ROGUE ACCESS POINT DETECTION AND TRACKING IN UTAR CAMPUS

BY

LEE CHIEW MIN

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION TECHNOLOGY (HONOURS)

COMMUNICATIONS AND NETWORKING

Faculty of Information and Communication Technology

(Kampar Campus)

JAN 2024

UNIVERSITI TUNKU ABDUL RAHMAN

REPORT STATUS DECLARATION FORM

Title: Rouge Access Point Detection and Tracking in UTAR Campus

Academic Session: Year 3 Trimester 3

I LEE CHIEW MIN

(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

Lee Chiew Min

(Author's signature)

(Supervisor's signature)

Address:
58, Persiaran Setia 2,
Setia Residen,
32000 Sitiawan, Perak.

Puan.Nor 'Afifah Binti Sabri
Supervisor's name

Date: 19/04/2024

Date:19/04/2024

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TUNKU ABDUL RAHMAN

Date: 19 April 2024

SUBMISSION OF FINAL YEAR PROJECT

It is hereby certified that ***Lee Chiew Min*** (ID No: **20ACB03861**) has completed this final year project entitled **"***Rouge Access Point Detection and Tracking in UTAR campus*" under the supervision of of Puan.Nor 'Afifah Binti Sabri (Supervisor) from the Department of Computer and Communication Technology, Faculty of Information and Communication Technology, and Dr. Adeb Ali Mohammed Ahmed Al-Samet (Co-Supervisor) from the Department of Computer and Communication Technology, Faculty of Information and Communication Technology.

I understand that University will upload softcopy of my final year project in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

(*Lee Chiew Min*)

DECLARATION OF ORIGINALITY

I declare that this report entitled "**ROUGE ACCESS POINT DETECTION AND TRACKING IN UTAR CAMPUS**" is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : Lee Chiew Min

Name : Lee Chiew Min

Date : 19/04/2024

ACKNOWLEDGEMENTS

I would like to express my sincere thanks and appreciation to my supervisors, **Puan Nor 'Afifah Binti Sabri** and **Dr Shekh Abdullah Al-Musa Ahmed** who has given me this bright opportunity to engage in an IC design project. It is my first step to establish a career in cybersecurity and computer network. A million thanks to you.

Besides my supervisor, I would like to thank my family member who was being supportive and considerate throughout my final year project.

ABSTRACT

In the contemporary age of ubiquitous wireless networks, the issue of rogue access points (RAPs) has emerged as a paramount apprehension in the realm of network security. The primary objective of this project is to address the challenge of detecting and monitoring unauthorized access points, commonly referred to as rogue access points (RAPs), within higher education institutions. The specific focus of this endeavour is to enhance the security protocols at University Tunku Abdul Rahman (UTAR). The primary aim of this study is to present a very efficient methodology for detecting rogue access points (RAPs) and a resilient signal strength that can improve the precision of the system. The study begins by doing a thorough analysis of network security vulnerabilities. This is followed by a detailed review of relevant literature on methods for detecting rogue access points (RAPs). The main aim of the proposed a signal strength to calculate an approximate distance and mitigate occurrences of unauthorized network access, consequently reducing the resulting financial and reputational implications. The project entails the development of a holistic system design that integrates the technical aspects of the algorithm alongside the hardware specifications. The system functions by evaluating the intensity of the received signal to detect rouge access points (RAPs), and subsequently use signal strength to calculate the distance and approximate location. The testing and evaluation activities will be conducted within the campus premises of UTAR. The provided content serves as a valuable resource for additional inquiries in the fields of network security and the identification of rogue access points (RAPs). The program demonstrates a commitment to ethical principles by strictly adhering to regulations for data protection.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

RAPs	Rouge Access Points
APs	Access Points
SSID	Service Set IDentifier
BSSID	Basic Service Set Identifier
RSSI	Received Signal Strength Indicator
HMM	Hidden Markov Model
RTT	Round-trip time
HRAPs	Hidden Rogue Access Points
NIDS	Network Intrusion Detection Systems
WIDS	Wireless Intrusion Detection Systems
CLI	Command Line Interface
dBm	Decible Miliwatts
WPS	WiFi-Protected Setup
Lck	Lockout

CHAPTER 1

Introduction

In this chapter, we will explore the fundamental elements that emphasise the extent of this project. We will delve into the problem statement and motivation, outline the project's scope and objectives, highlight its contributions, and provide essential background information about this project.

1.1 Problem Statements and Motivations

In the modern digital age, wireless network communication has become an indispensable and essential part of human society, revolutionizing how humans connect and communicate. As wireless connectivity has brought us convenience and flexibility of browsing the internet from anywhere at any time, it has also brought forth a critical security concern, which is the emergence of rouge access points (RAPs) where unauthorized individuals perform within the network without any authorization, making more potential entry points for performing various malicious activities. In the academic environment, like many other public spaces, rouge access points (RAPs) can be set up easily by both insiders and outsiders. Once the rouge access point (RAP) is successfully installed, these RAPs can initiate an attack on the network it targeted, which will cause security breaches, including compromising data confidentiality, stealing network resources, and even sniffing out the packet through the network using Man-in-the-Middle (MITM) attacks, where this attack performs a sniffing attack in between the servers and clients to gain unauthorized access to sensitive data.

Furthermore, the RAPs can interrupt network interface by affecting low performance and reliability. When a rouge access point (RAP) is broadcasting its services set identifier (SSID), it will disrupt the signal of a legitimate access point operating on the same range and frequency. This scenario can be worsened if the fake SSID is set by a malicious actor, baiting users to connect networks that appear with the identical SSID but trap them for data theft. While the motivation behind setting up the Rouge access point can be many, it will not diminish the risk regardless of the intention of individuals

or malicious actors; the Rouge access point will and can pose significant harm to the network security. In short, it is crucial to monitor and detect rouge access points to prevent potential data breaches and network intrusions.

In this era of widespread wireless internet, many wireless networks exist in public places, especially within institutions like universities. Rogue access points, which constitute a serious security threat to companies, especially educational institutions like UTAR, are more likely to appear as wireless access points proliferate. In this environment, where students, faculty, and staff access sensitive data over wireless networks, the potential vulnerabilities are not always easy for network administrators to identify. This led the motivation to develop an effective system to detect and track these unauthorized access points. The UTAR campus needs an effective detection algorithm created especially for the campus network, much like any other network environment. Therefore, the motivation behind this title is to develop an efficient system that can help organizations detect and track rogue access points and prevent unauthorized access to their network, where it can improve network security by preventing data theft, data breaches, and other malicious activities that can be carried out by unauthorized users through rouge access points and having the features of tracking the rogue access points so that it can help network administrators to take necessary actions to safeguard their networks and maintain the security of their data.

1.2 Project Scope

This project scope covers developing and implementing a rouge access point detection and tracking system with restrictions on the UTAR campus network. The scope will focus on identifying potential security vulnerabilities in the campus, exploring current research on the Rouge access point and detection method, and a subsequent design and deployment that will detect and track the Rouge access point.

The system will be developed by using hardware and software where a laptop, Kali-Linux virtual machine, and Python will be installed when conducting the system. Moreover, the project's primary focus will be improving the network security within the specific context of the UTAR campus. In addition, the scope will perform a test review to ensure the algorithm is accurate and reliable for further performance else it can fix once any errors to ensure the system is entirely bug-free and document all the outcomes in a report for the reader with structured table and data so it would be easy for other when referencing. Nevertheless, the focus is on the UTAR campus network, not legal inquiry or prosecution, on top of that. The project implies that rogue access points are not installed with sufficient authorization, cause security threats to a network, and do not address realistic circumstances. Finally, the project seeks to provide a safer and more secure network environment by offering a workable solution to reduce the risks posed by rogue access points.

1.3 Project Objectives

The preliminary objective of this project includes the development of a new dedicated Rouge Access Point Detection and Tracking System specifically designed for the campus of University Tunku Abdul Rahman (UTAR) 's network environment, and this system is expected to detect the rouge access point effectively and efficiently within the UTAR campus's network environment. The main objective of this project is to design a system that is expected to perform 2 main features, which are precise detection of the rogue access point by scanning the network around the campus and after detected, able to track the movement or location of the rogue access point in real-time. Achieving these objectives, can improve the security of the network around the campus in terms of preventing potential security breaches and can ensure the confidentiality and integrity of sensitive data. Furthermore, the system will also provide features such as providing network administrators at UTAR an invaluable tool for real-time monitoring, enabling swift responses to emerging rouge access point threats while minimizing the risk that will be caused to the operations. Nevertheless, this project will ensure its standard matches the highest level of research ethics and institutional norms by highlighting a commitment to ethical principles and procedures that cover data collection, analysis, and system implementation by testing the credibility and accuracy of detection and tracking of rouge access point to maximize the effectiveness of detect and track and found out the potential of bugs in the algorithm. In short, the proposed objectives are expected to be conducted through a Kali-Linux virtual machine along with Python codes for detection and a Signal Strength for tracking the rouge access point. To put it briefly, the goal of this project is to do the following, simplified:

- Develop a dedicated Rouge Access Point Detection and Tracking System tailored for the University Tunku Abdul Rahman (UTAR) campus network environment.
- Efficiently detect rogue access points within the UTAR campus network to enhance overall network security.
- Design a system capable of precise rogue access point detection by scanning the campus network.
- Implement real-time tracking of detected rogue access points to monitor their

movement or location.

- Enhance network security to prevent potential security breaches and safeguard sensitive data integrity.
- Provide network administrators with real-time monitoring tools to swiftly respond to rogue access point threats.
- Ensure adherence to high research ethics and institutional norms in data collection, analysis, and system implementation.
- Test and validate the detection and tracking accuracy of rogue access points to optimize system effectiveness.
- Utilize a Kali-Linux virtual machine and Python codes for detection, along with a Signal Strength algorithm for tracking rogue access points.

1.4 Contributions

The contribution of this paper includes a rouge access point detection designed for detecting rogue access points within the UTAR campus network environment using techniques and methods. The methods can involve detecting and identifying rogue access points based on the pattern of their broadcasted SSID, MAC addresses and signal strength. Secondly, this paper also tries to develop a method for tracking rogue access points once detected. The tracking method can involve identifying the rogue access point's physical location through triangulation or other techniques. Lastly, this paper can also contribute to developing network security protocols and policies on the UTAR campus to prevent and mitigate the effects of rogue access points. The study results can help UTAR administrators identify vulnerabilities in the network and take appropriate measures to improve network security.

1.5 Background Information

According to the user guide of Junos Space [1], the rogue access point, which is frequently employed in Denial of Service and data theft attacks, is a widespread wireless security problem. Employees looking for unfettered wireless access frequently set up soft access points, another rogue access point. Furthermore, nearby businesses might set up rogue access points that use a company's network to gain free access. These access points are often low-cost and consumer-grade, and since they do not always announce their presence over the wire, it might be challenging to find them. Additionally, because they are frequently installed in default mode, authentication and encryption are frequently disabled, providing a significant security risk. A wireless LAN access point linked to a corporate network that is an open access point is a prime target for war driving since wireless LAN signals may pass through building barriers. Any client connecting to a malicious access point needs to be considered a rogue client as it circumvents the IT department's approved security measures.

In this digital era, the frequent occurrence of rogue access points emphasizes the urgent requirement for effective detection and mitigation techniques. These unauthorized access points may cause chaos by impairing network performance and compromising private information. They frequently operate as entrance sites for criminal activity, such as man-in-the-middle attacks and other hacks that can result in serious data breaches and financial losses. It is critical to understand the significance of rogue access points in the larger context of network security as the reliance on wireless networks continues to increase across various industries.

Lastly, knowing how rouge access point threats have evolved over the time can help us to visualize the changes as wireless technology has developed. Initially emerging as adaptable connections by employees seeking convenience, rogue access points have morphed into a sophisticated security challenge. Recently, attackers have exploited these vulnerabilities with more remarkable finesse, making them more elusive and dangerous. The treat of the attackers emphasizes how urgent it is to build cutting-edge detection and monitoring technologies because conventional security measures

frequently fail to detect these stealthy threats. Therefore, a thorough analysis of the historical trajectory of rogue access points becomes necessary to develop efficient countermeasures.

CHAPTER 2

Literature Reviews

2.1 History of Access Point

According to [2], Wi-Fi was preceded by the first wireless access points. In 1994, RangeLAN2, a product of Proxim Corporation (a distant relative of Proxim Wireless), was the first of its kind. Soon after the first Wi-Fi commercial devices arrived in the late 1990s, access points became widely used. Although some APs are wired devices, the industry progressively switched from calling them WAP devices to calling them AP devices (in part to prevent confusion with Wireless Application Protocol). Virtual assistants for smart homes have gained popularity recently. These include Google Home and Amazon Alexa, which connect wirelessly to access points like laptops, smartphones, printers, and other peripherals to become part of a wireless network.

2.2 Methods of Detections and Tracking Rouge Access Point

This part summarizes the techniques for detecting and tracking the Rouge Access Points (RAPs) in the system. Detection will involve network scanning to gather essential information such as SSID, BSSID, Channel (Ch), dBm (signal strength), WPS status, Lock (Lck) status, and Vendor details. Python functions will be employed to analyze this data, similar to the functionalities provided by tools like airodump-ng and Wash. The system will actively scan the network for the detection phase, collecting vital information about nearby access points. In order to detect possible Rouge Access Points based on particular criteria, such as suspicious BSSIDs, unauthorized WPS status, or other features, this data will be analyzed using Python routines. Users will receive a clear indication of any possible network security issues thanks to this method.

Moving on to track, Python will also play a pivotal role in this aspect. The system will

compute the coordinates of Rouge Access Points using Python routines. Two approaches can accomplish the tracking method; the first method would be using a trilateration algorithm to calculate the rouge access point coordinates, or the second method would use Receive Signal Strength to determine the area of the rouge access point. By analysing the RSSI from multiple sources or using trilateration algorithms, the system will estimate the physical location or area of the Rouge Access Point. Moreover, the network administrators can locate the unauthorized access point thanks to this tracking feature, enabling quick response and mitigation.

Overall, the system will be able to recognize and track Rouge Access Points using a combination of network scanning, Python-based detection analysis, position estimate utilizing signal strength, and mathematical techniques.

2.3 A Novel Approach for Rouge Access Point Detection on the Client-Side

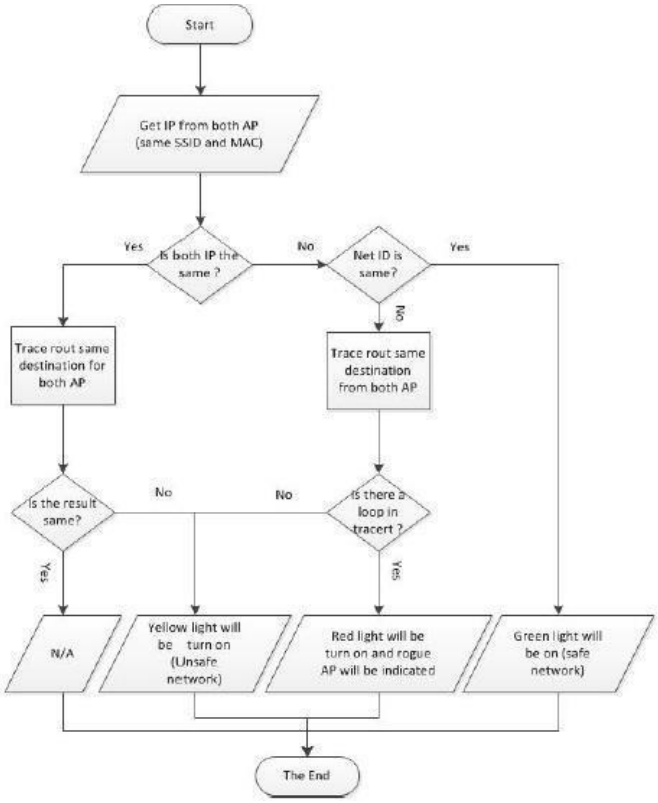


Figure 2.1: *Flow chart of detection RAP algorithm*

According to [3], this paper propose a practical method for detecting rouge access points on the client side that can warn users and prevent them from connecting to the unauthorized access point. Based on the rogue access point detection algorithm flow chart provided, as Figure 2.1 shows, it consists of three states based on the information collected to determine the access point's legitimacy and show whether it is safe or dangerous.

In this paper, the researchers implement a technique where the algorithm will use the IP address it collected to determine whether the access point is legitimate or has the potential to be a rouge access point. In the first step of the algorithm, the IP addresses of two access points will be compared to determine whether both APs are broadcasting the identical SSID and MAC addresses but different traceroutes. this step is crucial as if the comparison is accurate the potential of an evil twin attack is high as both APs has the identical SSID and MAC addresses but it direct in two different routes and according to how the network function, the scenario of two identical SSID, MAC

is possible but alongside with same IP address will not be happened, because this will cause the IP address conflict and both of the devices will not able to be function, thus showing N/A for the result. Next, when the IP comparison shows the result where both APs have different IPs but identical SSID and MAC address, this method implements the calculation of network ID based on the IP classes. If the result shows that both APs are the same, it indicates both of the APs are within the same network, and it is most likely for load balancing purposes. Additionally, a traceroute comparison will be executed if the algorithm collected both APs has different IPs and different network IDs; if the traceroute consists of any sign of an extra hop, it indicates that the presence of Man-in-the-Middle where the attacker tricks users into connecting to the rogue access point it creates to capture the packet they may send when passing through the legitimate access point.

In summary, the purpose of rouge access point detection is a client-side solution that can utilize client devices to perform scanning instead of a dedicated device. It also shows different colors like green, yellow, and red to signal to users whether the access point that the user connected is safe and prevent users from connecting to rouge access points.

2.3.1 Strengths and Weaknesses

Through the proposed method from this paper, the approach by conducting the researchers has several notable strengths:

1. The method can identify evil-twin-attack and Man-in-the-Middle attacks (MITM) very effectively, thus preventing further damages that might occur and enhancing the network security from the client side.
2. The system interpreted the colors of the traffic lights (green, yellow, red) to indicate to users whether the network is safe or unsafe to connect. Such a design makes the system more user-friendly in understanding the analytical outcomes without users having much technical knowledge about rouge access points.
3. The technique performs real-time evaluations using IP address comparisons, network ID assessments, and traceroute studies, enabling quick detection of suspect access points and rapid alerts to users. Another strength of its versatility is how well it can handle a variety of network circumstances, including those with access points that have similar SSIDs and MAC addresses, successfully classifying and handling each case.
4. The approach runs independently on the client side, eliminating the need for prior network knowledge and broadening its usefulness.

However, the proposal is not without limitations. As stated in the paper, the authors state that although it can detect the possibility of Man-in-the-Middle attacks and Evil Twin Attacks, it cannot check which one is the legitimate access point, and MITM relays on the existence of extra hop in the trace result, which lead to skilled hacker able to obfuscate, thus compromising the method's effectiveness. Furthermore, the method proposed is client-side operation restricts the access, causing the lack of network information that it can retrieve for decision making. Consequently, the reliance of the method on observable characteristics will be a challenge as it will limit its efficiency against more advanced attackers capable of mimicking legitimate network configurations.

2.4 Server-side Approach using Hidden Markov Model

According to [4], the Hidden Markov Model (HMM) is used to identify intrusive activities in the computer system, and their use has drawn attention in several different contexts [16-18]. In the context of the detection of Rouge Access Point (RAP), the reasons to use HMMs are supported by several factors:

1. A wireless local area network (WLAN) frequently has many access points linked to different devices, each producing a steady stream of packet requests. Given the limited number of repeating requests from these devices, it is possible to simulate access point behaviors with a restricted set of states, a job well suited for HMMs.
2. Because HMMs can analyze sequence relationships, WLANs' dependency on earlier packet arrivals makes them a logical setting to perform well.
3. In line with the HMM paradigm, state changes in this network environment may be effectively described as a modified Markov process.

The capacity of HMMs to simulate the probability of false positives and false negatives associated with observations—a critical factor in anomalous intrusion detection—is another significant component. Nevertheless, the proposed method inspired by Rabiner's work on Hidden Markov Model (HMMs) [19] consists of training the HMM and applying the learned model to find rogue access points. The detecting phase employs the Viterbi algorithm. The authors have trained HMM using three DoS attacks: Pod (DoS attack using large ping packets), Portsweep (DoS attack by scanning numerous ports), and Neptune (DoS attack utilizing Syn flood). Subsequently, the HMM is inferred from this observation sequence, laying the foundation for anomaly detection.

2.4.1 Strengths and Weaknesses

In the approach by G. Shivaraj et al. [4], to accomplish its goal, the system makes use of inherent WLAN connection properties and DoS assaults. It works by tracking how long it takes packets in each traffic flow to arrive one after the other, keeping track of

how much traffic is passing via access points. Significant differences in inter-arrival durations between authorized access points and RAPs are shown by the approach, which is crucial. The trained HMM can discriminate between the two by using these characteristics, which helps with RAP detection. This method, which is client-side, presents itself as an easy-to-use and effective solution, especially for finding malicious access points in a network.

