CAPSTONE PROJECT REPORT

(January – May 2022)

TIGER INTRUSION DETECTION SYSTEM

Submitted by

Rejuan Ahamed Anik	**Reg. No. 11801114**
Anik Sorkar	**Reg. No. 11816014**
Md Hasibul Ahasan Shakil	**Reg. No. 11800440**

Project Group Number: KC042

Course Code: CSE445

Under the Guidance of

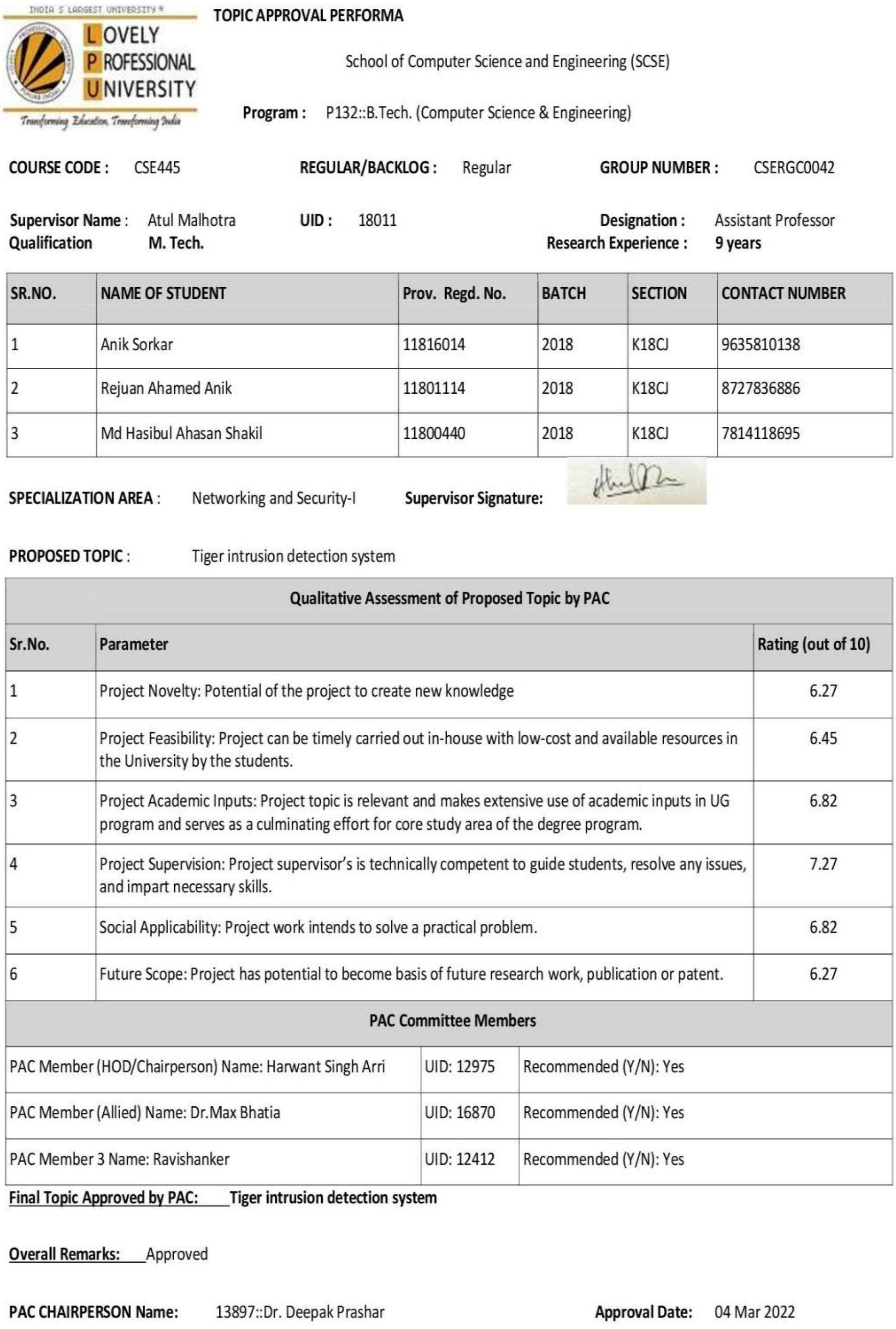
Mr. Atul Malhotra (Assistant Professor)

School of Computer Science and Engineering

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

PAC FORM



INDIA'S LARGEST UNIVERSITY®
LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering (SCSE)

Program : P132::B.Tech. (Computer Science & Engineering)

COURSE CODE : CSE445 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGC0042

Supervisor Name : Atul Malhotra **UID :** 18011 **Designation :** Assistant Professor
Qualification **M. Tech.** **Research Experience :** **9 years**

SR.NO.	NAME OF STUDENT	Prov. Regd. No.	BATCH	SECTION	CONTACT NUMBER
1	Anik Sorkar	11816014	2018	K18CJ	9635810138
2	Rejuan Ahamed Anik	11801114	2018	K18CJ	8727836886
3	Md Hasibul Ahasan Shakil	11800440	2018	K18CJ	7814118695

SPECIALIZATION AREA : Networking and Security-I **Supervisor Signature:**

PROPOSED TOPIC : Tiger intrusion detection system

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	6.27
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	6.45
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	6.82
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.27
5	Social Applicability: Project work intends to solve a practical problem.	6.82
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	6.27

PAC Committee Members		
PAC Member (HOD/Chairperson) Name: Harwant Singh Arri	UID: 12975	Recommended (Y/N): Yes
PAC Member (Allied) Name: Dr.Max Bhatia	UID: 16870	Recommended (Y/N): Yes
PAC Member 3 Name: Ravishanker	UID: 12412	Recommended (Y/N): Yes

Final Topic Approved by PAC: **Tiger intrusion detection system**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 13897::Dr. Deepak Prashar **Approval Date:** 04 Mar 2022

DECLARATION

We hereby declare that the project work entitled “Tiger Intrusion Detection System” is an authentic record of our own work carried out as requirements of Capstone Project for the award of B.Tech degree in Computer Science and Engineering (B. Tech) from Lovely Professional University, Phagwara, under the guidance of Mr. Atul Malhotra, during January to April 2022. All the information furnished in this capstone project report is based on our own intensive work and is genuine.

Project Group Number: KC042

Name of Student 1: Rejuan Ahamed Anik

Registration Number: 11801114

Name of Student 2: Anik Sorkar

Registration Number: 11816014

Name of Student 3: Md Hasibul Ahasan Shakil

Registration Number: 11800440

	Anik	SHAKIL
(Signature of Student 1)	**(Signature of Student 2)**	**(Signature of Student 3)**
Date:21/05/2022	**Date:21/05/2022**	**Date:21/05/2022**

CERTIFICATE

This is to certify that the declaration statement made by this group of students is correct to the best of my knowledge and belief. They have completed this Capstone Project under my guidance and supervision. The present work is the result of their original investigation, effort and study. No part of the work has ever been submitted for any other degree at any University. The Capstone Project is fit for the submission and partial fulfilment of the conditions for the award of B.Tech degree in Computer Science and Engineering (B. Tech) from Lovely Professional University, Phagwara.

(Signature)

Mr. Atul Malhotra

(Assistant Professor)

School of Computer Science and Engineering,

Lovely Professional University,

Phagwara, Punjab.

Date:

ACKNOWLEDGEMENT

We humbly present our vote of thanks to all the guidance and assistance ship that helped us complete this project successfully.

We take this opportunity to express our sincere gratitude to our mentor Mr. Atul Malhotra for guiding and providing us with assistance through the course of the entire project. The frequent encouragement and direction provided by him was vital for the successful completion of the project work. We are thankful for his active support, valuable time, advice, whole-hearted guidance, and sincere cooperation during the study and in completing the capstone project.

We are grateful to the faculty and staff of Lovely Professional University for providing us with the necessary facilities and for cooperative with us throughout the duration of the capstone project.

Lastly, we are thankful to all those, particularly our family and friends, who have been instrumental in providing a conducive environment and innovative suggestions for the problems faced during the project without which it would have been difficult to complete this project.

TABLE OF CONTENTS

1. Introduction

Nowadays, the involvement of the internet in normal life has increased rapidly. The use of the internet has become very crucial for everyone. So, with the increase in the use of the internet for personal activities, it is also necessary to keep the system secure from malicious activities as cyber-attacks are increasing at an alarming rate with the evolution of technology. There are a variety of attacks which target the information system in order to steal the information or corrupt the data present with in them. The prominent attacks which target the networks are evil twin attack, de-authentication attack etc. A list of prominent attacks has been presented in table 1. So, to identify and prevent the system from such attacks, the intrusion detection systems came into existence. Intrusion detection systems (IDSs) have the capacity to identify any anomalous network usage or access. Intrusion detection system can monitor, collect, and analyze data to detect known assaults, identify abnormal network usages, and reveal network misuse. IDSs collect data and issue alerts based on the type of intrusion detected.

Year	Attack vector	Method
2016	Bangladesh Bank cyber heist	Footprint
2014	Sony hacked and paid 8million to his client	Shamoon wiper malware
1994	Phonemasters.	Tapping
1995	Citibank / Vladimir Levin.	Tapping
1999	Melissa Virus.	Macro virus
2000	MafiaBoy.	DDoS
2004	Delta Airlines / Sven Jaschan.	Sasser Computer worms
2005	Operation Get Rich.	ARP Spoofing
2006	Operation Shady RAT.	Remote access tool
2007	Iceman.	Stealing credit card
2007	Estonia DDos	DDoS
2008	Conflicker	Worm
2010	Stuxnet	Worm
2011	Epsilon	Phishing

Table 1. The top cyber-attack statistics reported in the last decade

1.1. Intrusion Detection System

An Intrusion Detection System (IDS) could be a system that monitors network traffic for suspicious activity and problems alerts once such activity is discovered. it's a software system application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is generally reportable either to AN administrator or collected centrally employing a security data and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for doubtless malicious activity, they're conjointly disposed to false alarms. Hence, organizations got to fine-tune their IDS merchandise after they initial install them. It suggests that properly fitting the intrusion detection systems to acknowledge what traditional traffic on the network sounds like as compared to malicious activity.

Intrusion interference systems conjointly monitor network packets incoming the system to ascertain the malicious activities concerned in it and directly send the warning notifications.

1.2. Classification of Intrusion Detection System

IDS are classified into 5 types:

1. Network Intrusion Detection System (NIDS)

Network intrusion detection systems (NIDS) square measure started at a planned purpose at intervals the network to look at traffic from all devices on the network. It performs Associate in nursing observation of passing traffic on the whole subnet and matches the traffic that's passed on the subnets to the gathering of renowned attacks. Once Associate in nursing attack is known or abnormal behavior is determined, the alert may be sent to the administrator. Associate in nursing example of a NIDS is putting in it on the subnet wherever firewalls square measure situated to check if somebody is attempting to crack the firewall.

2. Host Intrusion Detection System (HIDS)

Host intrusion detection systems (HIDS) run on freelance hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device solely and can alert the administrator if suspicious or malicious activity is detected. It takes a photo of existing system files and compares it with the previous photo. If the analytical system files were altered or deleted, Associate in nursing alert is shipped to the administrator to analyze. Associate in nursing example of HIDS usage may be seen on mission-critical machines, that do not seem to be expected to vary their layout.

3. Protocol-based Intrusion Detection System (PIDS)

Protocol-based intrusion detection system (PIDS) contains a system or agent that may systematically resides at the forepart of a server, dominant and decoding the protocol between a user/device and therefore the server. It's attempting to secure the net server by often watching the HTTPS protocol stream and settle for the connected HTTP protocol. As HTTPS is un-encrypted and before instantly getting into its net presentation layer then this technique would wish to reside during this interface, between to use the HTTPS.

4. Application Protocol-based Intrusion Detection System (APIDS)

Application Protocol-based Intrusion Detection System (APIDS) could be a system or agent that usually resides at intervals a bunch of servers. It identifies the intrusions by watching and decoding the communication on application-specific protocols. as an example, this can monitor the SQL protocol express to the middleware because it transacts with the information within the net server.

5. Hybrid Intrusion Detection System

Hybrid intrusion detection system is formed by the mixture of 2 or additional approaches of the intrusion detection system. Within the hybrid intrusion detection system, host agent or system knowledge is combined with network info to develop an entire read of the network system. Hybrid intrusion detection system is simpler compared to the opposite intrusion detection system. Prelude is Associate in nursing example of Hybrid IDS.

1.3. Different types of network Attacks

A network attack is an attempt to obtain unauthorized access to a network in order to steal data or perform in other malicious activity. Following are some attacks:

i. Evil twin Attack

The Evil Twins attack is a spoof cyber-attack that tricks users into connecting to fake Wi-Fi hotspots that mimic legitimate networks. When a user connects to an "evil twin" network, hackers can access everything from victim network traffic to personal logins and credentials. The Evil Twin attack gets its name from its ability to mimic legitimate Wi-Fi networks indistinguishably one from another. This type of attack is highly dangerous because it is almost impossible to identify.

ii. Address Resolution Protocol (ARP) poisoning attack

ARP spoofing is also known as routing ARP poisoning or ARP cache poisoning. This is a type of malicious attack in which cybercriminals send bogus ARP messages to the target local network with the intention of associating their MAC address with the IP address of a legitimate device or server on the network. The link could send data from the victim's computer to the attacker's computer rather than the original target.

iii. A man in the middle (MITM) attack

A man in the middle (MITM) attack is a type of eavesdropping in which the cyber attacked intercepts, relays, and alters messages between two parties—who have no idea that a third party is involved—to steal information.

iv. Denial service attack

One way in which a wireless network can be attacked is to try to flood the Access Point (AP) with authentication and association frames. To association flood, the attacking device will spoof its wireless MAC address then, rapidly and repeatedly, try associating to the AP. At each attempt the attacker will change its MAC address, mimicking the existence of many clients. This has the effect of consuming the AP's memory and processing ability, denying service to legitimate clients.

v. Deauthentication Attack

Deauthentication attack: A Wi-Fi deauthentication attack is a type of denial-of-service attack where attacker sends deauthentication frame to AP.

vi. Authentication association flooding

A wireless network can be attacked is to try to flood the Access point (AP) with authentication and association frames. For performing association flood, the attacking device will spoof its wireless attacking address then, mac and repeatedly, attempt associating to the AP. At each attempt the attacker can change its mac address, mimicking the existence affect clients. This has the effect of consuming the AP's memory and processing ability, denying service to legitimate of many.

vii. Rogue access point

A rogue access point is an access point that has been established on a network without the consent of the network owner. If an attacker controls the access point, they can intercept data (e.g., personally identifiable information) passing through the network. This is why the coffee shop sent the warning to its customers; they wanted to prevent an unauthorized access point on their network from capturing users' data.

