CS302 – ASSIGNMENT 4 REPORT

Ragul N S – 191CS146 & Rakshith H R – 191CS148

1) Develop a basic port scanner to check if particular ports are open or closed for an input remote host.

Program:

We have used the function connect from the socket python library. If the connection is successful then it means that port is open. We store it and print it at last.

```
#  A basic port scanner to check if particular ports are open or c
losed for an input remote host.

import socket

newSocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
targetMachine = input("Input the website to scan: ")
openPorts = []


def portScan(portNumber):
    try:
        connection = newSocket.connect((targetMachine, portNumber)
)
        return True
    except:
        return False


print("Scaning 100 ports -", end="")
for portNumber in range(1, 101):
    print("#", end="")
    if portScan(portNumber):
        openPorts.append(portNumber)

print("\nThe open ports are: ", end="")
for i in openPorts:
    print(f'{i} ', end="")
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\Computer Networks Lab> python -u "d:\Computer Networks Lab\Week - 4\Q1.py"
Input the website to scan: iris.nitk.ac.in
Scaning 100 ports -####################################################################################################
The open ports are: 53
```

2) Develop a threaded port scanner to check if particular ports are open or closed for a remote host. Determine which Port scanner is efficient.

Program: We have used threading library to create separate threads, queue library to maintain them in a queue and socket library for network related function.

```python
import threading
from queue import Queue
import time
import socket

print_lock = threading.Lock()
target = 'iris.nitk.ac.in'


def portscan(port):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    try:
        con = s.connect((target, port))
        with print_lock:
            print('port', port)
        con.close()
    except:
        pass


def threader():
    while True:
        worker = q.get()
        portscan(worker)
```

```
        q.task_done()


q = Queue()

for x in range(30):
    t = threading.Thread(target=threader)
    t.daemon = True
    t.start()


start = time.time()
for worker in range(1, 100):
    q.put(worker)
q.join()
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\Computer Networks Lab> python -u "d:\Computer Networks Lab\Week - 4\Q2.py"
port 53
port 80
PS D:\Computer Networks Lab>
```

In the output screenshot we can see that the ports 53 and 80 are open for the target “iris.nitk.ac.in”.

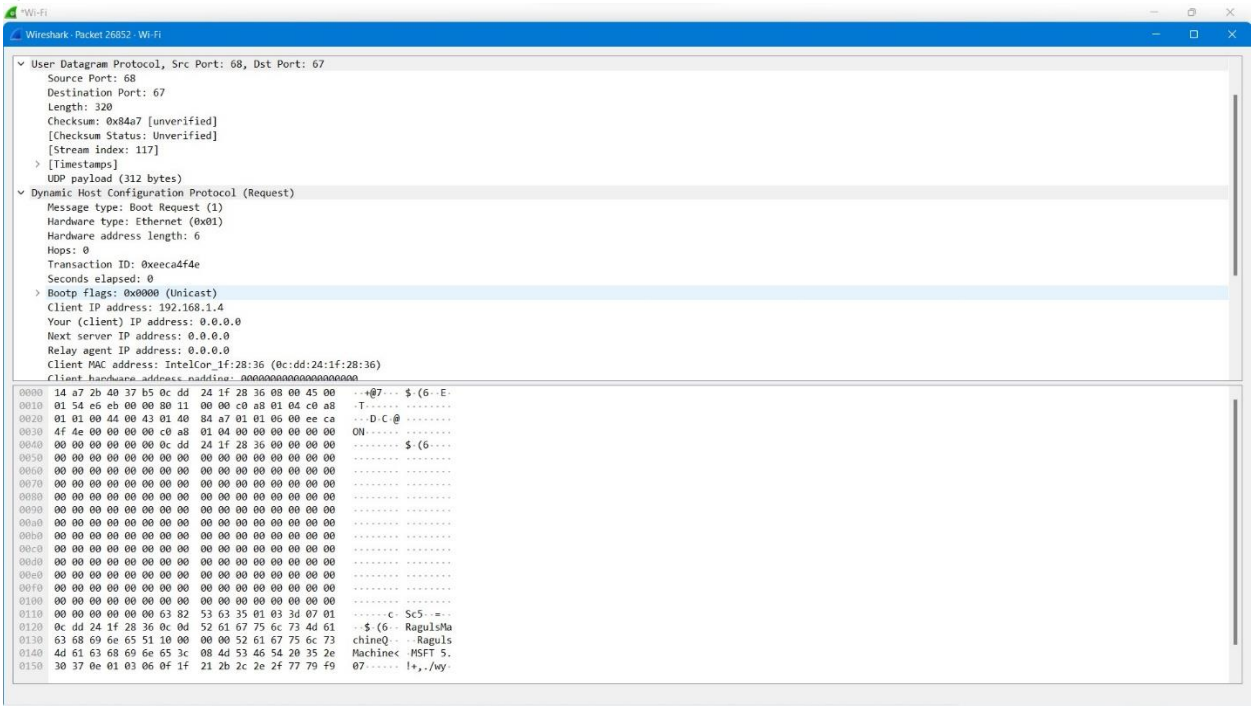
3.Capture UDP packets and with the help of the captured UDP Packets.

a. Analyze UDP DHCP Packets.

b. Analyze UDP DNS Packets.

