# CW1

## NETWORKING- KH5064CEM

Toqa Mahmoud

CU1900305

## TABLE OF CONTENTS

## INTRODUCTION

Security for network infrastructure is intended to provide sophisticated and diversified resources for defending against internal and external attacks. Each of these essential components—hardware, software, and services—may have flaws that might be exploited by malicious or inadvertent activities. Infrastructures can be harmed by denial-of-service attacks, illegal access, spam, malware, etc. Although external assaults are the most common source of these risks, network security solutions should also include internal vulnerabilities. Deletion, alteration, data leakage, unintentional downloads of harmful information, and unlawful acts are just a few examples. In this report, I revised a finance advisory startup's (myFinTech) current network infrastructure so that remote users get uninterrupted access to the network and system resources hosted at the main data center in the company's Headquarter (HQ). As a result, in this report, I came up with a plan to upgrade the network to accommodate the new requirements and ensure the confidentiality, integrity, and availability (CIA) of the systems.

## ANALYSIS OF THE CURRENT NETWORK

Figure 1 below shows myFinTech's network map before it was upgraded. As illustrated in figure 1, the network consists of - 1 Web Application Server, 1 Router, 2 Access points, 1 Switch , and 1 Firewall. This is an example of a classic network that is incapable of handling contemporary data demands.

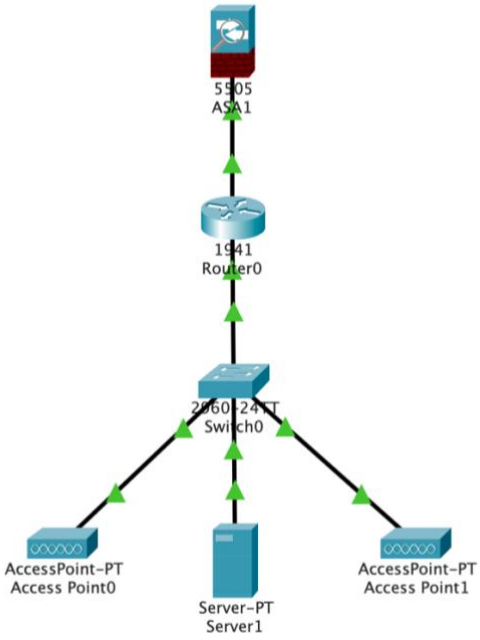



**Figure 1 Current Network**

## UPGRADED NETWORK

Figure 2 below shows the startup network map after it was upgraded. As illustrated in the diagram, the network now consists of - 1 proxy servers, 1 database server, 1 web application server, 3 routers, 4 multilayer switches, 2 layer 2 switches, 2 access points, and 2 firewalls.

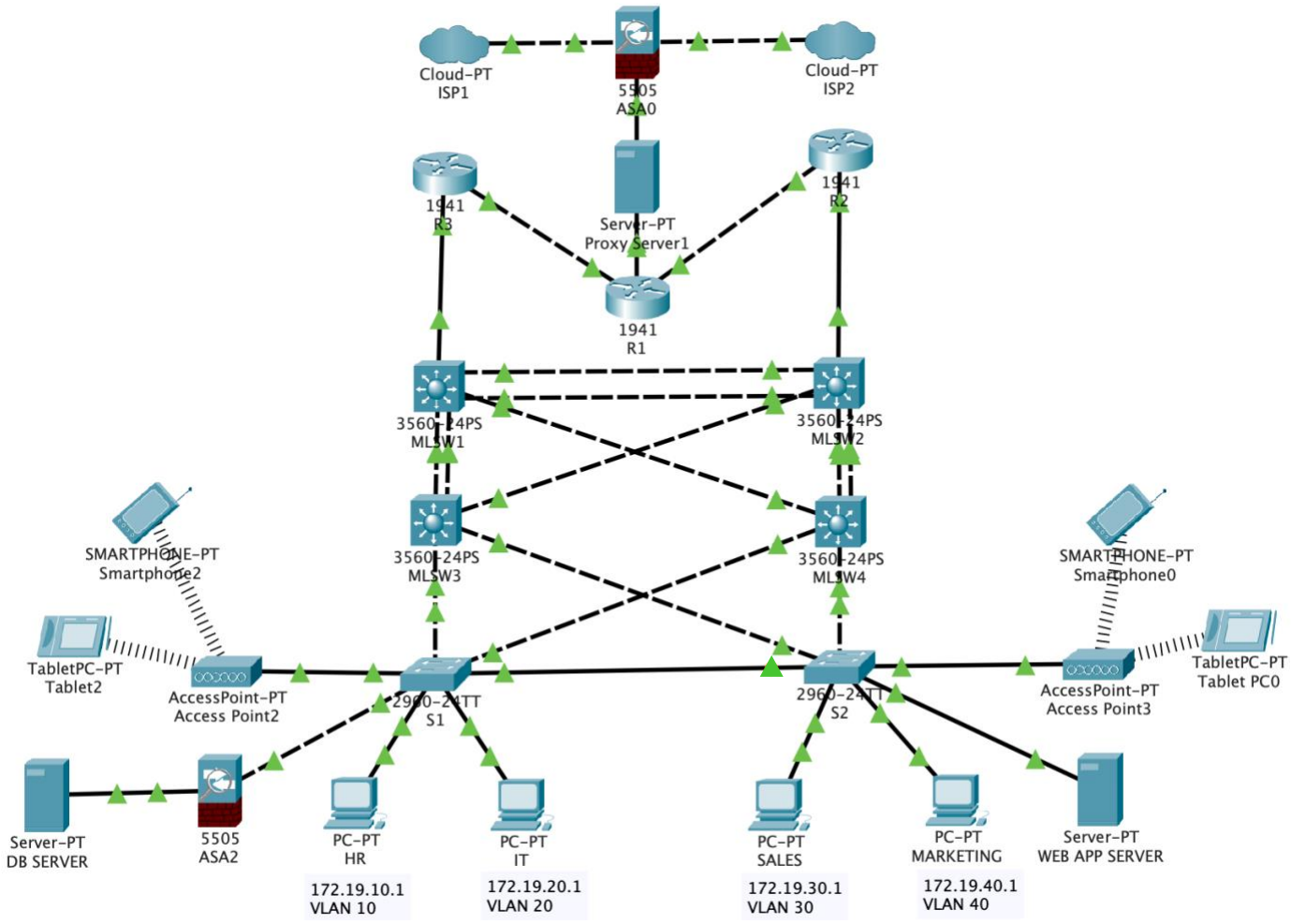



Figure 2 Upgraded Network

## HARDWARE PRICE LIST:

Table 1 Devices' Prices

| Device Name | Quantity | Price |
|---|---|---|
| **Router 1941** | 2 | $3,000 |
| **Switch 3560** | 4 | $24,000 |
| **Switch 2960** | 1 | $1,500 |
| **DB Firewall 5505** | 1 | $600 |
| **Total** | | $29,100 |

## SOFTWARE PRICE LIST:

Table 2 Software's Prices

| Software Name | Plan | Price |
|---|---|---|
| **Norton 360 with LifeLock** | Ultimate Plus | $299.88/yr |

## IMPLEMENTATION

Network Security is mainly about asset protection. Assets might be concrete assets like a Web page or a client database, or intangible stuff like the company's reputation. Security is a journey, not a goal. Therefore, we detect possible risks when we evaluate the infrastructure and applications, and we recognise that each threat has a different level of risk. By ensuring the CIA of data, security is about risk management and deploying appropriate countermeasures.