On the controversy, this approach consists of several weaknesses. The first potential weakness is its reliance on a typical network data set for training the HMM model. If the network data used for training is not representative of the actual network traffic, the model may not be accurate in detecting rogue access points. Additionally, the inter-arrival time of packets from these rogue access points may not considerably differ from that of authorized access points, and the technique may also be ineffective in detecting rogue access points that are set up to mimic the behaviour of authorized access points.

2.5 Hidden Rouge Access Point Detection Technique for Wireless Local Area Network

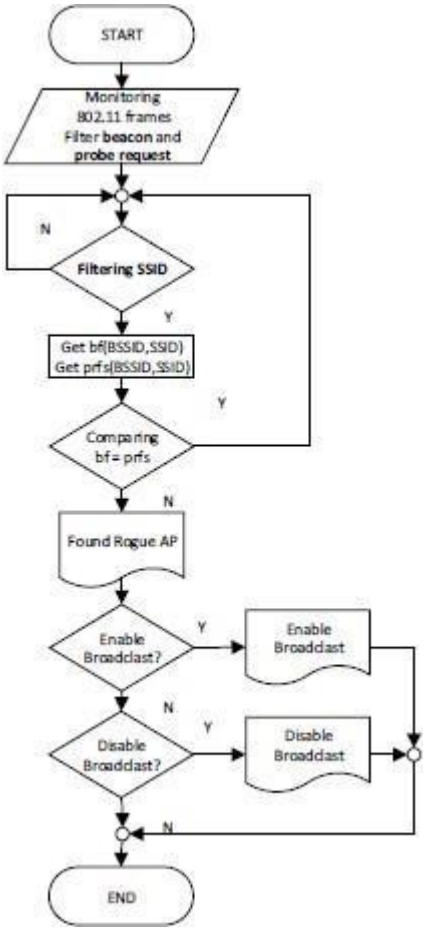


Figure 2.2: *Flow chart of Hidden Rogue Access Point*

Throughout [5], this paper has proposed a Hidden Rogue Access Point (HRAP) detection technique that takes into account the possibility of RAPs operating clandestinely within networks. For the proposed method, the researchers have reviewed various strategies to identify rouge access points (RAPs) that could affect network integrity. For instance, some approaches focus on fingerprint frameworks and using data gathered from beacon frame information. Elements such as SSID, MAC address, and beacon frame size have been compared with legitimate access point data to identify abnormalities suggestive of RAPs [1]. Signal intensity and SSID from beacon frames have also been compared with data from real access points, using variations in signal strength as a surefire indicator of RAP existence [2]. In addition to time stamps, research has examined the transmitting beacon frames' sequence and length [3], and it has used thresholds generated from clock skew for comparison as a RAP detection

approach [4]. Moving on towards the suggested Rogue Access Point (HRAP) detection method, it considers the possibility of RAPs operating covertly within networks.

In a Wireless Local Area Network (WLAN), many devices such as computers, tablets, or smartphones are connected to the network, established connection from the list broadcast in beacon frames. When several access points share an identical SSID, devices often choose the AP with the strongest signal. HRAPs take advantage of this trend by imitating real APs. However, with closer inspection, differences between the beacon and probe request frames of HRAPs and genuine APs become apparent. In particular, HRAPs frequently lack an SSID or the name of the HRAP, even if they have a comparable tag length as APs. HRAPs can use one of two tactics: either a phony MAC address identical to a real AP or a different MAC address but keep the identical SSID. Nevertheless, HRAP detection relies heavily on these minutes but significant differences. In short, the three main steps of the proposed HRAP detection technology are summarized as follows:

- **Monitoring:** Data from beacon frames and probe request frames is gathered in the monitoring mode.
- **Selection:** Frames are selected using the MAC address (BSSID) criterion.
- **Detection:** Analysis of the SSID and BSSID data included in beacon and probe requestframes is used to detect HRAPs.

2.5.1 Strengths and Weaknesses

The suggested HRAP detection method has several advantages. First, it is particularly good at locating hidden rogue access points (HRAPs), a security hazard frequently underappreciated by traditional detection techniques. Second, it performs a detailed analysis of the data included in both beacon frames and probe request frames, enhancing the RAP detection's resilience by considering various factors that might indicate the presence of fraudulent access points. Thirdly, it successfully minimizes false positives by carefully examining SSID and BSSID data with an emphasis on anomalies suggestive of HRAP existence.

Nonetheless, there are several issues with the method. It is primarily designed to find hidden rogue access points (HRAPs) and may not be able to find other kinds of rogue access points that do not try to hide their presence. The technique also largely depends on the SSID and BSSID information in beacon and probe request frames. Knowledgeable attackers may be able to modify this data to avoid detection. Furthermore, implementation difficulties might arise due to the algorithmic representation's complexity, especially for network managers with low technical knowledge. Last, this methodology acts solely on the client side, similar to many RAP detection methods, potentially restricting access to network-level data required to evaluate access point legality.

2.6 Client-side Rogue Access-Point Detection using Round-trip Time Analysis

According to Kitisriworapan et al. [6], it states that an approach includes the protection of users from mistakenly connecting to malicious access points (APs) by the use of straightforward round-trip time (RTT) measurement and analysis. A probe-walking approach is employed to acquire enough timing instants for precise analysis. Users can only get one data instant for each active AP connection at a specific location. Walking patterns are suggested based on the signal strength, relative angle, and distance from the linked AP in terms of steps. Once enough data instants exist, a rogue AP is found using k-means clustering classification.

2.6.1 Strengths and Weaknesses

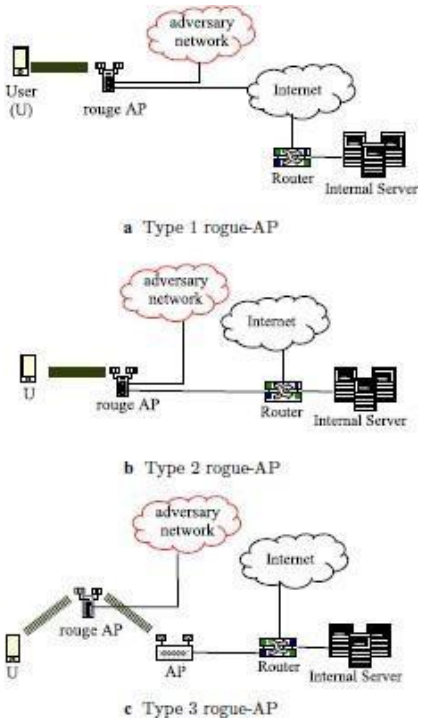


Figure 2.3: ***Various Rouge AP categories in term of Wi – Fi topology***

One advantage of client-side rogue access-point detection is utilizing round-trip time. Using Round-trip time (RTT) for analysis sit gives normal users a quick and affordable option to identify rogue access points without requiring specialized tools or technical know-how. Users can discover unusual delays caused by rogue access points and take steps to safeguard their devices from potential security hazards by monitoring the RTT

between them and the access points to which they are connected.

This scalability of this approach is another advantage, as the detection can be performed on the client side, and it is simple to deploy on a wide scale without needing extra resources or substantial changes to the network architecture. It is, therefore, a workable choice for businesses operating under tight financial or resource restrictions. Additionally, by adding an extra layer of security for individual users, client-side detection utilizing RTT analysis can support current network-based detection techniques like network intrusion detection systems (NIDS) or wireless intrusion detection systems (WIDS). Assisting in detecting rogue access points that network-based procedures may overlook can enhance overall network security.

On the other hand, there are a few flaws in the client-side rogue access point detection method that uses round-trip time analysis. First, because the technique depends on users being proactive in taking the RTT measurements—which might not always be the case—it could result in a lack of coverage and inaccurate data. Second, environmental variables like interference and obstructions may influence the method's accuracy and lead to erroneous timing readings. Third, According to Kitisriworapan [6], there are 3 types of rogue access points: type 1 rogue access point is an access point that is set up by broadcasting known SSIDs for WLAN services, type 2 rogue access point is a rogue AP that is typically used in institutions like schools and colleges, and type 3 rogue access point that can be found both inside or outside the organization's boundaries. Hardware-based can quickly install Type 3 rogue-APs [7]. It is, however, hard to find [8] in which type 1 and type 2 rogue access points do not cause extra time delays and may not be able to be detected using this approach, which may only help detect type 3 rogue access points. Fourth, the method requires users to walk around and probe the network, which can be time-consuming and inconvenient. Finally, this method may not be suitable for large-scale networks, where the number of users and access points may be too high for efficient probing and analysis.

2.7 Rogue Access-Point Tracking Using Received Signal Strength Indicator

According to Qawasmeh & Awad, 2021[7], an approach for tracking mobile rogue access points using the received signal strength associated with beacon frames. The approach involves estimating the distances to the rogue access point based on the received signal strength measurements at three reference wireless devices. The distance set is then used as input to a trilateration algorithm to estimate the location of the rogue access point. The mobility of the rogue access point is tracked by extracting its speed and direction using consecutive estimated locations, which are then used to predict its following location.

2.7.1 Strengths and Weaknesses

This approach effectively tracks mobile rogue access points using readily available information from the received signal strength of beacon frames. Trilateration and mobility prediction algorithms ensure that the location and movement of the rogue access point can be accurately estimated. On the other hand, the effectiveness of this approach may be limited in areas with high levels of signal interference or congestion, which can affect the accuracy of the received signal strength measurements as this method relies on received signal strength measurements, which can be affected by various factors such as interference and obstacles in the environment. Additionally, the approach may be susceptible to spoofing attacks where an attacker mimics the beacon frames of a legitimate access point to confuse the tracking algorithm. Therefore, it may not be completely reliable in all situations.

2.8 An Improved Trilateration Positioning Algorithm with Anchor Node Combination and K-means Clustering

According to [8], The trilateration positioning algorithm calculates the coordinates of an unknown node by using the distances between the unknown node and three neighbouring nodes. It involves the following steps:

- Distance Obtaining: The distances between the unknown node and all anchor nodes areestimated using RSSI (Received Signal Strength Indicator).
- Combination of Anchor Nodes: Different combinations of anchor nodes are formed to perform trilateration calculations. Each combination consists of three anchor nodes.
- Trilateration Positioning Calculation: For each combination of anchor nodes, trilateration is performed. The coordinates of the anchor nodes and the distances between the unknown node and the anchor nodes are used to create three circles. The intersection point of these circles corresponds to the position of the unknown node.
- Coordinate Clustering: After performing trilateration calculations for multiple combinations of anchor nodes, multiple groups of coordinates for the unknown node are obtained. To improve positioning accuracy, K-Means clustering is applied to filter out situations where the circles do not intersect, or other errors occur.
- Optimal Coordinate Selection: The final coordinates of the unknown node are determined by selecting the optimal coordinates from the clustered groups. The least amount of information is used to improve localization accuracy.

Overall, the trilateration positioning algorithm uses geometric relationships and distance measurements to calculate the coordinates of an unknown node. It can be used for various applications but may have limitations in terms of positioning accuracy and computational complexity.

2.8.1 Strengths and Weaknesses

The proposed method demonstrates similar average positioning error and average positioning time compared to other cluster numbers when the cluster number is set to two (2). Moreover, the method show that it is robust and consistent across different group numbers, and able to utilizes a combination of anchor nodes and ranging information to estimate the distance between the unknown node and the anchor nodes. Lastly, this approach allows for accurate localization in both indoor and outdoor environments.

However, the approach does not provide specific information about the positioning accuracy and efficiency of the proposed method compared to the reference methods (least-squares method, maximum likelihood method, random selection trilateration method, and fixed selection trilateration method). Therefore, it is difficult to assess the superiority of the proposed method over these reference methods and the document does not mention any potential limitations or challenges associated with the proposed method, such as the impact of environmental factors or the scalability of the method to larger networks. Further research is needed to address these aspects.

CHAPTER 3

System Methodology/Approach

The development process was categorized into several phases: pre-development research by reviewing existing literature on detection methods and tracking methods, obtaining the authorized access points information in the UTAR campus, system planning, and algorithm development for the prototype.

3.1 System Design Diagram

The use case and system architecture diagrams will be provided in this section to give an overview of the proposed system.

3.1.1 System Architecture Diagram

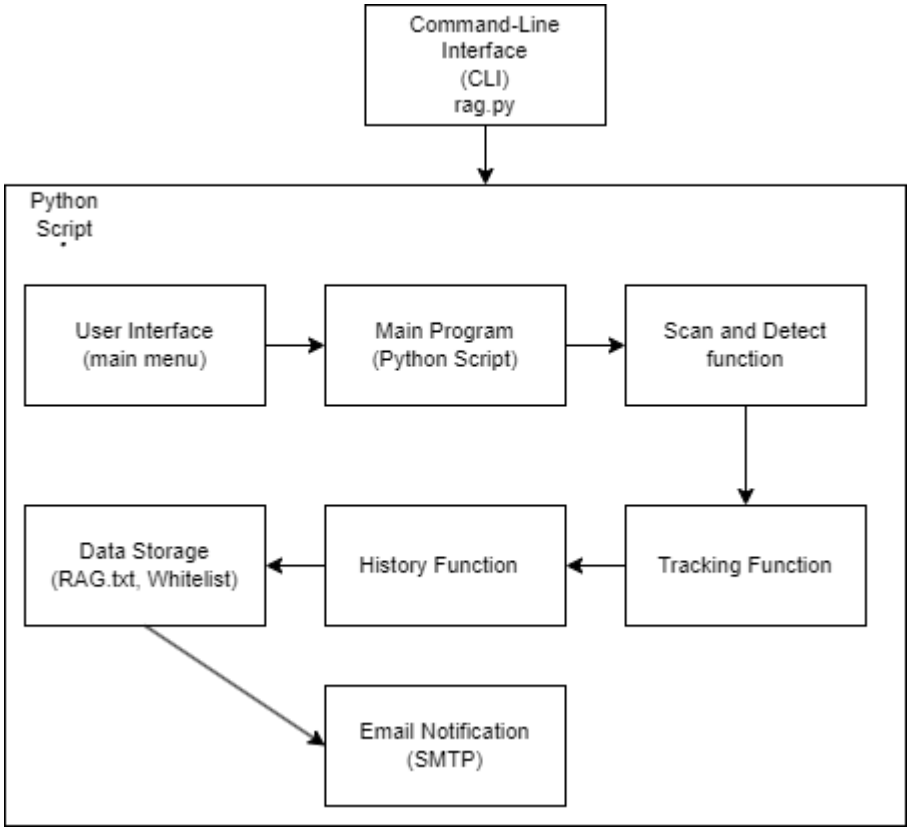


Figure 3.1 System Architecture Diagram

In this section, as shown above is the system architecture diagram that represent the functionalities of the system:

- User Interface (Main Menu):

– The user interacts with the system through a main menu interface, where they can choose from different options such as scanning for Rogue Access Points (RAPs), tracking detected RAPs, viewing RAP detection history, or exiting the program.

- Main Program (Python Script):
  - The main program is responsible for coordinating the various functionalities of the Rogue Access Point Detection and Tracking System.
  - It handles user inputs, initiates the appropriate functions based on user selections, and manages data flow between different components.

- Scan and Detect Function:
  - This function conducts network scanning using a wireless adapter capable of detecting nearby access points.
  - Upon scanning, the function compares the detected SSID and BSSID combinations with a whitelist of trusted network identifiers (whitelist.txt).
  - If an SSID match is found but the BSSID does not match the whitelist, the system identifies this as a potential Rogue Access Point (RAP) and logs relevant information into RAP.txt.
  - Additionally, an email notification is triggered to alert network administrators about the potential RAP.

- Tracking Function:
  - The Tracking Function is invoked after a RAP is detected and stored in RAP.txt.
  - It utilizes the received signal strength indicator (RSSI) or dBm value associated with the detected RAP to estimate the approximate distance between the scanning device and the RAP.
  - The distance calculation is performed using a simplified path loss model, translating RSSI values into estimated distances.

- History Function:
  - The History Function provides a view of previously detected Rogue Access Points (RAPs) stored in RAP.txt.
  - Users can access this function through the main menu to review past RAP detections, including relevant details such as SSID, BSSID, and detection timestamps.

- Data Storage (RAP.txt, Whitelist):
  - RAP.txt: This file stores information about detected Rogue Access Points (RAPs), including SSID, BSSID, and other relevant details.
  - whitelist.txt: Contains a list of trusted SSID-BSSID pairs that are considered legitimate within the network environment.

- Email Notification (SMTP):
  - Upon detecting a potential Rogue Access Point (RAP), an email notification is automatically sent to designated network administrators.
  - This email alert serves as a proactive measure to notify administrators of security risks and potential network breaches.

The Rogue Access Point Detection and Tracking System's primary functionalities are depicted in this system architecture diagram, which highlights the interactions and flow of information between various components. It gives administrators an organized perspective of how the system finds, follows, and controls rogue access points in a network environment, improving network security and enabling real-time monitoring.

3.1.2 Use Case Diagram

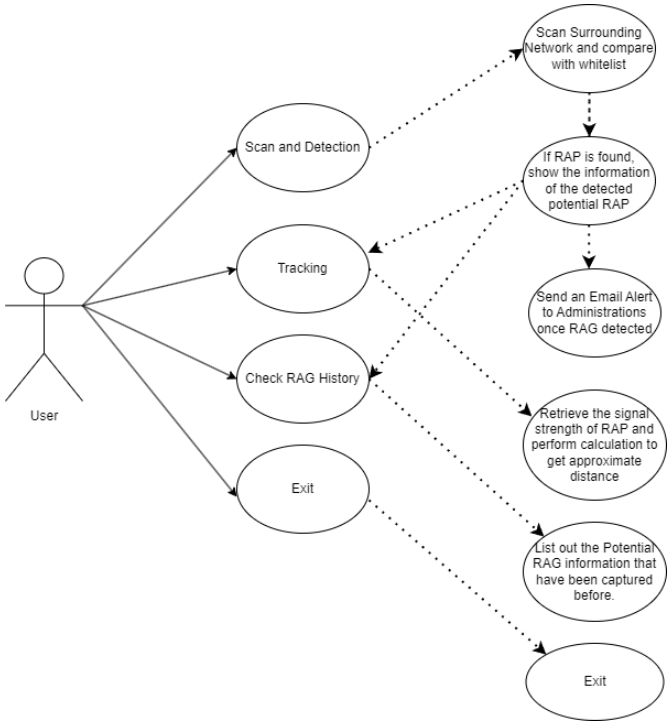


Figure 3.2 Use Case Diagram

In this section, as refer to the above Use Case Diagram, it shows that the Rogue Access Point Detection and Tracking System offers several key functionalities for network security management. When a user selects the "Scan and Detect" option from the main menu, the system performs a wireless network scan using the configured adapter. Detected SSID-BSSID combinations are cross-referenced with a whitelist of trusted network identifiers. If a mismatch is detected, indicating the presence of a Rogue Access Point (RAP), the system logs the RAP details in `RAP.txt` and triggers an email notification to network administrators for prompt action. Subsequently, users can utilize the "Tracking" option to estimate the distance to previously detected RAPs. By retrieving the Received Signal Strength Indicator (RSSI) associated with a RAP, the system calculates an approximate distance using a path loss model, providing users with valuable insights into the proximity of potential threats. Additionally, the system supports a "History" option, allowing users to view past RAP detections stored in `RAP.txt`. This feature provides visibility into SSID-BSSID pairs, timestamps, and other relevant details, empowering users to monitor and analyze historical rogue access point activities within the network environment. Together, these use cases enable effective detection, tracking, and historical review of rogue access points, enhancing network security and facilitating proactive response measures.