Solution:

a)



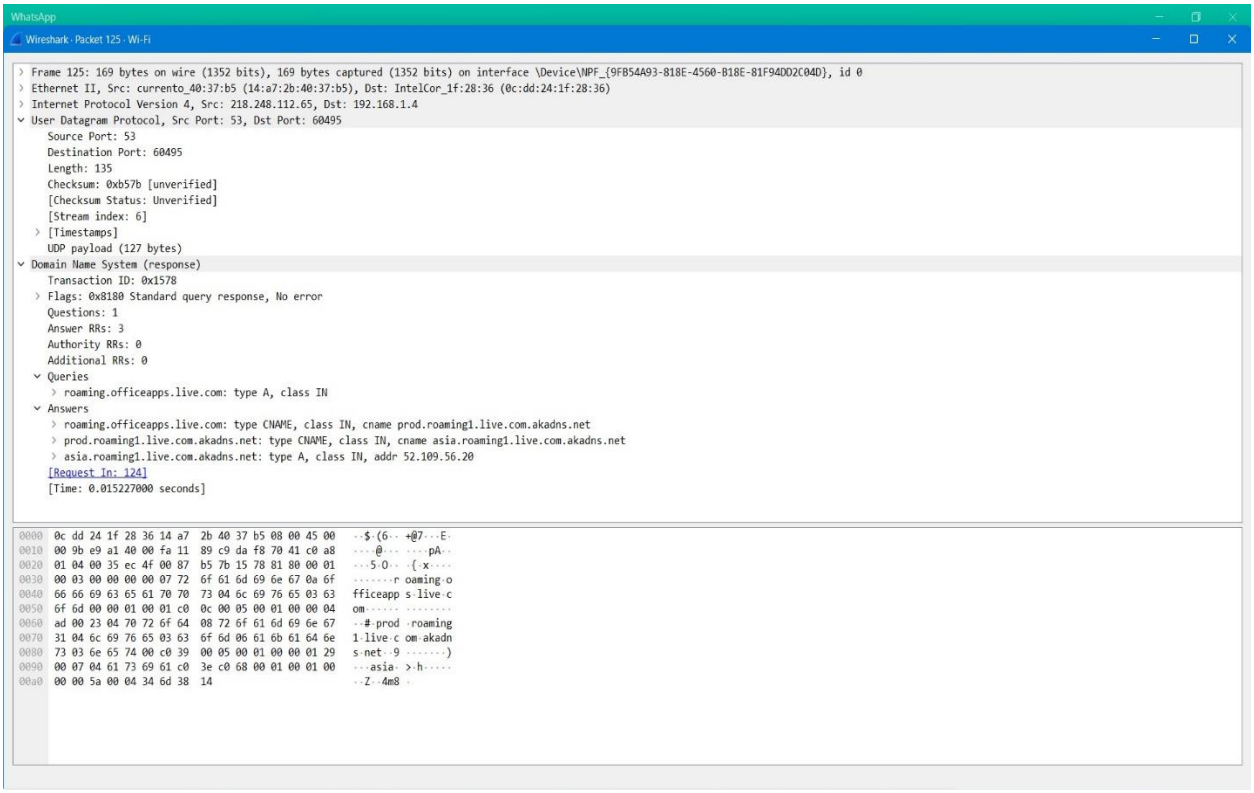
This screenshot contains a UDP DHCP packet. Details regarding the UDP protocol is given under the field User Datagram Protocol. The source port: 68, Destination Port: 67, Length of the packet: 320 it also contains the checksum details.

The field “Dynamic Host Configuration Protocol” contains details regarding the DHCP protocol. It has details like Message type: Boot Request,

Client IP Address: 192.168.1.4, hardware type: ethernet, hardware address length:6

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.

b)



The screenshot has a packet of UDP DNS packet. The UDP field contains information regarding the transfer of the packet. For ex, source port: 53, destination port: 60495, length of the packet: 135, checksum:0xb57b.

The Domain name system field has details like Questions:1, Answer RRs:3, Queries, which in our case is roaming.officeapps.live.com, Answer, which is the ip address of the domain in the question which is 52.109.56.20. It also has the response time which is 0.01522 seconds.

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.