2. Problem Statement

Available intrusion detection systems are good, but they are most Paid and able to provide False-positive results to the user. They perform excellently in real-time, but their cost is too much that everyone cannot afford. Despite that, they are compatible with only fewer security researchers and users can't modify them to detect anomalies that they want. So, we have introduced a framework to detect anomalies for the wireless network system. This will help to mitigate network anomalies. User will be able to configure the mode of sensibility as per their requirements which makes our framework more friendly and compatible to the users.

3. Existing System

3.1. Introduction

There are several existing services for intrusion detection system like Solarwinds security event manager, Kismet, zeek, suricate etc but all these are very costly for end-users and can't modify them according to the end user's need. The report of the IDS will be downloaded via the software itself but in our framework end user just need to run the framework, our framework will automatically identify the attacks in wireless system.

3.2. Existing Software

The software available in the markets are below:

- Zeek: Formerly known as Bro, can run on Unix, Linux and Mac OS and follow two functions: traffic logging and analysis. Zeek is different from Snort as it also works in the application layer, giving you the ability to track different resources from different OSI platforms such as HTTP, DNS, SNMP and FTP. Zeek uses signature-based diagnostic and detection methods based on ambiguity and has a diverse user community.
- Snort: Leader of a free Open-source NIDS hosted by Cisco Systems. A well-known open-source tool that can work on Windows, Linux and Unix operating systems while analysing real-time traffic. Snort has three types: packet sniffing mode, packet logger and login detection. Entry access mode is based on a set of rules you can create or download in the Snort community. Snort is able to detect OS fingerprints, hole scanning, SMB testing and many other attacks using signature-based and non-signature-based techniques. The two main disadvantages of Snort are its lack of GUI (publicity has introduced some) and the fact that creating rules can be difficult, leading to false results.
- Suricate: Snort's direct competitor uses signature-based, confusing entry-based and policy-based acquisition methods. Snort provides real-time detection and prevention, as well as network security monitoring. For many, Suricata is one of the most modern Snort with multi-track capability, GPU acceleration and confusing mathematical discovery of multiple models. It also complies with the Snort data structure, and you can apply Snort policies in Suricata. Suricata can check TLS / SSL certificates, HTTP requests and DNS purchases.
- OpenWIGS-ng: OpenWIGS-ng is a free open-source NIDS dedicated to wireless networks, developed by the same team as the entry-level network tool Aircrack-ng. OpenWIGS-ng can be used as a wallet for Wi-Fi or access. Too bad it only works on linux systems. OpenWIGS-ng has three main components, a command collector and sender, a server containing an analysis engine and an interface for displaying events and alerts.

- Security Onion: Security Onion is a Ubuntu-based Linux distribution for IDS and network security monitoring (NSM), and contains several additional open source technology that works with concert. The platform offers complete access, network security monitoring, and log management with the best integration of Snort, Suricata, Zeek, and other tools like Sguil, Squert, Snorby, ELSA, Xplico, among others. For those who wish the best tools mentioned above in a single package, Onion Safety is worth considering.
- Sagan: Sagan is another open-source network access system, included in my favorites list because it provides high performance and real-time log analysis. Sagan is powered by robust analytics and integration engines running under nix * applications, so it is available in FreeBSD, Linux, and OpenBSD, among others. I like Sagan because it uses a multidisciplinary architecture approach to help with optimal performance levels. This app was designed to make its design and rules work in the same way as the Suricata IDS / IPS (which will later appear in my list) and Snort, as this helps to maintain compliance with law enforcement software like Oinkmaster, PulledPork, and others. This is similar and means that you can link log events via the Suricata or Snort system. Sagan can write on the Snort website and is compatible with Suricata and Snort consoles.
- Open DLP: OpenDLP is an open-source program that focuses on data loss (DLP). This tool scans the site and file system data when resting and searches for sensitive organization data to detect unauthorized data transfers or data duplication. It can detect sensitive data at rest in thousands of Unix programs, MySQL sites, Microsoft Windows programs, and Microsoft SQL sites. All of this is done through an intermediate web application. OpenDLP works to detect malicious intruders and to identify employees who make common mistakes, such as sending data when they are not authorized to do so. This tool supports Linux and Windows and can be used as a standalone program or agents. There are two main components of OpenDLP. Part of the web application manages Windows agents and Windows / database / Unix free scanners. The second part is a Microsoft Windows agent, which can perform quick scanning of thousands of applications at once. Non-agent-based database scanning can be done on MySQL and Microsoft SQL Server websites.

3.3. WHAT'S NEW

Existing intrusion detection systems are too costly. Some of existing tool is effective for one layer where our framework is capable to detect anomalies from network layer, data-link layer and transport layer and we provide an easy to setup and user interface which provides real time monitoring, one command to start, Free of cost and it will give warning on your device, and it is customizable according to your desire level of sensitivity. Only we require a device with Kali Linux distribution in order to execute the framework and to start monitoring the traffic. Due to the widespread use of internet-connected systems for enterprise globally. The enterprise systems are targeted by a variety of network layer and transport layer attacks which result in critical monetary and technological damages that's why necessity of real time intrusion detection framework is increasing exponentially day by day.

4. PROBLEM ANALYSIS

Tiger intrusion detection and prevention system is an automated traffic monitoring framework that makes network monitoring system easy and reliable that can be used in any available Linux distribution. This framework performs various tasks in network monitoring system and detect various network layer, data-link layer and transport layer attacks including ARP poisoning, Evil-Twin, deauthentication, MiTm attacks.

Firstly, it will obtain all available SSID’s and BSSID’s then it starts listing of connected devices of Wi-Fi after that it will start capture the traffic. In the meantime, of capturing traffic, it will also get ready detecting Evil-Twin attack by as per the user threshold value. TIDPS also check for deauthentication or flooding attack by checking if single or group of IPs sending deauthentication packet and TIDPS also prevent them by blocking there IP. For ARP attack detection TIDPS check for uniqueness of every IP’s mac address besides of this some another attack can detect by TIDPS are given bellow:

- Association / Authentication flooding
- Detect possible WEP attack using chopchop method
- Detect possible WPS pin brute force attack by Reaver, Bully, etc.
- Detection of Rogue Access Point

Which Attacks describes and named adobe TIDPS can detect them at impressive detection rate.

4.1. FEASIBILITY STUDY

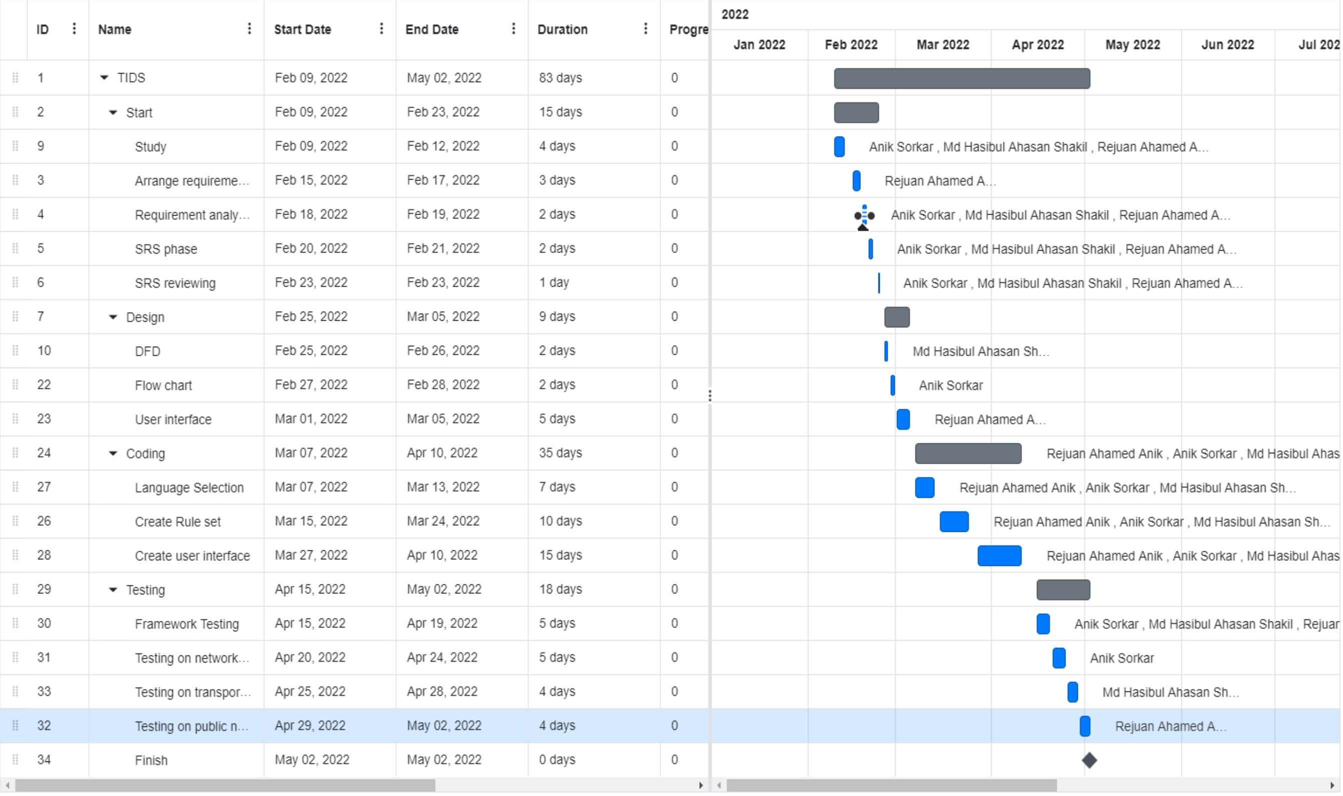
It is an analysis of our system-related vision and provides validity and makes our idea important. It takes effort and the need for thinking ability about the possibility of a problem-solving system. Feasibility is the study of an important or dynamic influence, which occurs during system development. The effect can be positive or negative. The plan is considered possible if the consent gives rise to doubts. Feasibility research can be done in a variety of ways with regard to different fields, we define four key feasibility study methods which are described as follows:

- **Technical Feasibility:** A system's technical feasibility specifies its compatibility, comfort, and ability to achieve with current available technology. It considers whether the essential technology is available, as well as available resources such as equipment and software tools for system development. We can declare that our produced system is technically feasible because we are not experiencing any difficulties with the project's development and maintenance resources. Whatever software tools are required for system development are widely available and easily obtained via the internet.
- **Economical Feasibility:** This method is highly cost-effective because it does not require any additional tools other than the ones we need for development, which are easily accessible and free to obtain and use for project development. We do not need to invest more money on system development. It is creating an atmosphere for development in an efficient manner. If we do so, we will witness the greatest utilization of the system's connected resources. We no longer need to be concerned about this system after it has been developed. As a result, we can conclude that this system is economically feasible.
- **Schedule Feasibility:** It is described as the state of being probable and completed on time. Our project may fail if it takes too long to complete before being used. It means estimating the project in terms of how long it will take to construct this system. The practicality of a project's timetable is measured by its schedule. We confer with our staff to see whether the project timeframe is reasonable. Our project has an established deadline. We've decided if the deadlines are required or desirable.
- **Operational Feasibility:** It is related to the performance measurement of the system for which it is designed. It refers to all of the system's functions and features and looks for the speed with

which requests from users are executed and the efficacy with which they are responded to. It takes advantage of the opportunities introduced during scope definition and meets the requirements identified. It also provides satisfaction for the system development phase. It ensures the desired operational results, which is part of the design and development process. It comprises criteria such as the system's stability, maintainability, supportability, and usability for users. At various stages of design, all parameters must be considered. A design and development system necessitates proper and timely application software development, as well as efforts to meet previously set parameters. When the technical and operational qualities of a system are defined in the design, it serves its intended function most effectively. So, we can argue that operational feasibility is a vital feature of systems engineering that must be considered early in the design process.

4.2. PROJECT PLAN

First of all we started figure out the methodology of real time packet capturing and methodology of creating the set of rules after that we choose our programming language as python 3.9.13 and we started our code ,every week we did meeting and we tried to make it more accurate in term of detecting various kind of attack including ARP poisoning, deauthentication, WEP attack using chopchop method, WPS pin bruteforce attack by Reaver, Bully and Evil-twin.



ID	Name	Start Date	End Date	Duration	Progre
1	▾ TIDS	Feb 09, 2022	May 02, 2022	83 days	0
2	▾ Start	Feb 09, 2022	Feb 23, 2022	15 days	0
9	Study	Feb 09, 2022	Feb 12, 2022	4 days	0
3	Arrange requireme...	Feb 15, 2022	Feb 17, 2022	3 days	0
4	Requirement analy...	Feb 18, 2022	Feb 19, 2022	2 days	0
5	SRS phase	Feb 20, 2022	Feb 21, 2022	2 days	0
6	SRS reviewing	Feb 23, 2022	Feb 23, 2022	1 day	0
7	▾ Design	Feb 25, 2022	Mar 05, 2022	9 days	0
10	DFD	Feb 25, 2022	Feb 26, 2022	2 days	0
22	Flow chart	Feb 27, 2022	Feb 28, 2022	2 days	0
23	User interface	Mar 01, 2022	Mar 05, 2022	5 days	0
24	▾ Coding	Mar 07, 2022	Apr 10, 2022	35 days	0
27	Language Selection	Mar 07, 2022	Mar 13, 2022	7 days	0
26	Create Rule set	Mar 15, 2022	Mar 24, 2022	10 days	0
28	Create user interface	Mar 27, 2022	Apr 10, 2022	15 days	0
29	▾ Testing	Apr 15, 2022	May 02, 2022	18 days	0
30	Framework Testing	Apr 15, 2022	Apr 19, 2022	5 days	0
31	Testing on network...	Apr 20, 2022	Apr 24, 2022	5 days	0
33	Testing on transpor...	Apr 25, 2022	Apr 28, 2022	4 days	0
32	Testing on public n...	Apr 29, 2022	May 02, 2022	4 days	0
34	Finish	May 02, 2022	May 02, 2022	0 days	0

2022
Jan 2022
Feb 2022
Mar 2022
Apr 2022
May 2022
Jun 2022
Jul 202
Anik Sorkar , Md Hasibul Ahasan Shakil , Rejuan Ahamed A...
Rejuan Ahamed A...
Anik Sorkar , Md Hasibul Ahasan Shakil , Rejuan Ahamed A...
Anik Sorkar , Md Hasibul Ahasan Shakil , Rejuan Ahamed A...
Anik Sorkar , Md Hasibul Ahasan Shakil , Rejuan Ahamed A...
Md Hasibul Ahasan Sh...
Anik Sorkar
Rejuan Ahamed A...
Rejuan Ahamed Anik , Anik Sorkar , Md Hasibul Ahas
Rejuan Ahamed Anik , Anik Sorkar , Md Hasibul Ahasan Sh...
Rejuan Ahamed Anik , Anik Sorkar , Md Hasibul Ahasan Sh...
Rejuan Ahamed Anik , Anik Sorkar , Md Hasibul Ahas
Anik Sorkar , Md Hasibul Ahasan Shakil , Rejuar
Anik Sorkar
Md Hasibul Ahasan Sh...
Rejuan Ahamed A...