3.2 Software Development Life Cycle

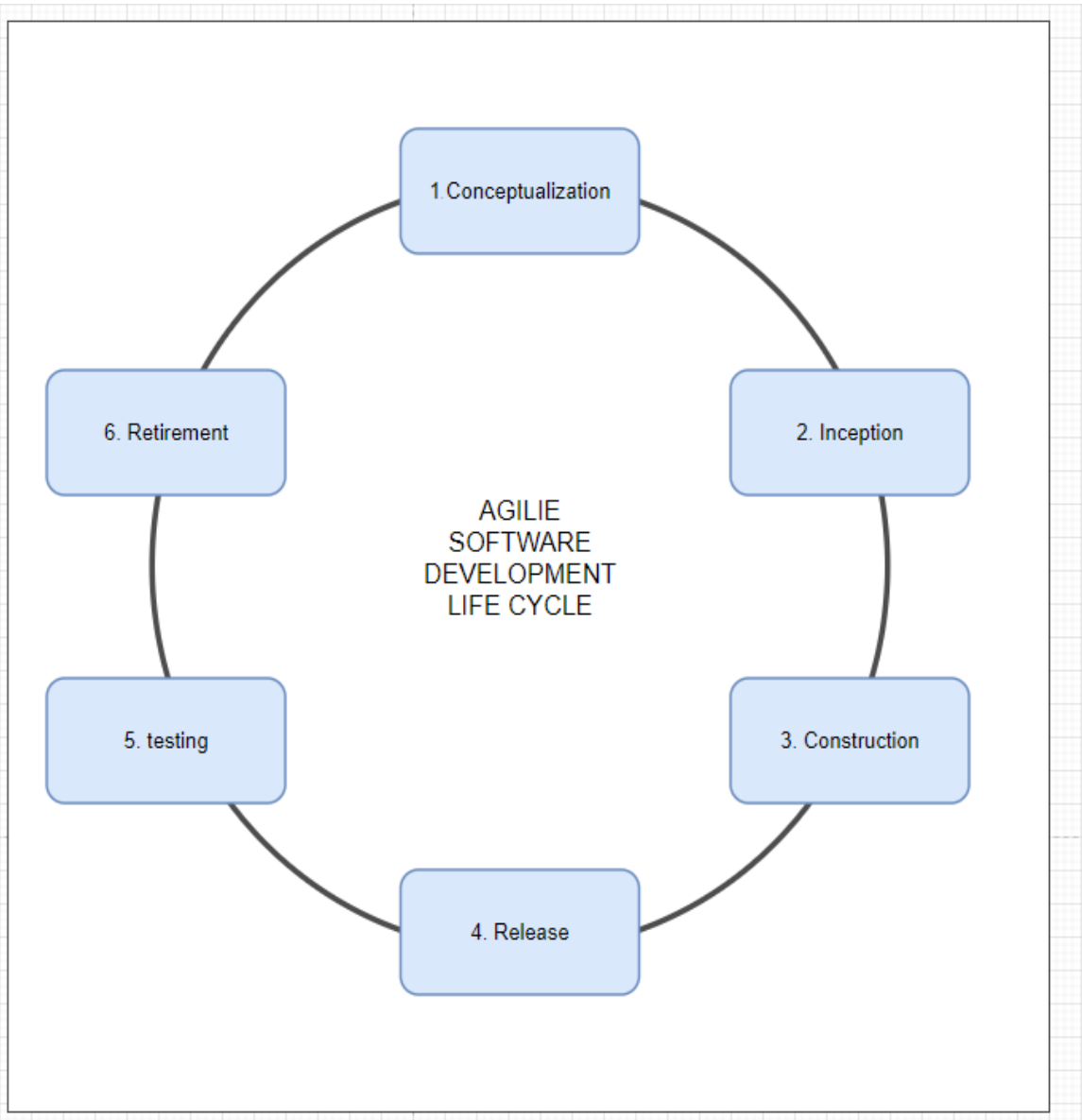


Figure 3.3 Agilie software development life cycle

The system methodology involves using an agile approach where the 5 development stages are shown in the Figure 3.3 above. The 6 stages involved are Conceptualization, Inception, Construction, Release, testing, Retirement.

- Conceptualization:
  - The conceptualization phase marks the initial stage of the Agile SDLC, where the idea for the Rouge Access Point Detection and Tracking System is formulated. During this phase, it is needed to identify the need for a dedicated system to enhance network security within the UTAR

campus environment. Concepts and objectives are outlined, including the precise detection and real-time tracking of rogue access points to prevent potential security breaches.

- Inception:
  - In the inception phase, the project objectives and requirements are further refined and translated into actionable tasks. This phase involves sprint planning sessions to break down project requirements into manageable user stories and backlog items. Author prioritize features based on criticality and the objectives needs. The inception phase sets the foundation for iterative development by establishing sprint goals, durations, and initial release milestones.

- Construction:
  - The construction phase encompasses the iterative development and implementation of features within sprints. Creator need collaborate closely to implement user stories, conduct code reviews, and perform continuous integration and testing. Agile principles such as daily stand-up meetings, sprint reviews, and sprint retrospectives guide the development process. Throughout this phase, the Rouge Access Point Detection and Tracking System takes shape, with features progressively added and tested.

- Release:
  - The release phase marks the deployment of the system's initial version or major feature releases. Incremental builds are delivered to supervisor for testing and feedback. Continuous integration and automated testing ensure the stability and quality of the release. Supervisor evaluate the system's performance against predefined acceptance criteria. The release phase emphasizes delivering value to users and addressing immediate security concerns identified during testing.

- Testing:
  - The testing phase focuses on validating the functionality, security, and performance of the Rouge Access Point Detection and Tracking System. Test cases are executed to ensure that the system meets specified requirements and effectively detects rogue access points under different network conditions. Agile testing practices, including regression testing and user acceptance testing, play a crucial role in verifying system capabilities and detecting potential vulnerabilities.

- Retirement:
  - The retirement phase involves the end-of-life management of the Rouge Access Point Detection and Tracking System. This phase may not apply directly to a security system, but it emphasizes the importance of ongoing maintenance, updates, and eventual decommissioning of software components. The creator will evaluate the system's effectiveness over time and plan for future enhancements or successor systems based on evolvingsecurity needs.

CHAPTER 4

System Design

4.1 System Flowchart

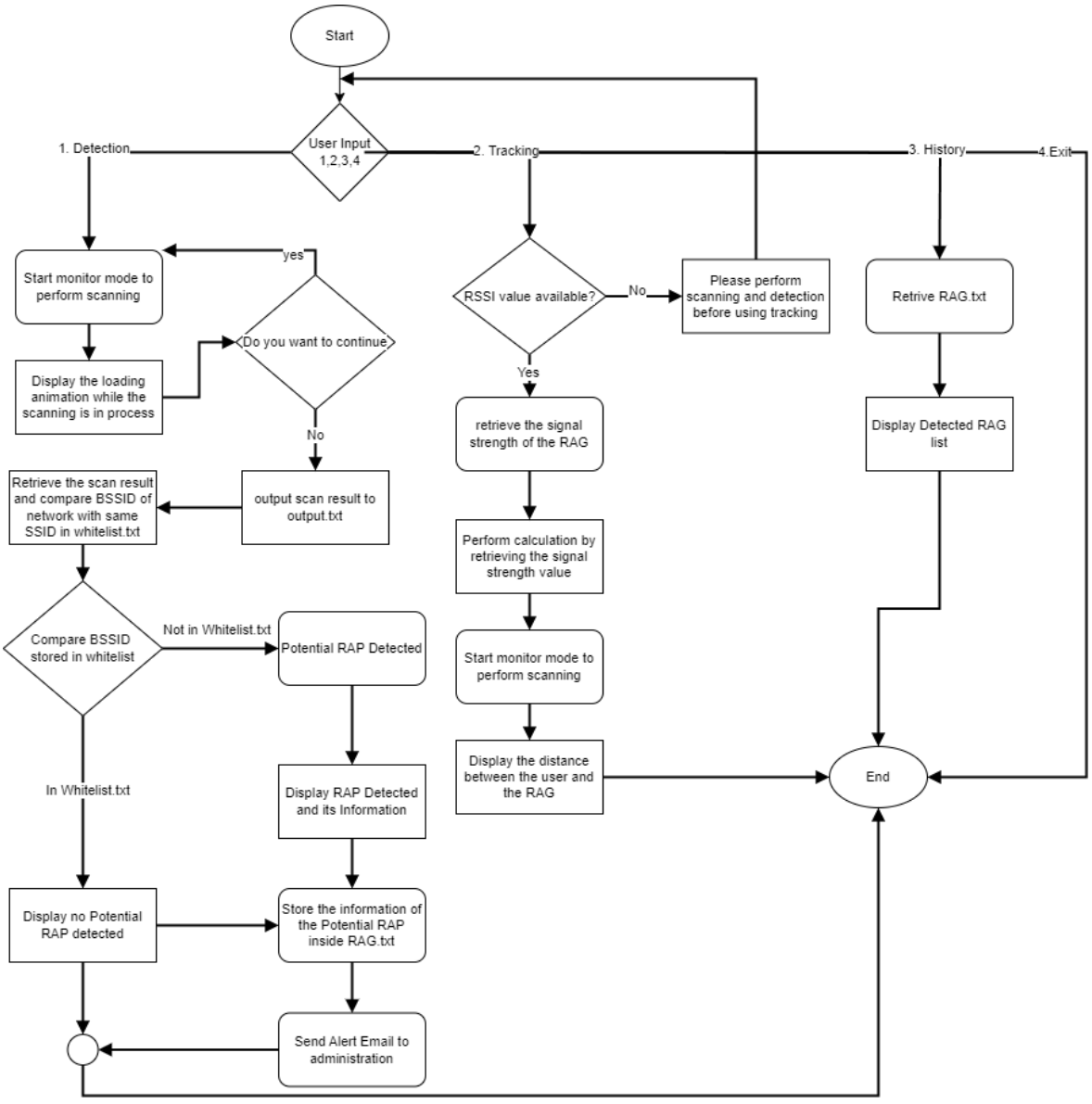


Figure 4.1 System Flow Chart

In Figure 4.1 shows the System Flow Chart of the Rouge Access Point Detection and tracking. To illustrates the System Flow Chart of the Rouge Access Point Detection and Tracking System. The system begins by presenting a main menu that displays the system title and author, followed by four menu choices labeled 1 through 4: Detection, Tracking, History, and Exit.

Detection (Scan and Detect):

- When the user selects the "Detection" option (choice 1) from the main menu, the system initiates the scanning process using the FYP1_scan.py script.
- The scanning operation involves gathering information about the surrounding wireless networks and storing the results in output.txt.
- The system then compares the detected SSID-BSSID combinations with entries in whitelist.txt to determine if any potential Rogue Access Points (RAPs) are present.
- If a mismatch is found between an SSID in output.txt and whitelist.txt, indicating a potential RAP, the system logs the RAP details in RAP.txt and notifies the user about the detected RAP.

Tracking:

- Choosing the "Tracking" option (choice 2) from the main menu triggers the tracking function (FYP_Track.py).
- This function retrieves the RSSI (Received Signal Strength Indication) value associated with previously detected RAPs stored in RAP.txt.
- Using the RSSI value, the system calculates an estimated distance to the RAP based on a distance approximation model.
- The calculated distance is then used to estimate the location of the RAP relative to a reference point (FICT campus coordinates) and displayed to the user.

History:

- Selecting the "History" option (choice 3) from the main menu allows users to view a list of previously detected RAPs stored in RAP.txt.
- The system reads the contents of RAP.txt and displays the details of each detected RAP, including SSID, BSSID, and detection timestamps, providing users with a historical record of detected RAPs.
- The system flow chart emphasizes the sequential operation of the Detection, Tracking, and History functions, each contributing to the overall goal of detecting and monitoring Rogue Access Points within the network environment. By offering these functionalities through a user-friendly menu

interface, the system enhances network security by enabling efficient detection and tracking of unauthorized access points.

4.2 Sequence Design

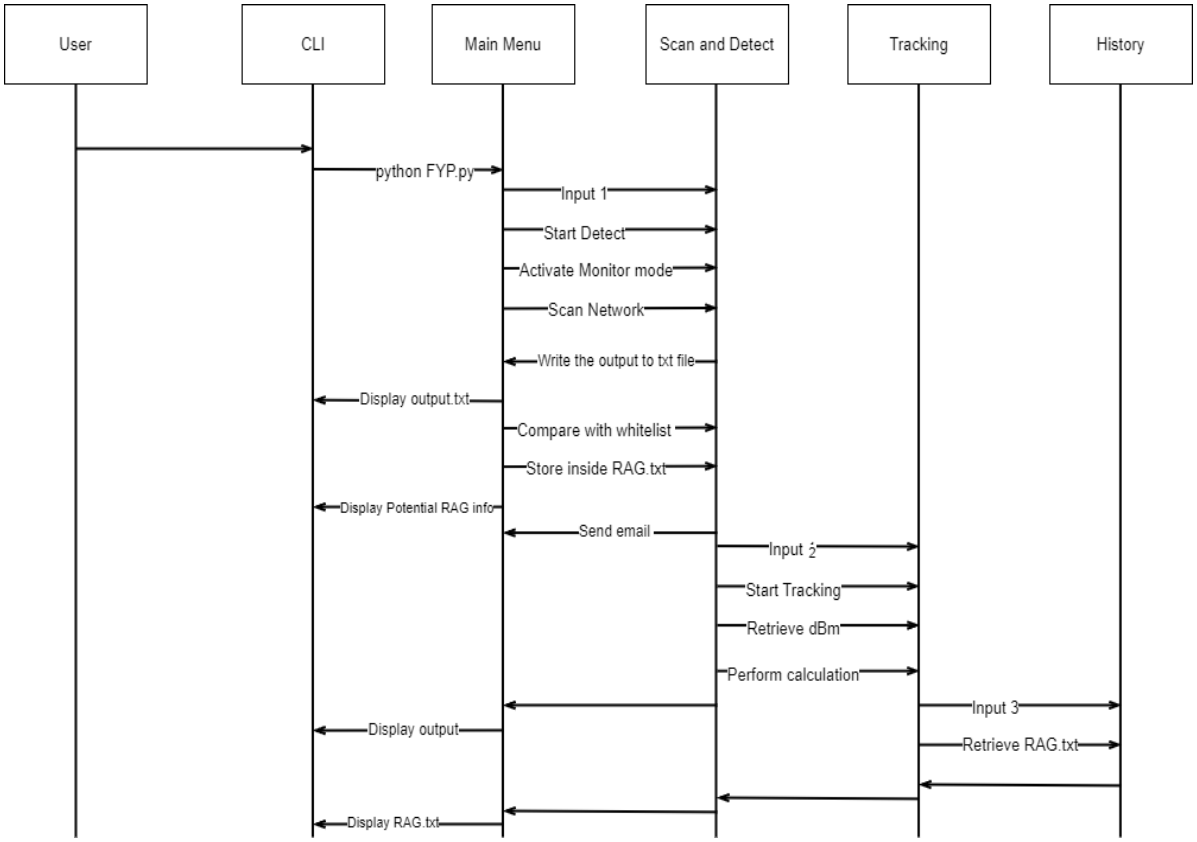


Figure 4.2 Sequence Flow Diagram

User Interaction:

- The user interacts with the system by selecting different options ("Scan and Detect", "Tracking", "History") from the main menu.

Scan and Detect Operation:

- When the user selects "Scan and Detect", the system initiates a network scan using the network adapter.
- Scan results are retrieved and compared with the whitelist to identify potential Rogue Access Points (RAPs).
- If a RAP is detected (mismatch with whitelist), its details are logged, and an email notification is sent.

Tracking Operation:

- Upon selecting "Tracking", the system retrieves the Received Signal Strength Indication (RSSI) associated with the detected RAP.
- Using the RSSI value, the system calculates the estimated distance to the RAP and displays it to the user.

History Operation:

- When the user selects "History", the system retrieves and displays logs of previously detected RAPs stored in the RAP logs (RAP.txt).

This sequence diagram visually represents the flow of operations within the Rouge Access Point Detection and Tracking System, showcasing the interactions between user actions, system functionalities, and the network adapter during different stages of detection, tracking, and historical data retrieval. Adjustments can be made based on specific implementation details and user requirements.

CHAPTER 5

System Implementation

To give a clearer and more complete view of the system design, the intricacies of the software configuration and system implementation are painstakingly detailed in this part.

5.1 Hardware

The hardware involved in this project is a laptop and wireless USB adapter. The laptop in this project plays a crucial role, as the majority of the research and development is using a laptop to perform, for instance, literature review, development of the system and physical platform for Oracle VM Virtual Box, Kali Linux virtual machine, and Python, in table 5.2 shows the specifications of the laptop. Next, the wireless USB adapter provides access to the virtual machine Kali-Linux to perform broader and more accurate network receptions. Correspondingly, table 5.2 and Table 5.3 show the specifications of the wireless USB adapter and the wireless features of the wireless USB adapter.

Table 5.1 Specifications of the laptop

Description	**Specifications**
Model	S340-14IWL Laptop (ideapad) - Type 81N7
Processor	Intel(R) Core (TM) i5-8265U CPU @ 1.60GHz, 1800 Mhz, 4 Core(s), 8 Logical Processor(s)
Operating System	Microsoft Windows 11 Home Single Language
Graphic	Intel(R) UHD Graphics 620
Memory	8GB
Storage	Window SSD 236GB

Table 5.2 Specifications of the wireless USB adapter

Description	**Specifications**
Model	tp-link TL-WN722N
Standards	IEEE 802.11n/g/b
Interface	USB 2.0
Button	WPS
Security	WEP, WPA/WPA2, WPA-PSK/WPA2-PSK
Dimensions	3.7 x 1.0 x 0.4 in (93.5 x 26 x 11 mm)
System compatibility	Windows 11/10/8.1/8/7/XP, Linux and macOS

Table 5.3 Wireless features of wireless USB adapter

Description	**Specifications**
Wireless Standards	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Frequency	2.400-2.4835GHz
Signal Rate	11n: Up to 150Mbps(dynamic) 11g: Up to 54Mbps(dynamic)11b: Up to 11Mbps(dynamic)
ReceptionSensitivity	130M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Transmit Power	<20dBm
Wireless Modes	Ad-Hoc / Infrastructure mode
Wireless Security	Support 64/128 bit WEP, WPA-PSK/WPA2-PSK
Modulation Technology	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM

5.2 Software

In this project, several tools are integrated into the research and development: Oracle VM Virtual Box, Kali-Linux virtual machine, and Python programming language. Oracle VM virtual machine as a platform for running the virtual machine within an isolated environment eliminates the need for a physical host. It allows the utilization of virtual machines like Kali-Linux. Moreover, Kali-Linux can be a robust cybersecurity-oriented system, offering extensive features and capabilities for ethical hacking and research activities. Thus, using Kali Linux as the operating system will enhance the performance and overall environment. Lastly, the Python programming language facilitates the development of the system's algorithm components.

5.3 Settings and Configurations

5.3.1 Setting up Kali-Linux Virtual Machine at Oracle VM Virtual Box

For this section, the procedure of setting up the **Kali-Linux Virtual Machine** at the **Oracle VM Virtual Box** will be guided. Once successfully downloaded both of the software, proceed to the step below:

Open Oracle VM Virtual Box and click "**new**".

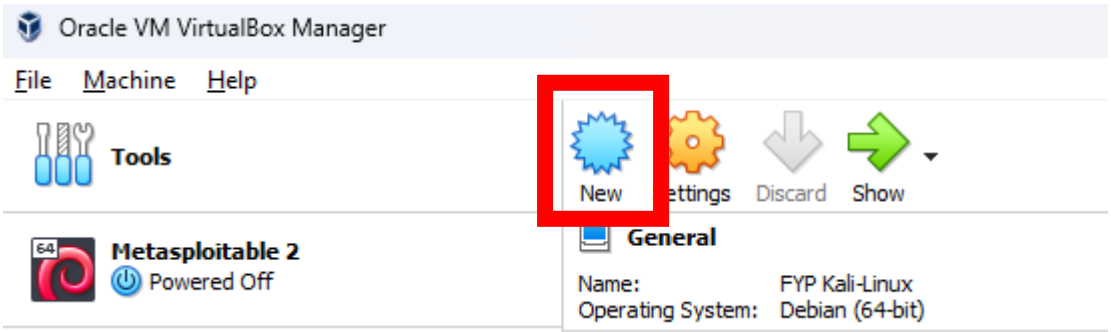


Figure 5.1: *Oracle VM Box new*

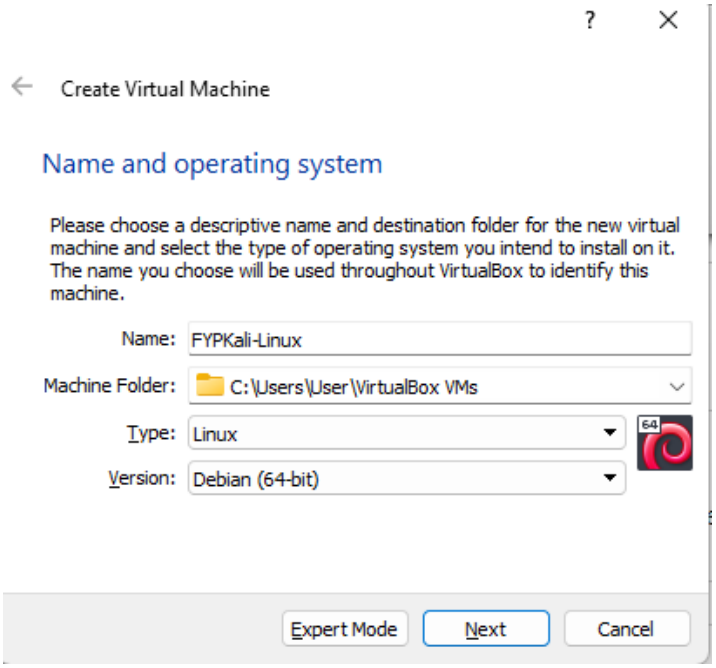


Figure 5.2: *Create Virtual Machine window*

After click "new", it will prompt this window and set the name for the Virtual Machine and thetype of VM is "Linux" with the Version "Debian(64bits), then click "next".