## THREE-TIER HIERARCHICAL NETWORK MODEL

I updated the network to a Three-Layer hierarchy, for a variety of reasons, including the simplicity with which to build, install, and manage a scalable, reliable, and cost-effective hierarchical internetwork. Furthermore, the Cisco Three Layer Network Model allows us to build high-performance networks, improve network administration, isolate network troubleshooting, create superior filter/policy generation applications, and easily accommodate future development. It also improves redundancy by utilising many links across various devices. If one of the switches fails, we can still get to our destination via another route. As shown in figure 3, the three–tier hierarchical network, consists of three layers: the Core layer, the Distribution layer, and the Access layer

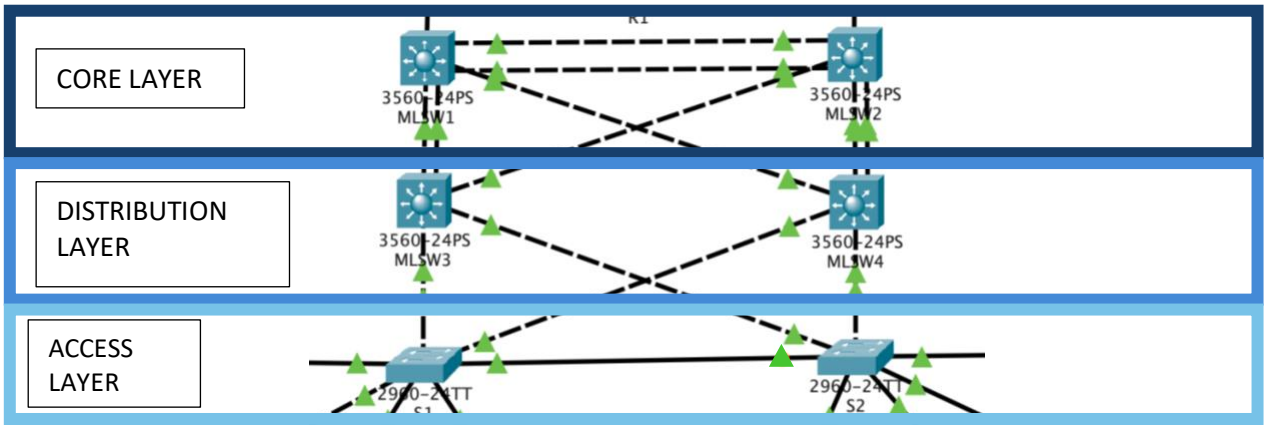



Figure 3 Three–Tier Hierarchical Network

**Core Layer**

The backbone of every network is the Core Layer. Core Layer routers connect networks that are geographically isolated. They are responsible for transferring data throughout the network.

**Distribution layer:**

Between the access and core levels comes the Distribution Layer. Its goal is to define boundaries by including access lists and other filters. Therefore, the Distribution Layer establishes network policies. It ensures that packets are routed correctly across subnets and VLANs.

**Access layer**

Access switches connects to end devices in the access layer and packets are supplied to end hosts by access layer switches.

## IP ADDRESSES

The DHCP is a network server that provides default gateways, IP addresses, and other network data to client computers on dynamic basis. To reply to client broadcast inquiries, this uses the standard protocol known as Dynamic Host Configuration Protocol or DHCP. As a results, R1 will act as a server as well as a router. On R1, I gave an ip address to the router interface that is connected to the routers. After that, I created a DHCP pool named IPD, where I mentioned ip addresses that will be given to the DHCP clients. Finally, I assigned the router's interface address as a default-router address for clients.

## VLANS

VLANs allows you to conceptually group hosts even though they are physically situated on different LAN segments. Each VLAN is treated as its own subnet or broadcast domain. On the access layer and distribution layer, VLANs were created by grouping some interfaces into one broadcast domain and others into another. Following that, the links were configured as trunks in the switches' access layer. Each department has its own VLAN, as shown below.

**Table 3 VLAN Distribution**

| Department | VLAN | IP Address |
|---|---|---|
| **HR** | VLAN 10 | 172.19.10.0/16 |
| **IT** | VLAN 20 | 172.19.20.0/16 |
| **SALES** | VLAN 30 | 172.19.30.0/16 |
| **MARKETING** | VLAN 40 | 172.19.40.0/16 |

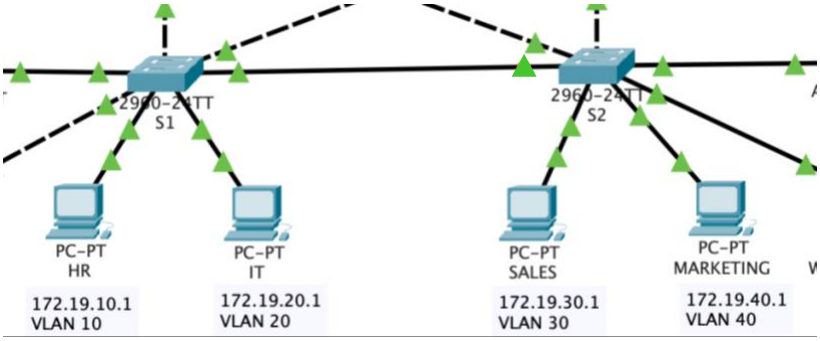



**Figure 4 VLAN Distribution**

## ROUTING

Routers must be configured with a default route for routing between routers to operate efficiently in an internetwork. Therefore, dynamic routing was implemented to ensure traffic always follows the most efficient pathways. Software programmes operating on the routers assist dynamic routing protocols by dynamically learning network destinations and how to get to them, as well as advertising those destinations to other routers. This advertisement function allows all routers to become aware of all available destination networks. Dynamic routing protocols communicate 'best route' information to other routers that use the same routing protocol, enlarging the knowledge of what networks are accessible and how to access them. To increase the security additional configuration settings will be implemented, which will be discussed further in the report. This allows dynamic routing

systems to adapt to changes in a network topology and device failures. The table below illustrates the advantages and disadvantages of dynamic routing.

**Table 4 Advantages and Disadvantages of Dynamic Routing**

| Advantages | Disadvantages |
|---|---|
| Flexible in communication between routers | More resources are needed, i.e. CPU, RAM, and bandwidth. |
| Adaptable to changes in the topology | Some machines may have communication problems |
| All routing modifications are provided to routers in the same order. | Due to its multicasting and broadcasting modifications, it's less secure. |
| More Uptime in the network | Complex implementation |
| In the network, there is less latency and higher performance. | |
| No configuration needed when a new router is added | |
| Network develops faster and bigger | |
| Rectifies problems in the network | |

Before traffic may reach its destination, it must first be routed through the default gateway. As a result, I generated virtual interfaces for all of the VLANS in the distribution layer after setting up the default gateways. On all devices in the core and distribution layer as well as all routers, I enabled IP routing by the "**ip routing**" command and then OSPF routing protocol by the "**router ospf 1**" command followed by the "**network 192.0.0.0 0.255.255.255 area**" command. OSPF is a routing protocol that uses the SPF algorithm to map the whole network and deliver quick convergence in the event of a router loss. The networks linked to the failing router are given a new route, and the network is kept running.