Figure 1: Gantt Chart

5. IMPLEMENTATION OF THE PROJECT

Project implementation is the final stage of a project's lifecycle (after initiation and planning), where developer put everything, developer has planned and constructed into action. Developer has made plans, ideas, and tactics and are now merely carrying them out. Then develop deliverables, present them, and track and monitor the status of each project piece.

5.1. SOFTWARE AND HARDWARE REQUIREMENTS

i. Hardware Recruitments for Attacker and NIDS Device

Ram 8 GB
SSD 512
Processor Intel core i7 10th gen
Display
Wi-Fi adapter what’s support monitor mode

ii. Software Requirements for Attacker and NIDS Device

Linux OS
Python 3.0
Python compiler
Aircrack-ng

iii. Attacker machine creation

we set up one laptop as an attacker machine and we install kali Linux for our pentesting tool so that we can perform different types of attack, we use mdk4 tool for deauthintication attack, for arp poisonings and wep chopchop attack we installed Aircrack-ng, for WPS pin brute force attack we installed Reaver, Bully and Evil-twin.

iv. Experimental network:

We use Wi-Fi routers, and we configure WEP security mode in routers. So that we can test some attack’s intentionally,

v. Rule set implementation:

For implementing any intrusion detection system some developers prefer to use machine learning algorithms and some developers prefer to create rule set for detecting different kind of anomalies, in our framework we used some set of rules for detecting network anomalies. We used python programming language to build our framework. A bit of rule set is given bellow in the form of pseudo code:

For deauthentication attack detection and prevention

```
    Get ip
    Set threshold_point =50
    Set temp_ip=ip
```

```
If (temp_ip =ip)  && ( deauthenthication_packet >= 50)
{
 Print response
             “deauthentication attack detected”
Call prevention(temp_ip)
}End of if
```

For Evil Twin Attack detection

```
Set threshhold_point=2
Get bssid
Get ssid
Set saved_bssid =bssid
Set saved_ssid = ssid
Get number_of_ssid
If (number_of_ssid)> threshold_point
{
        Print response
        “Evil twin attack detected”
} End of if
 else {
        Get beacon_packet
         If (bssid != saved_bssid) && (ssid !=saved ssid)
                {
                        Print response
                         “Evil twin attack detected”
                         Print response
                        “attacker”+bssid “attacker”+ssid
                }End of if
 }end of else
```

For ARP poisoining attack detection

```
For each ip address
If (ip_1.mac = ip_2.mac)
{
        Print response
        “Arp poisioning attack detected for ip_1 and ip_2”
         Call prevention(ip_1,ip_2)
 }
End of if
```

5.2. DFD

Data Flow Diagram shows the flow of data within a system. It provides information about the outputs and inputs of each object and the process itself.

Data Flow diagram elements:

i. The process: Output conversion in the system occurs due to process function. The signs of the process are rectangular with round, oval, rectangular or circular corners. This process is called a short sentence, with one word or phrase to express its context

ii. Data Flow: Data mobility describes the data that is transmitted between different parts of the system. An arrow icon is a data flow symbol. The associated name must be given to the flow to retrieve deleted information. Data mobility also represents objects and information that is moved. Property change is followed by programs that are not limited to education. The flow provided should convey only one type of information. Flow direction must be an arrow that can also be on both sides.

iii. Storage space: The information is stored in a repository for later use. The two horizontal lines represent the store sign. Storage is not limited to a data file but can be anything like a folder with a document, an optical disc, a locker. The database may be viewed as independent of its use. When data flows from a repository is stored as data readings and when data flows to the store it is called data entry or data recovery.

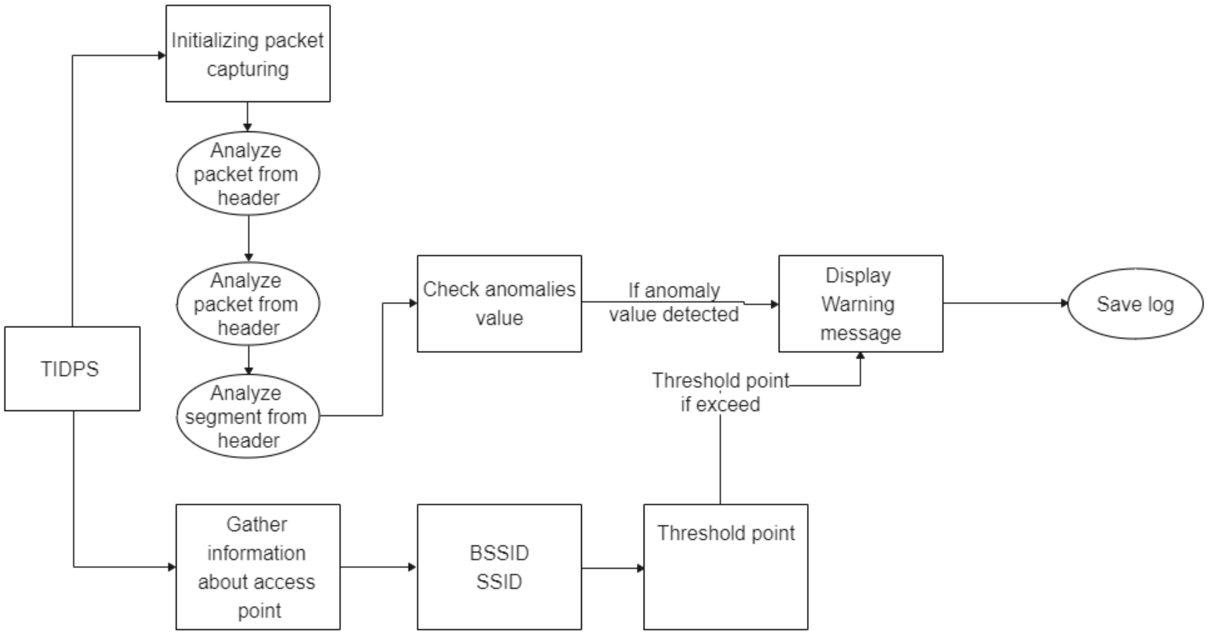

Initializing packet capturing
Analyze packet from header
Analyze packet from header
Analyze segment from header
Check anomalies value
If anomaly value detected
Display Warning message
Save log
TIDPS
Threshold point if exceed
Gather information about access point
BSSID SSID
Threshold point

Figure 2: Data flow diagram showing the flow of control from one module to another.

5.3. FLOW CHART

When we start our framework, it initializes packet capture; then it analyzes frame, packet, and segment from the header parameter. Then it checks the parameters for any anomalies value. If we find any anomalies value from the parameter, it will block the traffic; then, it will generate the alarm. Otherwise, it will allow traffic over the network.

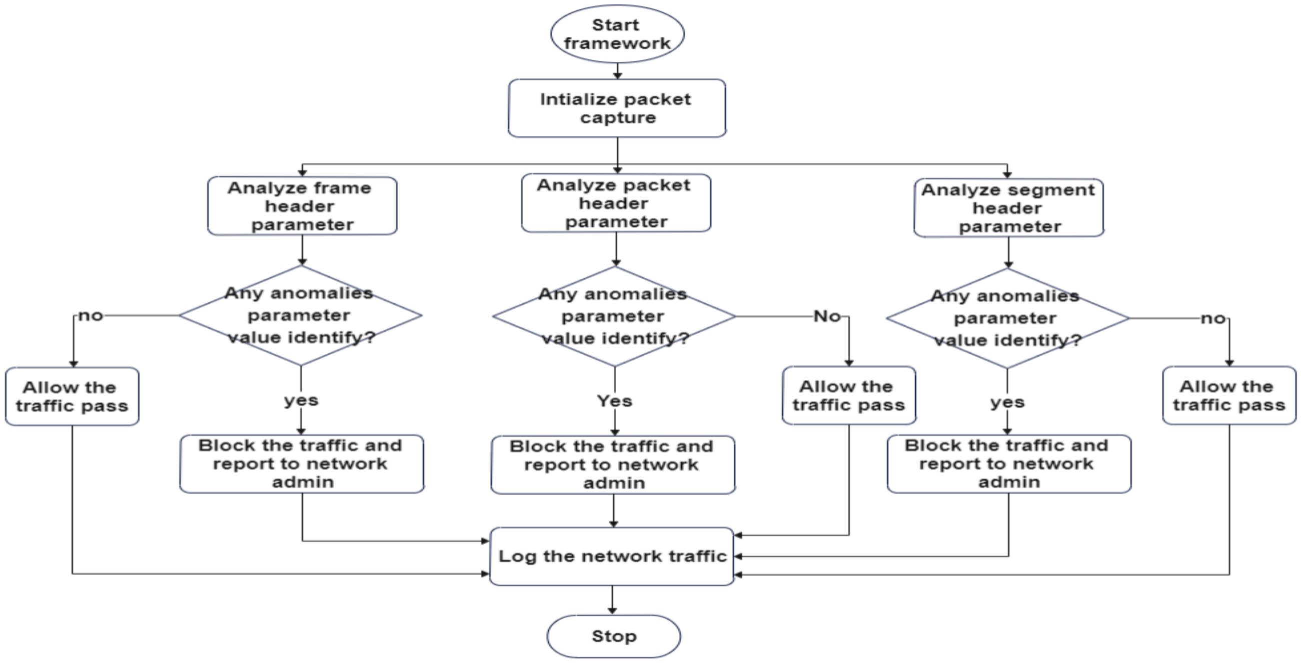

Start framework
Intialize packet capture
Analyze frame header parameter
Analyze packet header parameter
Analyze segment header parameter
Any anomalies parameter value identify?
Any anomalies parameter value identify?
Any anomalies parameter value identify?
no
No
no
yes
Yes
yes
Allow the traffic pass
Allow the traffic pass
Allow the traffic pass
Block the traffic and report to network admin
Block the traffic and report to network admin
Block the traffic and report to network admin
Log the network traffic
Stop

Figure 3: Flow Chart

5.4. Configure TIDPS framework device and Attacker Device

For our framework device we select Kali Linux as our distribution, and we select monitor mode Network Interface Card (NIC) as our framework is monitor various activity AP and its client including packets and fragments.

On the other hand, as our attack node, we use a laptop that also runs Kali Linux v2021.1. We also use an integrated NIC that monitors the channel, injects packets as needed, and supports the 802.11 protocol. All of the attacks detailed in this experiment were done by this method. In addition, while the attacks are being carried out, we use another NIC to monitor, capture, and record packets from the channel. To monitor mode functionality is required for this NIC. Finally, we assault an organization Access points. It has three radios and supports the 802.11 protocol and WPA/WPA2/WEP Wi-Fi security. We configured the first radio as a WEP AP on the 2.4 GHz band, the second radio as unused, and the third radio as the IDS offered. We use two extra laptops for the client, both running windows 7 xp operating and supporting WPA/WPA2/WEP.

5.5. Setup monitor mode using aircrack-ng and use case

Monitor Mode captures all relevant data packets in order to determine whether the router is vulnerable. It's also used to see if the network is vulnerable to any kind of assault. Monitor Mode displays all critical information on each device and can also be used to observe massive amounts of network traffic. In our work we use aircrack-ng to enable monitor mode.

The **aircrack-ng** package includes **Airmon-ng**, which puts the network interface device in monitor mode. Airmon-ng accepts all wireless packets, regardless of whether they are aimed for them or not. Without linking or authenticating with the access point, you should be able to catch these packets. By setting the network interface in monitor mode, it can verify the status of an Access Point. Firstly, configure the wireless cards to enable monitor mode, then terminate all background programs that you think are interfering with it. After terminating the processes, use the command below to enable monitor mode on the wireless interface:

```
sudo airmon-ng start wlan0 #<network interface name>
```

To disable the monitor mode by stopping the airmon-ng anytime by using the command below:

```
sudo airmon-ng stop wlan0 #<network interface name>
```

Airplay-ng uses packets to generate or increase traffic on a wireless network. Aireplay-ng may capture packets from two separate sources. When a deauthentication attack is launched against a wireless access point and a user, Airplay-ng comes in handy. You can also use airplay-ng, a program that lets you retrieve a key from the client's system, to launch assaults like the coffee latte attack. This can be accomplished by catching an ARP packet, manipulating it, and then returning it to the system.The client will then create a packet that can be captured by **airodump.**

```
airodump-ng -c 1 --bssid XX:XX:XX:XX:XX:XX -w out wlan0
```

- -c 1 is the channel to listen on
- –bssid XX:XX:XX:XX:XX:XX limits the packets collected to this one access point
- -w out is the file prefix of the file name to be written
- wlan0 is the interface name

```
aireplay-ng -0 5 -a YY:YY:YY:YY:YY:YY -c YY:YY:YY:YY:YY:YY wlan0
```

- -0 means deauthentication attack
- 5 is number of groups of deauthentication packets to send out
- -a YY:YY:YY:YY:YY:YY is MAC address of the access point
- -c YY:YY:YY:YY:YY:YY is MAC address of the client to be deauthenticated

```
aireplay-ng -3 -b XX:XX:XX:XX:XX:XX -h 00:0F:B5:AB:CB:9D wlan0
```

After sending the five batches of deauthentication packets, we start listening for ARP requests with attack 3. The -h option is mandatory and has to be the MAC address of an associated client.

