

PROFESSIONAL TRAINING REPORT
at
Sathyabama Institute of Science and Technology
(Deemed to be University)

Submitted in partial fulfillment of the requirements for the
award of Bachelor of Engineering Degree in Information
Technology

By
Edupuganti Srivalli
REG. NO. 39120028



DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF COMPUTING

**SATHYABAMA INSTITUTE OF SCIENCE AND
TECHNOLOGY**

**JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600119, TAMILNADU**

APRIL 2022



Type your text

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited with Grade “A” by NAAC
(Established under Section 3 of UGC Act, 1956)
JEPPIAAR NAGAR, RAJIV GANDHI SALAI
CHENNAI- 600119
www.sathyabama.ac.in



DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of
Edupuganti Srivalli (Reg. No: 39120028) who carried out the
project entitled

“TO PERFORM HOST,PORT AND SERVICE DISCOVERY” under my
supervision from March 7,2022 to March 26,2022.

Internal Guide

Dr. Nirmalrani, M.E., Ph.D.,

Head of the Department

Dr. Subhashini, M.E., Ph.D.,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I Edupuganti Srivalli hereby declare that the project report entitled "TO PERFORM HOST, *PORT AND SERVICE DISCOVERY*" *done by me under the guidance of Dr.Nirmalrani*, is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering Degree in Information technology.

DATE: 16-04-2022

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph.D., Dean**, School of Computing, **Dr. R. Subhashini, M.E., Ph.D. Head of the Department of Information technology** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.Nirmalrani, M.E., Ph.D., for** his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project

TRAINING CERTIFICATE



ABSTRACT

Nowadays, computer networks have continuously expanded in different aspects including the size of the infrastructure, complexity, number of users. With all of this growth, managing, maintaining, and analyzing networks have become significantly important to make sure that the networks work smoothly.

Besides that, network analysis tasks are helpful when it comes to identifying intruders, discovering hidden services in a network, troubleshooting, and so forth. These aims can be achieved by performing tasks like host discovery, port scanning and capturing traffic. However, several challenges can be observed with the available tools that perform the mentioned tasks such as accuracy issue, integration of various tasks, presentation of the task's result and more.

Therefore, the primary aim of the project is to design and develop an integrated standalone system that allows system administrators, penetration testers, and security practitioners to perform different network analysis and monitoring tasks with more flexibility, customizability, and ease of use.

The main proposed system consists of two subsystems which are the python tool and the web application portal. The kali Linux tool is responsible for performing tasks such as host discovery for LAN networks and PIPs, port scanning with a variety of techniques and capturing traffic. The second subsystem is the web application portal which is responsible for handling the task's result.

TABLE OF CONTENTS

SI No.	TITLE	PAGE No
1.	INTRODUCTION	1
2.	IMPORTANCE OF NETWORK SECURITY	2
3.	TYPES OF NETWORK SECURITY	3
4.	COMMON NETWORK ANALYSIS TASKS	4
5.	PERFORM HOST,PORT AND SERVICE DISCOVERY	11
6.	RESULT AND CONCLUSIONS	21
	REFERENCES	22
	APPENDIX	23
	A. SOURCE CODE	23
	B. SCREENSHOTS	31

LIST OF FIGURES

FIGURE NO.	FIGURE NAME
01.	Screenshot for the PIP Host Discovery
02.	Screenshot for the full scan(Host Discovery&Port Scanning)

INTRODUCTION

The literature review is the part where the developer finds out an extensive reference to the related research as well as the theory in the particular project (Ridley, 2012). Hence, two main types of research will be carried out in this section. These parts are domain research and technical research.

In the domain research, the importance of network security and available network analysis tasks are discussed. Additionally, the network analysis tasks domain has some subdomains including network host discovery, port scanning, and capturing traffic. Also, all the techniques of network analysis tasks will be discussed. As an example, network discovery techniques which are using ICMP or ARP protocol, port scanning techniques which are using SYN, Full TCP Scan, FIN, NULL and XAMS methods. Besides, capturing traffic techniques are discussed using some methods such as a port mirror, bridge mode, and ARP spoof.

Further, the technical research will have the similar systems that perform the network analysis tasks that are discussed in the domain research. These similar systems like Nmap, Netdiscover, Angry IP scanner, and Tcpdump. After highlighting their primary functions, these systems will be compared to the developer.

Importance of network security

Network security is one of the essential aspects of information security as it aims to safeguard the sensitive information of the companies and organizations. All of the organizations have to control and monitor their networks to protect their infrastructure from various types of attacks.

These attacks could be either from inside the network or outside the network. Therefore, it is essential to have network and security administrator teams that have a primary routine job to monitor and protect the network from the frequent attacks such as identifying the online clients and distinguish intruders, logging traffic of suspected user and prevent the sniffers and performing vulnerability assessments.

There are numerous reasons of implementing network security, as it assists to protect the company's assets and the users on the organization network as well as to ensure that that data transmits in a highly confidential manner.

The significant impact of not implementing network security procedures could be significantly high as well as it costs a lot. The number of attacks continued to increase recently, and hackers comprise organization's networks to gain a high confidential data and destroy the reputation of a company. The main reason for that, companies and organizations do not invest in protecting their network infrastructure, and they do not follow the best practice of configuring their network resources. Because of that, the level of the risk could differ from organization to another organization.

For protecting the network against attacks, the network should have different security layers. These layers could help to minimize the risk since there is no system offers full protection against all the threats. So, if the attacker could bypass one of the security layers, the other layers could prevent the attacker from gaining access to the network .

In a nutshell, implementing a proper network security procedure could protect and eliminate the risk of the companies and organization from intruders and sniffers. Besides, network security provides the three aims of security which are the confidentiality, integrity, and availability.

Types of Network Security

Network security is a way of protecting the network and manage the usability and the access to the network. Several technologies and techniques assist in mitigating the network threats and attacks.

There are different types of network security including Access control, Behavioural Analytics, firewalls, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), Virtual Private Network (VPN), Wireless Security, Network Analysis. Each of these types has different mechanisms and benefits in protecting the network from various attacks. According to (Cisco.com, 2018), some of these network security types are highlighted below.

1-Access Control Networks could be protected by implanting an access control which works by recognizing each user and device in the network based on a set of rules that could deny unauthorized access to the network. This type of access control is called Network Access Control (NAC).

2- Behavioral Analytics (BA) BA is the process of detecting abnormal behavior in the network. It can identify the attacks such Denial of Service attack since this attack works by sending a massive Page 31 of 218 number of packets to the target system. As a result of that, the network administrators could identify a list of regular traffic, and the Behavioral system will work based on that. If there is a traffic type that is not listed in the regular traffic list is considered as abnormal traffic.

3-Firewall A firewall is a barrier layer between the trusted network and untrusted network. One example is between Local Area Network and the Public Internet. It works by defining a set of rules that based on allow and block. The firewall could be either hardware device or software. One of the great firewalls is UTM from CISCO.

4- Virtual Private Network (VPN): VPN encrypts the connection between the source and the target destination as well as providing confidentiality. If there is an attacker who sniffs the packets in the network, all the packets will be encrypted. There are some protocols such as IPsec and Secure Sockets Layers. The mainly use of these protocols to authenticate the compunction between devices and the network.

5- Network Analysis: Network analysis is the process of analysing the network by performing various tasks such as capturing network traffic, identifying the life host in a network and identifying hidden services in the networks and devices. Most of the network administrators use this type of tasks to identify the intruder, analyze service such as FTP or SSH or troubleshooting the network issues through capturing the network traffic. Additionally, numerous tools perform these mentioned tasks such as NMAP, Nessus, Netdiscover and so on

COMMON NETWORK ANALYSIS TASKS

There are many network analysis tasks that network administrators and security engineering frequently do to monitor their networks. All of them have their purposes and functionality. These tasks could be host discovery, port scanning, and logging traffic. These available tasks are chosen to integrate them into the proposed system. This part of the section will discuss what these tasks are, how they work and the standard techniques that they have.

Network host discovery is the process of discovering out the devices that connected to the network. These devices could be workstations, routers, printers and so on. Many network administrators use the host discovery to verify the reachability between two hosts. As long as the host has an IP address, they could verify if the host is reachable or unreachable. Network host discovery is a big topic and has a variety of techniques that can perform the discovery such as using Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP). Both work differentially and have their strengths and weaknesses in some scenarios.