## REMOTE ACCESS

SSH (Secure Shell) is among the most popular network protocols. SSH is always preferred over Telnet, since it is more secure. TCP port 22 is used by SSH. It connects a distant device to a secure (encrypted) administration connection. When a device is authorised, SSH provides robust encryption for both the transferred data between the conversing devices and the distant connections, which contributes with maintaining the confidentiality of the Company. I went through the below steps to configure SSH:

1 **Password Encryption**
   - On the routers, I used the "**service password-encryption**" command, which encrypts passwords. Passwords are shown as hashed in the router config file using this command.

2 **Domain Data Encryption**
   - Here, I set the domain name to MyFinTech.com. Then I used the "**crypto key generate rsa**" command to encrypt the data within. Moreover, The module sizes were set to 512.

3 **Router User Config**
   - This is the standard router user definition step. I utilised the username, password, and privilege level to do this. Our user's name is User1, and their password is abc123, with the privilege mode set to 15.

4 **SSH Config**
   - Here, I configured SSH in line mode. First, I set up ssh for a certain number of users. After that, I used the command "**transport input ssh**", which only allows SSH access and denies telnet connections. Then, using the "**login local**" command, I made the login local. We may utilise local router users to ssh with this command.

- Following that, I set up the SSH version. SSH v1 and SSH v2 are the two versions of SSH. The second one has a stronger security algorithm. Therefore, I used SSH version 2, by the "**ip ssh version 2**" command. Last but not least, we'll save our SSH Configuration.

**5 SSH Verification**

- Finally, I opened the command prompt on the PC and typed "**ssh –l User1 127.19.0.1**" to verify the connection to the router.

## REMOTE ACCESS THREATS

The remote location in which these gadgets are employed might potentially be dangerous. For example, there may be security worries about:

- The lack of physical security controls.
- Eavesdropping.
- Unauthorised access of information or systems.
- Data monitoring and manipulation.

## REMOTE ACCESS RISK ASSESSMENT

The IT team must evaluate the risks connected with working remotely and giving employees remote access by:

- Limiting authorization for people to work remotely.
- Offering monitoring and support for devices.
- Identifying the types of data or services that's allowed to be accessed or stored on devices.
- Implementing security measures that must be in place at all times.

## REMOTE ACCESS SECURITY MEASURES

In order to safeguard remote access and lower the risk as much as possible, some security measures should be carefully implemented. After researching thoroughly, the best option we came across was Norton 360. Norton 360 with lifelock ultimate plus plan is the best suitable plan for myFinTech. The following summarizes what is included in the plan, to learn more click here.

**Table 5 Norton 360 with lifelock ultimate plus plan**

| Norton 360 with lifelock ultimate plus plan | |
|---|---|
| Anti-Spyware, Antivirus, Malware & Ransomware Protection | Privacy Monitor |
| Online Threat Protection | PC SafeCam |
| Cloud Backup | Dark Web Monitoring |
| Smart Firewall | LifeLock Identity Alert™ System |
| Password Manager | U.S.-based Identity Restoration Specialists |
| 100% Virus Protection Promise | Stolen Wallet Protection |
| Secure VPN | Million Dollar Protection™ Package |
| School Time | Credit Monitoring |
| SSN & Credit Alerts | Court Records Scanning |

| | |
|---|---|
| ID Verification Monitoring | Fictitious Identity Monitoring |
| Data Breach Notification | 401(k) & Investment Activity Alerts |
| Identity Lock | Bank & Credit Card Activity Alerts |

## ETHERCHANNEL

EtherChannel is a link aggregation technology which permits more than one physical link connecting switches to be grouped into one logical link to allow high-speed links and redundancy, ignoring Spanning Tree Protocol's (STP) blocking. EtherChannel provides fault tolerance, load balancing, higher bandwidth, and redundancy. This protocol is formed with a combination of Port Aggregation Protocol (PAgp) and Link Aggregation Control Protocol (LACP). As a result, I created etherchannel in the distribution and core layers by grouping the local interfaces into a port channel by the "**channel-group 1 mode desirable**" command and assigned them IP addresses.

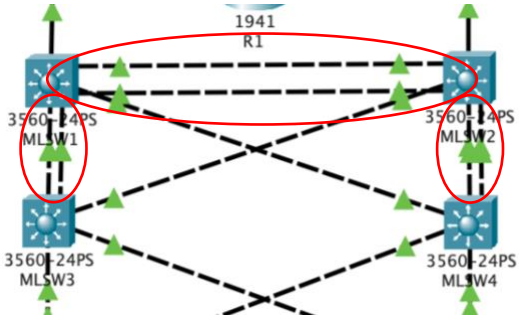



Figure 5 EtherChannel

## FIREWALLS

The updated network is connected by two ISPs (Internet service providers), while both ISPs are going through an ASA firewall. This model is ideal for small enterprises or branch offices, as it has the same firewall protection features as the larger variants. The ASA firewalls' Adaptive Security technology provides stable and dependable firewall protection, enhanced application-aware security, denial of service attack defense, etc. Furthermore, the firewall's appliance's performance provides 150 Mbps firewall throughput and 4000 firewall connections per second, which is more than sufficient for small networks. This firewall is connected to the ISPs to govern data flow from the internet to the local network. This is the initial stage in developing an integrated system and any practical work that aids the network, particularly in terms of overall technology. The configuration of the failover tool has an important role on the result of the design. When one of the ISPs failed, this utility allowed the firewall to swap between ISP1 and ISP2. Figure 4 shows the connection arrangement.

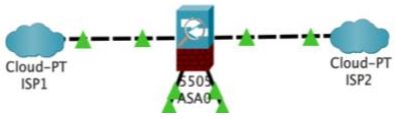



Figure 6 First ASA Firewall

The second ASA firewall was installed in the Database server, it was connected to one of the switch ports.The first consideration in firewall location design is that it should be able to serve as a control checkpoint and a query mechanism. This improved security for the database, which is the network's most vulnerable portion. This Firewall was created to secure the server from the outside as well as from within the network. This guarantees that access to the database server is controlled, ensuring that the data on that server is kept secure. Moreover, the IT team, which is responsible on the database, should ensure that all data is backed up, in case of any loss occurrences. Figure 5 demonstrates how the firewall is linked to the switch.