Airbase-ng is a tool that turns an intruder's machine into a vulnerable connection point for others to connect to. You can use Airbase-ng to pose as a legal access point and conduct man-in-the-middle attacks on computers connected to your network. These attacks are known as Evil Twin Attacks. Basic users have no way of knowing

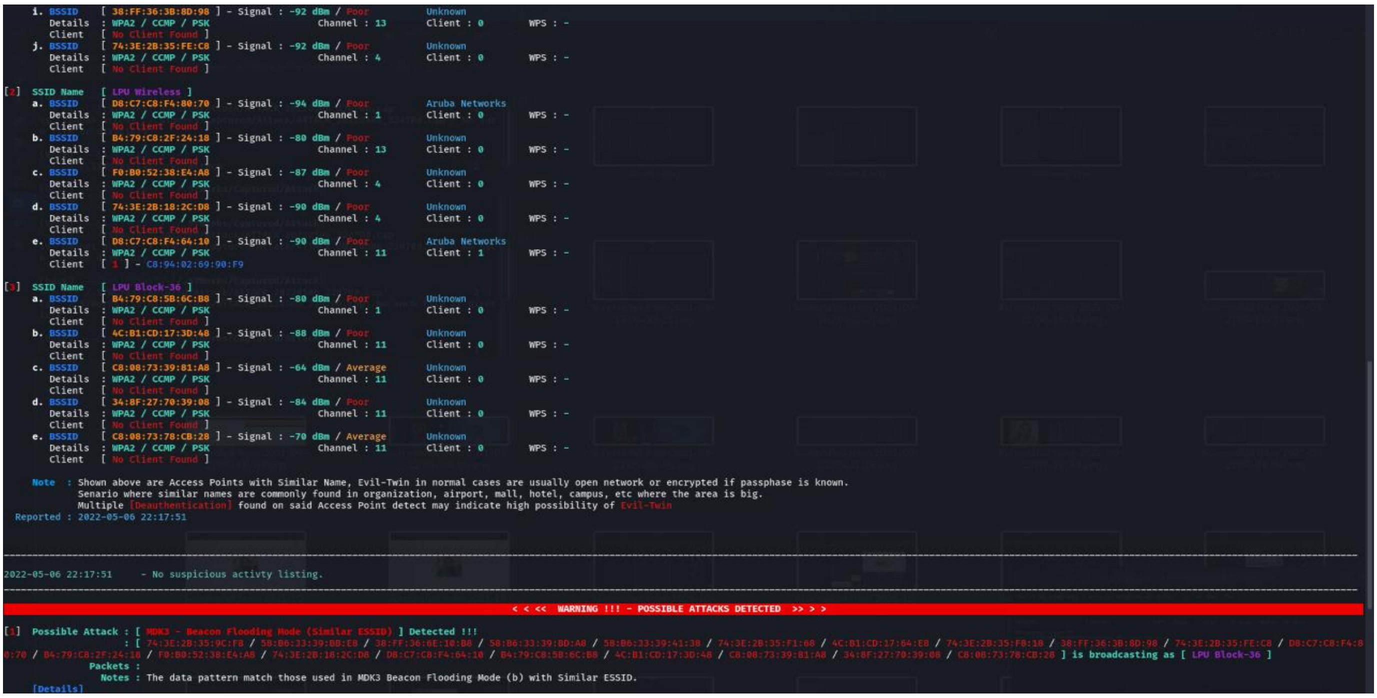
6. TESTING

Testing is a procedure where we test our framework for finding its pros and cons in different aspects of attack for enhancing intrusion detection framework accuracy level before introducing it to real-time environment.

6.1. FUNCTIONALITY TESTING

In functional testing we run our framework for test its capability for detecting various types of attacks in several networks, when we run our framework, it works automatically until we stop it. After running our framework, it is searching for Wi-Fi Access Points and connected clients and the process will automatically refresh in every 30 seconds for detecting updates of newly join Access point and clients. In this mean time, it will also capture various kind of fragment and packets and check them with some rule sets.

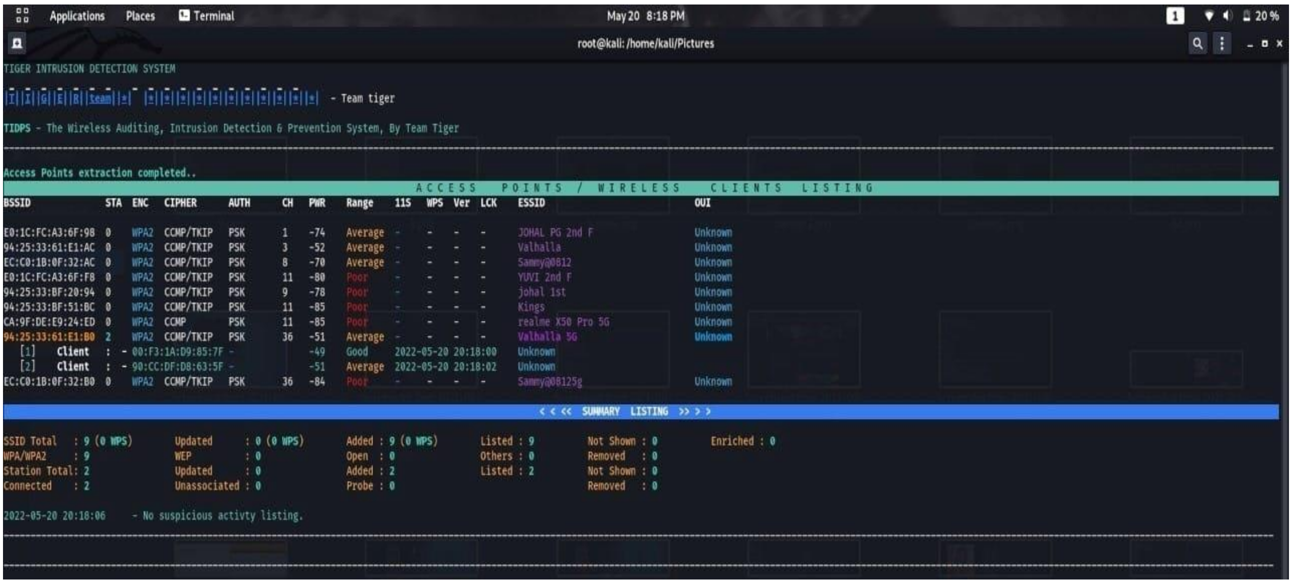
As our framework showing in Figure 4 focus on detecting various kind malicious traffic, malicious fragments and other attacks like rough access point detection, Arp poisoning attack, DE authentication attack, WPS pin brute force, WEP attack, Authentication flooding and evil twin attack. We test our framework with some intentional and unintentional attack.



```
    i. BSSID    [ 38:FF:36:3B:8D:98 ] - Signal : -92 dBm / Poor         Unknown
       Details  : WPA2 / CCMP / PSK               Channel : 13        Client : 0        WPS : -
       Client   [ No Client Found ]
    j. BSSID    [ 74:3E:2B:35:FE:C8 ] - Signal : -92 dBm / Poor         Unknown
       Details  : WPA2 / CCMP / PSK               Channel : 4         Client : 0        WPS : -
       Client   [ No Client Found ]

[2] SSID Name   [ LPU Wireless ]
    a. BSSID    [ D8:C7:C8:F4:80:70 ] - Signal : -94 dBm / Poor         Aruba Networks
       Details  : WPA2 / CCMP / PSK               Channel : 1         Client : 0        WPS : -
       Client   [ No Client Found ]
    b. BSSID    [ B4:79:C8:2F:24:18 ] - Signal : -80 dBm / Poor         Unknown
       Details  : WPA2 / CCMP / PSK               Channel : 13        Client : 0        WPS : -
       Client   [ No Client Found ]
    c. BSSID    [ F0:B0:52:38:E4:A8 ] - Signal : -87 dBm / Poor         Unknown
       Details  : WPA2 / CCMP / PSK               Channel : 4         Client : 0        WPS : -
       Client   [ No Client Found ]
    d. BSSID    [ 74:3E:2B:18:2C:D8 ] - Signal : -90 dBm / Poor         Unknown
       Details  : WPA2 / CCMP / PSK               Channel : 4         Client : 0        WPS : -
       Client   [ No Client Found ]
    e. BSSID    [ D8:C7:C8:F4:64:10 ] - Signal : -90 dBm / Poor         Aruba Networks
       Details  : WPA2 / CCMP / PSK               Channel : 11        Client : 1        WPS : -
       Client   [ 1 ] - C8:94:02:69:90:F9

[3] SSID Name   [ LPU Block-36 ]
    a. BSSID    [ B4:79:C8:5B:6C:B8 ] - Signal : -80 dBm / Poor         Unknown
       Details  : WPA2 / CCMP / PSK               Channel : 1         Client : 0        WPS : -
       Client   [ No Client Found ]
    b. BSSID    [ 4C:B1:CD:17:3D:48 ] - Signal : -88 dBm / Poor         Unknown
       Details  : WPA2 / CCMP / PSK               Channel : 11        Client : 0        WPS : -
       Client   [ No Client Found ]
    c. BSSID    [ C8:08:73:39:81:A8 ] - Signal : -64 dBm / Average      Unknown
       Details  : WPA2 / CCMP / PSK               Channel : 11        Client : 0        WPS : -
       Client   [ No Client Found ]
    d. BSSID    [ 34:8F:27:70:39:08 ] - Signal : -84 dBm / Poor         Unknown
       Details  : WPA2 / CCMP / PSK               Channel : 11        Client : 0        WPS : -
       Client   [ No Client Found ]
    e. BSSID    [ C8:08:73:78:CB:28 ] - Signal : -70 dBm / Average      Unknown
       Details  : WPA2 / CCMP / PSK               Channel : 11        Client : 0        WPS : -
       Client   [ No Client Found ]

    Note  : Shown above are Access Points with Similar Name, Evil-Twin in normal cases are usually open network or encrypted if passphase is known.
            Senario where similar names are commonly found in organization, airport, mall, hotel, campus, etc where the area is big.
            Multiple [Deauthentication] found on said Access Point detect may indicate high possibility of Evil-Twin
  Reported : 2022-05-06 22:17:51


----------------------------------------------------------------------------------------------------------------------------------------

2022-05-06 22:17:51     - No suspicious activty listing.
----------------------------------------------------------------------------------------------------------------------------------------
                                                              < < <<  WARNING !!! - POSSIBLE ATTACKS DETECTED  >> > >

[1] Possible Attack : [ MDK3 - Beacon Flooding Mode (Similar ESSID) ] Detected !!!
                    : [ 74:3E:2B:35:9C:F8 / 58:B6:33:39:BB:E8 / 38:FF:36:6E:10:B8 / 58:B6:33:39:BD:A8 / 58:B6:33:39:41:38 / 74:3E:2B:35:F1:68 / 4C:B1:CD:17:64:E8 / 74:3E:2B:35:F8:18 / 38:FF:36:3B:8D:98 / 74:3E:2B:35:FE:C8 / D8:C7:C8:F4:8
0:70 / B4:79:C8:2F:24:18 / F0:B0:52:38:E4:A8 / 74:3E:2B:18:2C:D8 / D8:C7:C8:F4:64:10 / B4:79:C8:5B:6C:B8 / 4C:B1:CD:17:3D:48 / C8:08:73:39:81:A8 / 34:8F:27:70:39:08 / C8:08:73:78:CB:28 ] is broadcasting as [ LPU Block-36 ]
             Packets :
               Notes : The data pattern match those used in MDK3 Beacon Flooding Mode (b) with Similar ESSID.
    [Details]
```

Figure 4: The picture given above is showing the searching result of wireless Access points and its client.