ICMP is a protocol that works in the third (3) layer of the OSI model which is the network layer. There are various of functions that ICMP protocol offers such as reporting functionality and error checking. The ICMP protocol is used with the Ping utility to check the reachability between two hosts. The ping utility works by sending an echo request to the specific host that could be on the LAN or the Internet. So, if that particular host receives the ICMP echo request, the particular host will send an ICMP echo reply to the sender host that identify the status of the particular host. There are different types of the ICMP reply messages such as

“destination unreachable” and “Time exceeded.” These messages occur when the Time to Live (TTL) has already exceeded. Here is below how the ICMP packet looks like .

IP Datagram				
	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		flags and offset	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (optional)	Payload Data			

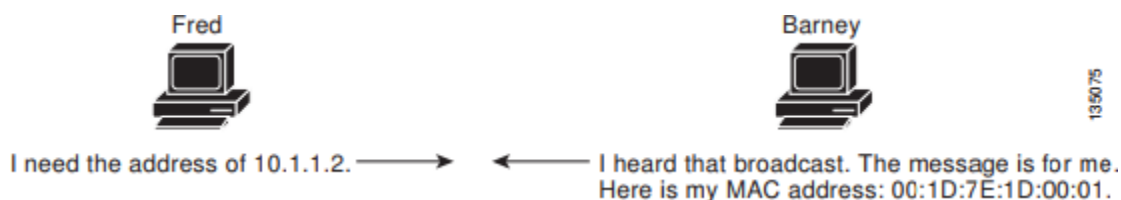
There are various types of flags that ICMP header has, these flags represent the type of the ICMP packet which could be an echo request, an echo reply. The below table illustrates all types of ICMP messages.

ICMP Message Types		
Type	Codes	Description
0/8	0	Echo Reply/Echo Request
3	0-15	Destination Unreachable
4	0	Source Quench
5	0-3	Redirect
9/10	0	Router Advertisement
11	0-1	Time Exceeded
12	0	Parameter Problem
13/14	0	Timestamp Request/Timestamp Reply
17/18	0	Address Mask Request/Address Mask Reply

Host Discovery Using ARP Protocol The Address Resolution Protocol (ARP) is a protocol that performs essential function which resolves the Internet Protocol address (IP) to Media Access Control (MAC) address. ARP protocol operates between data link layer which is layer 2 and network layer which is layer 3 of the Open System Interconnection (OSI) as it maps the IP to the corresponding MAC address. All the operating systems support ARP protocol such as Windows, Linux, and MAC OS. Besides that, all routers and switches support ARP protocol as well (Cisco.com, 2013).

Mainly, when any device in a local area network wants to send data, the sender device must use the ARP protocol to get the MAC address of the destination system by broadcasting an ARP request. If the destination system does not reply to the ARP discovery message, it means that the destination system is not alive in a network. As a result of that, the sender device cannot start the communication with destination system.

In addition, if the destination system receives the ARP request, the destination system will send its MAC address to the sender machine (Cisco.com, 2013). Furthermore, all of the operating systems have the functionality of storing the resolved IP addresses and their corresponding MAC address temporally into a table that is called ARP cache table. This table always checked when the computer system wants to start communicating with any machine in a network. So, if there is no entry for the destination system in the ARP cache table, the ARP protocol will send a broadcast message to all IPs in the subnet to get the Mac address for that protocol. The figure below illustrates the ARP process.

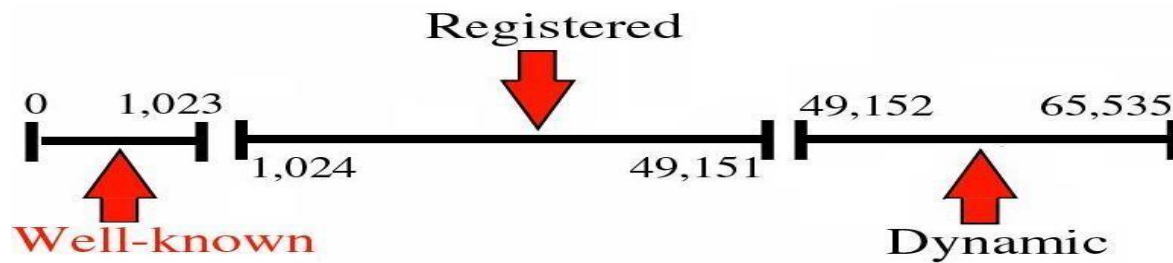


:
Port Scanning Port Scanning is the process of discovering and finding out the services that any computer system is running them. There are many available services such as file transfer protocol (FTP), secure shell (SSH), hypertext transfer protocol (HTTP) and so on. Every particular service has own functionality such as SSH provides a remote shell to the server, FTP provides a remote file transfer and HTTP which is used by World Wide Web (WWW) that helps to define how the data could transmit. Moreover, every service has its port number (Gont, 2016). Port numbers are categorized into three categories which are well-known ports, registered ports, and dynamic ports. The well-known ports are reserved ports from 1 to 1023 for particular services such as HTTP is port 80, HTTPS is port 443 and so on. Commonly, the well-known ports are used by the system process that provides some network services. Here are common ports

Table 4 - Common Ports (TONY PICKETT, 2013)

Port	Service	Protocol
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
67/68	DHCP	UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
161/162	SNMP	UDP
443	HTTPS	TCP

Additionally, Internet Assigned Number Authority assigns the registered ports (IANA), and the range of the ports are from 1024 to 49151. The advantages of the registered ports that could run without the superuser privileges. The third type is called dynamic ports which are from 49152 to 65535. These range of ports is not registered by IANA and can be used for any private services.



The port scanning task is used by many specialists such as network administrators, penetration testers, and security practitioners. The reason that network administrator uses this task is, when they configure a new service, they need to confirm that the service is in listening mode to get any upcoming connection. So, they use the port scanning concept to verify that. Besides that, penetration testers and security practitioners use the port scanning in the first phase of the system hacking. When they have a system hacking task for a computer system, so based on that, they have to know what type of services that the server is running them. After that, they could proceed with their penetration testing.

Several techniques of port scanning could help the network administrators and penetration tester to identify the status of the specific port if it is open filter or close mode.

Capturing network traffic: Capturing traffic means the process of capturing the traffic that the user generates in a local area network. It is also known as a network analyzer or packet sniffer technique. The logging traffic technique could be used as an administrative method or as attacking method which depends on the user's intention. Most of the time, the network administrators use this technique to log the traffic in a network for many reasons such as identifying malicious traffic, network management, and troubleshooting issues in the network. However, there are many black hat hackers use this technique to sniff and collect a sensitive data in a network. Based on that, network analysis tools can be used on the wrong side or the right side.

Furthermore, several techniques allow network administrators to log traffic such as using port mirroring, bridge mode or ARP spoofing. All these techniques have their way to capture the traffic. a. Port Mirroring The port mirroring is a capturing traffic feature that is available in the modern switches devices. So, it gives the network administrators the ability to log the traffic by using port mirroring technique. The technique works by duplicating the network traffic between one or more of the switch ports and mirror it to another switch port. The switch port of the switch should be configured as a mirror port which is available in most of the CISCO switches. The network administrators could plug any computer system that has an application that logs the traffic, to the mirror port. Also, access control list can be implemented to the mirror port.



Summary

To sum up, after conducting the literature review section, it has been found that the network security is one of the critical aspects for all organizations and companies since implementing network security procedures could help to eliminate the risk against the threats and protect their network infrastructure from various attack. Hence, many procedures and tasks that help network administrators and security practitioners to perform in order to monitor and protect the network. These tasks could start from network host discovery, port scanning, and logging traffic. There are several reasons for conducting these tasks such as to identify intruders, to discover unauthorized port and illegal traffic. Each of them can assist securing the network.

PERFORM HOST,PORT AND SERVICE DISCOVERY

INTRODUCTION

The proposed system is considered a network analysis system hence there are several techniques and features that should be implemented and involved to achieve the primary aim of the project. These techniques include host discovery using ICMP & ARP protocols, port scanning through different methods (SYN, ACK, FIN, XMAS, and Nul), and also capturing traffic using ARP Cache Poising technique.