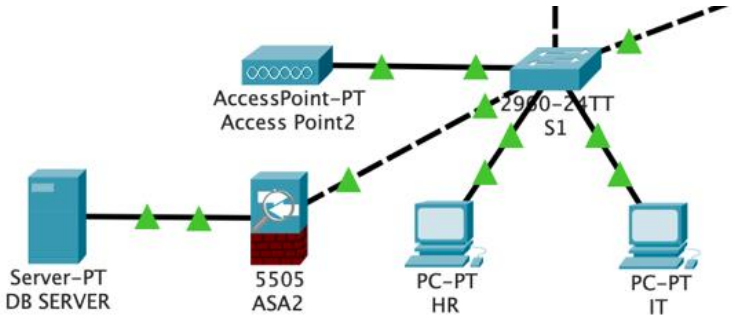



Figure 7 Second ASA Firewall

## PROXY SERVERS

The proxy server was utilised to provide additional security. The server function as a filter, allowing all packets to be inspected again as they transit through the proxy server. This layer of security is meant to add a layer of protection from outside attacks by encrypting the data. All communication passing via the proxy server, regardless of where it is located, is encrypted and sent through a proxy tunnel that connects the user to the Internet. Because everything has been encrypted, an intruder attempting to overhear the conversation and observe packets transported to or from the user's system will be unable to understand the packets' data that travel through the server. It is obvious that when a proxy server is used in any network architecture, the degree of security increases substantially.

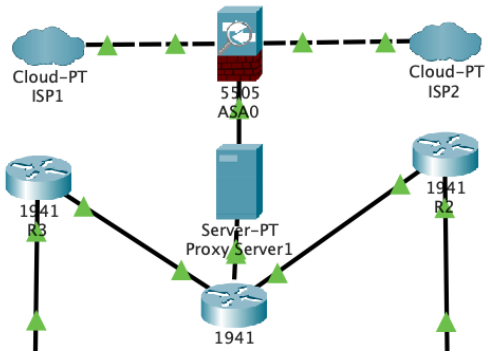



Figure 8 Proxy Server

## STANDARD ACCESS LIST

For every company, several techniques are required to secure the network from untrustworthy users. High-privileged web servers are continually scanned for security flaws and ways for hackers to get access to them and change their contents. By restricting the sort of packets a router sends to the servers, these web servers may be effectively secured against this and other types of attacks.

As a result, the three routers have been set up with list access control to prohibit clients from gaining access to any departments by the "**ip access-list standard 1**" command. Only the web application server is accessible to them. Furthermore, because the workers of the other departments do not require access to the database server, they have been configured in list access control to prohibit the employees of other departments from doing so. This server can be trusted to a selected number of IT department staff only.

The network traffic was decided by the access control list tool, which gave a high degree of security to the network. Furthermore, this technology assisted in preventing hackers from gaining access to other departments on the network and stealing or destroying

data. As a consequence, packets may be filtered and controlled inside the local network using the ACL. This technology assisted in presenting a network of high-security by defending it against both external and internal threats.

## SWITCH SECURITY

Here, I implement the range of security measures on the switches that would keep the network secure. This was done by creating secure trunks. Then securing unused ports by shutting down all unused ports and moving them to a specifically created vlan. After that, I activated port security on all the active ports and allowing a certain number of MAC addresses. Moreover, I enabled DHCP spoofing by configuring the trunk ports as trusted ports and limiting the untrusted ports to a certain number of DHCP packets per second. Finally, I enabled Rapid PVST PortFast and BPDU Guard on all active ports.

Furthermore, I specified the action that the switches will do if an illegal device is connected to the same port, such as discarding the traffic, issuing a warning, or shutting down the port. To warn a network monitoring solution that a port has been disabled for security reasons, the switch was configured to transmit an SNMP trap. As a result, it is obvious the increase of security that will protect the startup's CIA.

# PACKET SNIFFER TOOL

This multi-user packet sniffing tool is listens to traffic originating from clients and displays them on server's console. For example, the client sends data packet to the server, and the server extracts the clients MAC address, IP address, and port address from the received packet. Then the server displays extracted information on the console. The tool also gives the user the ability to select which protocol (TCP or UDP) to monitor.

## GITHUB REPO LINK:

https://github.com/Toqahassib/Packet-Sniffer.git

## PRE-REQUISITES:

- Unix Operating System.
- Installing Scapy, install scapy in your operating system.

## WRITING THE CODE

I created a python file and imported all the following modules:

```
import scapy.all as scapy
from scapy.layers.inet import IP, TCP, UDP
import datetime
from tabulate import tabulate
```

Figure 9 Imported Modules

After importing all the required modules, I created an empty list to store the packets details.

```
packet_list = []
```

Figure 10 Packet List

I then created a sniffing function that sniffs a given interface by using the iface parameter. Moreover, using the prn parameter implements a customized function to sniff packets.

```
def sniffing(interface):
    scapy.sniff(iface=interface, prn=packets)
```

Figure 11 Sniffing Function

After that, I created a function that filters out packets by either TCP protocol or UDP protocol. haslayer() is a builtin function in Scapy that identifies packets by the specified protocol, such as packet.haslayer(TCP) and packet.haslayer(UDP). Moreover, I used the tabulate module to print out the data in a well formatted table.

```
def packets(packet):
    time = datetime.datetime.now()

    if answer == '1':
        if packet.haslayer(TCP):

            packet_info = [str(time), len(packet[TCP]), str(packet.src), str(packet.dst), str(
                packet.sport), str(packet.dport), str(packet[IP].src), str(packet[IP].dst)]

            packet_list.append(packet_info)
            print(tabulate(packet_list, headers=[
                'TIME', 'BYTES', 'SRC-MAC', 'DST-MAC', 'SRC-PORT', 'DST-PORT', 'SRC-IP', 'DST-IP'], showindex=len(packet_list), tablefmt='fancy_grid'))

    elif answer == '2':
        if packet.haslayer(UDP):

            packet_info = [str(time), len(packet[UDP]), str(packet.src), str(packet.dst), str(
                packet.sport), str(packet.dport), str(packet[IP].src), str(packet[IP].dst)]

            packet_list.append(packet_info)
            print(tabulate(packet_list, headers=[
                'Time', 'BYTES', 'SRC-MAC', 'DST-MAC', 'SRC-PORT', 'DST-PORT', 'SRC-IP', 'DST-IP'], showindex=len(packet_list), tablefmt='fancy_grid'))
```

**Figure 12 Packet Filtering**

Here, I ask the user whether they want to capture TCP or UDP packets.

```
print("\nChoose the type of packets:\n\n1: TCP\n2: UDP\n")
answer = input('1 or 2: ')

while True:
    if answer not in ('1', '2'):
        print("Please choose 1 or 2.")
        print("\nChoose the type of packets:\n\n1: TCP\n2: UDP\n")
        answer = input('1 or 2: ')
    else:
        break
```

**Figure 13 User Choice**

Finally, I used the python builtin main function to call the sniffing function.

```
if __name__ == '__main__':
    sniffing('en0')
```

**Figure 14 main function**

Now, we can sniff packets by just runing the script. The screenshot below, shows the output.

