vulnerabilities linked to that version.

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

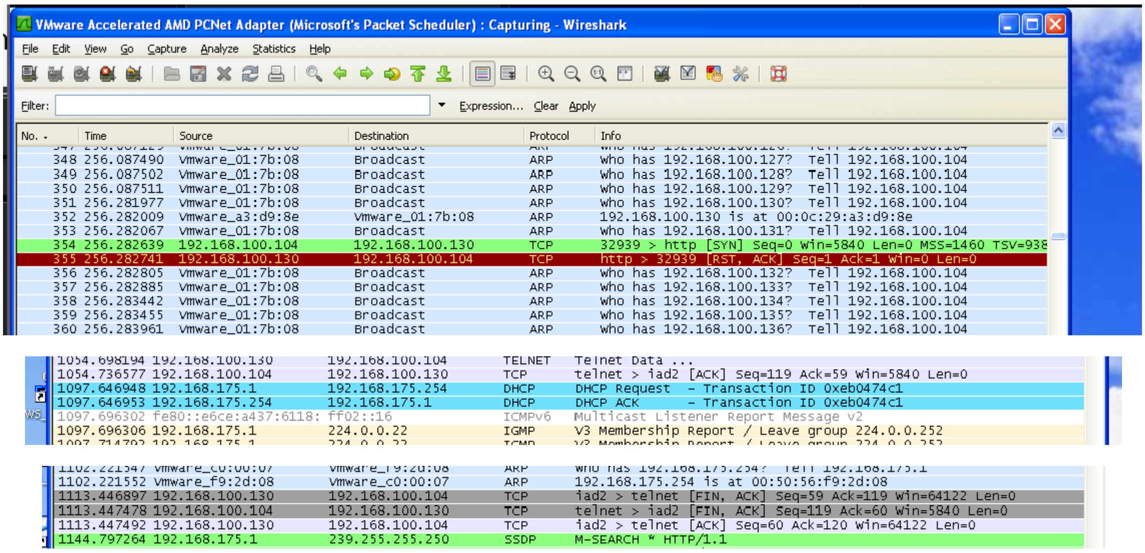


```
[student@server student]$ nmap -sP 192.168.100.0/24

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Warning:  You are not root -- using TCP pingscan rather than ICMP
Host server.com (192.168.100.104) appears to be up.
Host  (192.168.100.130) appears to be up.

Nmap run completed -- 256 IP addresses (2 hosts up) scanned in 5 seconds
[student@server student]$ _
```

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



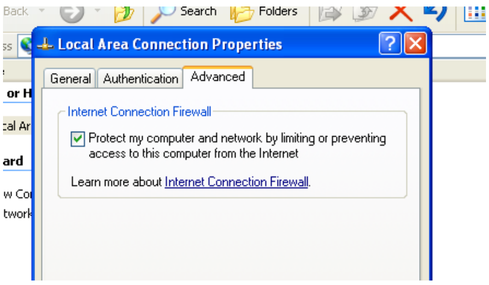
VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Help
Filter:
Expression...
Clear
Apply

```
No. -  Time        Source                Destination          Protocol  Info
348 256.087490  Vmware_01:7b:08       Broadcast            ARP       Who has 192.168.100.127?  Tell 192.168.100.104
349 256.087502  Vmware_01:7b:08       Broadcast            ARP       Who has 192.168.100.128?  Tell 192.168.100.104
350 256.087511  Vmware_01:7b:08       Broadcast            ARP       Who has 192.168.100.129?  Tell 192.168.100.104
351 256.281977  Vmware_01:7b:08       Broadcast            ARP       Who has 192.168.100.130?  Tell 192.168.100.104
352 256.282009  Vmware_a3:d9:8e       Vmware_01:7b:08      ARP       192.168.100.130 is at 00:0c:29:a3:d9:8e
353 256.282067  Vmware_01:7b:08       Broadcast            ARP       Who has 192.168.100.131?  Tell 192.168.100.104
354 256.282639  192.168.100.104       192.168.100.130      TCP       32939 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=938
355 256.282741  192.168.100.130       192.168.100.104      TCP       http > 32939 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
356 256.282805  Vmware_01:7b:08       Broadcast            ARP       Who has 192.168.100.132?  Tell 192.168.100.104
357 256.282885  Vmware_01:7b:08       Broadcast            ARP       Who has 192.168.100.133?  Tell 192.168.100.104
358 256.283442  Vmware_01:7b:08       Broadcast            ARP       Who has 192.168.100.134?  Tell 192.168.100.104
359 256.283455  Vmware_01:7b:08       Broadcast            ARP       Who has 192.168.100.135?  Tell 192.168.100.104
360 256.283961  Vmware_01:7b:08       Broadcast            ARP       Who has 192.168.100.136?  Tell 192.168.100.104

1054.698194 192.168.100.130          192.168.100.104      TELNET    Telnet Data ...
1054.736577 192.168.100.104          192.168.100.130      TCP       telnet > iad2 [ACK] Seq=119 Ack=59 Win=5840 Len=0
1097.646948 192.168.175.1            192.168.175.254      DHCP      DHCP Request  - Transaction ID 0xeb0474c1
1097.646953 192.168.175.254          192.168.175.1        DHCP      DHCP ACK      - Transaction ID 0xeb0474c1
1097.696302 fe80::e6ce:a437:6118:    ff02::16             ICMPv6    Multicast Listener Report Message v2
1097.696306 192.168.175.1            224.0.0.22           IGMP      V3 Membership Report / Leave group 224.0.0.252

1102.221552 Vmware_f9:2d:08          Vmware_c0:00:07      ARP       192.168.175.254 is at 00:50:56:f9:2d:08
1113.446897 192.168.100.130          192.168.100.104      TCP       iad2 > telnet [FIN, ACK] Seq=59 Ack=119 Win=64122 Len=0
1113.447478 192.168.100.104          192.168.100.130      TCP       telnet > iad2 [FIN, ACK] Seq=119 Ack=60 Win=5840 Len=0
1113.447492 192.168.100.130          192.168.100.104      TCP       iad2 > telnet [ACK] Seq=60 Ack=120 Win=64122 Len=0
1144.797264 192.168.175.1            239.255.255.250      SSDP      M-SEARCH * HTTP/1.1
```