HOST DISCOVERY:-

As we have defined previously, network host discovery is the process of discovering alive hosts in a network by using protocols that are designed to offer this action which is including the use of ICMP protocol and ARP protocol. The proposed system divides the host discovery into two types, host discovery in LAN network and Host discovery for Public IP addresses. For the first type, the proposed system uses the ARP protocol to perform the scan. The main reason of choosing ARP rather than ICMP, most of the network administrators block ICMP scan whereas the ARP protocol is an essential protocol in every network to enable the hosts to start communicating in the network and it cannot be blocked. For scanning the Public IP addresses, the proposed system scans them using ICMP protocol.

PORT SCANNING:-

Port scanning is one of the techniques that assist in discovering open ports. This technique is being used from a long time, and therefore several techniques were discovered that help administrators identifying open, filtered or closed ports such as SYN scan, FIN scan, ACK scan, XMAS scan, and Null scan. Some of them can Most of them have strengths and weaknesses (explained in literature review). Additionally, the proposed system offers the ability to perform port scanning using the mentioned techniques. The proposed system provides the network administrators the ability to perform any of them.

CAPTURING TRAFFIC:-

Capturing traffic basically is the process of intercepting packets and have a copy of the transmitted packets. This technique is one of the features that the system offers for the end user. To start capturing the traffic, the system requires some information from the administrator such as the IP address of the target client/user, the router IP address and the name of the external wireless adapter. After gaining this information, the system uses an ARP spoofing technique for capturing traffic

ABSTARCT ARCHITECTURE

SYSTEM DESIGN

According to the MITRE Corporation, (n. d) system design is described as the process of the figuring and identifying the main elements of the system that can be the overall architecture, main components, data, interfaces for a system. These elements can assist the developer in getting the clear and full picture of the system to be developed.

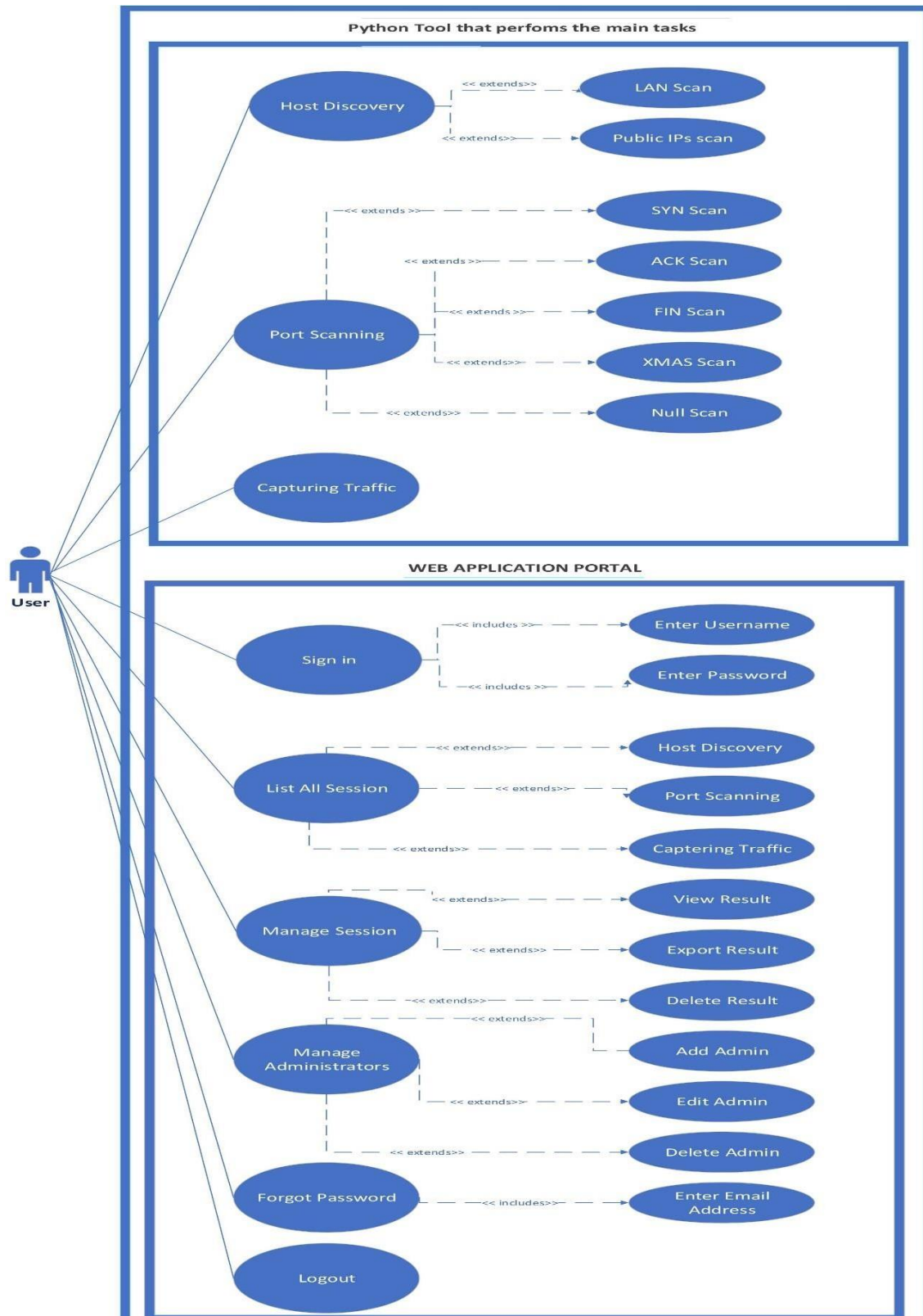
For this project, the system design phase is essential since it will help to define the primary requirements of the proposed system. Therefore, several system design diagrams will take place in this chapter such as use case diagram, class diagram, activity diagram as well as a sequence diagram.

USE-CASE DIAGRAM

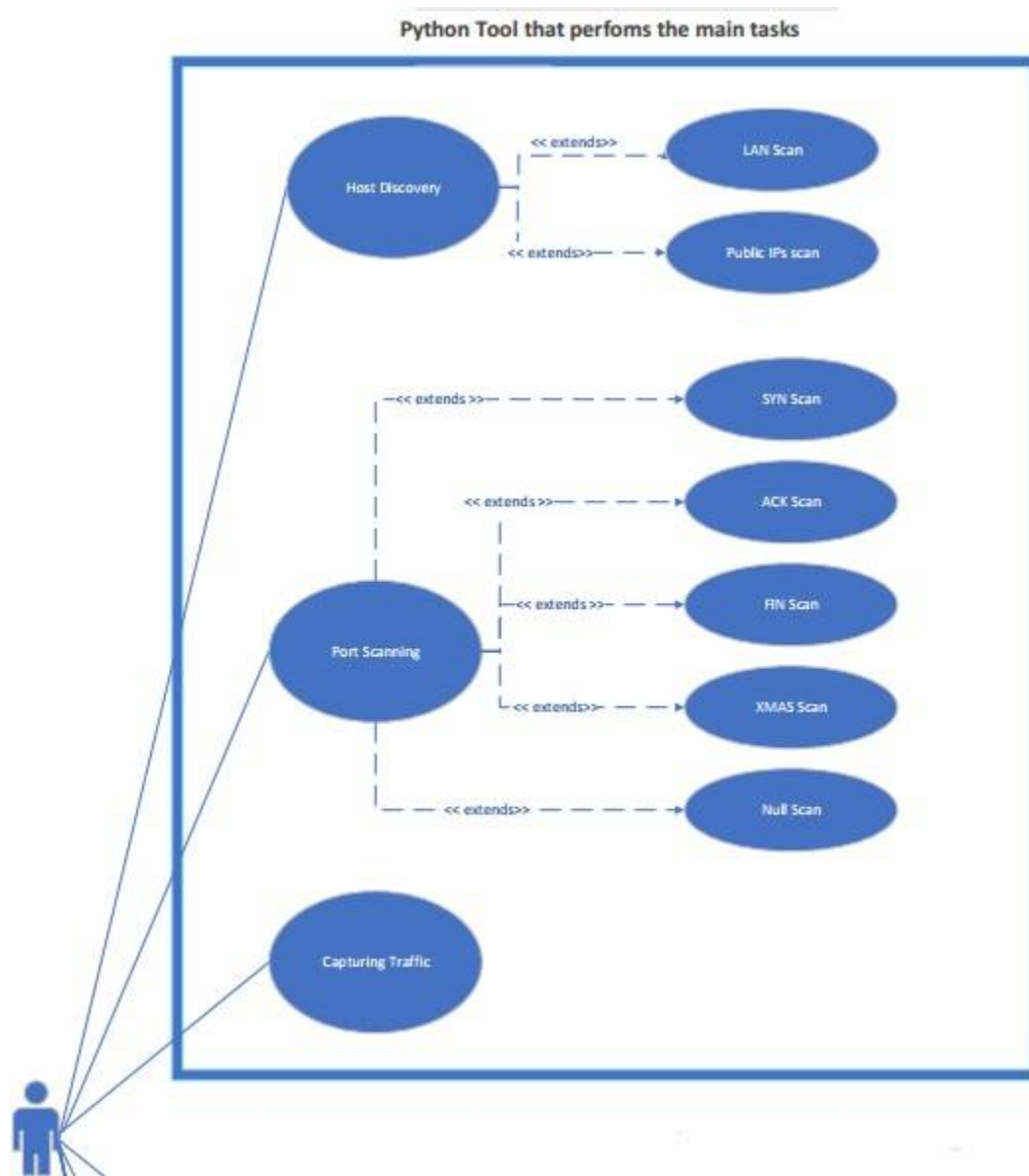
According to (Uml-diagrams.org, 2017), use-case diagram is also known as behavior diagram which is used to identify the actors as well as the actions that the developed system should perform. Based on the previous statement, those actions can be played by the actors.