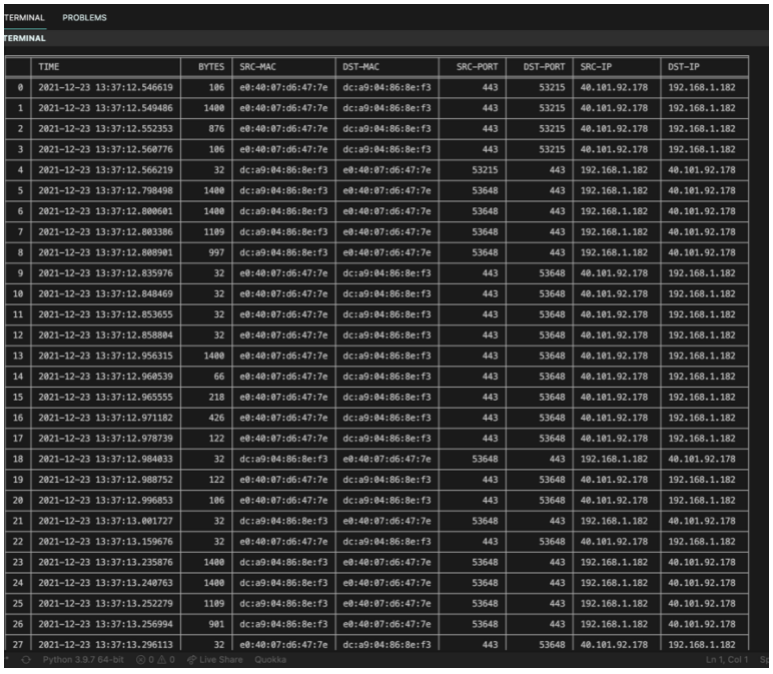
| | TIME | BYTES | SRC-MAC | DST-MAC | SRC-PORT | DST-PORT | SRC-IP | DST-IP |
|---|---|---|---|---|---|---|---|---|
| 0 | 2021-12-19 18:00:58.751951 | 44 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 50921 | 443 | 192.168.1.182 | 192.124.249.13 |
| 1 | 2021-12-19 18:00:58.795627 | 44 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 50921 | 192.124.249.13 | 192.168.1.182 |
| 2 | 2021-12-19 18:00:58.796959 | 32 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 50921 | 443 | 192.168.1.182 | 192.124.249.13 |
| 3 | 2021-12-19 18:00:58.798732 | 549 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 50921 | 443 | 192.168.1.182 | 192.124.249.13 |
| 4 | 2021-12-19 18:00:58.846956 | 32 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 50921 | 192.124.249.13 | 192.168.1.182 |
| 5 | 2021-12-19 18:00:59.095507 | 32 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 50921 | 192.124.249.13 | 192.168.1.182 |
| 6 | 2021-12-19 18:00:59.323978 | 1380 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 50921 | 192.124.249.13 | 192.168.1.182 |
| 7 | 2021-12-19 18:00:59.329445 | 32 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 50921 | 443 | 192.168.1.182 | 192.124.249.13 |
| 8 | 2021-12-19 18:00:59.337341 | 1380 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 50921 | 192.124.249.13 | 192.168.1.182 |
| 9 | 2021-12-19 18:00:59.342900 | 926 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 50921 | 192.124.249.13 | 192.168.1.182 |
| 10 | 2021-12-19 18:00:59.346909 | 32 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 50921 | 443 | 192.168.1.182 | 192.124.249.13 |
| 11 | 2021-12-19 18:00:59.350984 | 112 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 50921 | 443 | 192.168.1.182 | 192.124.249.13 |
| 12 | 2021-12-19 18:00:59.356675 | 124 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 50921 | 443 | 192.168.1.182 | 192.124.249.13 |
| 13 | 2021-12-19 18:00:59.362991 | 1008 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 50921 | 443 | 192.168.1.182 | 192.124.249.13 |

**Figure 15 Output**

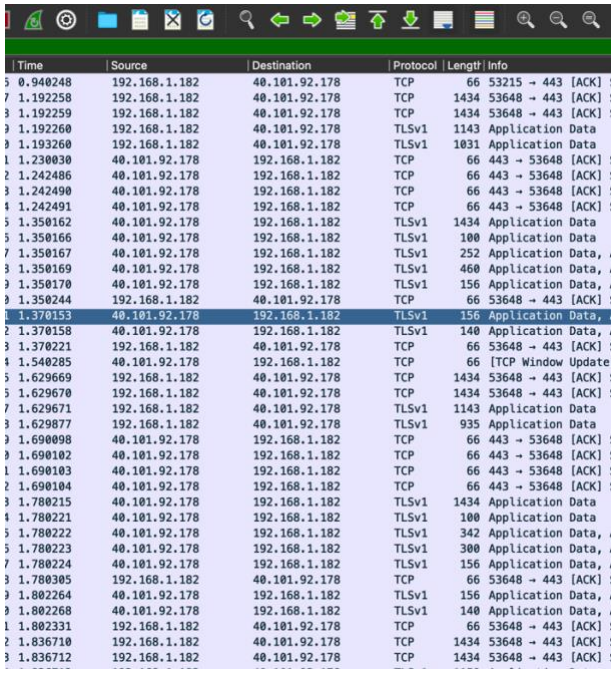
# WIRESHARK VS. MY TOOL

## TCP PACKETS

The 2 screenshots below compare the TCP packet details extracted by my tool with information collected by Wireshark on the same network environment.



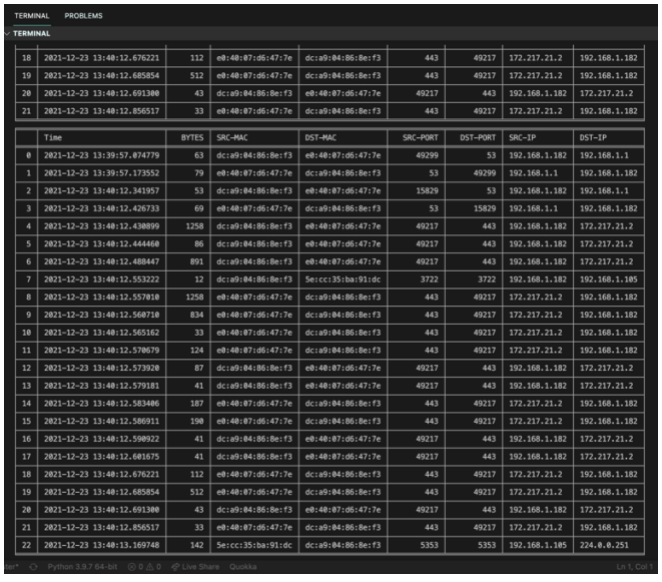
| | TIME | BYTES | SRC-MAC | DST-MAC | SRC-PORT | DST-PORT | SRC-IP | DST-IP |
|---|---|---|---|---|---|---|---|---|
| 0 | 2021-12-23 13:37:12.546619 | 106 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53215 | 40.101.92.178 | 192.168.1.182 |
| 1 | 2021-12-23 13:37:12.549486 | 1400 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53215 | 40.101.92.178 | 192.168.1.182 |
| 2 | 2021-12-23 13:37:12.552353 | 876 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53215 | 40.101.92.178 | 192.168.1.182 |
| 3 | 2021-12-23 13:37:12.560776 | 106 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53215 | 40.101.92.178 | 192.168.1.182 |
| 4 | 2021-12-23 13:37:12.566219 | 32 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53215 | 443 | 192.168.1.182 | 40.101.92.178 |
| 5 | 2021-12-23 13:37:12.798498 | 1400 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53648 | 443 | 192.168.1.182 | 40.101.92.178 |
| 6 | 2021-12-23 13:37:12.800601 | 1400 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53648 | 443 | 192.168.1.182 | 40.101.92.178 |
| 7 | 2021-12-23 13:37:12.803386 | 1109 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53648 | 443 | 192.168.1.182 | 40.101.92.178 |
| 8 | 2021-12-23 13:37:12.808901 | 997 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53648 | 443 | 192.168.1.182 | 40.101.92.178 |
| 9 | 2021-12-23 13:37:12.835976 | 32 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 10 | 2021-12-23 13:37:12.848469 | 32 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 11 | 2021-12-23 13:37:12.853655 | 32 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 12 | 2021-12-23 13:37:12.858804 | 32 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 13 | 2021-12-23 13:37:12.956315 | 1400 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 14 | 2021-12-23 13:37:12.960539 | 66 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 15 | 2021-12-23 13:37:12.965555 | 218 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 16 | 2021-12-23 13:37:12.971182 | 426 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 17 | 2021-12-23 13:37:12.978739 | 122 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 18 | 2021-12-23 13:37:12.984033 | 32 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53648 | 443 | 192.168.1.182 | 40.101.92.178 |
| 19 | 2021-12-23 13:37:12.988752 | 122 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 20 | 2021-12-23 13:37:12.996853 | 106 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 21 | 2021-12-23 13:37:13.001727 | 32 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53648 | 443 | 192.168.1.182 | 40.101.92.178 |
| 22 | 2021-12-23 13:37:13.159676 | 32 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |
| 23 | 2021-12-23 13:37:13.235876 | 1400 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53648 | 443 | 192.168.1.182 | 40.101.92.178 |
| 24 | 2021-12-23 13:37:13.240763 | 1400 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53648 | 443 | 192.168.1.182 | 40.101.92.178 |
| 25 | 2021-12-23 13:37:13.252279 | 1109 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53648 | 443 | 192.168.1.182 | 40.101.92.178 |
| 26 | 2021-12-23 13:37:13.256994 | 901 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 53648 | 443 | 192.168.1.182 | 40.101.92.178 |
| 27 | 2021-12-23 13:37:13.296113 | 32 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 53648 | 40.101.92.178 | 192.168.1.182 |