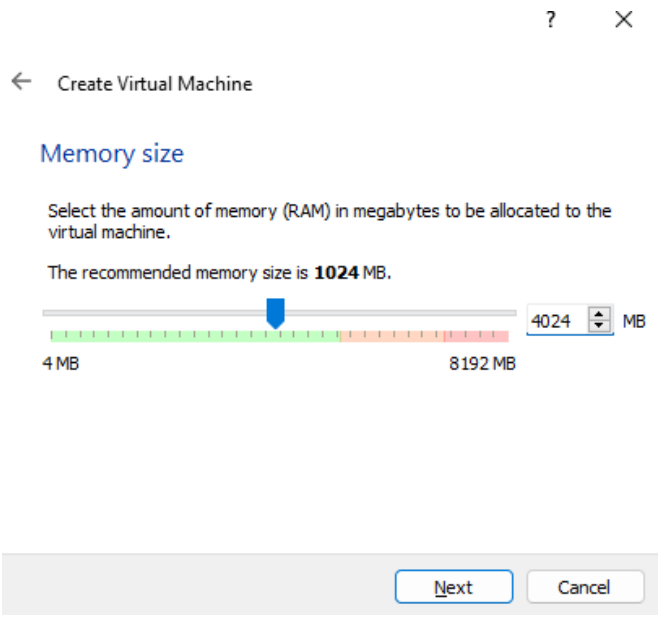


Figure 5.3: *Preferred Memory Size*

On the memory size, it is advised that it should be more than 4024 for this system as it need a lot of spaces to be able to run the system smoothly.

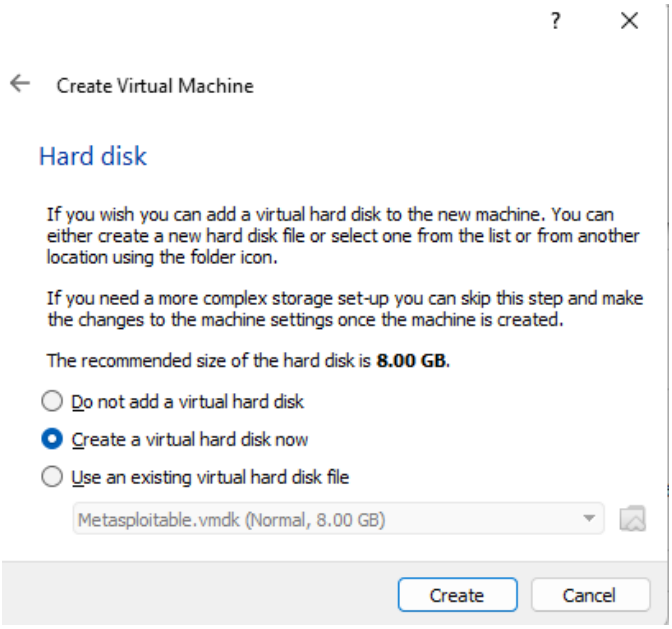


Figure 5.4: *Virtual Hard Disk set up*

Next, the hard disk we choose "create a virtual hard disk now", the Virtual hard disk will eventually hold all the data for the virtual machine.

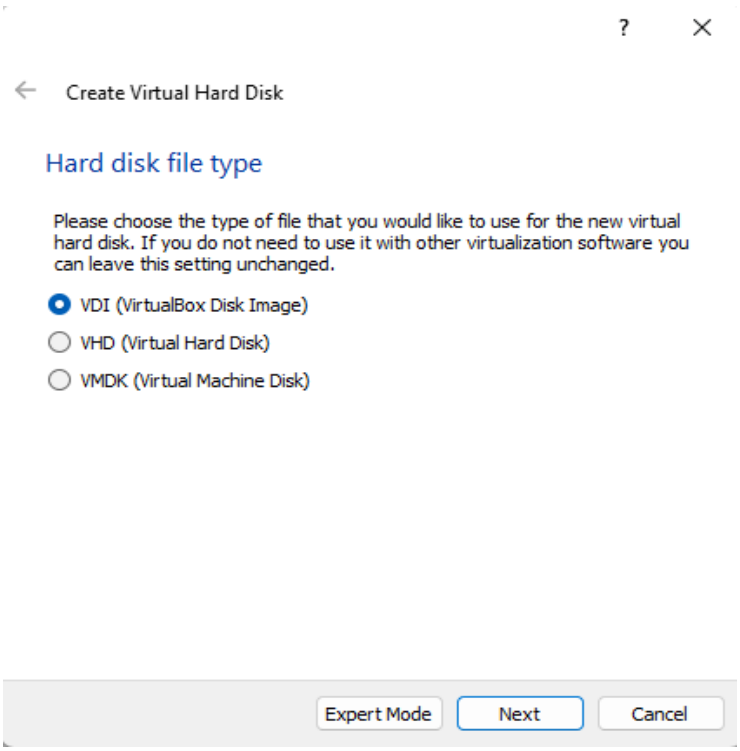


Figure 5.5: *types of Hard disk file*

For the hard disk file type, select VDI as the hard disk file type for this system.

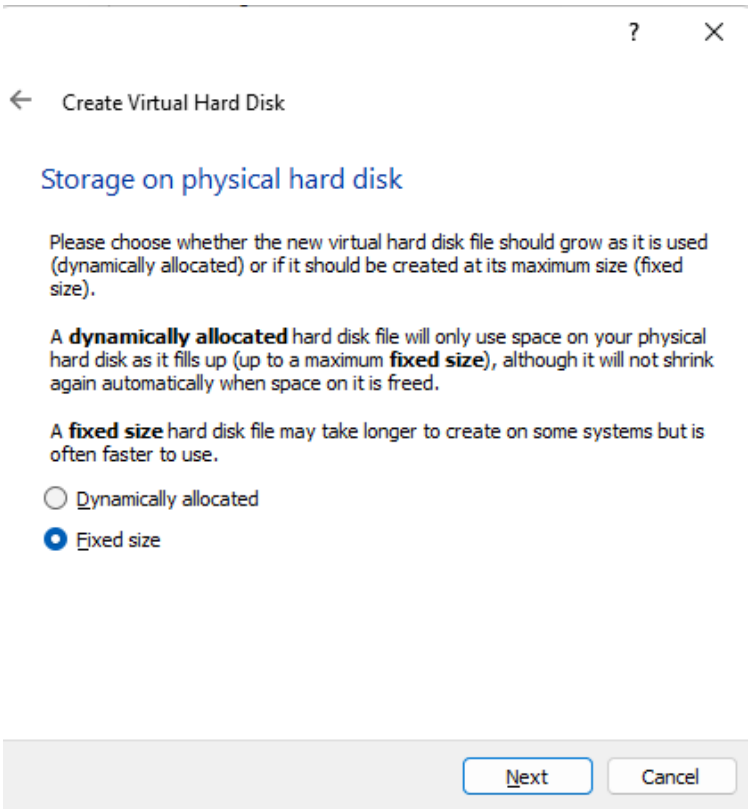


Figure 5.6: *Fixed Size for VDI*

Fixed Size is chosen for the method storing on physical hard disk. Click next to proceed.

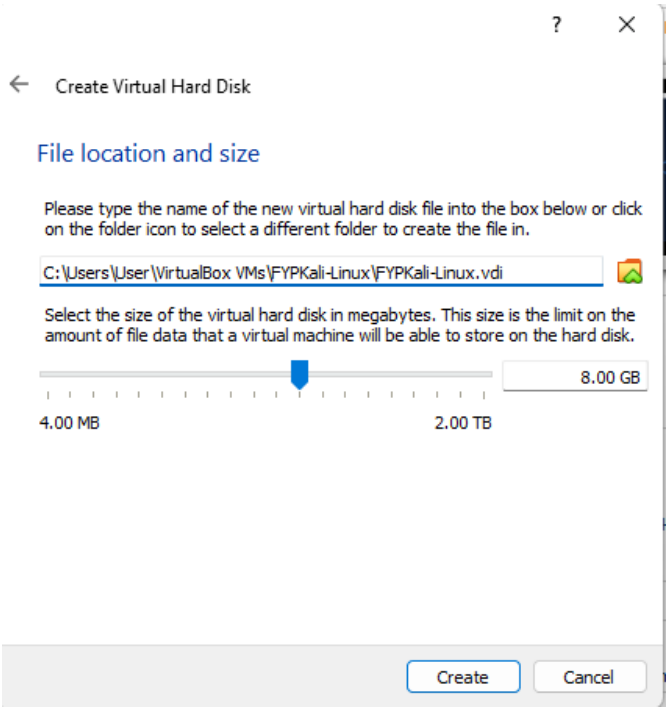


Figure 5.7: *File location and Preferred size*

On the file location and size, specify the location and maximum size of the new virtual harddisk system and then “create”.

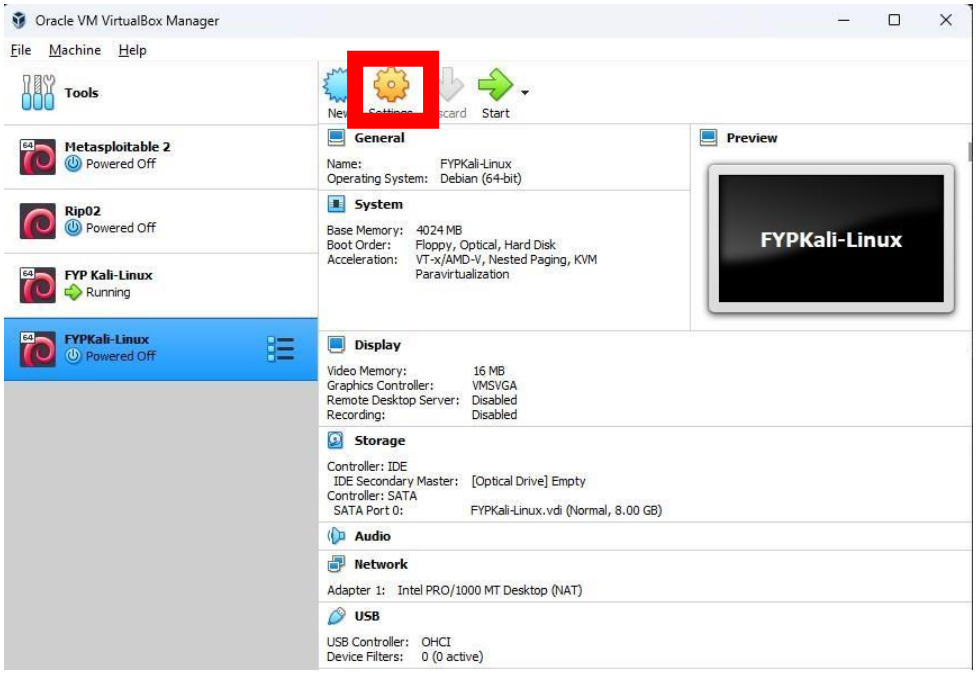


Figure 5.8: *Oracle VM Virtual Box setting*

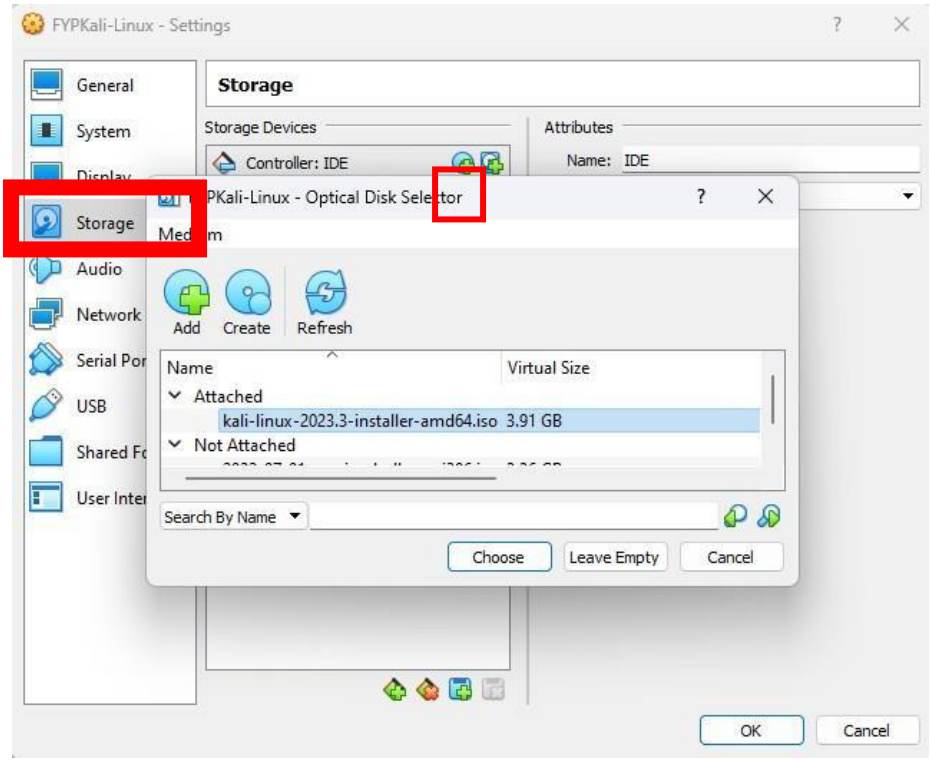


Figure 5.9: *Storage disk file*

After successfully creating the new virtual machine, go to setting -> storage -> adds opticaldevice, then click “ok” once choose the right file for the optical device.

5.3.2 Kali-Linux Virtual Machine installation

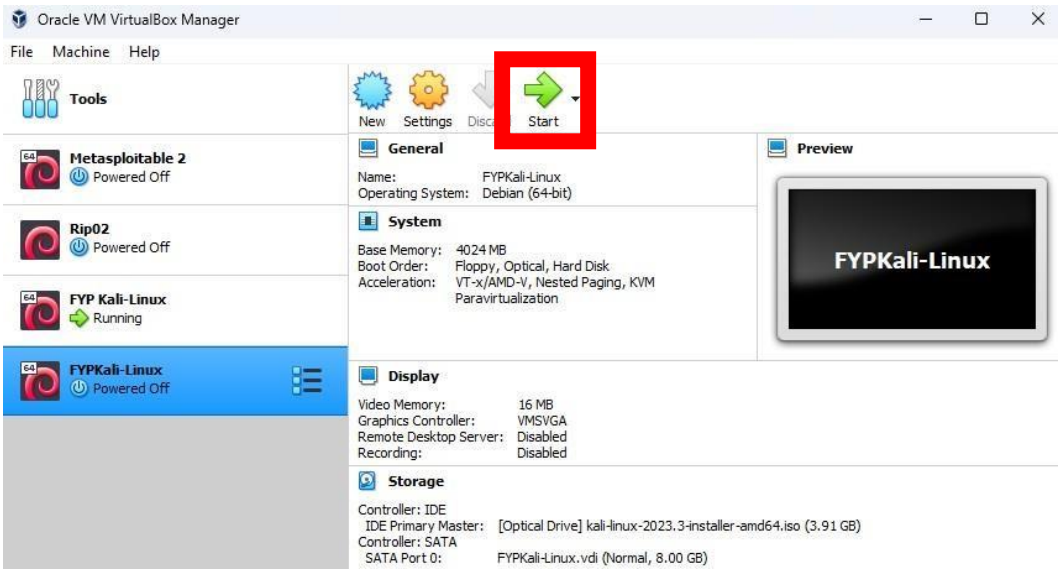


Figure 5.10: *Oracle VM Box start*

Start the VM by clicking the start button in the oracle VM VirtualBox, this action will boot the from the ISO file.

Figure 5.11: *Kali Linux installer menu*

After greeted by this Kali-Linux Boot screen, choose Graphical Install to have better visualization for the Linux Operation System.

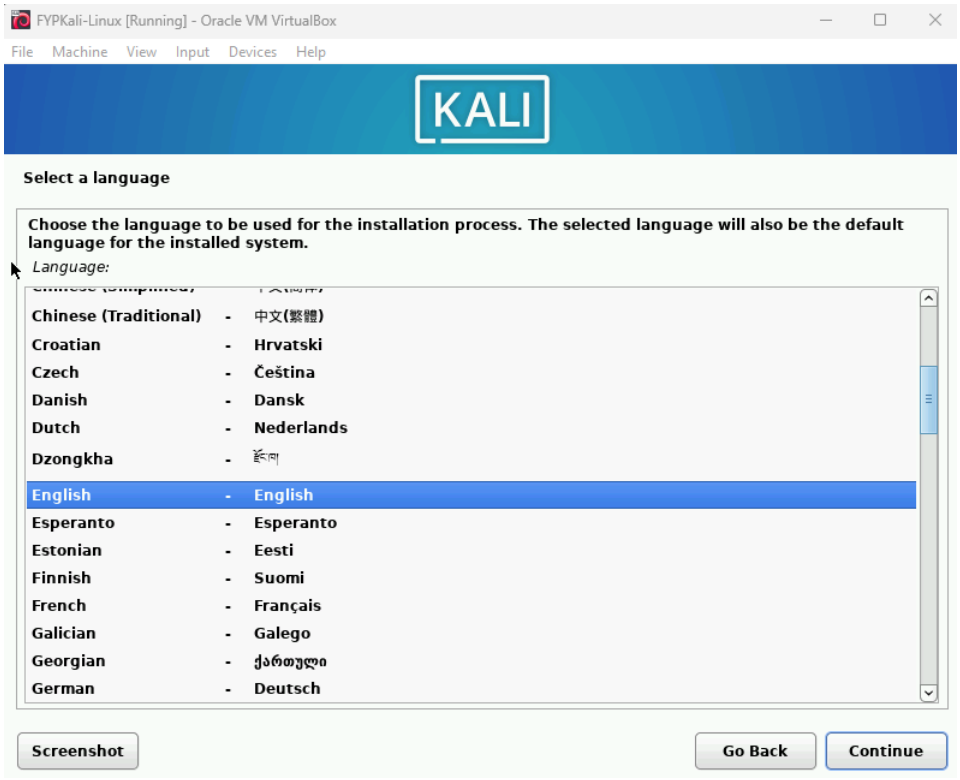


Figure 5.12: *Select a language*

Select preferred language, the language chosen will be used in setup process once confirm, in this case English will be chosen.

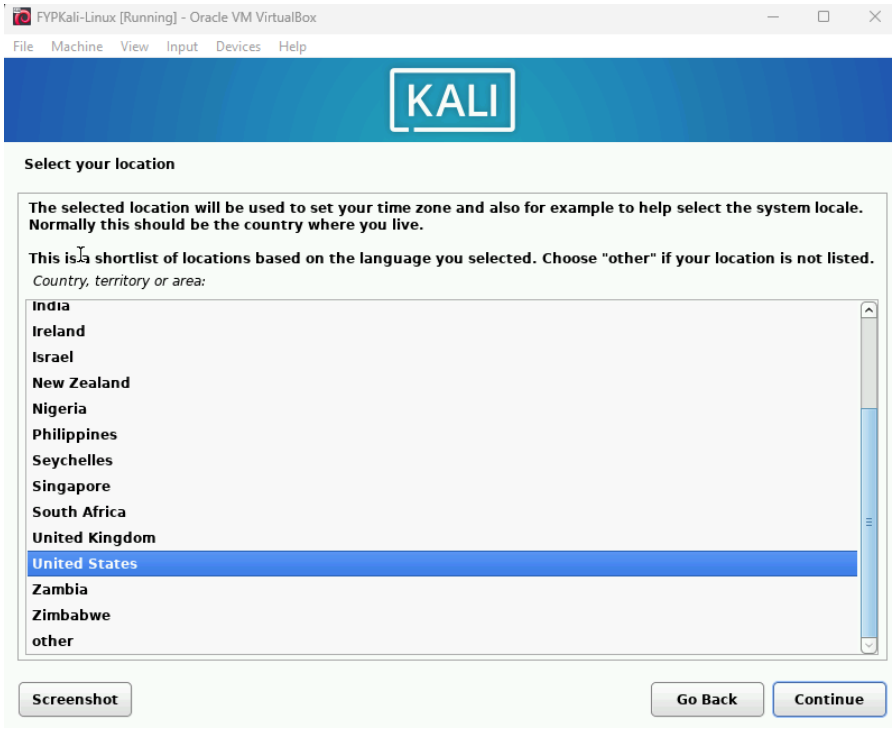


Figure 5.13: *Select your location*

Provide the specific geographical location of your residence.