For the proposed system, the first actor is the user who is either network administrators, security practitioner or penetration tester, and the second actor is the system who will be responsible for performing the tasks as well as storing the result.

Use-case diagram for NetSec system – Full Picture

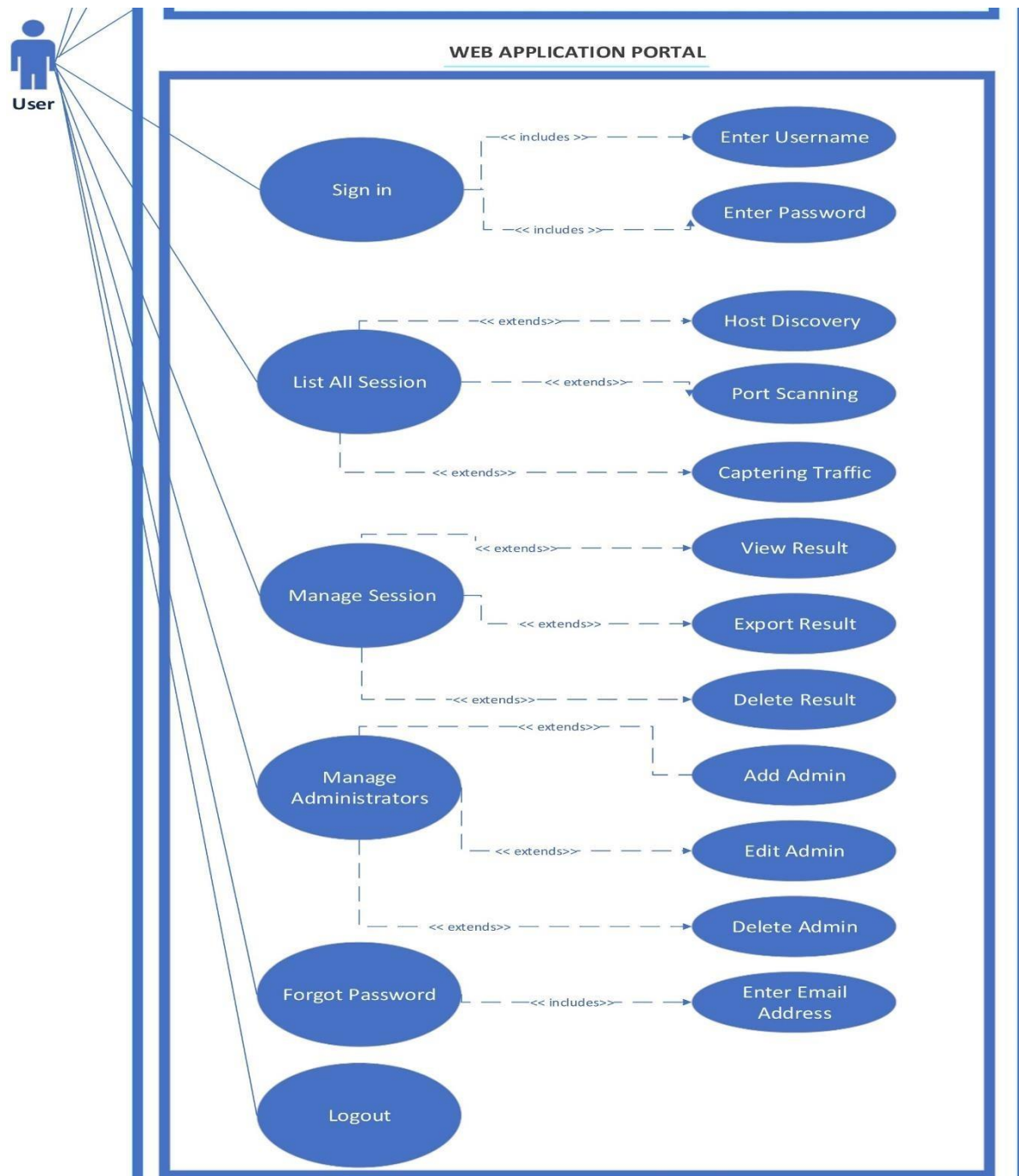


USE-CASE DIAGRAM FOR PYTHON TOOL:-

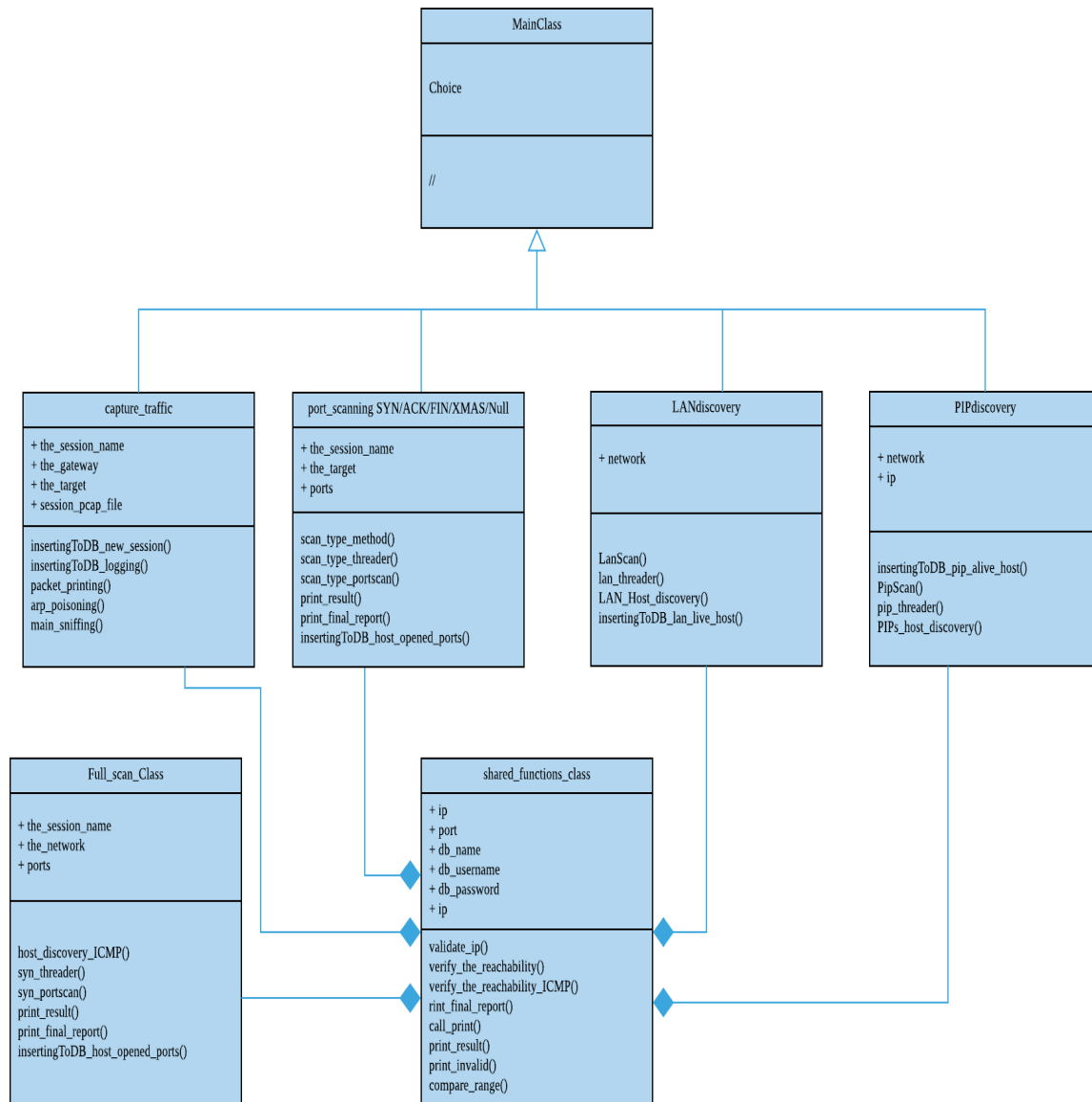


The screenshot above shows the use case diagram for the python tool that NetSec system offers. As it is displayed, the user can use the tool to perform multiple tasks such as host discovery, port scanning and capturing traffic. First host discovery is extended with two options which