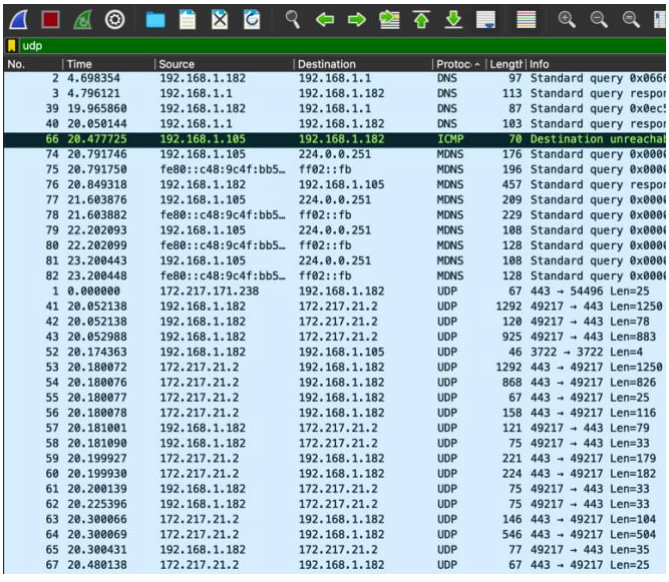
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5 | 0.940248 | 192.168.1.182 | 40.101.92.178 | TCP | 66 | 53215 → 443 [ACK] |
| 7 | 1.192258 | 192.168.1.182 | 40.101.92.178 | TCP | 1434 | 53648 → 443 [ACK] |
| 8 | 1.192259 | 192.168.1.182 | 40.101.92.178 | TCP | 1434 | 53648 → 443 [ACK] |
| 9 | 1.192260 | 192.168.1.182 | 40.101.92.178 | TLSv1 | 1143 | Application Data |
| 0 | 1.193260 | 192.168.1.182 | 40.101.92.178 | TLSv1 | 1031 | Application Data |
| 1 | 1.230030 | 40.101.92.178 | 192.168.1.182 | TCP | 66 | 443 → 53648 [ACK] |
| 2 | 1.242486 | 40.101.92.178 | 192.168.1.182 | TCP | 66 | 443 → 53648 [ACK] |
| 3 | 1.242490 | 40.101.92.178 | 192.168.1.182 | TCP | 66 | 443 → 53648 [ACK] |
| 4 | 1.242491 | 40.101.92.178 | 192.168.1.182 | TCP | 66 | 443 → 53648 [ACK] |
| 5 | 1.350162 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 1434 | Application Data |
| 6 | 1.350166 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 100 | Application Data |
| 7 | 1.350167 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 252 | Application Data, |
| 8 | 1.350169 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 460 | Application Data, |
| 9 | 1.350170 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 156 | Application Data, |
| 0 | 1.350244 | 192.168.1.182 | 40.101.92.178 | TCP | 66 | 53648 → 443 [ACK] |
| 1 | 1.370153 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 156 | Application Data, |
| 2 | 1.370158 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 140 | Application Data, |
| 3 | 1.370221 | 192.168.1.182 | 40.101.92.178 | TCP | 66 | 53648 → 443 [ACK] |
| 4 | 1.540285 | 40.101.92.178 | 192.168.1.182 | TCP | 66 | [TCP Window Update |
| 5 | 1.629669 | 192.168.1.182 | 40.101.92.178 | TCP | 1434 | 53648 → 443 [ACK] |
| 6 | 1.629670 | 192.168.1.182 | 40.101.92.178 | TCP | 1434 | 53648 → 443 [ACK] |
| 7 | 1.629671 | 192.168.1.182 | 40.101.92.178 | TLSv1 | 1143 | Application Data |
| 8 | 1.629877 | 192.168.1.182 | 40.101.92.178 | TLSv1 | 935 | Application Data |
| 9 | 1.690098 | 40.101.92.178 | 192.168.1.182 | TCP | 66 | 443 → 53648 [ACK] |
| 0 | 1.690102 | 40.101.92.178 | 192.168.1.182 | TCP | 66 | 443 → 53648 [ACK] |
| 1 | 1.690103 | 40.101.92.178 | 192.168.1.182 | TCP | 66 | 443 → 53648 [ACK] |
| 2 | 1.690104 | 40.101.92.178 | 192.168.1.182 | TCP | 66 | 443 → 53648 [ACK] |
| 3 | 1.780215 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 1434 | Application Data |
| 4 | 1.780221 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 100 | Application Data |
| 5 | 1.780222 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 342 | Application Data, |
| 6 | 1.780223 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 300 | Application Data, |
| 7 | 1.780224 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 156 | Application Data, |
| 8 | 1.780305 | 192.168.1.182 | 40.101.92.178 | TCP | 66 | 53648 → 443 [ACK] |
| 9 | 1.802264 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 156 | Application Data, |
| 0 | 1.802268 | 40.101.92.178 | 192.168.1.182 | TLSv1 | 140 | Application Data, |
| 1 | 1.802331 | 192.168.1.182 | 40.101.92.178 | TCP | 66 | 53648 → 443 [ACK] |
| 2 | 1.836710 | 192.168.1.182 | 40.101.92.178 | TCP | 1434 | 53648 → 443 [ACK] |
| 3 | 1.836712 | 192.168.1.182 | 40.101.92.178 | TCP | 1434 | 53648 → 443 [ACK] |