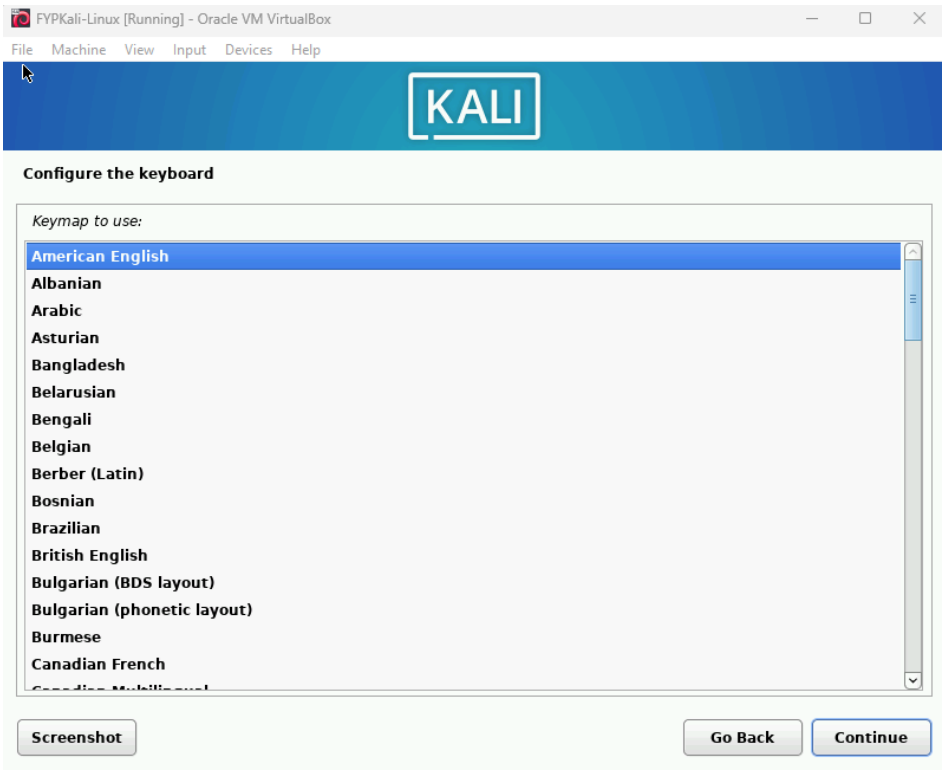


Figure 5.14: *Configure the keyboard*

Choose your preferred keyboard layout, in this case American English keyboard layout is chosen.

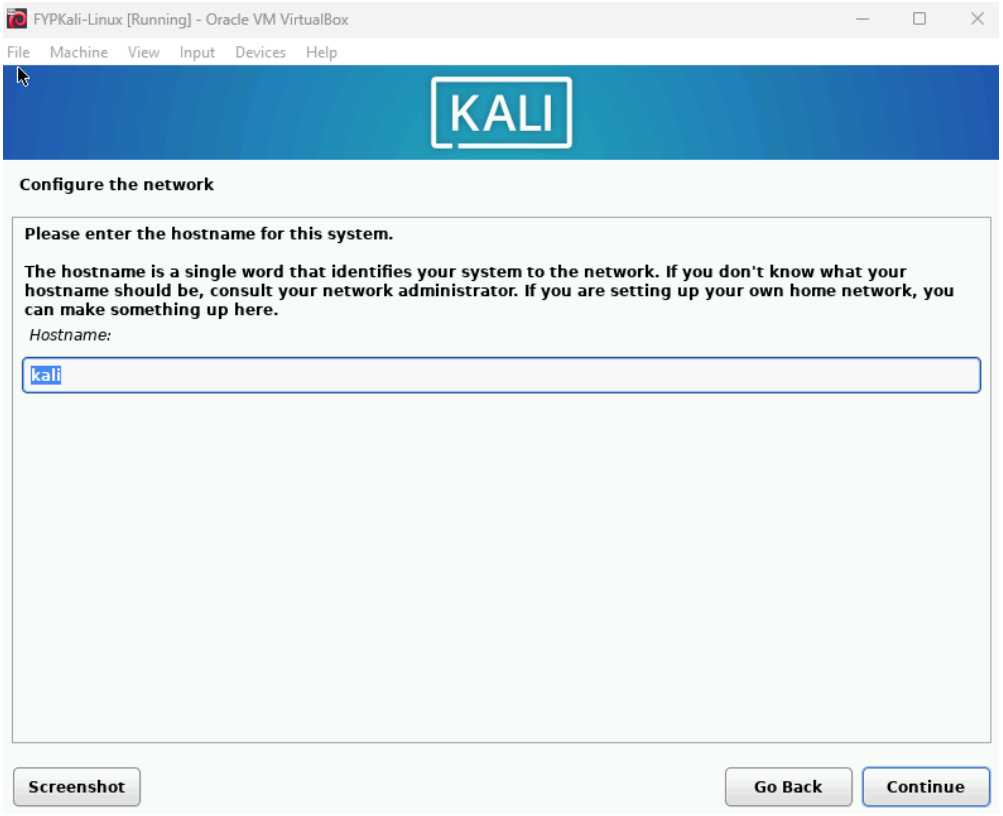


Figure 5.15: *Configure the network* 1

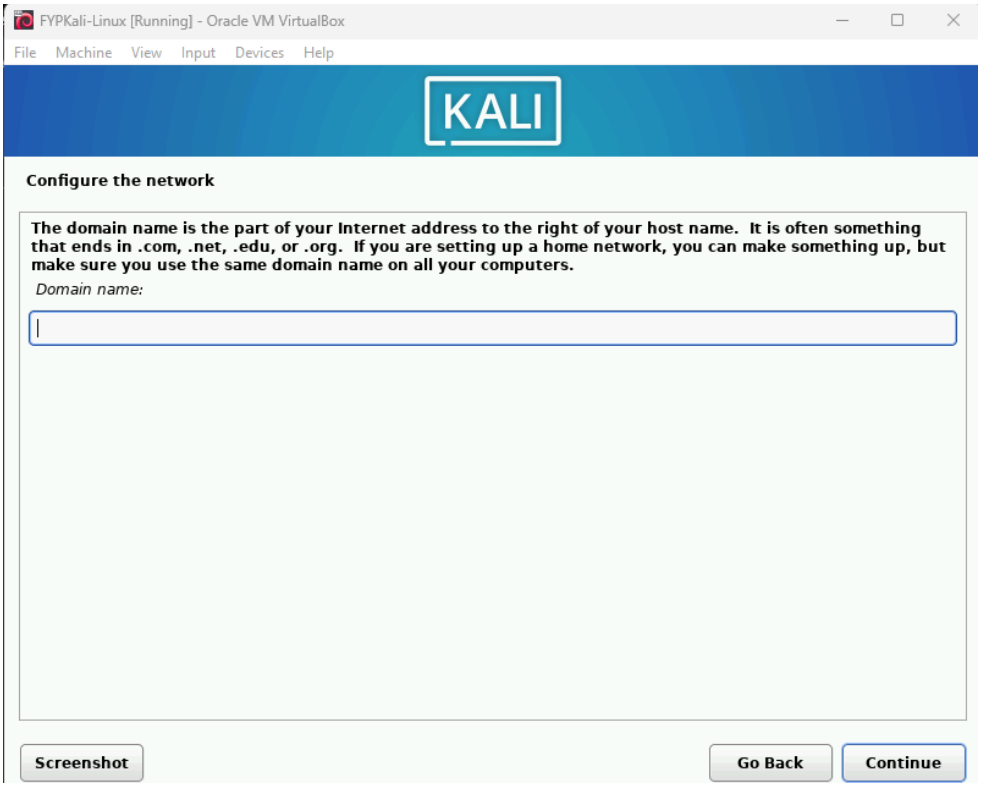


Figure 5.16: *Configure the network* 2

The current configuration will proceed to examine the network interfaces, search for a DHCP service, and subsequently request the user to provide a hostname for their machine. In the given illustration, the chosen hostname is "kali".

In this scenario, the absence of a DHCP service on the network necessitates my decision to refrain from proceeding.

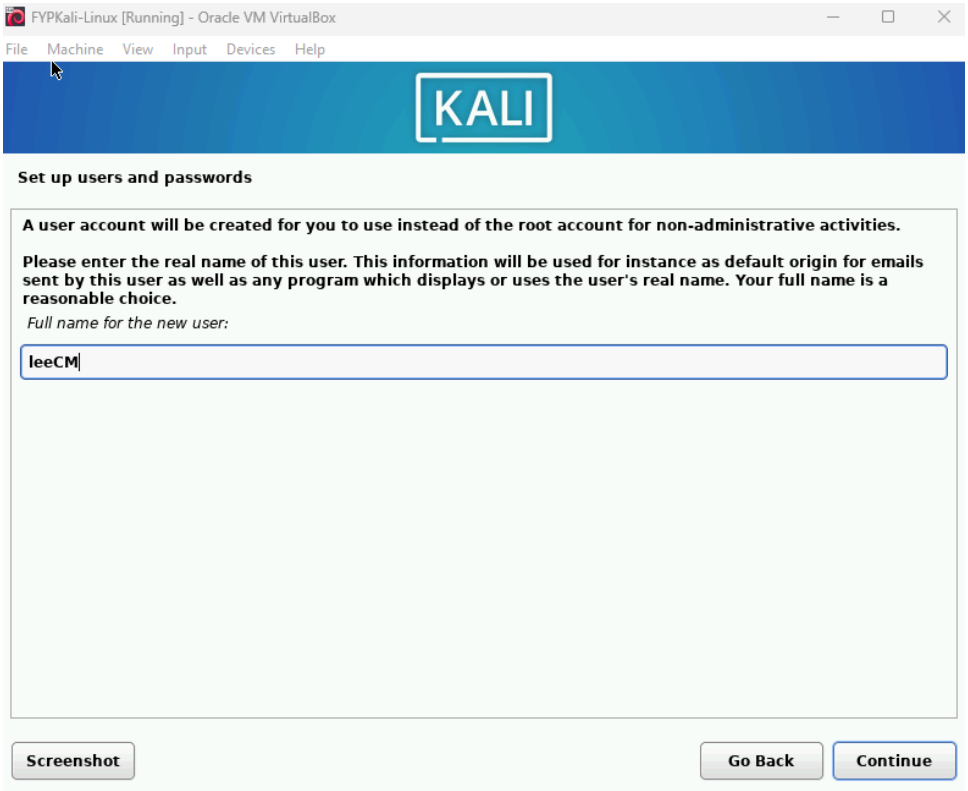


Figure 5.17: *set up username*

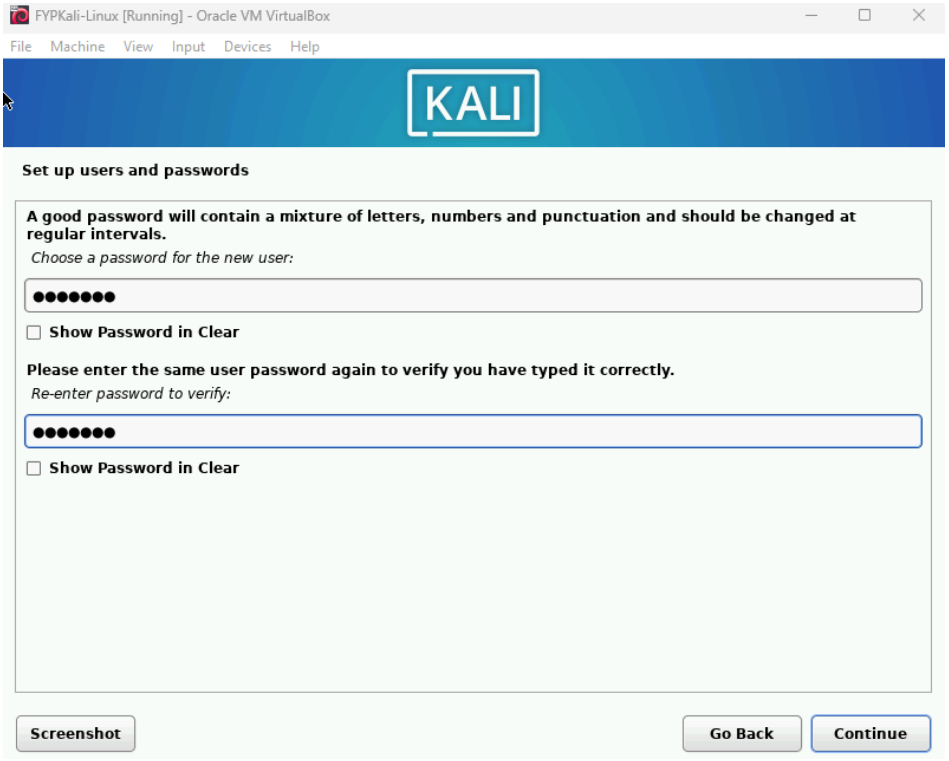


Figure 5.18: *set up password*

Subsequently, proceed to generate the user account within the system, encompassing the individual's whole name, a unique username, and a robust password.

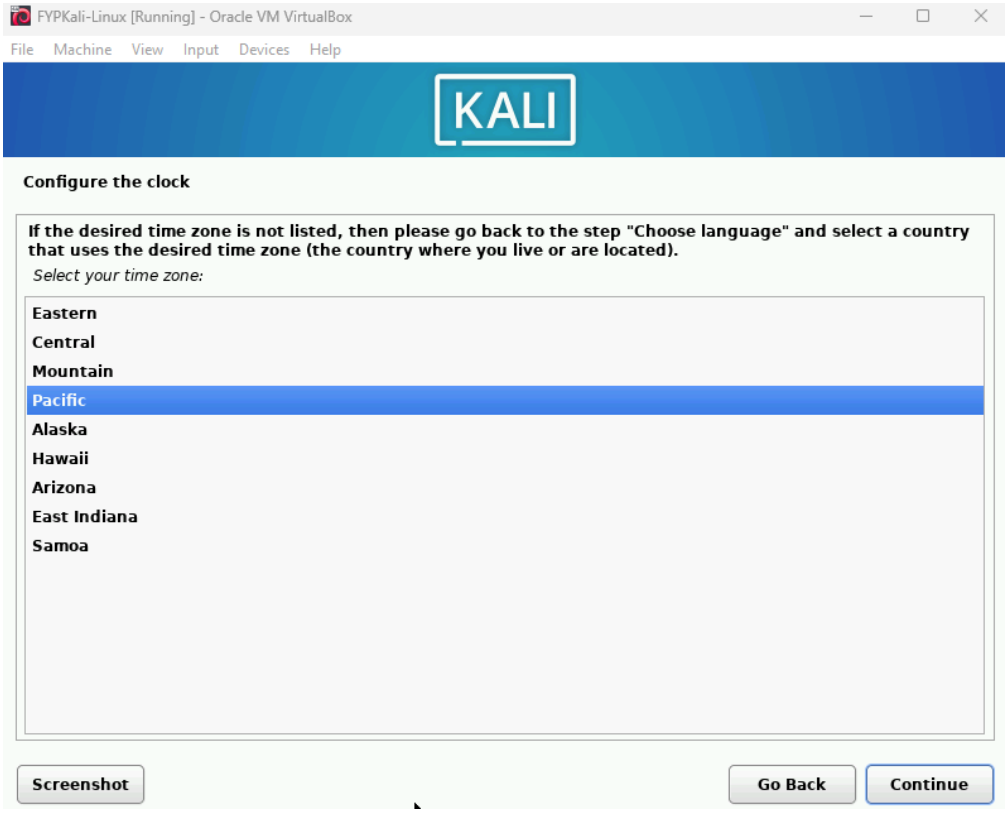


Figure 5.19: *Congfigure clock*

Select the time zone.

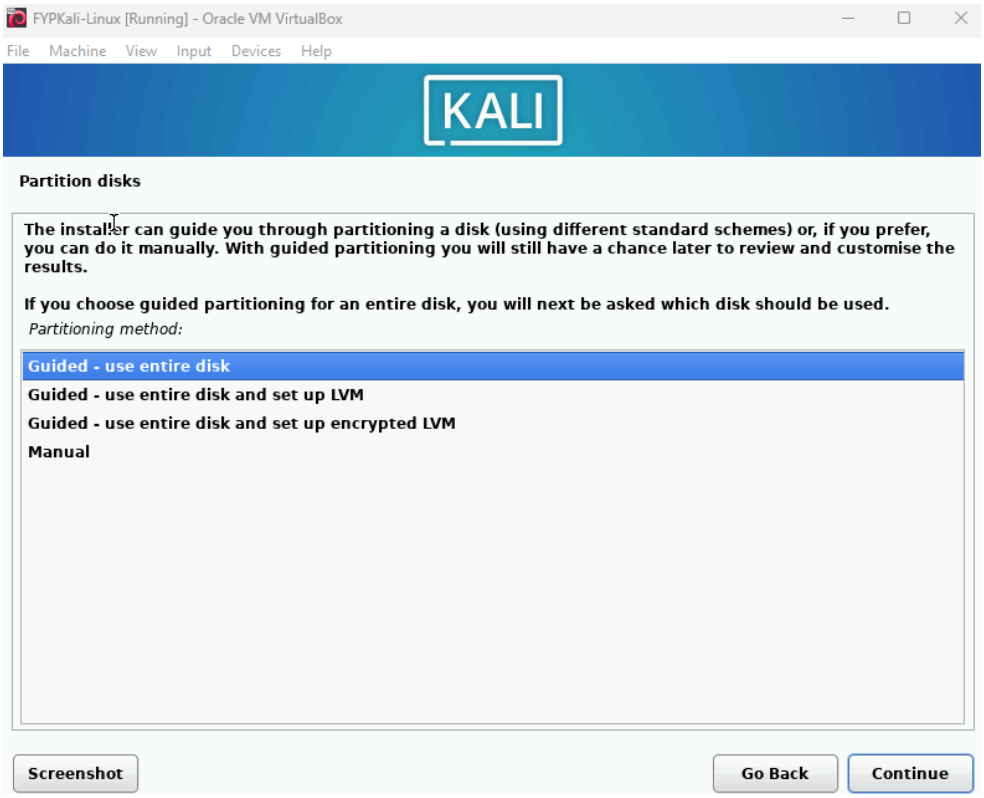


Figure 5.20: *Partition Disk* 1

The installer will proceed to examine the disks and present a range of options based on the specific configuration. In the present scenario, we are utilizing an unblemished disk, hence presenting us with a selection of four alternatives to choose from. The option of selecting "Guided - the entire disk" will be chosen for the installation of Kali Linux, since it is intended to be the sole operating system. Consequently, there is no desire to retain any other operating systems, and so, the disk will be completely erased.

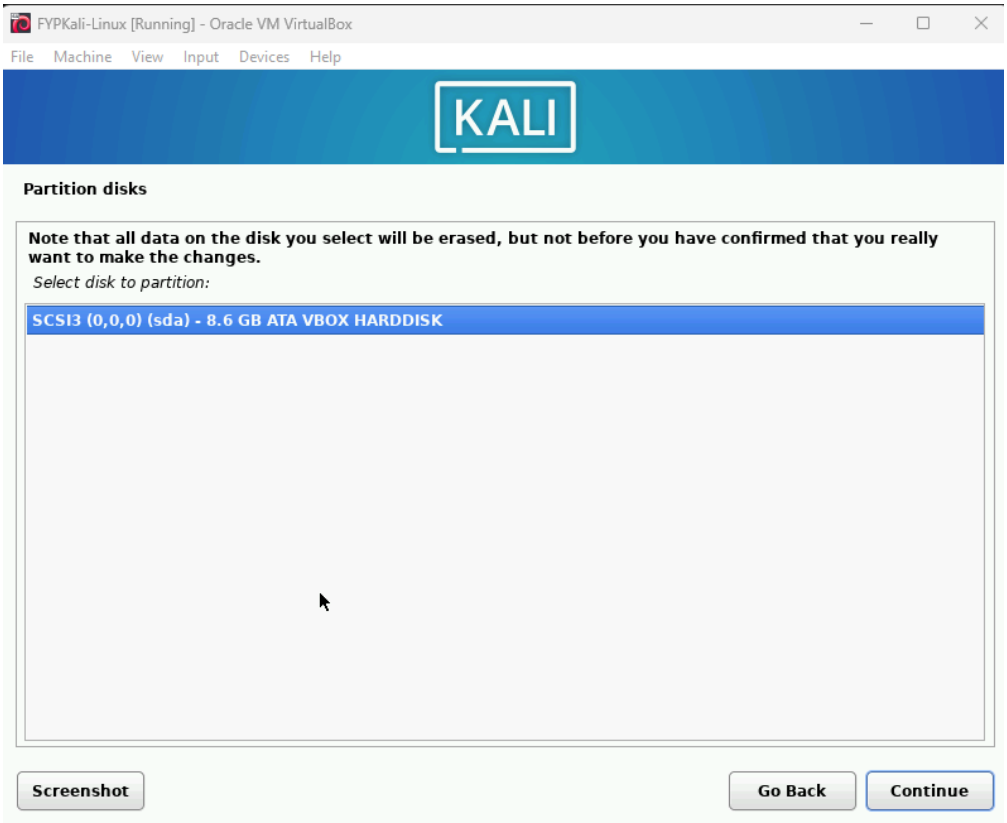


Figure 5.21: *Partition data* 1

Please choose the disk that will be partitioned.

Depending on the individual's requirements, they have the option to retain all their files within a singular partition, which is the default setting, or alternatively, they can opt for distinct partitions for one or more of the primary folders.

If the user is uncertain about their preference, the recommended option would be to select "All files in one partition."