are LAN scan and PIP scan. Another task is port scanning where the user can perform SYN scan, ACK scan, FIN scan, XMAS and Null scan.

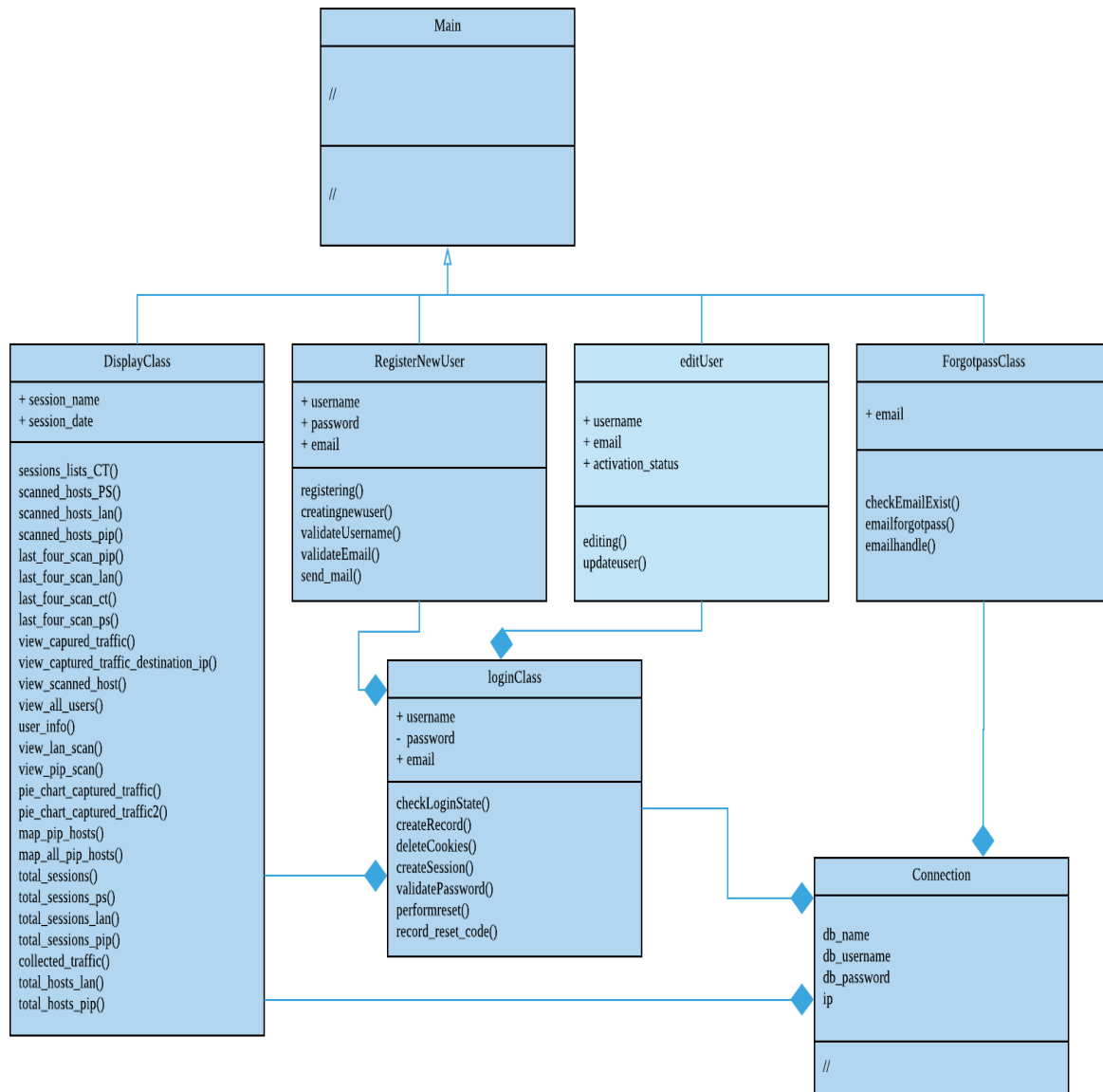
USE-CASE DIAGRAM FOR WEB APPLICATION PLATFORM:-



CLASS DAIGRAM:-



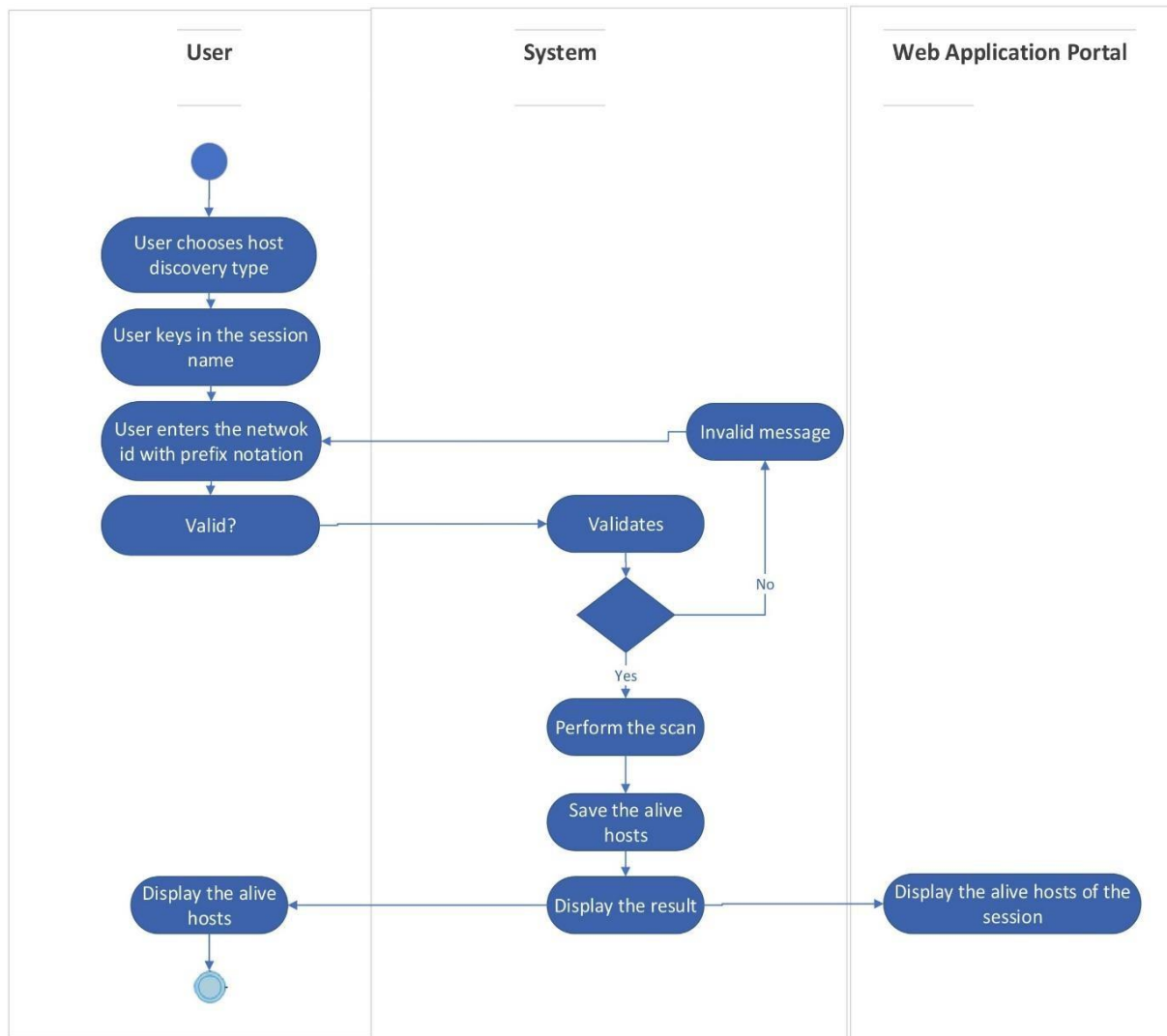
The above figure shows the different classes that the main tool will create along with their various attributes/variable, functions and the relationships. Based on the above diagram, it can be seen that “shared_functions_class” is the main class of tool, and all the other classes have a composition relationship with this main class. By another word, this means other classes cannot run if the main class is missing.