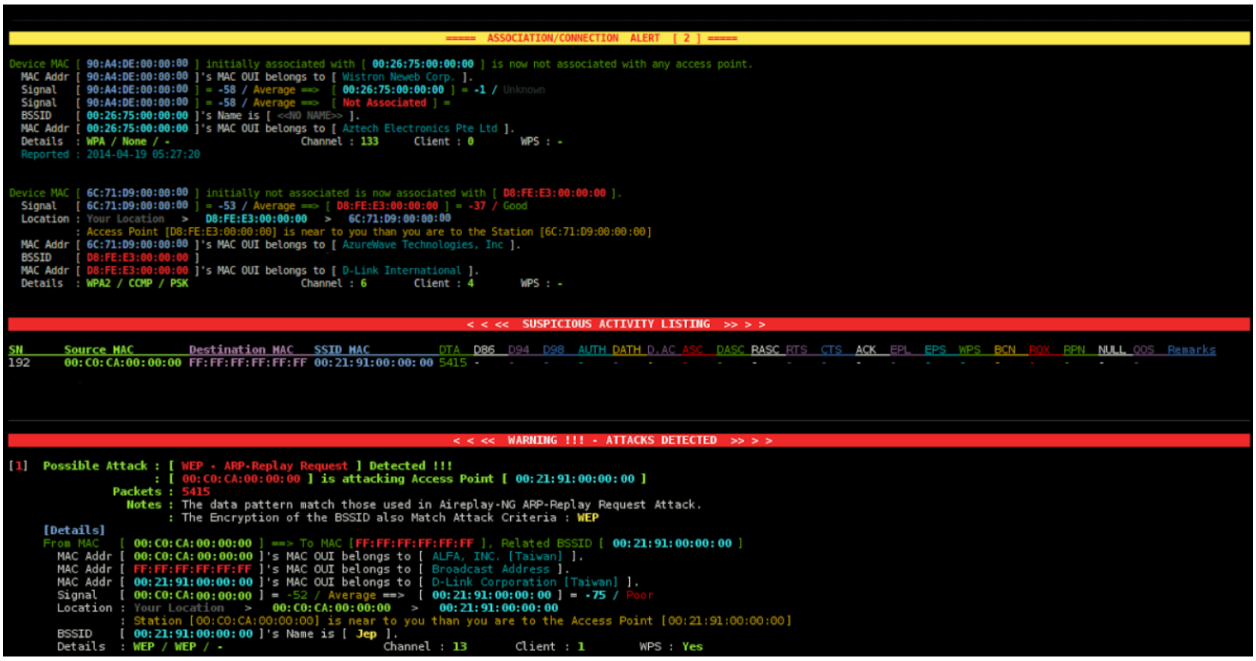
As we can notice in figure 5 the place of attack is a public network of one university, and someone is trying to perform Evil twin attack over this network and our framework detected this attack perfectly.



```
TIGER INTRUSION DETECTION SYSTEM

|T||I||G||E||R||team||*| |*||*||*||*||*||*||*||*||*||*||*|  - Team tiger

TIDPS - The Wireless Auditing, Intrusion Detection & Prevention System, By Team Tiger
----------------------------------------------------------------------------------------------------------------------------------------

Access Points extraction completed..
                                        A C C E S S   P O I N T S  /  W I R E L E S S   C L I E N T S   L I S T I N G
BSSID              STA  ENC   CIPHER     AUTH    CH   PWR   Range    11S   WPS  Ver  LCK   ESSID                  OUI

E0:1C:FC:A3:6F:98  0    WPA2  CCMP/TKIP  PSK     1    -74   Average  -     -    -    -     JOHAL PG 2nd F         Unknown
94:25:33:61:E1:AC  0    WPA2  CCMP/TKIP  PSK     3    -52   Average  -     -    -    -     Valhalla               Unknown
EC:C0:1B:0F:32:AC  0    WPA2  CCMP/TKIP  PSK     8    -70   Average  -     -    -    -     Sammy@0812             Unknown
E0:1C:FC:A3:6F:F8  0    WPA2  CCMP/TKIP  PSK     11   -80   Poor     -     -    -    -     YUVI 2nd F             Unknown
94:25:33:BF:20:94  0    WPA2  CCMP/TKIP  PSK     9    -78   Poor     -     -    -    -     johal 1st              Unknown
94:25:33:BF:51:BC  0    WPA2  CCMP/TKIP  PSK     11   -85   Poor     -     -    -    -     Kings                  Unknown
CA:9F:DE:E9:24:ED  0    WPA2  CCMP       PSK     11   -85   Poor     -     -    -    -     realme X50 Pro 5G      Unknown
94:25:33:61:E1:B0  2    WPA2  CCMP/TKIP  PSK     36   -51   Average  -     -    -    -     Valhalla 5G            Unknown
   [1]    Client   :  - 00:F3:1A:D9:85:7F -         -49   Good     2022-05-20 20:18:00   Unknown
   [2]    Client   :  - 90:CC:DF:D8:63:5F -         -51   Average  2022-05-20 20:18:02   Unknown
EC:C0:1B:0F:32:B0  0    WPA2  CCMP/TKIP  PSK     36   -84   Poor     -     -    -    -     Sammy@08125g           Unknown

                                                                          < < <<  SUMMARY  LISTING  >> > >

SSID Total    : 9 (0 WPS)     Updated      : 0 (0 WPS)     Added : 9 (0 WPS)     Listed : 9     Not Shown : 0     Enriched : 0
WPA/WPA2      : 9             WEP          : 0             Open  : 0             Others : 0     Removed   : 0
Station Total: 2              Updated      : 0             Added : 2             Listed : 2     Not Shown : 0
Connected     : 2             Unassociated : 0             Probe : 0                            Removed   : 0

2022-05-20 20:18:06     - No suspicious activty listing.
----------------------------------------------------------------------------------------------------------------------------------------

----------------------------------------------------------------------------------------------------------------------------------------
```

Figure 5: The picture given above is a perfect example of detecting unintentional attack

As we can notice in figure 6 the place of attack is experimental network and attack is done intentionally. The network is created by using Wi-Fi router and with the help of two devices one is attacker, and one is victim device and tool of attack is being used Aircrack-ng.



```
                              =====  ASSOCIATION/CONNECTION  ALERT  [ 2 ] =====

Device MAC [ 90:A4:DE:00:00:00 ] initially associated with [ 00:26:75:00:00:00 ] is now not associated with any access point.
  MAC Addr [ 90:A4:DE:00:00:00 ]'s MAC OUI belongs to [ Wistron Neweb Corp. ].
  Signal   [ 90:A4:DE:00:00:00 ] = -58 / Average ==>  [ 00:26:75:00:00:00 ] = -1 / Unknown
  Signal   [ 90:A4:DE:00:00:00 ] = -58 / Average ==>  [ Not Associated ] =
  BSSID    [ 00:26:75:00:00:00 ]'s Name is [ <<NO NAME>> ].
  MAC Addr [ 00:26:75:00:00:00 ]'s MAC OUI belongs to [ Aztech Electronics Pte Ltd ].
  Details  : WPA / None / -                   Channel : 133      Client : 0        WPS : -
  Reported : 2014-04-19 05:27:20


Device MAC [ 6C:71:D9:00:00:00 ] initially not associated is now associated with [ D8:FE:E3:00:00:00 ].
  Signal   [ 6C:71:D9:00:00:00 ] = -53 / Average ==> [ D8:FE:E3:00:00:00 ] = -37 / Good
  Location : Your Location   >   D8:FE:E3:00:00:00   >   6C:71:D9:00:00:00
           : Access Point [D8:FE:E3:00:00:00] is near to you than you are to the Station [6C:71:D9:00:00:00]
  MAC Addr [ 6C:71:D9:00:00:00 ]'s MAC OUI belongs to [ AzureWave Technologies, Inc ].
  BSSID    [ D8:FE:E3:00:00:00 ]
  MAC Addr [ D8:FE:E3:00:00:00 ]'s MAC OUI belongs to [ D-Link International ].
  Details  : WPA2 / CCMP / PSK                Channel : 6        Client : 4        WPS : -

                              < < <<  SUSPICIOUS ACTIVITY LISTING  >> > >

SN      Source MAC          Destination MAC    SSID MAC            DTA  D86  D94  D98  AUTH DATH D.AC ASC  DASC RASC RTS  CTS  ACK  EPL  EPS  WPS  BCN  RQX  RPN  NULL QOS  Remarks
192     00:C0:CA:00:00:00   FF:FF:FF:FF:FF:FF  00:21:91:00:00:00   5415 -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -


                              < < <<  WARNING !!! - ATTACKS DETECTED  >> > >

[1]  Possible Attack : [ WEP - ARP-Replay Request ] Detected !!!
                     : [ 00:C0:CA:00:00:00 ] is attacking Access Point [ 00:21:91:00:00:00 ]
               Packets : 5415
                 Notes : The data pattern match those used in Aireplay-NG ARP-Replay Request Attack.
                       : The Encryption of the BSSID also Match Attack Criteria : WEP
     [Details]
     From MAC   [ 00:C0:CA:00:00:00 ] ==> To MAC [FF:FF:FF:FF:FF:FF ], Related BSSID [ 00:21:91:00:00:00 ]
       MAC Addr [ 00:C0:CA:00:00:00 ]'s MAC OUI belongs to [ ALFA, INC. [Taiwan] ].
       MAC Addr [ FF:FF:FF:FF:FF:FF ]'s MAC OUI belongs to [ Broadcast Address ].
       MAC Addr [ 00:21:91:00:00:00 ]'s MAC OUI belongs to [ D-Link Corporation [Taiwan] ].
       Signal   [ 00:C0:CA:00:00:00 ] = -52 / Average ==>  [ 00:21:91:00:00:00 ] = -75 / Poor
       Location : Your Location   >   00:C0:CA:00:00:00   >   00:21:91:00:00:00
                : Station [00:C0:CA:00:00:00] is near to you than you are to the Access Point [00:21:91:00:00:00]
       BSSID    [ 00:21:91:00:00:00 ]'s Name is [ Jep ].
       Details  : WEP / WEP / -                      Channel : 13       Client : 1        WPS : Yes
```

Figure 6: The picture given above is a perfect example of detecting attack intentionally

6.2. User Interface

We design our framework is too much user friendly that any non-technical person also feels very comfortable with it. After running our framework in Linux environment with in second it will show you all available access point, bssid, ssid and connected client in the below int will show you warning box either attack is happening or not. Main functionality interface:

1. Tiger intrusion detection system configuration.

2. Tiger intrusion prevention system.

3. History logs.

4.Operation option

5.Look up/mac Detail

6.Monitor Mac Adrr / Names.

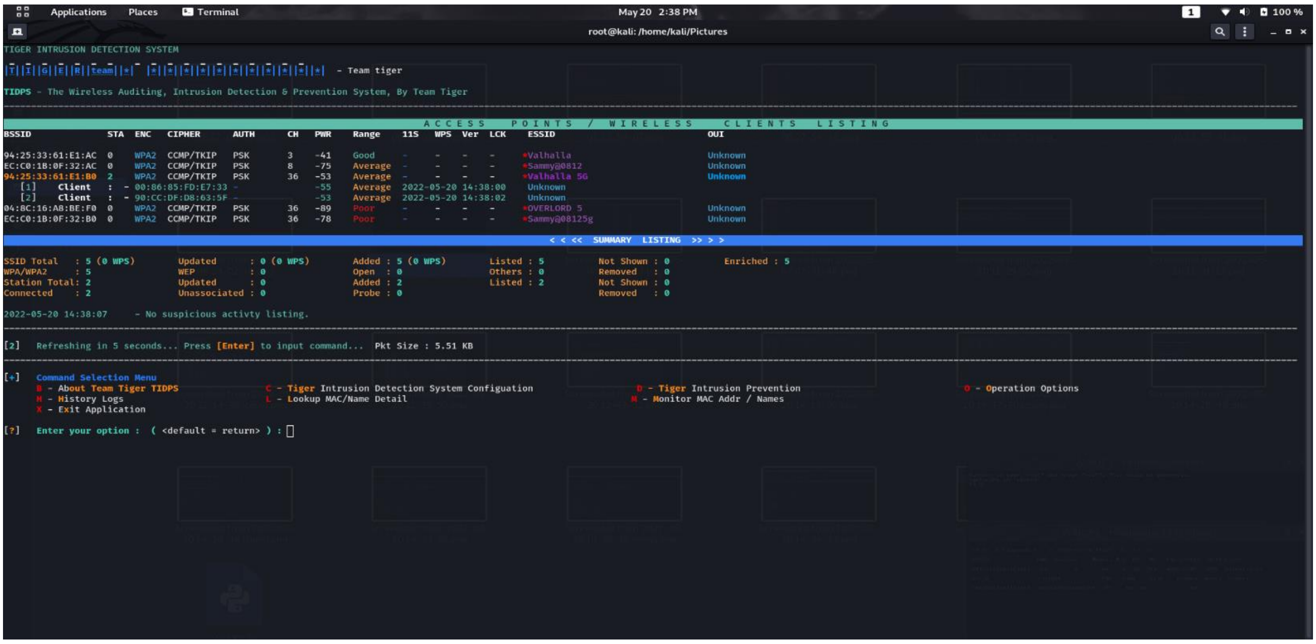
And all red color alphabet’s are the option to choose functionality.

Tiger Intrusion Detection System configuration

This configuration option in Figure 7 contains some sub-options by which the user can configure the framework as per their use case.

- Sensitivity of IDS

- Refreshing rate of information
- Time before removing inactive AP/Station
- Hide inactive Access Point/Station
- Beep if alert found
- Save PCap when Attack detected
- Save PCap when Monitored MAC/Name seen
- Whitelist Setting (Bypass alert for MAC/Name

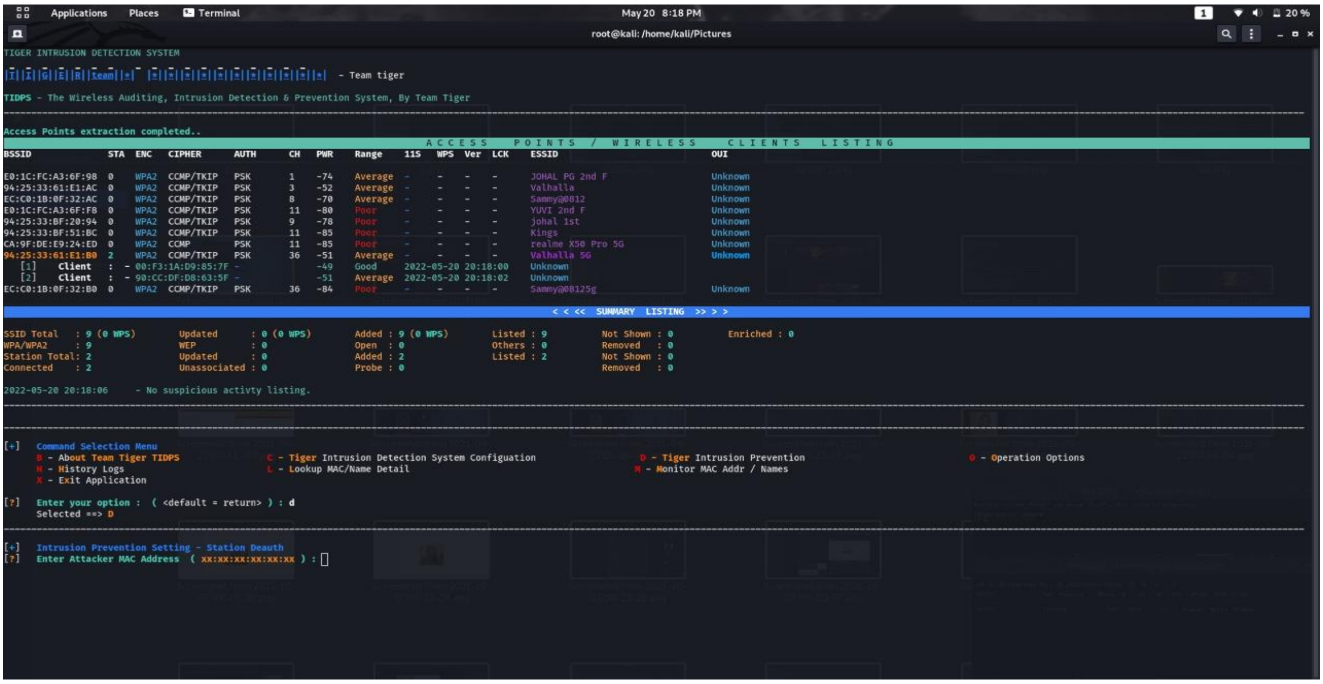


```
TIGER INTRUSION DETECTION SYSTEM

|T||I||G||E||R||team||*|  |*||*||*||*||*||*||*||*||*||*||*|  - Team tiger

TIDPS - The Wireless Auditing, Intrusion Detection & Prevention System, By Team Tiger
---------------------------------------------------------------------------------------------------------------------------------------
                                                     A C C E S S   P O I N T S  /  W I R E L E S S   C L I E N T S   L I S T I N G
BSSID              STA  ENC   CIPHER     AUTH     CH   PWR    Range    11S    WPS  Ver  LCK    ESSID                      OUI

94:25:33:61:E1:AC  0    WPA2  CCMP/TKIP  PSK      3    -41    Good     -      -    -    -      *Valhalla                  Unknown
EC:C0:1B:0F:32:AC  0    WPA2  CCMP/TKIP  PSK      8    -75    Average  -      -    -    -      *Sammy@0812                Unknown
94:25:33:61:E1:B0  2    WPA2  CCMP/TKIP  PSK      36   -53    Average  -      -    -    -      *Valhalla 5G               Unknown
   [1]     Client  :  - 00:86:85:FD:E7:33 -            -55    Average  2022-05-20 14:38:00     Unknown
   [2]     Client  :  - 90:CC:DF:D8:63:5F -            -53    Average  2022-05-20 14:38:02     Unknown
04:8C:16:A8:BE:F0  0    WPA2  CCMP/TKIP  PSK      36   -89    Poor     -      -    -    -      *OVERLORD 5                Unknown
EC:C0:1B:0F:32:B0  0    WPA2  CCMP/TKIP  PSK      36   -78    Poor     -      -    -    -      *Sammy@08125g              Unknown

                                                                   < < <<  SUMMARY  LISTING  >> > >

SSID Total    : 5 (0 WPS)      Updated       : 0 (0 WPS)      Added : 5 (0 WPS)      Listed : 5        Not Shown : 0       Enriched : 5
WPA/WPA2      : 5              WEP           : 0              Open  : 0              Others : 0        Removed   : 0
Station Total: 2               Updated       : 0              Added : 2              Listed : 2        Not Shown : 0
Connected     : 2              Unassociated : 0               Probe : 0                                Removed   : 0

2022-05-20 14:38:07     - No suspicious activty listing.
---------------------------------------------------------------------------------------------------------------------------------------
[2]   Refreshing in 5 seconds... Press [Enter] to input command...  Pkt Size : 5.51 KB
---------------------------------------------------------------------------------------------------------------------------------------
[+]   Command Selection Menu
      B - About Team Tiger TIDPS                C - Tiger Intrusion Detection System Configuation         D - Tiger Intrusion Prevention          O - Operation Options
      H - History Logs                          L - Lookup MAC/Name Detail                               M - Monitor MAC Addr / Names
      X - Exit Application

[?]   Enter your option :  ( <default = return> ) : □
```