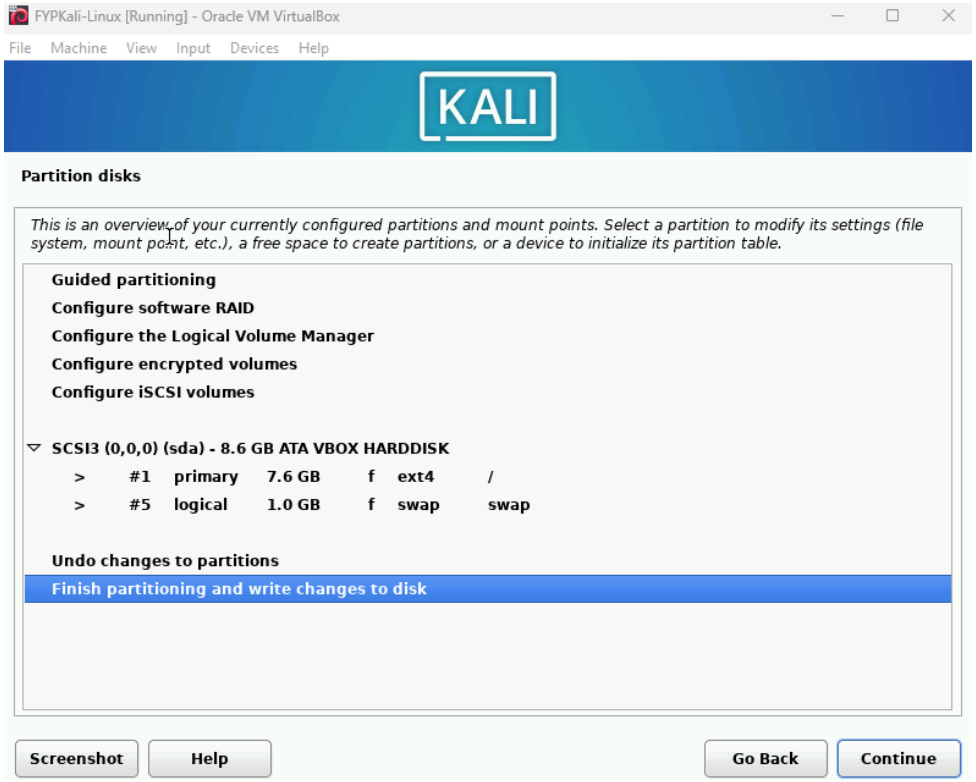


Figure 5.22: *Partition data* 2

Subsequently, the user will be provided with a final opportunity to thoroughly examine the disk configuration prior to the commencement of the installation process, during which any modifications made will be permanent and cannot be undone. Once the user clicks on the "Continue" button, the installer will commence its operations, resulting in an installation that is nearly complete.

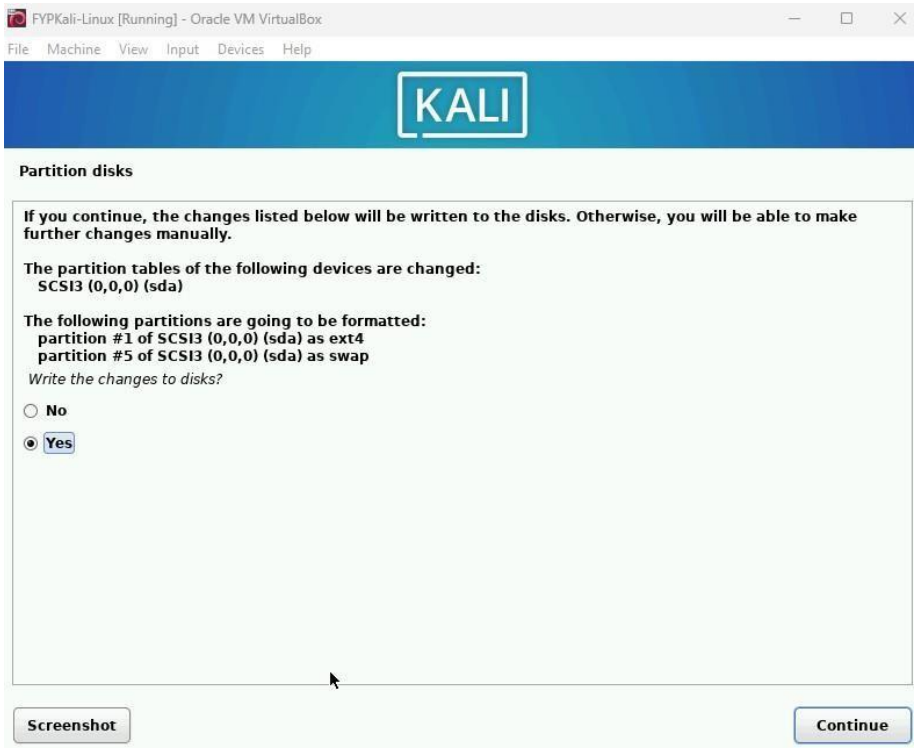


Figure 5.23: *Partition disks* 2

Next confirm to install the GRUB boot loader.

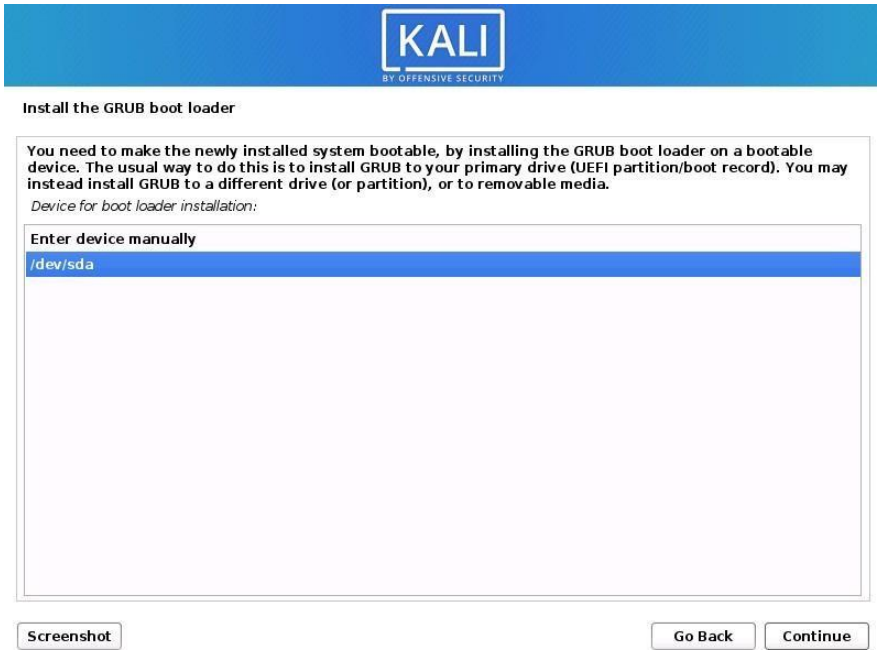


Figure 5.24: *GRUB bootloader*

Choose the hard disk on which you would like to install the GRUB bootloader. By default, the installation process does not automatically select any drive.

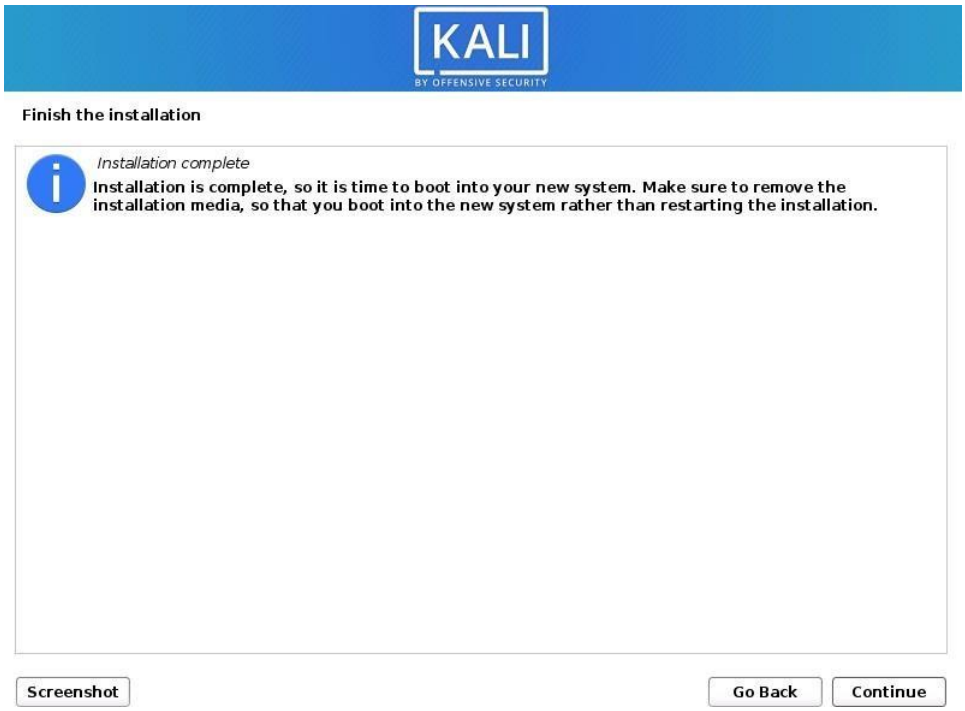


Figure 5.25 *Installation*

Lastly, proceed to select the "Continue" option in order to initiate the reboot process, so facilitating the transition into the newly installed Kali Linux operating system.

This section will present screenshots of the output illustrating the capabilities of the current system prototype. The prototype primarily focuses on scanning and detecting, followed by determining the presence of rogue access points by displaying probable RAP network information. Another finished function is the exit function, which displays an animation to signify the termination of the system and afterwards clears the screen.

5.4 System Operation

This section will provide a detailed snapshot of the system behavior for the scenarios where no RAPs are discovered and where possible RAPs are detected with the tracking funciton.

5.4.1 Interface

Figure 5.26 RAG System Interface

The Figure above shows the System main menu, when user lunch the python code of the Rouge Access Point detection and tracking system. It displays the name of the system, author's name, versions and the options for each function.

5.4.2 Scenario with no RAPs

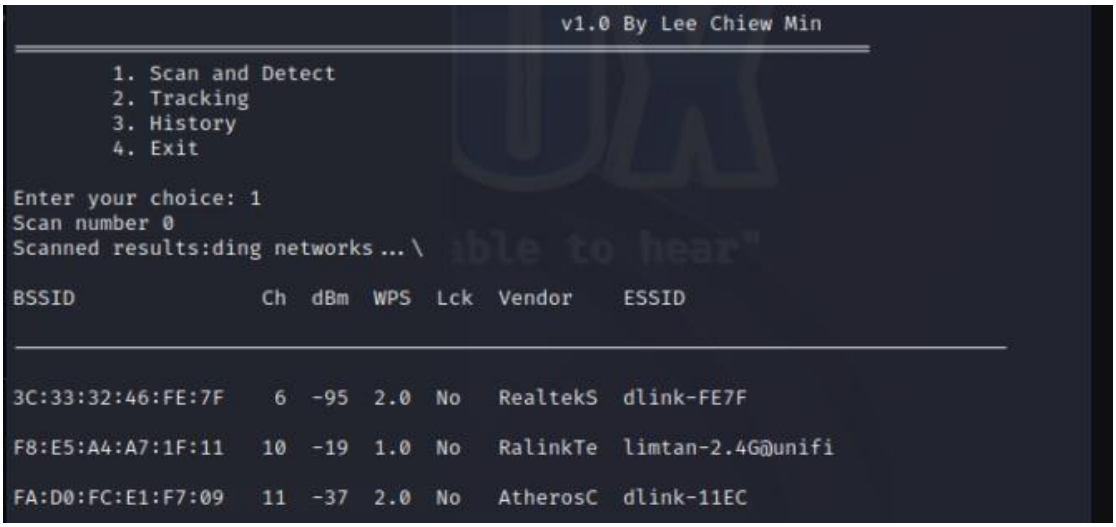


Figure 5.27 Scan and Detect function

As depicted in Figure 5.27, when the user selects option 1, "Scan and Detect," the system initiates a scan event, commencing from 0. The scanning process typically requires approximately 20 seconds to complete and display the results.

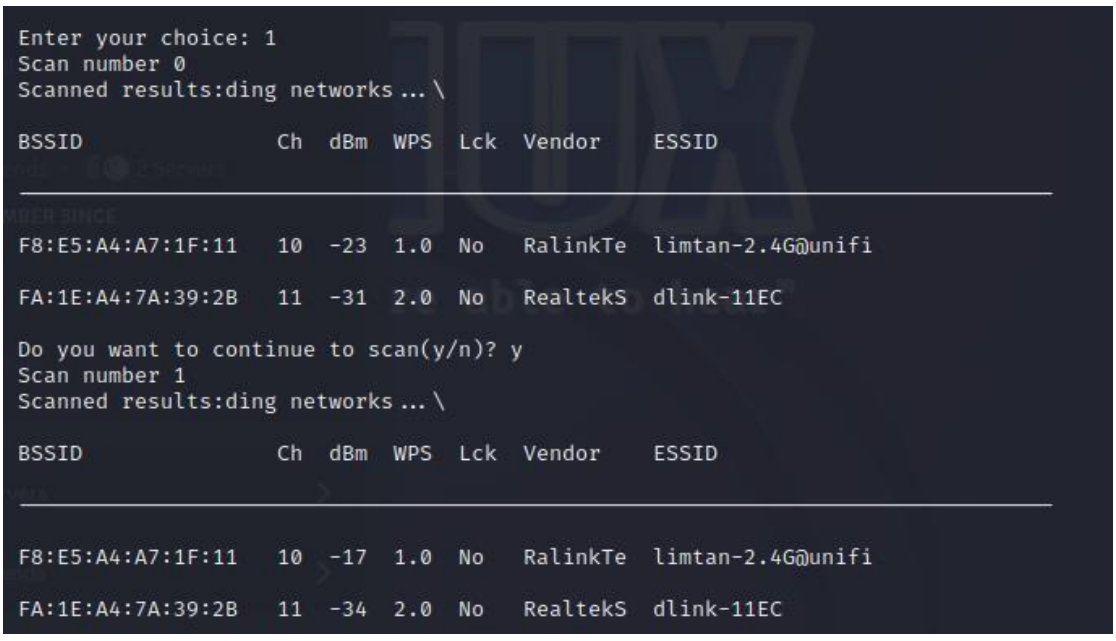


Figure 5.28 Scan Result and continue scanning

Figure 5.27 illustrates the user's decision to continue scanning by confirming with the input 'y'. Subsequently, the scanning process repeats, following the same procedure as before.

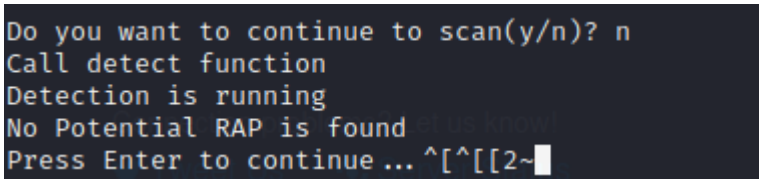


Figure 5.29 Scan Result without RAP

Figure 5.28 depicts the scenario where the user opts not to initiate a rescan and proceeds with the detection process by comparing the results of the BSSID and SSID scanned and stored inside output.txt with the whitelist.txt file. In this instance, since no rogue access points (RAPs) have been identified or added to the whitelist, the system does not detect any potential RAPs and shows “No Potential RAP is found”.

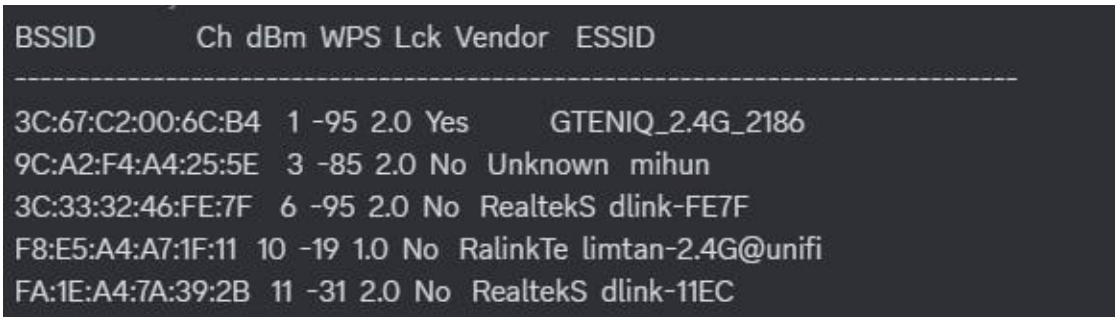


Figure 5.30 output. txt without RAP

Figure 5.29 displays the contents of the output.txt file, where it confirms the legitimacy of the "dlink-11EC" access point based on its BSSID matching an entry in the whitelist. This indicates that the system has identified "dlink-11EC" as a legitimate access point because its BSSID matches an entry in the whitelist file, affirming its authorized status within the network.

5.4.3 Scenario with RAP

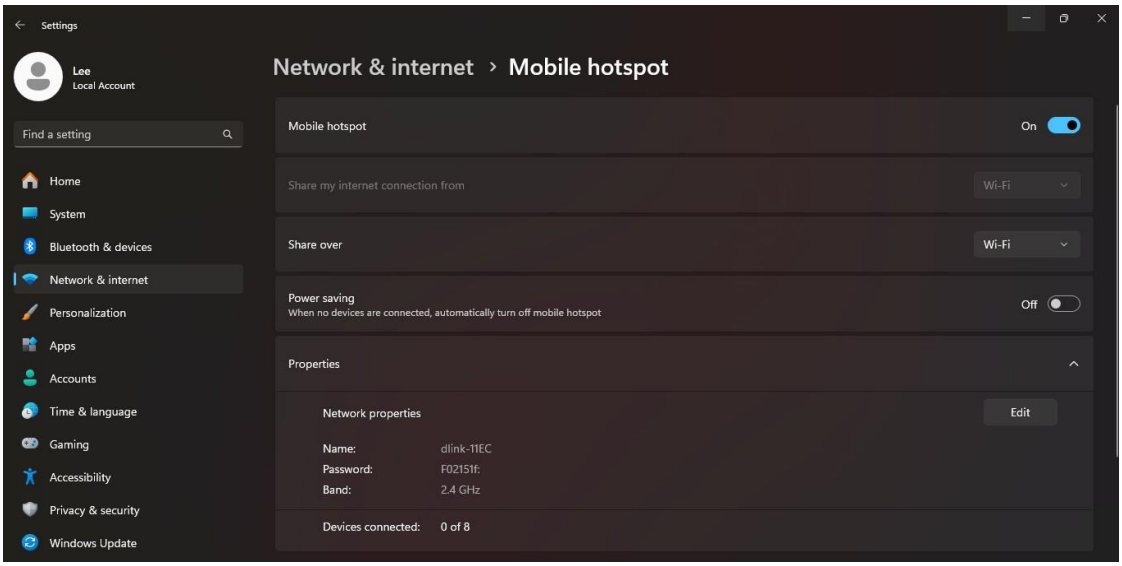


Figure 5.31 Setting up RAP

For this section, the system's detection capabilities are tested with the creation of a rogue access point (RAP) having the same BSSID ("dlink-11EC") as depicted in Figure 5.30. This scenario is designed to assess how the system handles the presence of a rogue access point with an identical BSSID to that of a legitimate access point listed in the whitelist. The system's ability to differentiate between authorized and unauthorized access points based on the BSSID match will be evaluated to determine its effectiveness in detecting and flagging rogue devices within the network.

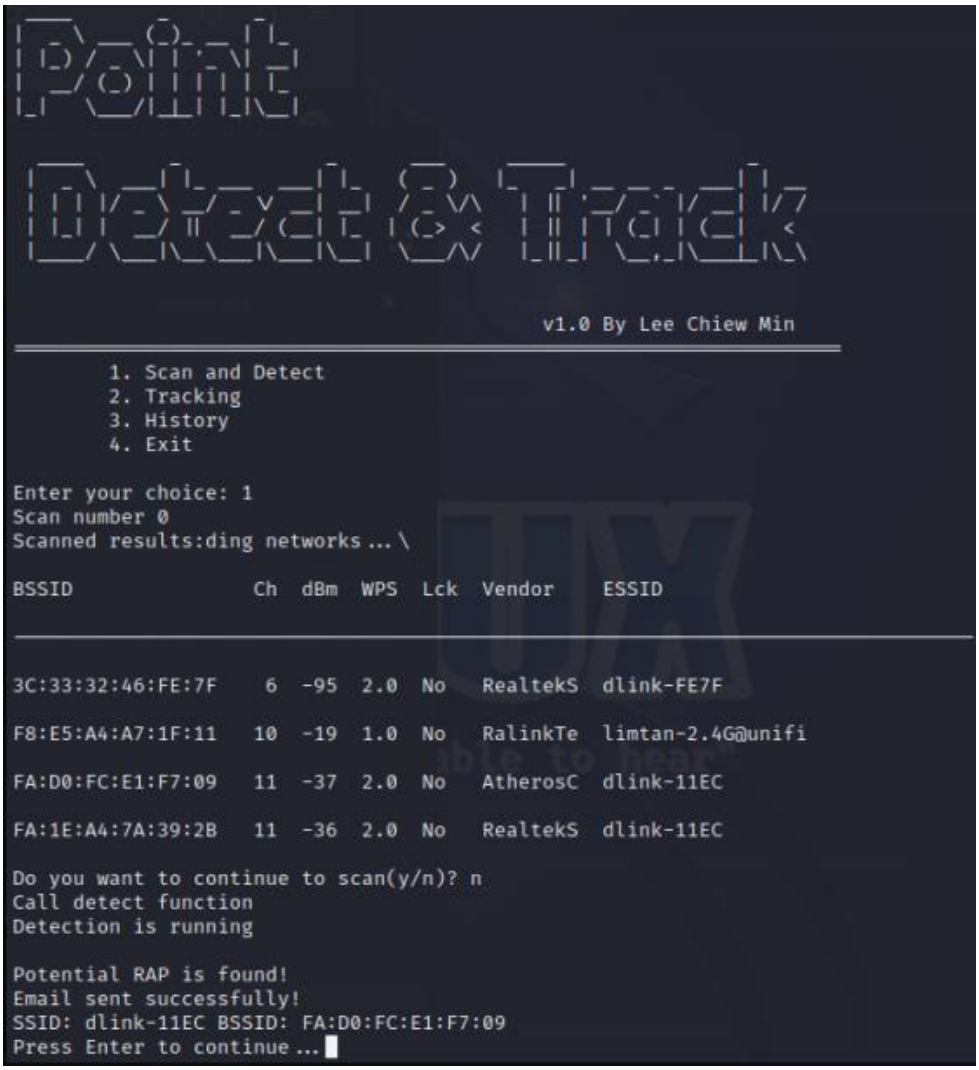


Figure 5.32 Scanning Result of RAP

As depicted in Figure 5.31, the user selects the "Scan and Detect" option to inspect for rogue access points (RAPs), with the RAP already set up. The system successfully detects the RAP since in the detection function the comparison of the BSSID and SSID of both network is done and displays detailed information including the SSID (Service Set Identifier) and BSSID (Basic Service Set Identifier) associated with the detected RAP. This outcome demonstrates the system's ability to identify and report the presence of rogue access points within the network environment.