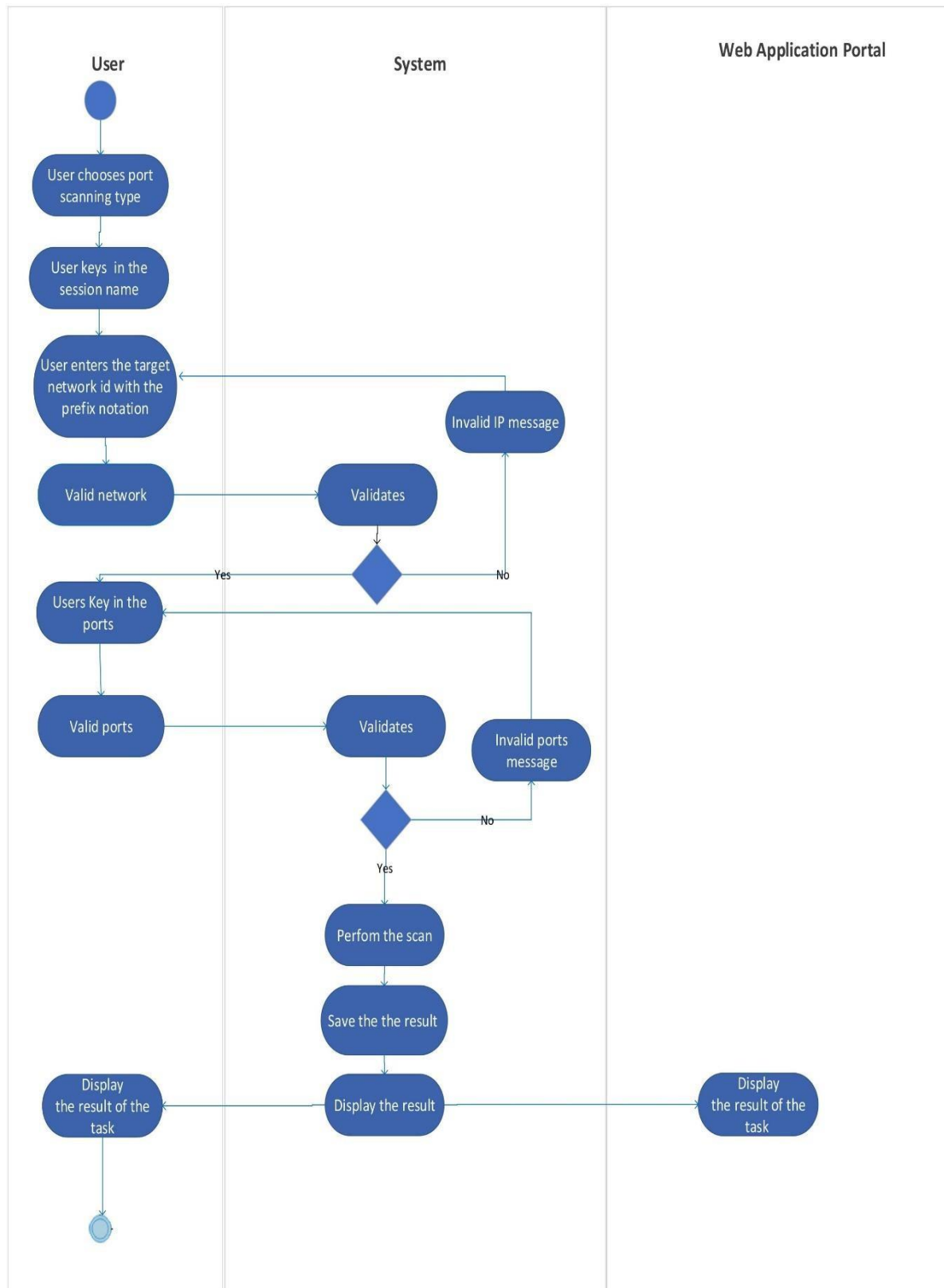
From the above picture, it can be utilized that the web application portal uses the Main class as the main class. Also, all the classes are having a composition relationship with the Connection Class as all the class will be useless if this class is missing. The primary function of this class is to handle all the connections and queries between the database and the web applications.

ACTIVITY DAIGRAM:-

Activity diagram can be defined as a type of system design where a developer can represent a serious of actions that should be followed to achieve a system functionality. This type of diagram is similar to two diagrams which are flowchart and flow diagram .



Activity diagram for port scanning (SYN/ACK/NULL/FIN/XMAS)

