



Cairo University, Faculty of Computers and
Artificial Intelligence

FACULTY OF COMPUTERS AND AI, CAIRO UNIVERSITY

IT331 – Data Communication Assignment #1

Course Instructors:
Dr. Iman EL-Sayed

Prepared By:

Belal Mohamed Youness (20220087) belalyouness494@gmail.com

Network Analysis Report

Introduction

This report provides an analysis of network traffic, results of subnet scanning, and performance measurement metrics. The tool was implemented using the Scapy library in Python and demonstrates functionalities such as network discovery, packet analysis, custom packet crafting, and network performance monitoring.

1. Network Discovery

Objective

To identify all active devices in a specified subnet.

Steps

1. Used the ARP protocol to scan the subnet 192.168.0.0/24.
2. Broadcasted ARP requests to the subnet using `Ether` and `ARP`.
3. Collected responses to determine active IP-MAC pairs.

Output

Below is the list of detected devices in the subnet:

IP Address	MAC Address
192.168.1.1	02:42:dd:bc:66:10
192.168.1.5	02:42:0a:09:00:05
192.168.1.7	02:42:0a:09:00:07
192.168.1.8	02:42:0a:09:00:08

2. Packet Analysis

Objective

To capture and analyze traffic for a specific IP and protocol.

Steps Performed

- 1. Targeted the IP 192.168.1.1 with a focus on the TCP protocol.
- 2. Captured the first 5 packets matching the filter using `sniff`.
- 3. Extracted details such as source IP, destination IP, protocol, ports, and packet size.

Findings

Captured packets (saved in “traffic_capture.pcap”):

Packet No.	Source IP	Destination IP	Protocol	Source Port	Destination Port	Size (bytes)
1	10.9.0.6	192.168.1.1	TCP	57882	80	74
2	192.168.1.1	10.9.0.6	TCP	80	57882	58
... till #5						

3. Custom Packet Creation

Objective

To craft and transmit custom packets to a specified destination.

Steps Performed

- 1. Created an ICMP packet and sent it to 8.8.8.8.
- 2. Sent a TCP SYN packet to port 80 of 10.9.0.5
- 3. Sent a UDP packet to port 53 of 192.168.1.20.

Findings

Packets successfully transmitted to their respective destinations. The transmission was verified by inspecting network traffic logs.

4. Network Performance Measurement

Objective

To measure latency, throughput, and jitter of the network.

Steps Performed

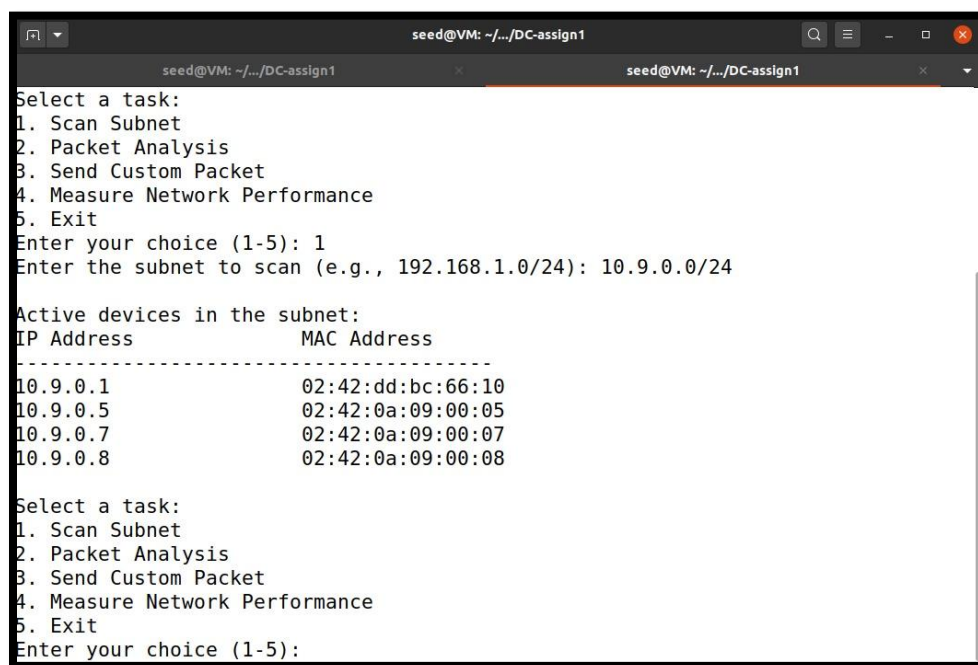
1. Sent ICMP packets to 8.8.8.8 and measured round-trip time for latency.
2. Calculated throughput based on the number of captured packets and elapsed time.
3. Estimated jitter as the variation in latency.

Results

Metric	Value
Latency	79.87 ms
Throughput	62.6 packets/s
Jitter	77.37 ms

Performance metrics were logged in `performance_log.txt`.

5. Screen Shots



```
seed@VM: ~/.../DC-assign1
Select a task:
1. Scan Subnet
2. Packet Analysis
3. Send Custom Packet
4. Measure Network Performance
5. Exit
Enter your choice (1-5): 1
Enter the subnet to scan (e.g., 192.168.1.0/24): 10.9.0.0/24

Active devices in the subnet:
IP Address      MAC Address
-----
10.9.0.1        02:42:dd:bc:66:10
10.9.0.5        02:42:0a:09:00:05
10.9.0.7        02:42:0a:09:00:07
10.9.0.8        02:42:0a:09:00:08

Select a task:
1. Scan Subnet
2. Packet Analysis
3. Send Custom Packet
4. Measure Network Performance
5. Exit
Enter your choice (1-5):
```