Figure 7: The picture given above is the user interface and functionality of our framework

Tiger intrusion prevention system

We use this function shown in Figure 8 for malicious device. We got the malicious device list from our intrusion detection method.

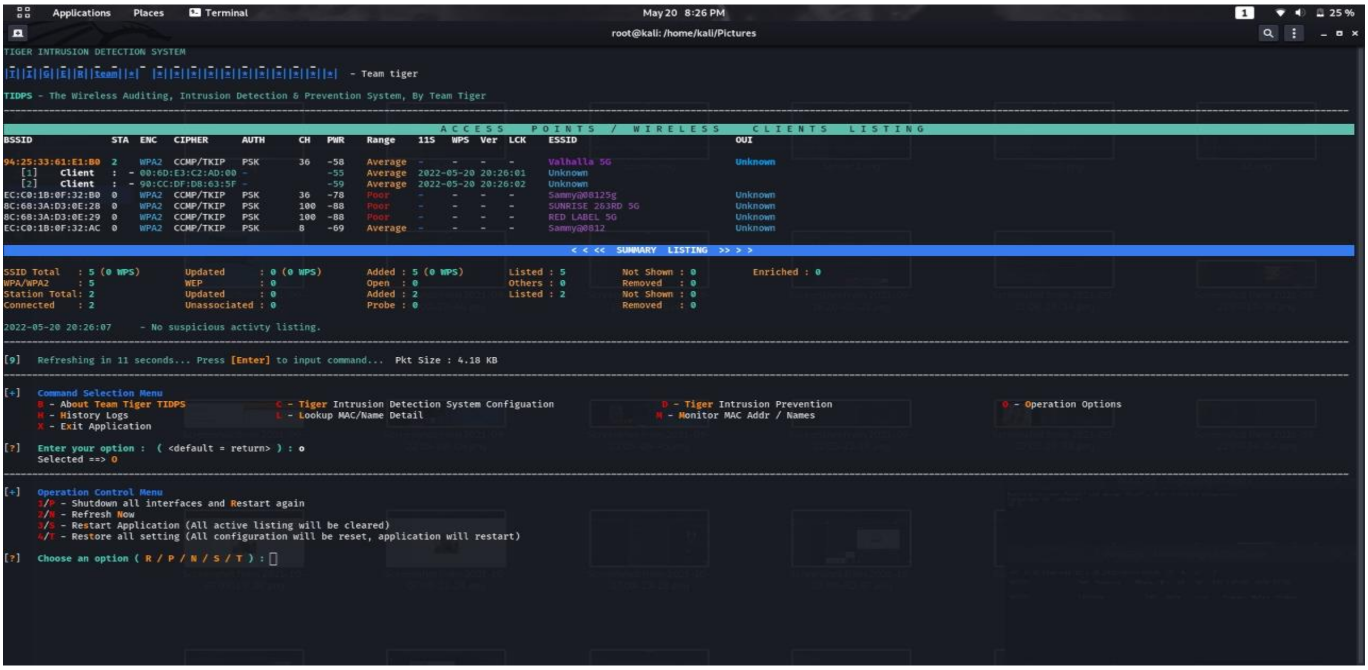


```
TIGER INTRUSION DETECTION SYSTEM

|T||I||G||E||R||team||*|  |*||*||*||*||*||*||*||*||*||*||*|  - Team tiger

TIDPS - The Wireless Auditing, Intrusion Detection & Prevention System, By Team Tiger
---------------------------------------------------------------------------------------------------------------------

Access Points extraction completed..
                                                           A C C E S S    P O I N T S  /  W I R E L E S S    C L I E N T S    L I S T I N G
BSSID              STA  ENC   CIPHER     AUTH     CH   PWR    Range    11S    WPS  Ver  LCK    ESSID                  OUI

E0:1C:FC:A3:6F:98  0    WPA2  CCMP/TKIP  PSK      1    -74    Average  -      -    -    -      JOHAL PG 2nd F         Unknown
94:25:33:61:E1:AC  0    WPA2  CCMP/TKIP  PSK      3    -52    Average  -      -    -    -      Valhalla               Unknown
EC:C0:1B:0F:32:AC  0    WPA2  CCMP/TKIP  PSK      8    -70    Average  -      -    -    -      Sammy@0812             Unknown
E0:1C:FC:A3:6F:F8  0    WPA2  CCMP/TKIP  PSK      11   -80    Poor     -      -    -    -      YUVI 2nd F             Unknown
94:25:33:BF:20:94  0    WPA2  CCMP/TKIP  PSK      9    -78    Poor     -      -    -    -      johal 1st              Unknown
94:25:33:BF:51:BC  0    WPA2  CCMP/TKIP  PSK      11   -85    Poor     -      -    -    -      Kings                  Unknown
CA:9F:DE:E9:24:ED  0    WPA2  CCMP       PSK      11   -85    Poor     -      -    -    -      realme X50 Pro 5G      Unknown
94:25:33:61:E1:B0  2    WPA2  CCMP/TKIP  PSK      36   -51    Average  -      -    -    -      Valhalla 5G            Unknown
   [1]   Client   :  - 00:F3:1A:D9:85:7F -         -49    Good     2022-05-20 20:18:00    Unknown
   [2]   Client   :  - 90:CC:DF:D8:63:5F -         -51    Average  2022-05-20 20:18:02    Unknown
EC:C0:1B:0F:32:B0  0    WPA2  CCMP/TKIP  PSK      36   -84    Poor     -      -    -    -      Sammy@08125g           Unknown
                                                              < < <<  SUMMARY  LISTING  >> > >
SSID Total    : 9 (0 WPS)      Updated       : 0 (0 WPS)      Added : 9 (0 WPS)      Listed : 9      Not Shown : 0      Enriched : 0
WPA/WPA2      : 9              WEP           : 0              Open  : 0              Others : 0      Removed   : 0
Station Total: 2               Updated       : 0              Added : 2              Listed : 2      Not Shown : 0
Connected     : 2              Unassociated : 0               Probe : 0                              Removed   : 0

2022-05-20 20:18:06     - No suspicious activty listing.
---------------------------------------------------------------------------------------------------------------------

---------------------------------------------------------------------------------------------------------------------

[+]    Command Selection Menu
       B - About Team Tiger TIDPS         C - Tiger Intrusion Detection System Configuation        D - Tiger Intrusion Prevention        O - Operation Options
       H - History Logs                   L - Lookup MAC/Name Detail                               M - Monitor MAC Addr / Names
       X - Exit Application

[?]    Enter your option :  ( <default = return> ) : d
       Selected ==> D
---------------------------------------------------------------------------------------------------------------------

[+]    Intrusion Prevention Setting - Station Deauth
[?]    Enter Attacker MAC Address  ( xx:xx:xx:xx:xx:xx ) : 
```

Figure 8: Tiger prevention system function

Operation option

By using operation options shown in Figure 9, the user can shut down all the interfaces so that he can restart them again newly. He can refresh the screen and restore all settings with the help of the operation option’s method.

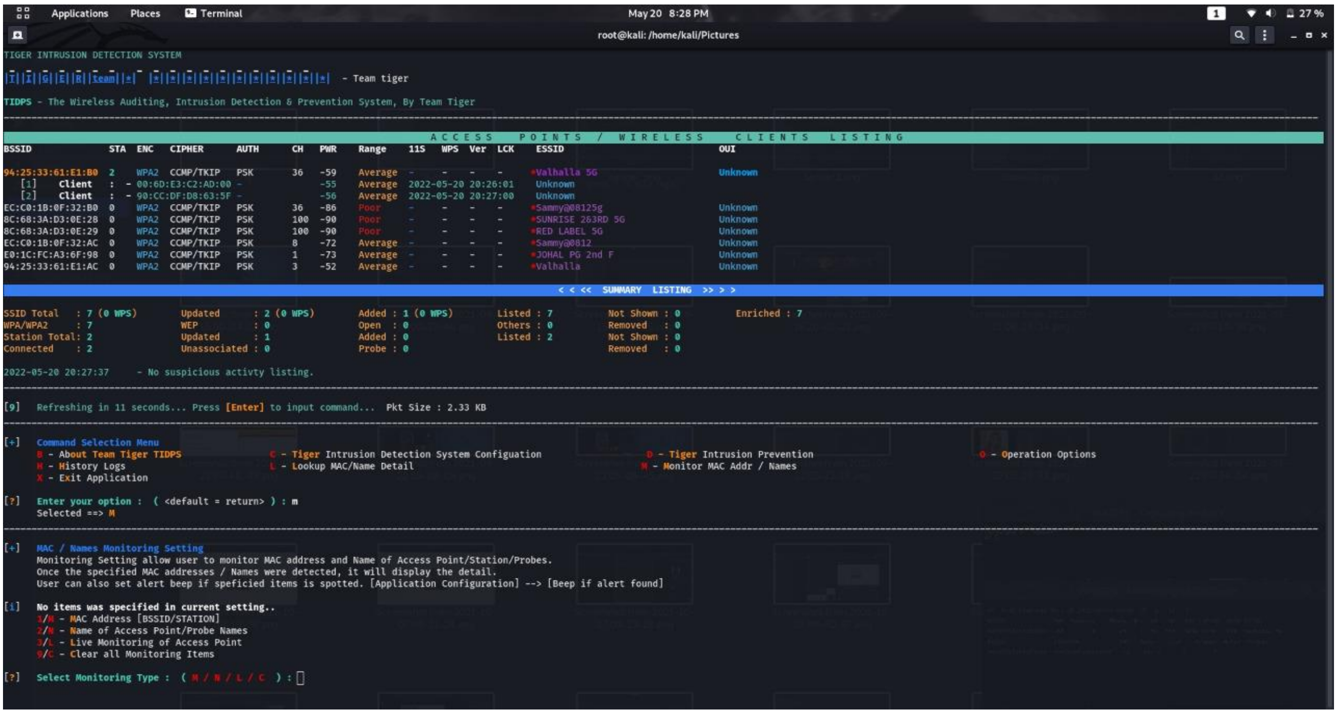


```
TIGER INTRUSION DETECTION SYSTEM

|T||I||G||E||R||team||*|  |*||*||*||*||*||*||*||*||*||*||*|  - Team tiger

TIDPS - The Wireless Auditing, Intrusion Detection & Prevention System, By Team Tiger
---------------------------------------------------------------------------------------------------------------------
                                                           A C C E S S    P O I N T S  /  W I R E L E S S    C L I E N T S    L I S T I N G
BSSID              STA  ENC   CIPHER     AUTH     CH   PWR    Range    11S    WPS  Ver  LCK    ESSID                  OUI

94:25:33:61:E1:B0  2    WPA2  CCMP/TKIP  PSK      36   -58    Average  -      -    -    -      Valhalla 5G            Unknown
   [1]   Client   :  - 00:6D:E3:C2:AD:00 -         -55    Average  2022-05-20 20:26:01    Unknown
   [2]   Client   :  - 90:CC:DF:D8:63:5F -         -59    Average  2022-05-20 20:26:02    Unknown
EC:C0:1B:0F:32:B0  0    WPA2  CCMP/TKIP  PSK      36   -78    Poor     -      -    -    -      Sammy@08125g           Unknown
8C:68:3A:D3:0E:28  0    WPA2  CCMP/TKIP  PSK      100  -88    Poor     -      -    -    -      SUNRISE 263RD 5G       Unknown
8C:68:3A:D3:0E:29  0    WPA2  CCMP/TKIP  PSK      100  -88    Poor     -      -    -    -      RED LABEL 5G           Unknown
EC:C0:1B:0F:32:AC  0    WPA2  CCMP/TKIP  PSK      8    -69    Average  -      -    -    -      Sammy@0812             Unknown
                                                              < < <<  SUMMARY  LISTING  >> > >
SSID Total    : 5 (0 WPS)      Updated       : 0 (0 WPS)      Added : 5 (0 WPS)      Listed : 5      Not Shown : 0      Enriched : 0
WPA/WPA2      : 5              WEP           : 0              Open  : 0              Others : 0      Removed   : 0
Station Total: 2               Updated       : 0              Added : 2              Listed : 2      Not Shown : 0
Connected     : 2              Unassociated : 0               Probe : 0                              Removed   : 0

2022-05-20 20:26:07     - No suspicious activty listing.
---------------------------------------------------------------------------------------------------------------------

[9]    Refreshing in 11 seconds... Press [Enter] to input command...   Pkt Size : 4.18 KB
---------------------------------------------------------------------------------------------------------------------

[+]    Command Selection Menu
       B - About Team Tiger TIDPS         C - Tiger Intrusion Detection System Configuation        D - Tiger Intrusion Prevention        O - Operation Options
       H - History Logs                   L - Lookup MAC/Name Detail                               M - Monitor MAC Addr / Names
       X - Exit Application

[?]    Enter your option :  ( <default = return> ) : o
       Selected ==> O
---------------------------------------------------------------------------------------------------------------------

[+]    Operation Control Menu
       1/P - Shutdown all interfaces and Restart again
       2/N - Refresh Now
       3/S - Restart Application (All active listing will be cleared)
       4/T - Restore all setting (All configuration will be reset, application will restart)

[?]    Choose an option ( R / P / N / S / T ) : 
```

Figure 9: Operation Option

Monitor Mac Adrr / Names

By using this function shown in Figure 10 user can save the mac address of malicious devices and BSSID+SSID of malicious network. If malicious device or network spotted it will warn user by beep sound and also generate the warning message on display.