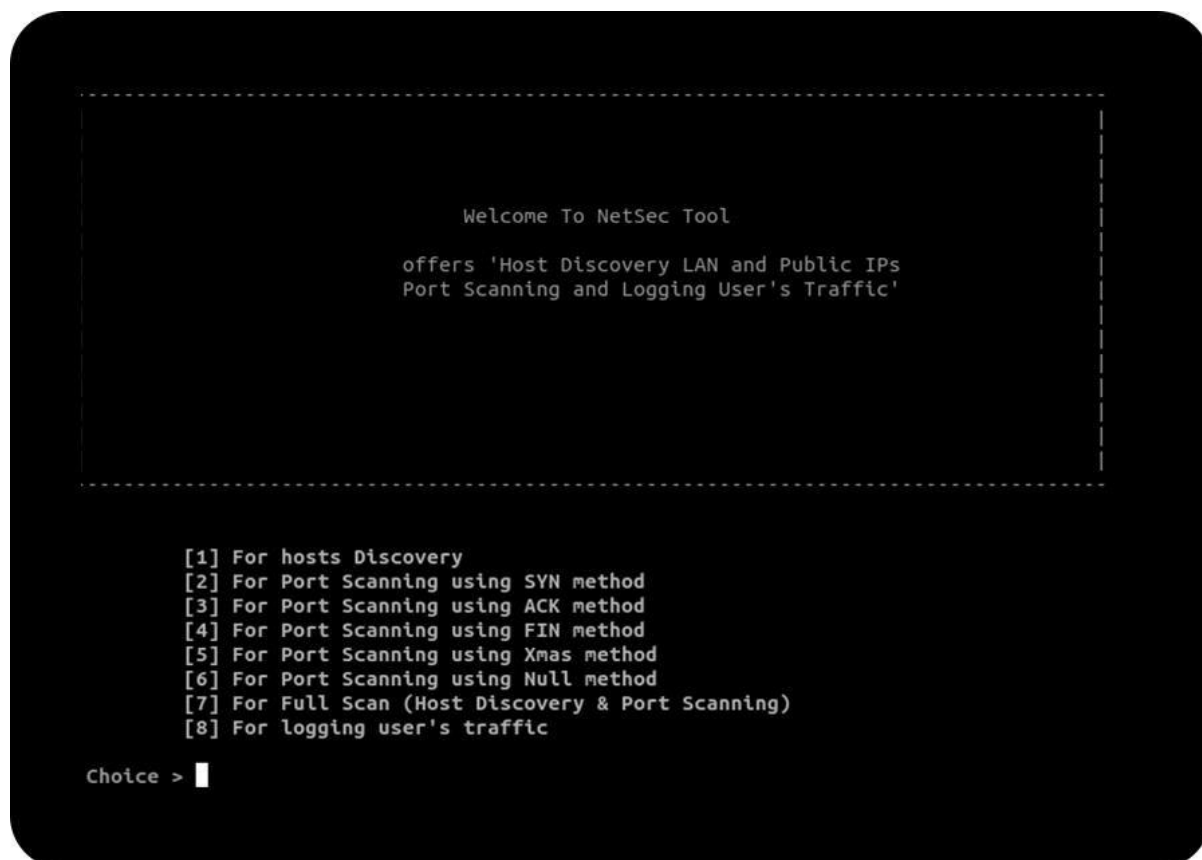


scans).

DATABASE DESIGN:-

As the developer has chosen MySQL database, there will be several tables used to store the result of the tasks. In general, every task will basically have two tables which the first one will store the session details such as session name, scan type, and date. The other table is for storing the session result such the target IP and the gathered information. The figure below shows all the tables with their relationships. Also, there is another table which stores admins information like username, password and email address. The last table is to store some information about the logged users in order to prevent some attacks like session hijacking.

Interface design (Storyboard) using Justinmind prototype software



INTERFACE DESIGN FOR HOST DISCOVERY:-

```
Choice > 1
    [1] For LAN Host Discovery
    [2] For Public IPs Host Discovery
Choice > 1
    [++] The Host Name is : OneOfThem
    [ * ] List of the interfaces
-----
[++] Network Interface : lo
[++] IP address       : 127.0.0.1
[++] Default Gateway  : 192.168.1.1
[++] Network Mask     : 255.0.0.0
-----
[++] Network Interface : wlo1
[++] IP address       : 192.168.1.35
[++] Default Gateway  : 192.168.1.1
[++] Network Mask     : 255.255.255.0
-----
[++] Network Interface : wlxa42bb0bc1d74
[++] IP address       : 192.168.1.2
[++] Default Gateway  : 192.168.1.1
[++] Network Mask     : 255.255.255.0
-----

[*] Session name > UR

[*] Network eg. 192.168.1.1/24 > 192.168.1.1/24
-----
[++] Updating MAC address vendors list

[++] Started scanning 192.168.1.0/24 network at   Tue Jun  5 00:47:16 2018
[++] Total Availabe IPs in the subnet are 256

[++] Found Alive Host : 192.168.1.21
[++] MAC Address      : 08:00:27:b5:e7:31
[++] NIC Vendor       : PcsCompu
[++] Hostname         : bryan-PC
```

IMPLEMENTATION

SCREENSHOTS

The below screenshot shows the main options that NetSec tool offers once it is started. The user just is required to key in the number of the scan type.

```
bryan@OneOfThem:~/Desktop/project$ sudo python "NetSec with DB.py"
[sudo] password for bryan:

Welcome To NetSec Tool

offers 'Host Discovery LAN and Public IPs
Port Scanning and Logging User's Traffic'

[1] For hosts Discovery
[2] For Port Scanning using SYN method
[3] For Port Scanning using ACK method
[4] For Port Scanning using FIN method
[5] For Port Scanning using Xmas method
[6] For Port Scanning using Null method
[7] For Full Scan (Host Discovery & Port Scanning)
[8] For logging user's traffic

Choice >

[++] [ DNS ] User : 192.168.1.5 requested : _airplay._tcp.local. on 2018-06-05 00:52:01.307460
..
```

Screenshot for the LAN host discovery

```
[1] For LAN Host Discovery
[2] For Public IPs Host Discovery

Choice > 1

[++] The Host Name is : OneOfThem

[ * ] List of the interfaces

-----
[++] Network Interface : lo
[++] IP address       : 127.0.0.1
[++] Default Gateway  : 192.168.1.1
[++] Network Mask     : 255.0.0.0
-----

[++] Network Interface : wlo1
[++] IP address       : 192.168.1.35
[++] Default Gateway  : 192.168.1.1
[++] Network Mask     : 255.255.255.0
-----

[++] Network Interface : wlx42bb0bc1d74
[++] IP address       : 192.168.1.2
[++] Default Gateway  : 192.168.1.1
[++] Network Mask     : 255.255.255.0
-----
```

```

[*] Session name > my home
[*] Network eg. 192.168.1.1/24 > 192.168.1.1/24
-----
[++] Updating MAC address vendors list

[++] Started scanning 192.168.1.0/24 network at   Fri Jun  8 23:14:22 2018
[++] Total Availabe IPs in the subnet are 256

[++] Found Alive Host : 192.168.1.21
[++] MAC Address : 08:00:27:b5:e7:31
[++] NIC Vendor : PcsCompu
[++] Hostname : bryan-PC
-----

[++] Found Alive Host : 192.168.1.1
[++] MAC Address : 48:f8:b3:f4:b1:65
[++] NIC Vendor : Cisco-Li
[++] Hostname : Linksys03300
-----

[++] Found Alive Host : 192.168.1.5
[++] MAC Address : ac:bc:32:3c:9a:41
[++] NIC Vendor : Apple
[++] Hostname : iPod-touch
-----

[++] Found Alive Host : 192.168.1.40
[++] MAC Address : 80:01:84:77:e6:42
[++] NIC Vendor : Htc
[++] Hostname : android-d5c939d87b885bef
-----

```

Screenshot for the full scan (Host Discovery & Port Scanning)

Once the user keys in all the session name, network ID and ports, the result of the scan will be displayed like the figure below.

```
Session name > libyan range
Network > 41.208.71.30/24
    [1] Single / Multiple ports
    [2] Range of ports
Choice > 2
Starting port > 1
Ending port > 600
[++] Started scanning 41.208.71.0/24 at Fri Jun 8 23:25:41 2018

-----
[++] Host is alive and its IP is | 41.208.71.1
[++] The IP Country & Timezone & Location : LY , Africa/Tripoli , (25.0, 17.0)
[+] Ports:
[++] Found Open Port 22 | ssh
[++] Found Open Port 80 | http
-----
[++] Host is alive and its IP is | 41.208.71.2
[++] The IP Country & Timezone & Location : LY , Africa/Tripoli , (25.0, 17.0)
[+] Ports:
[++] Found Open Port 80 | http
[++] Found Open Port 110 | pop3
[++] Found Open Port 143 | imap2
[++] Found Open Port 443 | https
[++] Found Open Port 465 | urd
[++] Found Open Port 587 | submission
-----
```

```

Choice > 8

[*] Session name > unknown user
[*] User's IP > 192.168.1.5
[*] Gateway's IP > 192.168.1.1
[*] External NIC interface > wLxa42bb0bcd74

[++] Host Discovery for 192.168.1.5 and 192.168.1.1
[++] 192.168.1.5 seems to be up
[++] 192.168.1.1 seems to be up

[++] We have successfully enabled the IP forwarding

[++] We started listening for user's traffic and all captured packets will be saved to var/www/html/netsec/pcaps/unknown user_1127965130.pcap

[++] [ HTTPS ] User : 192.168.1.5 requested : 17.173.66.101 on 2018-06-08 23:36:42.159893
[++] [ HTTPS ] User : 192.168.1.5 requested : 17.173.66.101 on 2018-06-08 23:36:42.230221
[++] [ UDP ] User : 192.168.1.5 requested : 17.253.82.125 on 2018-06-08 23:36:42.417529
[++] [ UDP ] User : 192.168.1.5 requested : 17.253.82.125 on 2018-06-08 23:36:42.475297
[++] [ UDP ] User : 192.168.1.5 requested : 17.253.82.253 on 2018-06-08 23:36:42.541865
[++] [ UDP ] User : 192.168.1.5 requested : 17.253.82.253 on 2018-06-08 23:36:42.586385
[++] [ UDP ] User : 192.168.1.5 requested : 17.253.68.125 on 2018-06-08 23:36:42.631193
[++] [ UDP ] User : 192.168.1.5 requested : 17.253.68.125 on 2018-06-08 23:36:42.674543
[++] [ DNS ] User : 192.168.1.5 requested : _fb._tcp.local. on 2018-06-08 23:36:42.783386
[++] [ DNS ] User : 192.168.1.5 requested : _fb._tcp.local. on 2018-06-08 23:36:43.799629
[++] [ DNS ] User : 192.168.1.5 requested : _fb._tcp.local. on 2018-06-08 23:36:46.871350
[++] [ IMAPS ] User : 192.168.1.5 requested : 106.10.231.25 on 2018-06-08 23:37:01.330737
[++] [ IMAPS ] User : 192.168.1.5 requested : 106.10.231.25 on 2018-06-08 23:37:01.388650
[++] [ HTTPS ] User : 192.168.1.5 requested : 104.103.46.54 on 2018-06-08 23:37:27.729301
[++] [ HTTPS ] User : 192.168.1.5 requested : 104.103.46.54 on 2018-06-08 23:37:27.793749
[++] [ DNS ] User : 192.168.1.5 requested : _companion-link._tcp.local. on 2018-06-08 23:37:28.868226
[++] [ DNS ] User : 192.168.1.5 requested : _companion-link._tcp.local. on 2018-06-08 23:37:29.893147