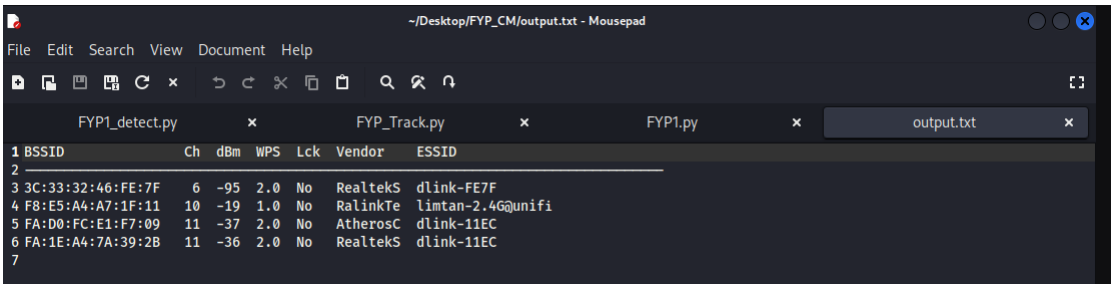


Figure 5.33 Output. txt 2 (RAP set)

The output shown in the figure above (Figure 5.31) demonstrates the content of the output.txt file, which confirms that the scanning process has successfully detected both networks with the SSID "dlink-11EC". This result indicates that the system is capable of identifying and distinguishing multiple instances of the same SSID, likely associated with different BSSIDs (Basic Service Set Identifiers), thereby providing detailed information about each detected network during the scanning operation.

Figure 5.34 Email Alert

As depicted in Figure 3.3, an email has been sent to the system administrator notifying them of an urgent issue that requires immediate attention. This email serves as a prompt for the network administrator to take swift action in response to the detected security threat or system event.

5.4.4 Tracking Rouge Access Point

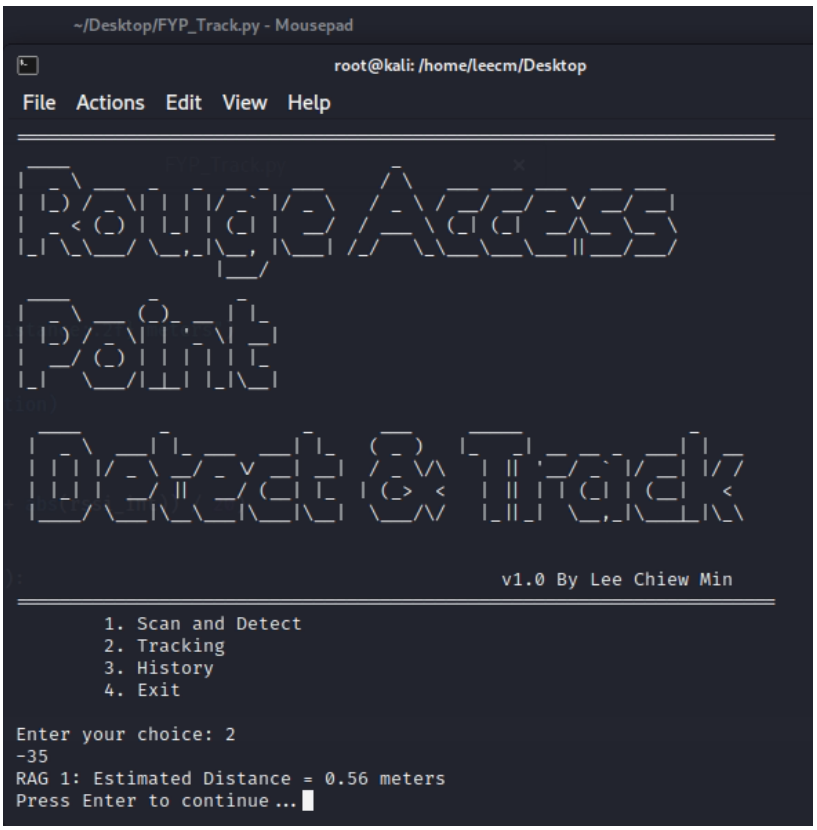


Figure 5.35 Tracking Result

Figure 5.35 illustrates the estimated distance between the user and the Rogue Access Point (RAP) based on the system's signal strength calculations. This estimation is a key aspect of the system's functionality, enabling it to assess the proximity of the user to detected RAPs within the network environment. The estimated distance is determined using the Received Signal Strength Indicator (RSSI) measurements obtained during the scanning process.

The distance estimation process is crucial for understanding the potential threat posed by detected RAPs. By accurately estimating distances, the system can evaluate the risk level associated with rogue devices and prioritize response actions accordingly. This information provides valuable insights into the spatial distribution of RAPs relative to the user's location, aiding in the implementation of effective security measures and threat mitigation strategies.

5.5 Implementation Issues and Challenges

Throughout the project, a significant challenge has been the realization that achieving perfect detection of all rogue access points in every conceivable scenario is an impractical goal. This complexity arises from the vast array of potential scenarios involving rogue access points, including sophisticated attacks such as man-in-the-middle attacks, evil twin attacks, or insider threats. As technology evolves, attackers are continually devising more complex strategies to evade current detection systems. In the current phase of development, our technology has been refined to the best of its ability to detect rogue access points within specific circumstances. However, it's important to acknowledge that our current solution may not comprehensively cover all potential scenarios. Our project plan recognizes the need for ongoing development efforts to enhance the current prototype into a more flexible and robust solution. This iterative approach ensures that our system evolves to effectively detect rogue access points within the UTAR campus environment, addressing emerging threats and evolving attack vectors over time. The goal is to continuously improve the system's capability to adapt and respond to new challenges, ensuring the security and integrity of the network infrastructure at UTAR.

CHAPTER 6

System Evaluation and Discussions

This chapter will include system testing across several networks, as well as detailed discussions on project challenges and objective evaluation.

6.1 System Evaluation

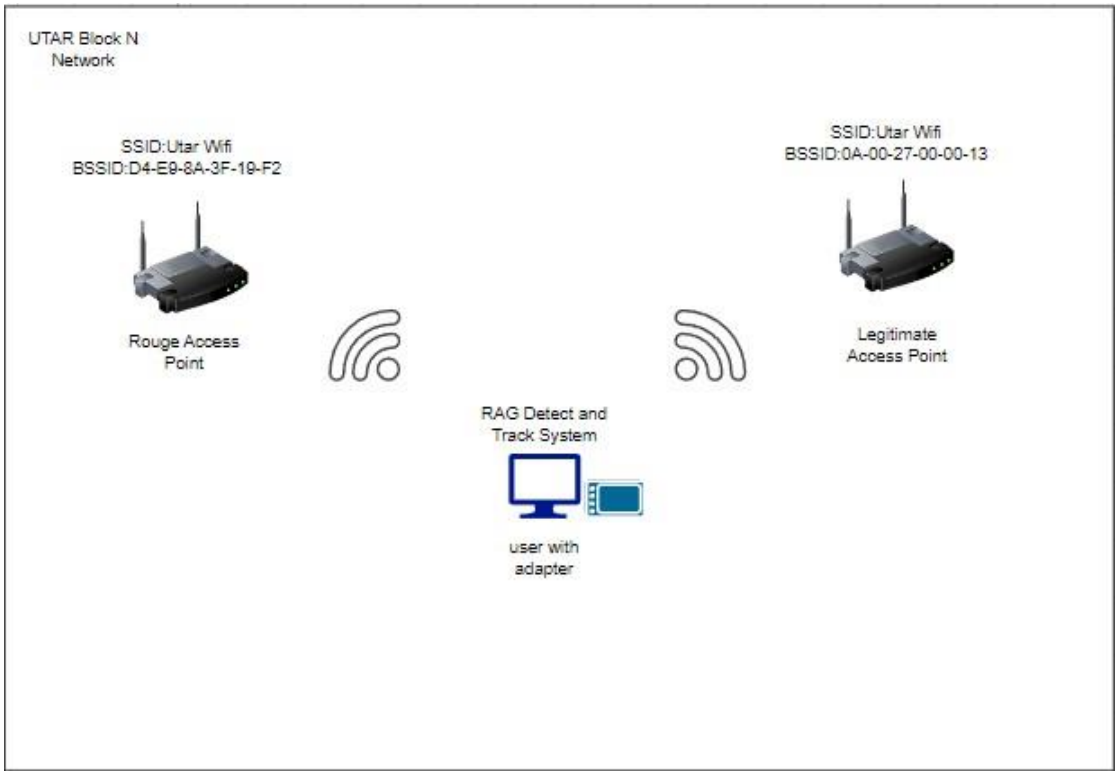


Figure 6.1 Example of System Testing Topology

To ensure the effectiveness and practicality of the Rogue Access Point Detection and Tracking System within the UTAR campus environment, comprehensive testing and evaluation were conducted across distinct network scenarios. The system's performance was assessed primarily within the UTAR network, representing a typical educational institution's network setting characterized by diverse device connections, variable network traffic patterns, and potential security vulnerabilities. Additionally, testing was conducted in a residential home local area network to gauge the system's adaptability in a smaller, residential network environment with unique usage patterns and security considerations.

Key metrics were analyzed to evaluate the system's performance and suitability:

- Detection Reliability: The system's ability to accurately identify rogue access points (RAPs) amidst legitimate access points was tested using known whitelist information. Detection accuracy was assessed across varying network conditions and configurations to ensure robust performance.

- Response Time: The system's responsiveness, from initiating a scan to detecting and reporting potential rogue access points, was measured to assess its efficiency in real-time threat detection.

- Scalability: The system's scalability was evaluated to determine its capacity to handle a large number of connected devices and network traffic typical of an educational institution environment.

- Resource Utilization: Resource consumption, including CPU and memory usage, was monitored to ensure optimal performance without excessive resource utilization.

- Incident Handling: The system's incident handling capabilities were assessed to evaluate its effectiveness in notifying administrators of detected rogue access points and initiating appropriate response actions.

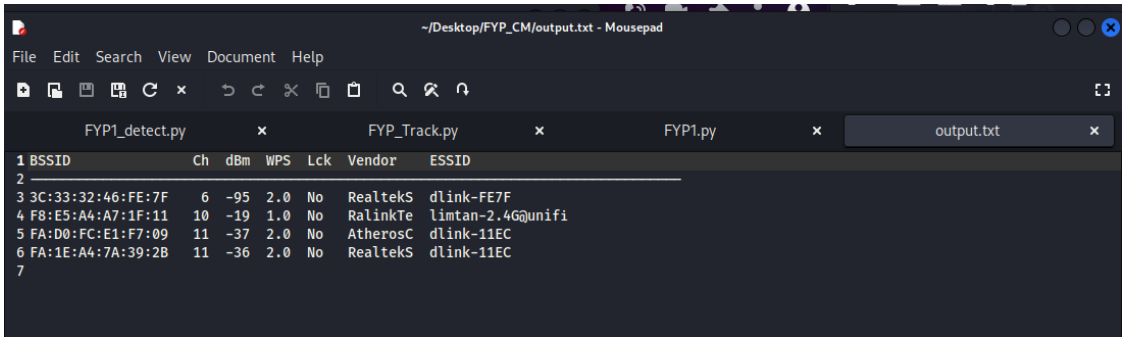
The testing approach involved deploying the system with USB/wireless adapters within specific UTAR campus blocks, focusing on Block N as a representative testing area. A comparative analysis between the UTAR network and a residential network provided valuable insights into the system's adaptability and performance across diverse network environments.

By conducting rigorous testing and analysis based on these metrics, the evaluation aims to validate the system's effectiveness in detecting and tracking rogue access points within the UTAR campus, addressing specific challenges and requirements unique to educational institution networks. This evaluation will inform future

enhancements and optimizations to further improve the system's capabilities and deployment readiness.

6.1.1 Detection Reliability

Detection reliability of the RAP in different network environments should be evaluated to assess how well the system works. It should measure the system’s ability to accurately detect possible RAPs using a comparison of SSID-BSSID combinations for whitelisted pairs. Detection rate should be tested there has to be estimation of number of actual RAPs and number of those which have been recognized correctly by the system. There also should be false positive rate – correct access points have been detected as RAPs and false negative rate – RAPs that have not been detected. False positive and false negative rates should be tested under different scenarios and how they depend on the network configuration. This testing should show how well the system can differentiate between RAP and right ap under different circumstances. As mentioned, to test how reliable the system here will provide some testing with the Access point with the SSID: dlink-11EC:



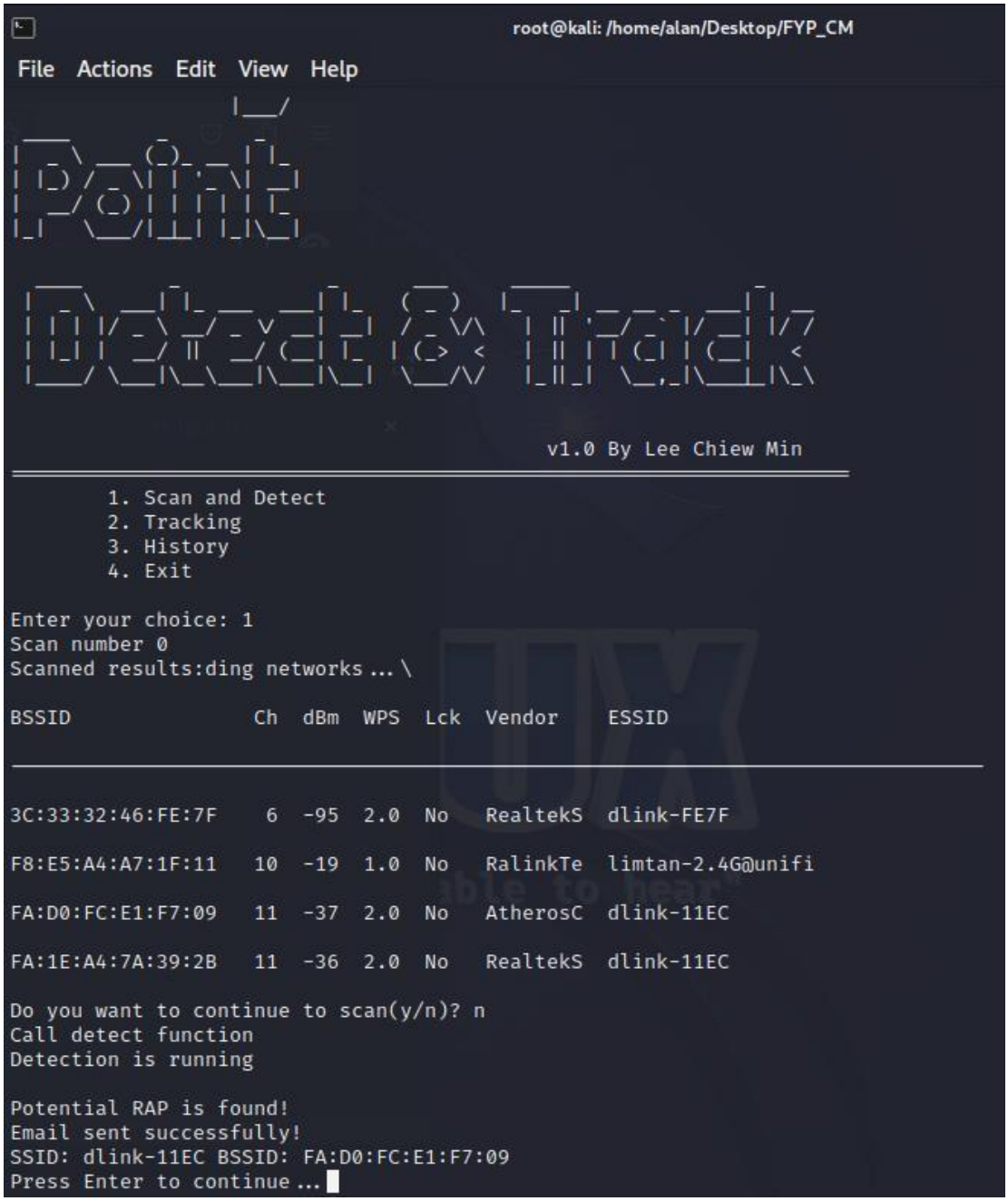


Figure 6.2 Scan result (RAG and legitamate setted up)

As shown above, the result of detecting the right AP and the RAP is successfully. However, there are concerns as the detection method is by using scanning tools/hardware of the user equipment and this might affect the scanning result based on the scanning efficiency and frequency it can received. Furthermore, as the system method is by using comparison between the scanned result's BSSID and SSID and in whitelist.txt, if it included a hole block of the legitimate AP available it might affect the efficiency of the detection.

6.1.2 Tracking Accuracy

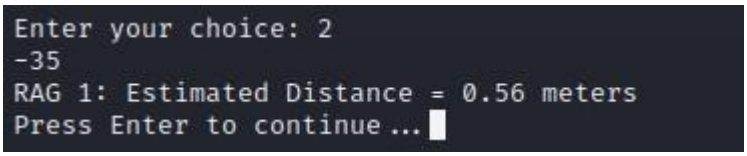


Figure 6.3 Track result

In the case of tracking accuracy, the system's efficiency in determining the locations of rogue access points (RAPs) during real-time operation is crucial. This process relies on utilizing Received Signal Strength Indicator (RSSI) computations to estimate the distances between the system and the detected RAPs. The tracking accuracy is evaluated based on how closely the estimated locations of RAPs align with their actual positions within the network.

The formula used for distance estimation based on RSSI readings is integral to this evaluation. The formula

$$d = 10\left(\frac{(27.55 - (20 \times log_{10}(f)) \pm |RSSI|)}{20}\right)$$

where:

- d represents the estimated distance between the system and the RAP in meters,
- f is the frequency of the Wi-Fi signal in MHz, in this system the frequency is set 2400.
- RSSI denotes the received signal strength indicator in dBm.

This distance estimation formula incorporates environmental factors such as

obstructions, interference, and signal propagation characteristics. The system's ability to accurately track RAPs is contingent upon minimizing the deviation between the estimated and actual locations of these rogue devices. By leveraging this formula and considering environmental conditions, the system can effectively assess its performance in identifying and tracking RAPs throughout the network.

6.1.3 Response Time

For the purpose of assessing how well the system detects and responds to Rogue Access Points (RAPs), the response time analysis is essential. It includes everything from starting a network search to finding and following a RAP in a 20-second scanning window.

- Network Scanning Duration: Each network scan lasts for the specified 20-second interval. This duration strikes a compromise between speed and resource economy, enabling the system to run numerous scans without taxing the capacity of the network. It's crucial to remember that system consistency and hardware dependability determine whether a scan is successful.

- Processing Scan Results: To find possible RAPs, the system examines the scan results once it has finished a network scan within the allotted period. The analysis of gathered data and decision-making based on found SSID-BSSID discrepancies when compared to the whitelist depend heavily on this processing time.

- Information Delivery to Users/Administrators: In the event that a RAP is identified, the system has to notify users or administrators right away. Initiating necessary responses to alleviate security risks provided by illegal access points requires completing this step.

- Response Time Variations: The response time analysis assesses the response times under various network loads and circumstances. This analysis contributes to confirming the effectiveness of the system in reliably

identifying RAPs in a variety of settings and use cases.