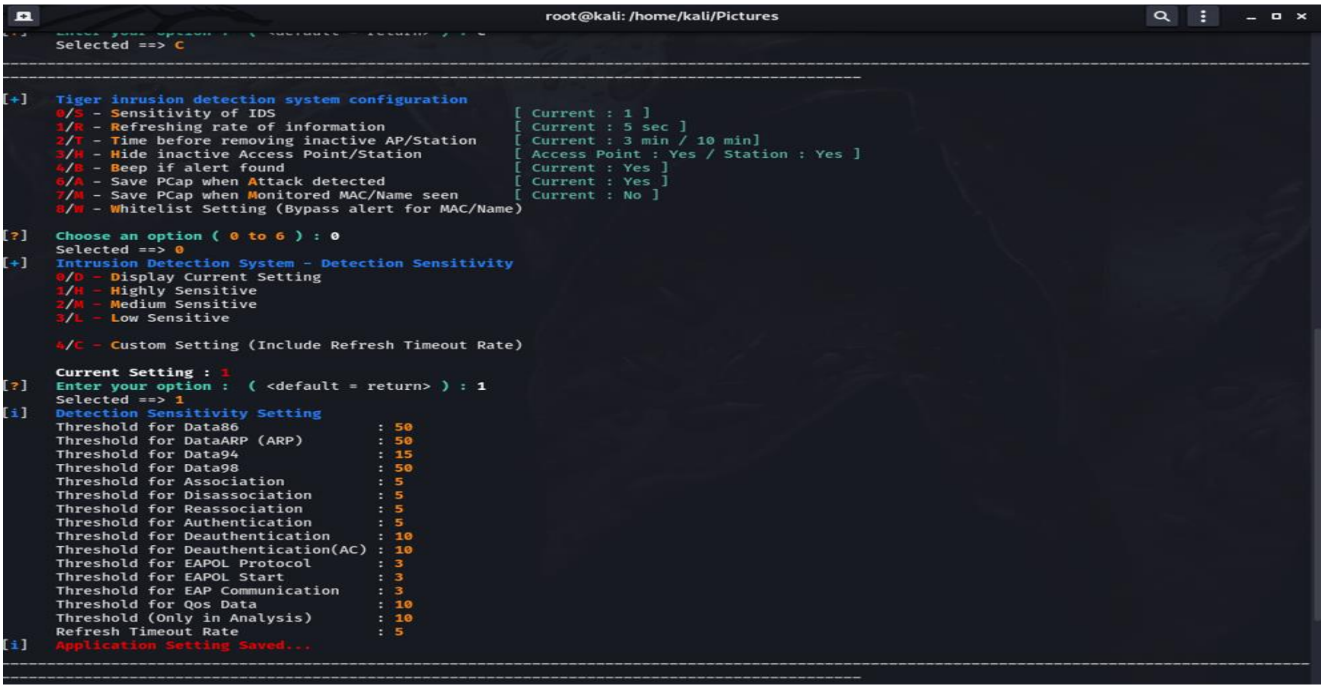
```
TIGER INTRUSION DETECTION SYSTEM

|T||I||G||E||R||team||*|  |*||*||*||*||*||*||*||*||*||*||*|  - Team tiger

TIDPS - The Wireless Auditing, Intrusion Detection & Prevention System, By Team Tiger
------------------------------------------------------------------------------------------------------------------------
                                                     A C C E S S   P O I N T S  /  W I R E L E S S   C L I E N T S   L I S T I N G
BSSID              STA  ENC   CIPHER     AUTH      CH   PWR   Range    11S   WPS  Ver  LCK    ESSID                 OUI

94:25:33:61:E1:B0  2    WPA2  CCMP/TKIP  PSK       36   -59   Average  -     -    -    -      *Valhalla 5G          Unknown
   [1]    Client   :  - 00:6D:E3:C2:AD:00 -         -55   Average  2022-05-20 20:26:01   Unknown
   [2]    Client   :  - 90:CC:DF:D8:63:5F -         -56   Average  2022-05-20 20:27:00   Unknown
EC:C0:1B:0F:32:B0  0    WPA2  CCMP/TKIP  PSK       36   -86   Poor     -     -    -    -      *Sammy@08125g         Unknown
8C:68:3A:D3:0E:28  0    WPA2  CCMP/TKIP  PSK       100  -90   Poor     -     -    -    -      *SUNRISE 263RD 5G     Unknown
8C:68:3A:D3:0E:29  0    WPA2  CCMP/TKIP  PSK       100  -90   Poor     -     -    -    -      *RED LABEL 5G         Unknown
EC:C0:1B:0F:32:AC  0    WPA2  CCMP/TKIP  PSK       8    -72   Average  -     -    -    -      *Sammy@0812           Unknown
E0:1C:FC:A3:6F:98  0    WPA2  CCMP/TKIP  PSK       1    -73   Average  -     -    -    -      *JOHAL PG 2nd F       Unknown
94:25:33:61:E1:AC  0    WPA2  CCMP/TKIP  PSK       3    -52   Average  -     -    -    -      *Valhalla             Unknown

                                                                 < < <<  SUMMARY  LISTING  >> > >

SSID Total    : 7 (0 WPS)      Updated       : 2 (0 WPS)      Added : 1 (0 WPS)      Listed : 7      Not Shown : 0      Enriched : 7
WPA/WPA2      : 7              WEP           : 0              Open  : 0              Others : 0      Removed   : 0
Station Total: 2               Updated       : 1              Added : 0              Listed : 2      Not Shown : 0
Connected     : 2              Unassociated : 0               Probe : 0                              Removed   : 0

2022-05-20 20:27:37     - No suspicious activty listing.
------------------------------------------------------------------------------------------------------------------------

[9]   Refreshing in 11 seconds... Press [Enter] to input command...  Pkt Size : 2.33 KB
------------------------------------------------------------------------------------------------------------------------

[+]   Command Selection Menu
      B - About Team Tiger TIDPS          C - Tiger Intrusion Detection System Configuation          D - Tiger Intrusion Prevention          O - Operation Options
      H - History Logs                    L - Lookup MAC/Name Detail                                 M - Monitor MAC Addr / Names
      X - Exit Application

[?]   Enter your option :  ( <default = return> ) : m
      Selected ==> M
------------------------------------------------------------------------------------------------------------------------

[+]   MAC / Names Monitoring Setting
      Monitoring Setting allow user to monitor MAC address and Name of Access Point/Station/Probes.
      Once the specified MAC addresses / Names were detected, it will display the detail.
      User can also set alert beep if speficied items is spotted. [Application Configuration] --> [Beep if alert found]

[i]   No items was specified in current setting..
      1/M - MAC Address [BSSID/STATION]
      2/N - Name of Access Point/Probe Names
      3/L - Live Monitoring of Access Point
      9/C - Clear all Monitoring Items

[?]   Select Monitoring Type :  ( M / N / L / C  ) : ▯
```

Figure 10: Monitor Mac Adrr / Names.

6.3. Flexibility of our Framework

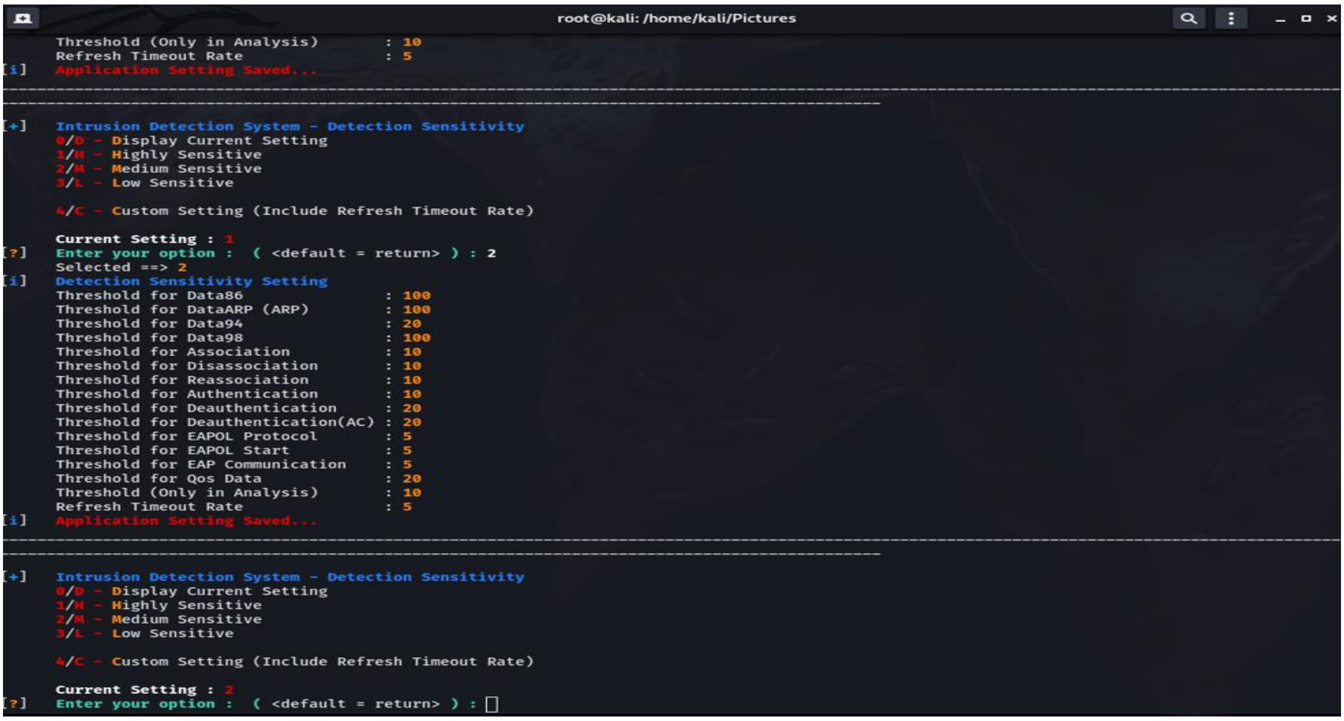
Our framework gives user to modify sensitivity as per requirement different devices has different number threshold values as an example in small network or website it is easy to do successfully DDoS attack on the contrary of companies like Google can handle this more than normally. It is easily understandable that different enterprise level network has different level of threshold, so we create four modes for our user.

1. First one is high level sensitivity shown in Figure 11.
2. Second one mid-level sensitivity shown in Figure 12.
3. Third one low level sensitivity shown in Figure 13.
4. Final one customized security shown in Figure 14.