```

Sample code for port scanning result

```

def print_final_report(self, target):

    print "
    print Style.BRIGHT +Fore.GREEN + " [++] Opened/filtered ports : "
    print ' ' + str(list_of_opened_filtered_ports)

    print " [++] Closed Ports : "
    print ' ' + str(list_of_closed_ports)

    print " [++] filtered ports : "
    print ' ' + str(list_of_filtered_ports)

    print "
    print " ***** Scan Report ***** "
    print " [++] Scan Result for : " + str(target) + " "
    print "      [++] found Opened/filtered ports      : " + str(len(list_of_opened_filtered_ports))
    print "      [++] found closed ports                  : " + str(len(list_of_closed_ports))
    print "      [++] found filtered ports                  : " + str(len(list_of_filtered_ports))

    print "
    print " [++] Scan finished! at " + time.ctime()

```

Sample code for host discovery function

```

def PipScan(self,host):

    try:

        with print_lock:
            ans, unans= sr( IP(dst=unicode(host))/ICMP(), timeout=2 , verbose=0)
            if int(ans[0][1].type) == 0 and int(ans[0][1].code==0):
                host = ans[0][1].src
                total_found.append(host)

            print Style.BRIGHT + Fore.CYAN
            print "-----"
            print " "
            print "[++] Host is alive and its IP is | " + str(host)
            print " "

            find_the_geo = geolite2.lookup(str(host))
            if find_the_geo is not None:

                print "[++] The IP Country : " + find_the_geo.country
                print " "
                print "[++] The IP Timezone : " + find_the_geo.timezone
                print " "
                print "[++] The IP location : " + str(find_the_geo.location)
                self.insertingToDB_pip_alive_host(str(host), str(find_the_geo.country),str(find_the_geo.location),str(find_the_geo.timezone))
            else :
                self.insertingToDB_pip_alive_host(host, 'N/A','N/A','N/A')
                print Style.BRIGHT + Fore.RED
                print "[--] We could not gather the location!, it might be a private address. "
                print " "

            total_found.append(host)

    except:
        pass

```

Sample code for capturing traffic function

```

def main_sniffing(self):

    global the_session_name
    global pktdump
    s_f = shared_functions()

    print Style.BRIGHT +Fore.BLUE
    print " "
    the_session_name = raw_input(" [*] Session name > ")

    while True:

        thevictim = unicode(raw_input(" [*] User's IP > "))
        #thevictim = unicode(thevictim)
        if (s_f.check_ip(thevictim) is True):
            break
        else:
            print Style.BRIGHT +Fore.RED
            s_f.print_invalid()

    while True:
        thegateway = unicode(raw_input(" [*] Gateway's IP > "))

        if (s_f.check_ip(thegateway) is True):
            break
        else:
            s_f.print_invalid()

    while True:
        theinterface = raw_input(" [*] External NIC interface > ")
        if (s_f.check_interface(theinterface) is True):
            break
        else:
            print Style.BRIGHT +Fore.RED
            print " "
            print "[--] There is no such device! "
            print " "

    arp_po_thread = []
    print Style.BRIGHT +Fore.GREEN
    print " "
    print " [++] Host Discovery for " + str(thevictim) + " and " + str(thegateway)
    print " "
    time.sleep(.5)
    s_f.verify_the_reachability(thevictim)
    s_f.verify_the_reachability(thegateway)

    try:
        os.system('echo 1 > /proc/sys/net/ipv4/ip_forward')
        print Style.BRIGHT +Fore.GREEN
        print " "
        print " [++] We have successfully enabled the IP forwarding "
        print " "
    except:
        print Style.BRIGHT +Fore.RED
        print " "
        print " [--] We were unable to enable forwarding!!"

    md5_hash = random.getrandbits(32)

    session_pcap_file = str(the_session_name)+"_"+str(md5_hash)+".pcap"

    pktdump = PcapWriter("/var/www/html/netsec/pcaps/"+session_pcap_file, append=True, sync=True)

    self.insertingToDB_new_session(str(the_session_name), str(session_pcap_file))
    time.sleep(1)
    print Style.BRIGHT +Fore.GREEN
    print " [++] We started listening for user's traffic and all captured packets will be saved to var/www/html/ne
    print " "

    while True:

        vpoison = threading.Thread(target=self.arp_poisoning, args = (thevictim,thegateway,))
        vpoison.setDaemon(True)
        arp_po_thread.append(vpoison)
        vpoison.start()

```

Conclusion

Network analysis is one of the crucial tasks that must be performed weekly to ensure the network security since it offers the ability to discover intruders in the network, unauthorized opened ports and capture & analysis traffic. Besides, network analysis is not limited to only be performed for security concerns, but it can also be used for troubleshooting where the administrators want to check if a particular protocol works or not. As a result, the primary aim and objective of this project is to study, analysis and evaluate the standard network analysis tasks. Also giving a software-based solution that assists network administrators, system administrators and security practitioners perform and monitor their network using various tasks including host discovery, port scanning and capturing traffic.

Based on the conducted interviews with specialists who perform the network analysis tasks continuously, there are several issues with the currently available systems such as the integration issue where the user has to look for more than one tool to perform the task. The storage issue where most of the tools do not store the result of the tasks into a centralized database. Followed by the presentation of the task's result could be another issue since most of the time, the user needs to explain the result of the tasks to non-technical employees and lastly is the knowledge issue. Most of the tools require some training to use them effectively. Also, the interviewees recommended tackling the mentioned issues since they face them almost every day.

Besides that, the conducted research, as well as development process, were completed successfully and without having any issues since there were several available resources like research papers and books that talk about network analysis and network security. However, the only challenge

that was faced is how to follow the given timeframe of the final year project as well as providing an excellent quality project. This obstacle was tackled by giving efforts on the project and time management. Also, the received feedback from the interviewees about the proposed system was helpful and opened an eye to various recommendations that should be presented in the proposed system. In addition, the development process was processed perfectly, and all the deliverables were completed successfully as well as the extra features such as the full scan that was requested from some specialists which the ability to scan a range of IP addresses and perform two tasks in one task which are the host discovery and port scanning at the same time.

An overall, several enhancements will be implemented and deployed to the current project in the nearest future in order to help the end users having the availability such as by providing a GUI interface for the NetSec tool. Also, expanding the web application portal feature by allowing administrators to separate the permissions by adding a user as normal user or as an admin. Those enhancements are not considered as difficult features to implement but they only take some time, and they will be implemented as soon as the developer has the time to do them. Also, they will bring significant improvement to the proposed system.