## UDP PACKETS

The 2 screenshots below compare the UDP packet details extracted by my tool with information collected by Wireshark on the same network environment.



| | Time | BYTES | SRC-MAC | DST-MAC | SRC-PORT | DST-PORT | SRC-IP | DST-IP |
|---|---|---|---|---|---|---|---|---|
| 0 | 2021-12-23 13:39:57.074779 | 63 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 49299 | 53 | 192.168.1.182 | 192.168.1.1 |
| 1 | 2021-12-23 13:39:57.173552 | 79 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 53 | 49299 | 192.168.1.1 | 192.168.1.182 |
| 2 | 2021-12-23 13:40:12.341957 | 53 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 15829 | 53 | 192.168.1.182 | 192.168.1.1 |
| 3 | 2021-12-23 13:40:12.426733 | 69 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 53 | 15829 | 192.168.1.1 | 192.168.1.182 |
| 4 | 2021-12-23 13:40:12.430899 | 1258 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 49217 | 443 | 192.168.1.182 | 172.217.21.2 |
| 5 | 2021-12-23 13:40:12.444468 | 86 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 49217 | 443 | 192.168.1.182 | 172.217.21.2 |
| 6 | 2021-12-23 13:40:12.488447 | 891 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 49217 | 443 | 192.168.1.182 | 172.217.21.2 |
| 7 | 2021-12-23 13:40:12.553222 | 12 | dc:a9:04:86:8e:f3 | 5e:cc:35:ba:91:dc | 3722 | 3722 | 192.168.1.182 | 192.168.1.105 |
| 8 | 2021-12-23 13:40:12.557010 | 1258 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 49217 | 172.217.21.2 | 192.168.1.182 |
| 9 | 2021-12-23 13:40:12.560710 | 834 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 49217 | 172.217.21.2 | 192.168.1.182 |
| 10 | 2021-12-23 13:40:12.565162 | 33 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 49217 | 172.217.21.2 | 192.168.1.182 |
| 11 | 2021-12-23 13:40:12.570679 | 124 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 49217 | 172.217.21.2 | 192.168.1.182 |
| 12 | 2021-12-23 13:40:12.573920 | 87 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 49217 | 443 | 192.168.1.182 | 172.217.21.2 |
| 13 | 2021-12-23 13:40:12.579181 | 41 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 49217 | 443 | 192.168.1.182 | 172.217.21.2 |
| 14 | 2021-12-23 13:40:12.583406 | 187 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 49217 | 172.217.21.2 | 192.168.1.182 |
| 15 | 2021-12-23 13:40:12.586911 | 190 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 49217 | 172.217.21.2 | 192.168.1.182 |
| 16 | 2021-12-23 13:40:12.590922 | 41 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 49217 | 443 | 192.168.1.182 | 172.217.21.2 |
| 17 | 2021-12-23 13:40:12.601675 | 41 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 49217 | 443 | 192.168.1.182 | 172.217.21.2 |
| 18 | 2021-12-23 13:40:12.676221 | 112 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 49217 | 172.217.21.2 | 192.168.1.182 |
| 19 | 2021-12-23 13:40:12.685854 | 512 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 49217 | 172.217.21.2 | 192.168.1.182 |
| 20 | 2021-12-23 13:40:12.691300 | 43 | dc:a9:04:86:8e:f3 | e0:40:07:d6:47:7e | 49217 | 443 | 192.168.1.182 | 172.217.21.2 |
| 21 | 2021-12-23 13:40:12.856517 | 33 | e0:40:07:d6:47:7e | dc:a9:04:86:8e:f3 | 443 | 49217 | 172.217.21.2 | 192.168.1.182 |
| 22 | 2021-12-23 13:40:13.169748 | 142 | 5e:cc:35:ba:91:dc | dc:a9:04:86:8e:f3 | 5353 | 5353 | 192.168.1.105 | 224.0.0.251 |



| No. | Time | Source | Destination | Protoc | Length | Info |
|---|---|---|---|---|---|---|
| 2 | 4.698354 | 192.168.1.182 | 192.168.1.1 | DNS | 97 | Standard query 0x066 |
| 3 | 4.796121 | 192.168.1.1 | 192.168.1.182 | DNS | 113 | Standard query respo |
| 39 | 19.965860 | 192.168.1.182 | 192.168.1.1 | DNS | 87 | Standard query 0x0ec |
| 40 | 20.050144 | 192.168.1.1 | 192.168.1.182 | DNS | 103 | Standard query respo |
| 66 | 20.477725 | 192.168.1.105 | 192.168.1.182 | ICMP | 70 | Destination unreacha |
| 74 | 20.791746 | 192.168.1.105 | 224.0.0.251 | MDNS | 176 | Standard query 0x000 |
| 75 | 20.791750 | fe80::c48:9c4f:bb5… | ff02::fb | MDNS | 196 | Standard query 0x000 |
| 76 | 20.849318 | 192.168.1.182 | 192.168.1.105 | MDNS | 457 | Standard query respo |
| 77 | 21.603876 | 192.168.1.105 | 224.0.0.251 | MDNS | 209 | Standard query 0x000 |
| 78 | 21.603882 | fe80::c48:9c4f:bb5… | ff02::fb | MDNS | 229 | Standard query 0x000 |
| 79 | 22.202093 | 192.168.1.105 | 224.0.0.251 | MDNS | 108 | Standard query 0x000 |
| 80 | 22.202099 | fe80::c48:9c4f:bb5… | ff02::fb | MDNS | 128 | Standard query 0x000 |
| 81 | 23.200443 | 192.168.1.105 | 224.0.0.251 | MDNS | 108 | Standard query 0x000 |
| 82 | 23.200448 | fe80::c48:9c4f:bb5… | ff02::fb | MDNS | 128 | Standard query 0x000 |
| 1 | 0.000000 | 172.217.171.238 | 192.168.1.182 | UDP | 67 | 443 → 54496 Len=25 |
| 41 | 20.052138 | 192.168.1.182 | 172.217.21.2 | UDP | 1292 | 49217 → 443 Len=1250 |
| 42 | 20.052138 | 192.168.1.182 | 172.217.21.2 | UDP | 120 | 49217 → 443 Len=78 |
| 43 | 20.052988 | 192.168.1.182 | 172.217.21.2 | UDP | 925 | 49217 → 443 Len=883 |
| 52 | 20.174363 | 192.168.1.182 | 192.168.1.105 | UDP | 46 | 3722 → 3722 Len=4 |
| 53 | 20.180072 | 172.217.21.2 | 192.168.1.182 | UDP | 1292 | 443 → 49217 Len=1250 |
| 54 | 20.180076 | 172.217.21.2 | 192.168.1.182 | UDP | 868 | 443 → 49217 Len=826 |
| 55 | 20.180077 | 172.217.21.2 | 192.168.1.182 | UDP | 67 | 443 → 49217 Len=25 |
| 56 | 20.180078 | 172.217.21.2 | 192.168.1.182 | UDP | 158 | 443 → 49217 Len=116 |
| 57 | 20.181001 | 192.168.1.182 | 172.217.21.2 | UDP | 121 | 49217 → 443 Len=79 |
| 58 | 20.181090 | 192.168.1.182 | 172.217.21.2 | UDP | 75 | 49217 → 443 Len=33 |
| 59 | 20.199927 | 172.217.21.2 | 192.168.1.182 | UDP | 221 | 443 → 49217 Len=179 |
| 60 | 20.199930 | 172.217.21.2 | 192.168.1.182 | UDP | 224 | 443 → 49217 Len=182 |
| 61 | 20.200139 | 192.168.1.182 | 172.217.21.2 | UDP | 75 | 49217 → 443 Len=33 |
| 62 | 20.225396 | 192.168.1.182 | 172.217.21.2 | UDP | 75 | 49217 → 443 Len=33 |
| 63 | 20.300066 | 172.217.21.2 | 192.168.1.182 | UDP | 146 | 443 → 49217 Len=104 |
| 64 | 20.300069 | 172.217.21.2 | 192.168.1.182 | UDP | 546 | 443 → 49217 Len=504 |
| 65 | 20.300431 | 192.168.1.182 | 172.217.21.2 | UDP | 77 | 49217 → 443 Len=35 |
| 67 | 20.480138 | 172.217.21.2 | 192.168.1.182 | UDP | 67 | 443 → 49217 Len=25 |