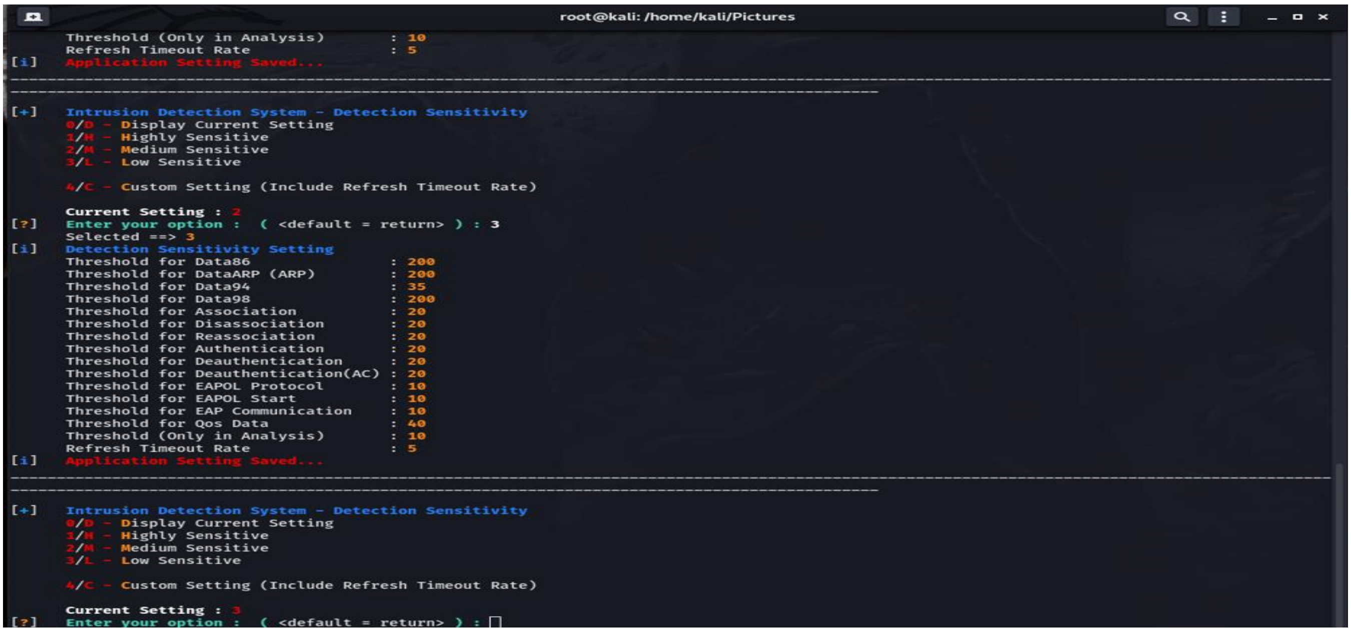
```
root@kali: /home/kali/Pictures
        Selected ==> C
------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------

[+]     Tiger inrusion detection system configuration
        0/S - Sensitivity of IDS                         [ Current : 1 ]
        1/R - Refreshing rate of information             [ Current : 5 sec ]
        2/T - Time before removing inactive AP/Station   [ Current : 3 min / 10 min]
        3/H - Hide inactive Access Point/Station         [ Access Point : Yes / Station : Yes ]
        4/B - Beep if alert found                        [ Current : Yes ]
        6/A - Save PCap when Attack detected             [ Current : Yes ]
        7/M - Save PCap when Monitored MAC/Name seen     [ Current : No ]
        8/W - Whitelist Setting (Bypass alert for MAC/Name)

[?]     Choose an option ( 0 to 6 ) : 0
        Selected ==> 0
[+]     Intrusion Detection System - Detection Sensitivity
        0/D - Display Current Setting
        1/H - Highly Sensitive
        2/M - Medium Sensitive
        3/L - Low Sensitive

        4/C - Custom Setting (Include Refresh Timeout Rate)

        Current Setting : 1
[?]     Enter your option :  ( <default = return> ) : 1
        Selected ==> 1
[i]     Detection Sensitivity Setting
        Threshold for Data86                 : 50
        Threshold for DataARP (ARP)          : 50
        Threshold for Data94                 : 15
        Threshold for Data98                 : 50
        Threshold for Association            : 5
        Threshold for Disassociation         : 5
        Threshold for Reassociation          : 5
        Threshold for Authentication         : 5
        Threshold for Deauthentication       : 10
        Threshold for Deauthentication(AC)   : 10
        Threshold for EAPOL Protocol         : 3
        Threshold for EAPOL Start            : 3
        Threshold for EAP Communication      : 3
        Threshold for Qos Data               : 10
        Threshold (Only in Analysis)         : 10
        Refresh Timeout Rate                 : 5
[i]     Application Setting Saved...
------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------
```

Figure 11: Configuring sensitivity at high



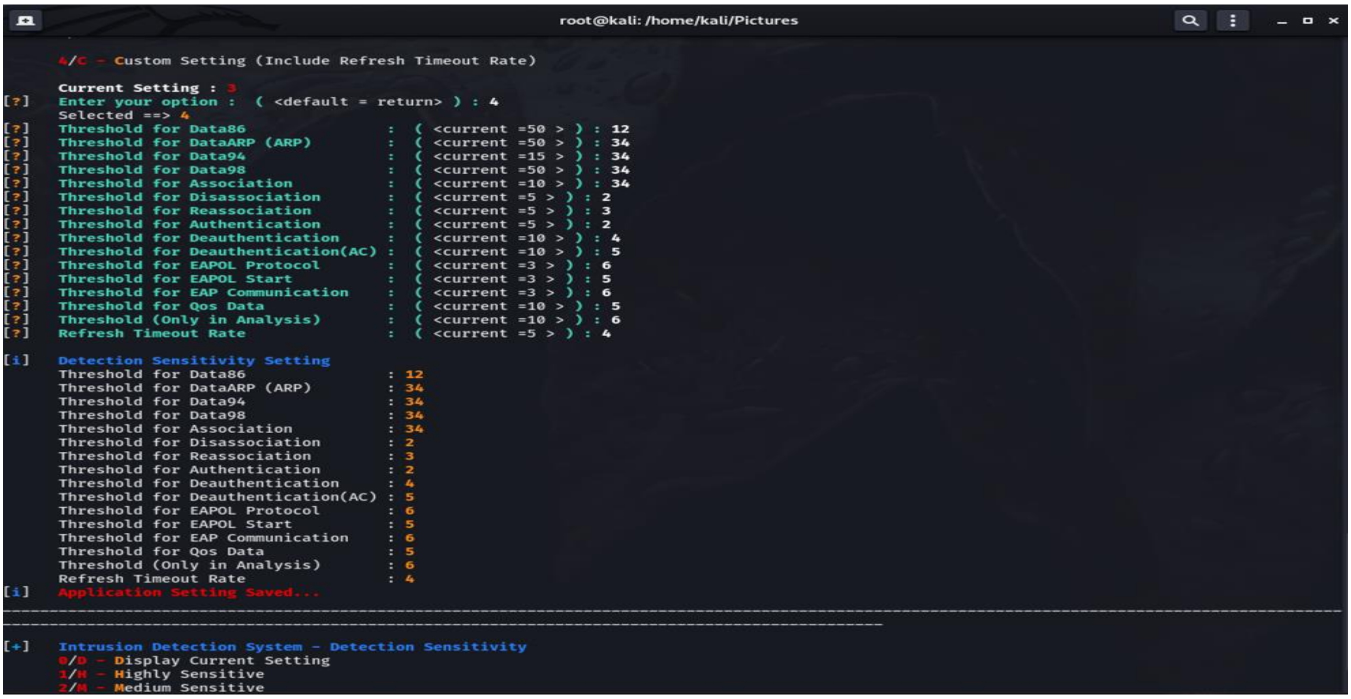
```
root@kali: /home/kali/Pictures
        Threshold (Only in Analysis)         : 10
        Refresh Timeout Rate                 : 5
[i]     Application Setting Saved...
------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------

[+]     Intrusion Detection System - Detection Sensitivity
        0/D - Display Current Setting
        1/H - Highly Sensitive
        2/M - Medium Sensitive
        3/L - Low Sensitive

        4/C - Custom Setting (Include Refresh Timeout Rate)

        Current Setting : 1
[?]     Enter your option :  ( <default = return> ) : 2
        Selected ==> 2
[i]     Detection Sensitivity Setting
        Threshold for Data86                 : 100
        Threshold for DataARP (ARP)          : 100
        Threshold for Data94                 : 20
        Threshold for Data98                 : 100
        Threshold for Association            : 10
        Threshold for Disassociation         : 10
        Threshold for Reassociation          : 10
        Threshold for Authentication         : 10
        Threshold for Deauthentication       : 20
        Threshold for Deauthentication(AC)   : 20
        Threshold for EAPOL Protocol         : 5
        Threshold for EAPOL Start            : 5
        Threshold for EAP Communication      : 5
        Threshold for Qos Data               : 20
        Threshold (Only in Analysis)         : 10
        Refresh Timeout Rate                 : 5
[i]     Application Setting Saved...
------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------

[+]     Intrusion Detection System - Detection Sensitivity
        0/D - Display Current Setting
        1/H - Highly Sensitive
        2/M - Medium Sensitive
        3/L - Low Sensitive

        4/C - Custom Setting (Include Refresh Timeout Rate)

        Current Setting : 2
[?]     Enter your option :  ( <default = return> ) : 
```

Figure 12: Configuring sensitivity at Medium



```
        Threshold (Only in Analysis)        : 10
        Refresh Timeout Rate                : 5
[i]     Application Setting Saved...
------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------

[+]     Intrusion Detection System - Detection Sensitivity
        0/D - Display Current Setting
        1/H - Highly Sensitive
        2/M - Medium Sensitive
        3/L - Low Sensitive

        4/C - Custom Setting (Include Refresh Timeout Rate)

        Current Setting : 2
[?]     Enter your option :  ( <default = return> ) : 3
        Selected ==> 3
[i]     Detection Sensitivity Setting
        Threshold for Data86                : 200
        Threshold for DataARP (ARP)         : 200
        Threshold for Data94                : 35
        Threshold for Data98                : 200
        Threshold for Association           : 20
        Threshold for Disassociation        : 20
        Threshold for Reassociation         : 20
        Threshold for Authentication        : 20
        Threshold for Deauthentication      : 20
        Threshold for Deauthentication(AC) : 20
        Threshold for EAPOL Protocol        : 10
        Threshold for EAPOL Start           : 10
        Threshold for EAP Communication     : 10
        Threshold for Qos Data              : 40
        Threshold (Only in Analysis)        : 10
        Refresh Timeout Rate                : 5
[i]     Application Setting Saved...
------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------

[+]     Intrusion Detection System - Detection Sensitivity
        0/D - Display Current Setting
        1/H - Highly Sensitive
        2/M - Medium Sensitive
        3/L - Low Sensitive

        4/C - Custom Setting (Include Refresh Timeout Rate)

        Current Setting : 3
[?]     Enter your option :  ( <default = return> ) : □
```

Figure 13: Configuring sensitivity at low



```
        4/C - Custom Setting (Include Refresh Timeout Rate)

        Current Setting : 3
[?]     Enter your option :  ( <default = return> ) : 4
        Selected ==> 4
[?]     Threshold for Data86                :  ( <current =50 > ) : 12
[?]     Threshold for DataARP (ARP)         :  ( <current =50 > ) : 34
[?]     Threshold for Data94                :  ( <current =15 > ) : 34
[?]     Threshold for Data98                :  ( <current =50 > ) : 34
[?]     Threshold for Association           :  ( <current =10 > ) : 34
[?]     Threshold for Disassociation        :  ( <current =5 > ) : 2
[?]     Threshold for Reassociation         :  ( <current =5 > ) : 3
[?]     Threshold for Authentication        :  ( <current =5 > ) : 2
[?]     Threshold for Deauthentication      :  ( <current =10 > ) : 4
[?]     Threshold for Deauthentication(AC) :  ( <current =10 > ) : 5
[?]     Threshold for EAPOL Protocol        :  ( <current =3 > ) : 6
[?]     Threshold for EAPOL Start           :  ( <current =3 > ) : 5
[?]     Threshold for EAP Communication     :  ( <current =3 > ) : 6
[?]     Threshold for Qos Data              :  ( <current =10 > ) : 5
[?]     Threshold (Only in Analysis)        :  ( <current =10 > ) : 6
[?]     Refresh Timeout Rate                :  ( <current =5 > ) : 4

[i]     Detection Sensitivity Setting
        Threshold for Data86                : 12
        Threshold for DataARP (ARP)         : 34
        Threshold for Data94                : 34
        Threshold for Data98                : 34
        Threshold for Association           : 34
        Threshold for Disassociation        : 2
        Threshold for Reassociation         : 3
        Threshold for Authentication        : 2
        Threshold for Deauthentication      : 4
        Threshold for Deauthentication(AC) : 5
        Threshold for EAPOL Protocol        : 6
        Threshold for EAPOL Start           : 5
        Threshold for EAP Communication     : 6
        Threshold for Qos Data              : 5
        Threshold (Only in Analysis)        : 6
        Refresh Timeout Rate                : 4
[i]     Application Setting Saved...
------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------

[+]     Intrusion Detection System - Detection Sensitivity
        0/D - Display Current Setting
        1/H - Highly Sensitive
        2/M - Medium Sensitive
```

Figure 14: Configuring customize sensitivity

7. Project Legacy

This framework has been developed to detect network anomalies in the network, data link, and transport layers. It helps users to identify various kinds of attacks like ARP poisoning, deauthentication attack, Evil twin attack etc.

7.1.CURRENT STATUS OF THE PROJECT

In the current state of the project, we can detect Evil twin, deauthentication, arp poisoning attacks, and we can whitelist and blacklist the malicious devices and networks.

7.2.REMAINING AREAS OF CONCERN

Following features can be added in the project in future:

- We will improve our algorithm so that we can detect more attack.
- We will add detecting mechanism of log4j attack.
- We will make it compatible for all kinds of operating system.

7.3.TECHNICAL AND MANAGERIAL LESION LEARNT

While working on the project, we experienced the importance of teamwork and learned various concepts about different types of attacks, and we also learned how to detect those attacks.

Here we also learned about time management, the importance of communication, responsibility and accountability.

8. CODE

https://drive.google.com/file/d/1D8j76zISde0CwVR2Rccfw_m9q1VIBTOh/view?usp=sharing

References

1. Raphael Hertzog, Jim O'Gorman (2017). Kali Linux Revealed: Mastering the Penetration Testing Distribution. Offsec Press.
2. Vivek Ramachandan,Cameron Buchanan (2017).Kali Linux Wireless Penetration Testing.Packt Publishing; 3rd edition
3. Justin Hutchens (2014). Kali Linux Network Scanning Cookbook.Illustrated edition.
4. Daniel W Dieterle (2022). Advanced Security Testing with Kali Linux. Independently published.
5. Ishan Girdhar (2017). Kali Linux Intrusion and Exploitation Cookbook.Packt Publishing.
6. Stuart McCure, Joel Scambray, George Kurtz (2012). Hacking Exposed 7: Network Security Secrets and Solutions.McGraw Hill; 7th edition.
7. Kevin Mitnick, William L. Simon, Steve Wozniak (2012). Ghost in the Wires. Back Bay Books; Illustrated edition.
8. Patrick Engebretson (2013). The Basics of Hacking and Penetration Testing. Syngress; 2nd edition.
9. Ali A. Ghorbani, Wei Lu, Mahbod Tavalle (2010). Network Intrusion Detection and Prevention: Concepts and Techniques.Springer;2010th edition.
10. Dileep Kumar G, Manoj Kumar Singh, M.K. Jayanthi (2016). Network Security Attacks and Countermeasures.IGI Global; 1st edition.
11. Dr Navid Behboodian (2012). ARP Poisoning Attack: An introduction to attack and mitigations. CreateSpace Independent Publishing Platform.
12. Richard Bejtlich (2013). *The Practice of Network Security Monitoring* No Starch Press; 1st edition.
13. Chris Sanders (2017). Practical Packet Analysis, 3E. No Starch Press; 3rd edition.
14. James Forshaw (2017). Attacking Network Protocols: A Hacker's Guide to Capture,Analysis, and Exploitation. No Starch Press; 1st edition.

15.Joshua Saxe, Hillary Sanders. (2018). Malware Data Science: Attack Detection and Attribution. No Starch Press