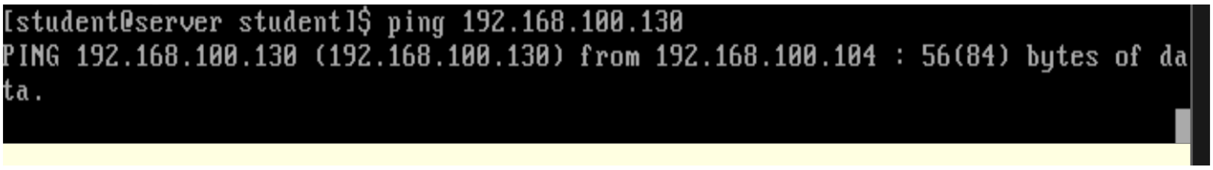
- **Firewall Enabled** – Ping replies from XP stopped



Back
Search
Folders
Local Area Connection Properties
General
Authentication
Advanced
Internet Connection Firewall

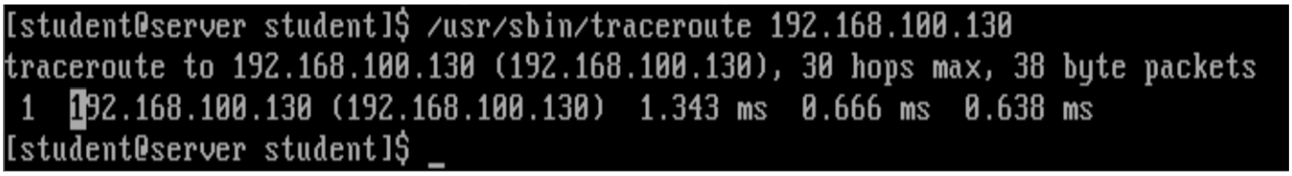
☑ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.



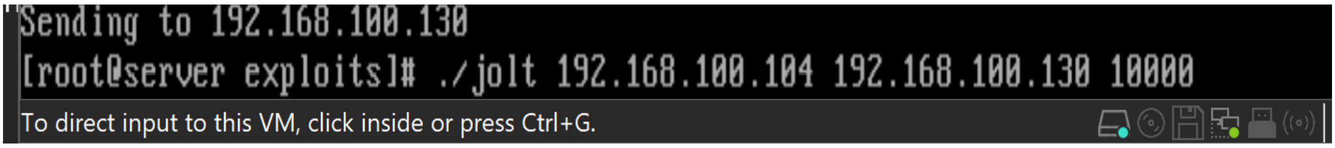
```
[student@server student]$ ping 192.168.100.130
PING 192.168.100.130 (192.168.100.130) from 192.168.100.104 : 56(84) bytes of da
ta.
```

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



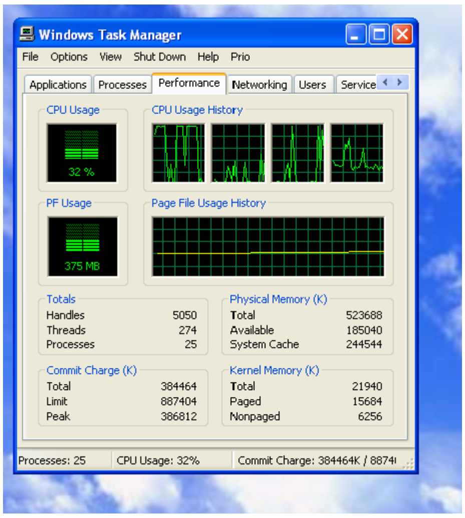
```
[student@server student]$ /usr/sbin/traceroute 192.168.100.130
traceroute to 192.168.100.130 (192.168.100.130), 30 hops max, 38 byte packets
 1  192.168.100.130 (192.168.100.130)  1.343 ms  0.666 ms  0.638 ms
[student@server student]$ _
```

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



```
Sending to 192.168.100.130
[root@server exploits]# ./jolt 192.168.100.104 192.168.100.130 10000
```

To direct input to this VM, click inside or press Ctrl+G.


Windows Task Manager
File Options View Shut Down Help Prio
Applications Processes Performance Networking Users Service
CPU Usage
32 %
CPU Usage History
PF Usage
375 MB
Page File Usage History

Totals

Handles	5050
Threads	274
Processes	25

Physical Memory (K)

Total	523688
Available	185040
System Cache	244544

Commit Charge (K)

Total	384464
Limit	887404
Peak	386812

Kernel Memory (K)

Total	21940
Paged	15684
Nonpaged	6256

Processes: 25 CPU Usage: 32% Commit Charge: 384464K / 8874

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.