## CODE

```python
import scapy.all as scapy
from scapy.layers.inet import IP, TCP, UDP
import datetime
from tabulate import tabulate

packet_list = []


def sniffing(interface):
    scapy.sniff(iface=interface, prn=packets)


def packets(packet):
    time = datetime.datetime.now()

    if answer == '1':
        if packet.haslayer(TCP):

            packet_info = [str(time), len(packet[TCP]), str(packet.src), str(packet.dst), str(
                packet.sport), str(packet.dport), str(packet[IP].src), str(packet[IP].dst)]

            packet_list.append(packet_info)
            print(tabulate(packet_list, headers=[
                  'TIME', 'BYTES', 'SRC-MAC', 'DST-MAC', 'SRC-PORT', 'DST-PORT', 'SRC-IP', 'DST-IP'], showindex=len(packet_list), tablefmt='fancy_grid'))

    elif answer == '2':
        if packet.haslayer(UDP):

            packet_info = [str(time), len(packet[UDP]), str(packet.src), str(packet.dst), str(
                packet.sport), str(packet.dport), str(packet[IP].src), str(packet[IP].dst)]

            packet_list.append(packet_info)
            print(tabulate(packet_list, headers=[
                  'Time', 'BYTES', 'SRC-MAC', 'DST-MAC', 'SRC-PORT', 'DST-PORT', 'SRC-IP', 'DST-IP'], showindex=len(packet_list), tablefmt='fancy_grid'))


print("\nChoose the type of packets:\n\n1: TCP\n2: UDP\n")
answer = input('1 or 2: ')

while True:
    if answer not in ('1', '2'):
        print("Please choose 1 or 2.")
        print("\nChoose the type of packets:\n\n1: TCP\n2: UDP\n")
        answer = input('1 or 2: ')
    else:
        break


if __name__ == '__main__':
    sniffing('en0')
```

Figure 16 Code

# CONCLUSION

## NETWORK DESIGN

The focus of the report of the upgraded network part was on the enhanced security that could be supplied to the FinTech network, while enabling remote access. As a result, the study incorporates several aspects of networking to present the finest technological alternatives accessible. The network of the company has been created and set to deliver excellent service. Unauthorized users were prevented from joining the network using firewalls, standard access list, switch security, a database server, and a proxy server. Another consideration used to help define a fully-featured network ideal for businesses was the quality of service. The implementation that helped to give a high end of service to the startup's network include the three-tier model, dynamic routing, and DHCP server, etc. Furthermore, the information of the customers has been safeguarded by using Norton security technologies to back up the database server information outside of the local network.

## PACKET SNIFFER

The Packet Sniffer tool was able to capture TCP and UDP packets. For each packet the data such as source ip, destination ip, source port, destination port, source mac, destination mac, and timestamp is extracted. This tool is tremendously useful for infosec and network professionals to capture packets by running such a small-scale script.

## LIST OF FIGURES

## LIST OF TABLES

## REFERENCES

0xbharath.github.io. 2021. *Inspecting packets - The Art of Packet Crafting with Scapy!*. [online] Available at: <https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/inspecting_packets/index.html> [Accessed 21 December 2021].

ALI, A., 2021. *Enterprise Network Design and Implementation for Airports*. [online] Scholar.valpo.edu. Available at: <https://scholar.valpo.edu/cgi/viewcontent.cgi?article=1001&context=ms_ittheses> [Accessed 21 December 2021].

Bagci, T., 2021. *How to Configure OSPF in Cisco Packet Tracer*. [online] sysnettechsolutions. Available at: <https://www.sysnettechsolutions.com/en/configure-ospf-in-cisco-packet-tracer/> [Accessed 21 December 2021].

IPCISCO. (2021, July 17). *2 Packet Tracer Router DHCP Config | Router DHCP Configuration*. https://ipcisco.com/lesson/router-dhcp-configuration-with-packet-tracer-ccna/

IpCisco. 2021. *SSH Configuration on Packet Tracer | Cisco SSH Config ⋆ IpCisco*. [online] Available at: <https://ipcisco.com/lesson/ssh-configuration-on-packet-tracer/> [Accessed 21 December 2021].

Nibusinessinfo.co.uk. 2021. *Remote access security issues | nibusinessinfo.co.uk*. [online] Available at: <https://www.nibusinessinfo.co.uk/content/remote-access-security-issues> [Accessed 21 December 2021].

NordVPN. 2021. *Best encryption software in 2021*. [online] Available at: <https://nordvpn.com/blog/best-encryption-software/> [Accessed 21 December 2021].

Poudel, R., 2021. *Writing an Quick Packet Sniffer with Python & Scapy*. [online] Exploit-db.com. Available at: <https://www.exploit-db.com/docs/48606> [Accessed 21 December 2021].

Robb, D., 2021. *Top Network Access Control (NAC) Solutions for 2022*. [online] eSecurityPlanet. Available at: <https://www.esecurityplanet.com/products/network-access-control-solutions/> [Accessed 21 December 2021].

Scapy.readthedocs.io. 2021. *Usage — Scapy 2.4.5. documentation*. [online] Available at: <https://scapy.readthedocs.io/en/latest/usage.html> [Accessed 21 December 2021].

Tech, R., 2021. *Static Routing vs. Dynamic Routing – Router Switch Blog*. [online] Blog.router-switch.com. Available at: <https://blog.router-switch.com/2011/12/static-routing-vs-dynamic-routing/> [Accessed 21 December 2021].

Us.norton.com. 2021. *Norton 360 + LifeLock Ultimate Plus | Starting $29.99/mo*. [online] Available at: <https://us.norton.com/products/norton-360-lifelock-ultimate-plus> [Accessed 21 December 2021].