A 20-second scanning period has advantages, but hardware reliability may also have drawbacks. Hardware problems can occasionally cause scanning to fail, producing inconsistent or incorrect scan results. This restriction emphasizes how crucial it is to preserve system stability and hardware integrity in order to provide reliable performance and precise Rogue Access Point identification.

All things considered, the response time analysis offers insightful information about the system's capacity to identify and react to RAPs within predetermined time frames, pointing out areas in need of refinement and optimization to strengthen security protocols.

6.1.4 Security

Examine the security controls in place within the system to guard against possible intrusions and assaults. Analyze the system's capacity to protect private information, stop illegal access, and identify any unusual behavior that might point to malicious activity (such as man-in-the-middle attacks or illegal access attempts).

6.1.5 Incident Handling

The incident handling capabilities of the Rouge Access Point Detection and Tracking system play a critical role in effectively responding to security threats and mitigating potential breaches. When rogue access points (RAPs) are detected by the system, immediate incident response protocols are initiated to contain the threat and notify network administrators promptly. The primary objectives of the system's incident handling processes are to minimize manual intervention through automated alerts and response procedures.

- Automated Incident Notification: Upon detection of a rogue access point (RAP) by the system, an automated email notification is generated and sent to the designated network administration team at UTAR campus. This notification includes critical details such as the detected RAP's SSID, BSSID,

location estimate, and any relevant diagnostic information for swift response.

- Integration with Network Security Frameworks: The incident handling capabilities of the system integrate with established network security frameworks at UTAR campus. This alignment ensures compliance with regulatory standards and facilitates collaboration with external security teams or partners.

- User Training and Awareness: The system emphasizes user training and awareness programs to empower network administrators with the knowledge and skills needed to respond effectively to security incidents involving rogue access points. Training sessions cover incident recognition, escalation procedures, and best practices for incident containment.

By leveraging robust incident handling capabilities, the Rouge Access Point Detection and Tracking system enhances network security at UTAR campus, minimizes disruption caused by security incidents, and fortifies defenses against evolving threats posed by rogue access points. Continuous evaluation and refinement of incident response protocols are essential to maintain operational readiness and adaptability to emerging security challenges.

6.1.6 Usability

Usability evaluation examines the system's user interface design, navigation flow, and overall user experience. This assessment includes collecting user feedback through surveys or usability testing to identify areas for improvement in terms of user satisfaction and ease of use. Usability evaluation ensures that the system is intuitive, accessible, and user-friendly, enhancing user adoption and satisfaction.

By conducting a comprehensive evaluation across these dimensions, the system's performance, reliability, security, and usability aspects can be thoroughly assessed to guide further enhancements and optimizations. This evaluation framework provides valuable insights into the system's strengths, weaknesses, and areas for improvement

to ensure its effectiveness in detecting and tracking rogue access points within the UTAR campus network. As far as for now, the current system user interface is straight forward but the only downside would be the requirement of hardware and the user might need to have knowledge regarding with RAP and simple network knowledge to fully understand the output of the result of the system.

6.2 Project Challenges and Mitigations

Throughout the project, it discovered a challenge where there will be no system that can achieve perfect detection of all rouge access points all conceivable scenarios and impractical goals as the vast variety of scenarios involving rogue access points is just one reason for this complexity. The situations might be in the form of man-in-the-middle attacks, evil twin attacks, or insider attacks. Moreover, with new attack methods appearing as technology develops, more and more attackers are known to use more complex strategies to get beyond current detection systems. In the current phase of development, our technology is now developed to the best of its ability to detect rogue access points inside particular circumstances. However, it is important to recognize that it might not completely cover all scenarios. The project plan calls for more development work to improve the current prototype into a more flexible and complete solution. To ensure that the system develops are able to effectively detect rouge access points in the UTAR campus.

6.3 Objective Evaluation

The assessment standards for the Rouge Access Point Detection and Tracking System are critical for assessing its impact and effectiveness in achieving the venture goals inside the UTAR campus community environment. Firstly, the detection overall performance criterion specializes in evaluating how successfully the gadget identifies rogue get entry to points. By appropriately detecting unauthorized get admission to factors, the device contributes extensively to enhancing community security and preventing ability protection breaches. This criterion will degree the gadget's capability to directly discover and document rogue get entry to point to network

directors, allowing speedy mitigation of protection threats.

Secondly, the monitoring precision criterion assesses the device's functionality to song the movement and place of detected rogue access points in real-time. This feature is crucial for tracking unauthorized get admission to and stopping malicious sports inside the network. A high stage of tracking precision guarantees that network directors can efficiently reply to rogue get admission to factor threats and take suitable action to stable the community environment.

The system responsiveness criterion measures the general responsiveness of the gadget, from the initiation of network scans to the detection and monitoring of rogue get admission to points. A responsive system ensures short detection and timely reporting of safety incidents, facilitating spark off incident response and mitigation. A system that responds correctly contributes to minimizing the effect of protection breaches and preserving community integrity.

Furthermore, the security enhancement criterion evaluates how efficaciously the system complements community safety and safeguards touchy records integrity. By detecting and tracking rogue get entry to factors, the machine enables prevent unauthorized get right of entry to and capability safety breaches, thereby improving standard community security posture.

User pleasure is also a key thing of evaluation, specializing in amassing remarks from community directors regarding the usability and effectiveness of actual-time monitoring equipment provided with the aid of the system. Positive person feedback indicates that the gadget efficiently empowers directors to manage and stable the network environment.

Lastly, moral compliance ensures that the challenge adheres to excessive studies ethics and institutional norms at some point of facts handling and machine implementation. Ethical concerns are paramount in ensuring the credibility and integrity of the assignment's results, reflecting a dedication to moral concepts in studies and era improvement.

In conclusion, the assessment criteria mentioned above together contribute to

assessing the effect and effectiveness of the Rouge Access Point Detection and Tracking System in enhancing network protection inside the UTAR campus environment. By meeting these criteria, the gadget ambitions to meet its goals of detecting and mitigating rogue get admission to factor threats, enhancing network protection, and imparting network directors with effective tools for real-time monitoring and incident reaction.

CHAPTER 7

7.1 Conclusions

In conclusion, we delve into the pressing issues of Rouge Access Point (RAPs) and their subsequent security implications within the context of the University Tunkul Abdul Rahman (UTAR) campus network. The final stage of our research involved the creation and deployment of a specialized Rouge Access Point Detection and Tracking System designed specifically to meet the unique requirements of the UTAR environment. The system described utilizes various sophisticated methods including SSID pattern analysis, MAC address validation, signal strength evaluation to allocate the approximate location of the RAP. Our contributions encompass not only the development of this advanced system but also significant insights towards enhancing network security. The primary objective of our research is to efficiently identify and monitor RAPs, with the ultimate goal of minimizing potential risks, safeguarding against data breaches, and ensuring the preservation of confidentiality and integrity for sensitive data. In addition, our research endeavors encompass the advancement of network security methods and policies tailored specifically to the context of UTAR. Our system's practicality and effectiveness have been acknowledged by the acquisition of the Gold Award at the JIICaS competition (refer to Appendix 1), serving as a witness to its recognition. Nevertheless, it is important to recognize some constraints associated with the process of identifying RAPs. These limitations encompass the narrow focus on individual campuses, the substantial allocation of resources required, and the legal implications that are inherently involved. In our future plans, we anticipate expanding the system's scalability to accommodate a wider range of applications. Additionally, we aim to integrate it with pre-existing security tools, investigate potential improvements using machine learning techniques, create a user interface that is intuitive and easy to use, and construct a legal framework to effectively manage any potential risks, anomalies, or problems (RAPs) that may arise. Within an ever-changing technical environment, our initiative represents a significant advancement in enhancing the security of wireless networks, hence emphasizing the criticality of network security in the era of digitalization.

7.2 Recommendations

The implementation of the Rouge Access Point Detection and Tracking System can be significantly enhanced by deploying it within a dedicated server environment. This approach not only ensures improved security but also enhances user-friendliness and accessibility. By integrating the system into a server-side architecture, users are relieved from performing scans using individual hardware devices, mitigating potential hardware limitations and inconsistencies in scanning results. Additionally, hosting the system on a server facilitates centralized management and control, allowing for streamlined administration and monitoring.

Web-Based User Interface:

- Integrating the system into a web-based platform hosted on the server enables convenient access and usage for users within the campus network. By requiring students to sign in to the system through a website hosted by the server, access to system functions can be regulated and authenticated, enhancing security and user accountability.

Logging and Analysis Capabilities:

- Centralized logging of scanning activities performed by students can be achieved through the server-hosted system. This logging mechanism provides network administrators with comprehensive logs and data, enabling analysis of scanning patterns and evaluation of campus network security. The collected data can be utilized to identify potential threats and vulnerabilities, aiding in proactive security measures.

Network Isolation and Incident Response:

- The server-based system can implement automated incident response protocols, such as isolating affected network segments and sending email notifications to students and faculty members within specific areas or blocks. This proactive approach prevents unauthorized network connections and mitigates potential data loss incidents. Notifications can alert users to avoid connecting to compromised networks, thereby enhancing overall network

security.

Location-Based Scanning Optimization:

- Utilizing location-based services through the web interface, the system can determine the geographical location of users and direct them to the nearest access control (AC) or server within their vicinity for scanning purposes. This optimization ensures reliable and accurate scanning results by minimizing network latency and interference.

In conclusion, integrating the Rouge Access Point Detection and Tracking System into a server-based architecture enhances its effectiveness, security, and usability within the UTAR campus network. By leveraging centralized management, logging capabilities, and automated incident response features, the system can proactively safeguard network integrity and prevent potential security breaches.

REFERENCES

[1] Junos Space Network Director, Sep. 2022, "Network Director User Guide," https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/information-products/pathway- pages/network-director-pwp.pdf (accessed Apr. 23, 2024).

[2] B. Mitchell. "What Is a Wireless Access Point?" Lifewire: Tech for Humans. https://www.lifewire.com/wireless-access-point-816545 (accessed Sep. 5, 2023).

[3] S. Nikbakhsh, A. B. A. Manaf, M. Zamani and M. Janbeglou, "A Novel Approach for Rogue Access Point Detection on The Client-side," in 26th Int. Conf. Adv. Inf. Netw. Appl. Workshops (AINA), Fukuoka, Japan, 2012, pp. 684-687, doi: 10.1109/WAINA.2012.108.

[4] G. Shivaraj, M. Song and S. Shetty, "A Hidden Markov Model Based Approach to Detect Rogue Access Points," in 2008 Mil. Commun. Conf. (MILCOM), San Diego, CA, USA, 2008, pp. 1-7, doi: 10.1109/MILCOM.2008.4753358.

[5] A.Ketkhaw and S. Thipchaksurar, "Hidden Rogue Access Point Detection Technique for Wireless Local Area Networks," in 21st Int. Comput. Sci. Eng. Conf. (ICSEC), Bangkok, Thailand, 2017, pp. 1-5, doi: 10.1109/ICSEC.2017.8443803.

[6] S. Kitisriworapan, A. Jansang and A. Phonphoem, "Client-side Rogue Access-Point Detection Using a Simple Walking Strategy and Round-trip Time Analysis," EURASIP J. Wirel. Commun. Netw., 2020:252, pp. 1-24, Dec. 2020, doi:10.1186/s13638-020-01864-5

[7] L. Qawasmeh and F. Awad, "Tracking a Mobile Rouge Access Point," in 2021 Int. Conf. Inf. Technol. (ICIT), Amman, Jordan, 2021, pp. 522-526, doi: 10.1109/ICIT52682.2021.9491684.

[8] Q. Luo, K. Yang, X. Yan, J. Li, C. Wang, and Z. Zhou, "An improved Trilateration Positioning Algorithm with Anchor Node Combination and K-Means

Clustering," Sensors 2022, vol. 22, no. 16, pp. 6085-6107, Aug. 2022, doi:10.3390/s22166085.

[9] B. Alotaibi and K. Elleithy, "An Empirical Fingerprint Framework to Detect Rogue Access Points," in 2015 Long Island Sys. Appl. Technol. (LISAT), Farmingdale, NY, USA, 2015, pp. 1-7, doi: 10.1109/LISAT.2015.7160206.

[10] S. Vanjale and P. B. Mane, "A Novel Approach for Elimination of Rogue Access Point in Wireless Network," in IEEE India Conf. (INDICON), Pune, India, 2014, pp. 1-4, doi: 10.1109/INDICON.2014.7030418.

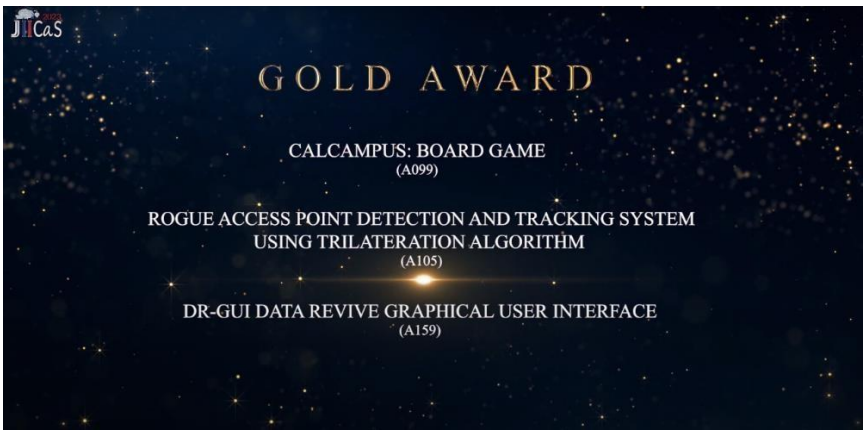
[11] K. F. Kao, W. C. Chen, J. C. Chang and H. T. Chu, "An Accurate Fake Access Point Detection Method Based on Deviation of Beacon Time Interval," in 8th Int. Conf. Softw. Secur. Rel. Companion (SSIRI-C), San Francisco, CA, USA, 2014, pp. 1-2, doi: 10.1109/SERE-C.2014.13.

[12] S. Jadhav, S. B. Vanjale and P. B. Mane, "Illegal Access Point Detection using Clock Skews Method in Wireless LAN," in 2014 Int. Con. Comput. Sustain. Global Develop. (INDIACom), New Delhi, India, 2014, pp. 724-729, doi: 10.1109/IndiaCom.2014.6828057.

[13] R. Jang, J. Kang, A. Mohaisen and D. Nyang, "Catch Me If You Can: Rogue Access Point Detection using Intentional Channel Interference," in IEEE Trans. Mobile Comput., vol. 19, no. 5, pp. 1056-1071, 1 May 2020, doi: 10.1109/TMC.2019.2903052.

[14] Y. Song, C. Yang and G. Gu, "Who is Peeping at Your Passwords at Starbucks? —To Catch an Evil Twin Access Point," in 2010 IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN), Chicago, IL, USA, 2010, pp. 323-332, doi: 10.1109/DSN.2010.5544302

APPENDIX A



Appendix 1

Appendix 2

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.: 2**
Student Name & ID: Lee Chiew Min20ACB03861	
Supervisor: Puan Nor'Afifiah Binti Sabri	
Project Title: Rouge Access Point Detection and Tracking	

1. WORK DONE

Discussion the possibility of implement the system via Ubutu server, and tracking method using google API services.

2. WORK TO BE DONE

To find the possible tracking method that can approximate the RAP location.

3. PROBLEMS ENCOUNTERED

Need to study how the google API services work, and Ubutu server.

4. SELF EVALUATION OF THE PROGRESS

Much research have been made, and further testing need to be done about the tracking methods. Overall, the progress of the project
so far is going well.

Supervisor's signature

Lee Chiew Min

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

Trimester, Year: Year 3 Trimester 3	**Study week no.: 4**
Student Name & ID: Lee Chiew Min20ACB03861	
Supervisor: Puan Nor'Afifiah Binti Sabri	
Project Title: Rouge Access Point Detection and Tracking	

(Project II)

1. WORK DONE

Trying the integrate the system on Ubutu Server.

2. WORK TO BE DONE

Discussion about the Ubutu server method as it encountered major issue to successfully integrate

3. PROBLEMS ENCOUNTERED

The Ubutu Server integrate with system and hosted on a website, has encountered problems as when using the TP link USB, it is not able to host the website and failed to run monitor mode.

4. SELF EVALUATION OF THE PROGRESS

Much research have been made, and further testing has been done regarding the system integrate with Ubutu server to make it as a website response with server but failed to implement.

Supervisor's signature

Lee Chiew Min

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.: 5**
Student Name & ID: Lee Chiew Min20ACB03861	
Supervisor: Puan Nor'Afifiah Binti Sabri	
Project Title: Rouge Access Point Detection and Tracking	

1. WORK DONE

Trying the integrate the system on Ubutu Server.

2. WORK TO BE DONE

Discussion about the Ubutu server method as it encountered major issue to successfully integrate

3. PROBLEMS ENCOUNTERED

The Ubutu Server integrate with system and hosted on a website, has encountered problems as when using the TP link USB, it is not able to host the website and failed to run monitor mode.

4. SELF EVALUATION OF THE PROGRESS

Much research have been made, and further testing has been done regarding the system integrate with Ubutu server to make it as a website response with server but failed to implement.

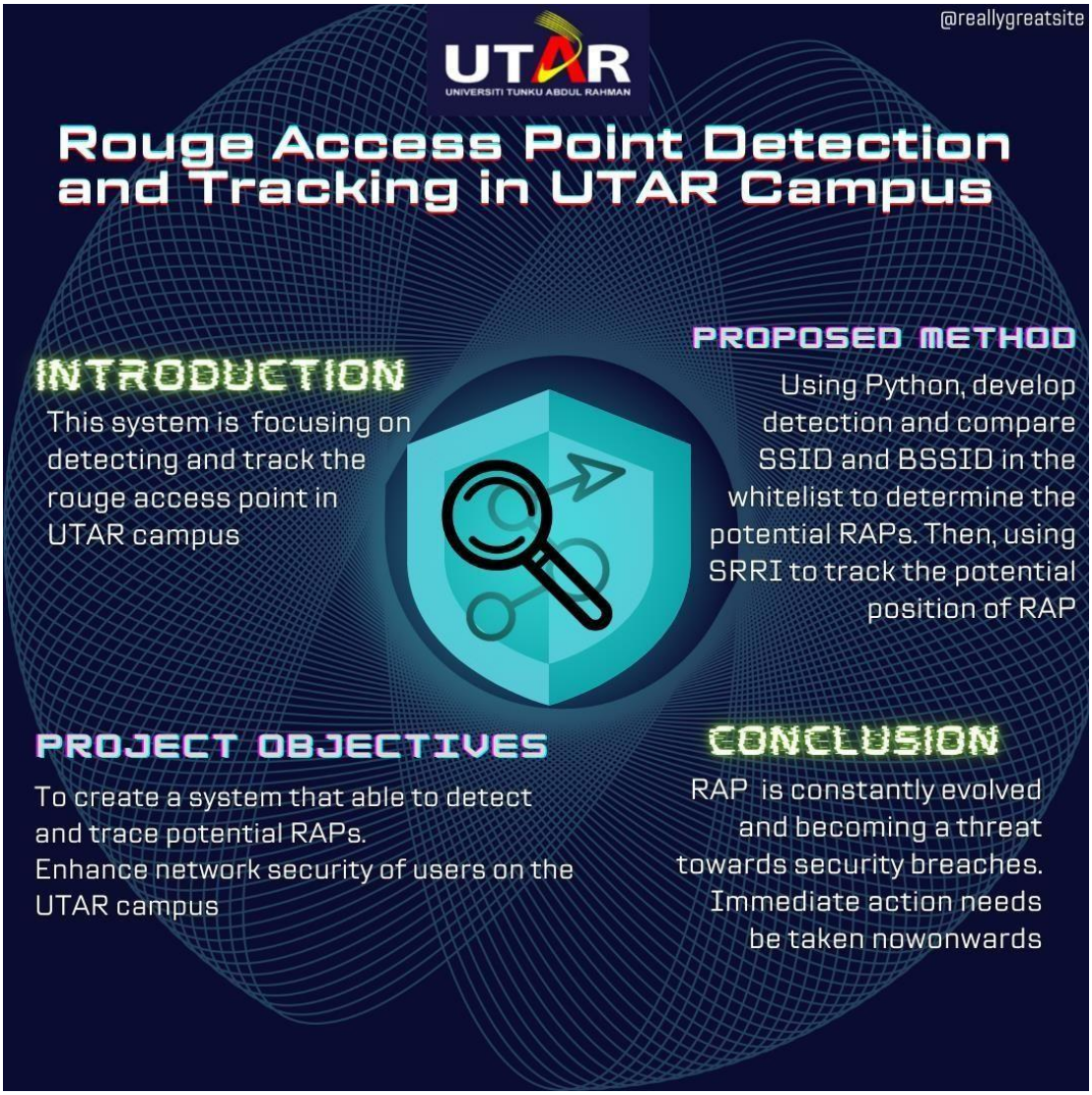
Supervisor's signature

Lee Chiew Min

Student's signature

APPENDIX

POSTER



Appendix 4

APPENDIX

Plagiarism Check Result

report

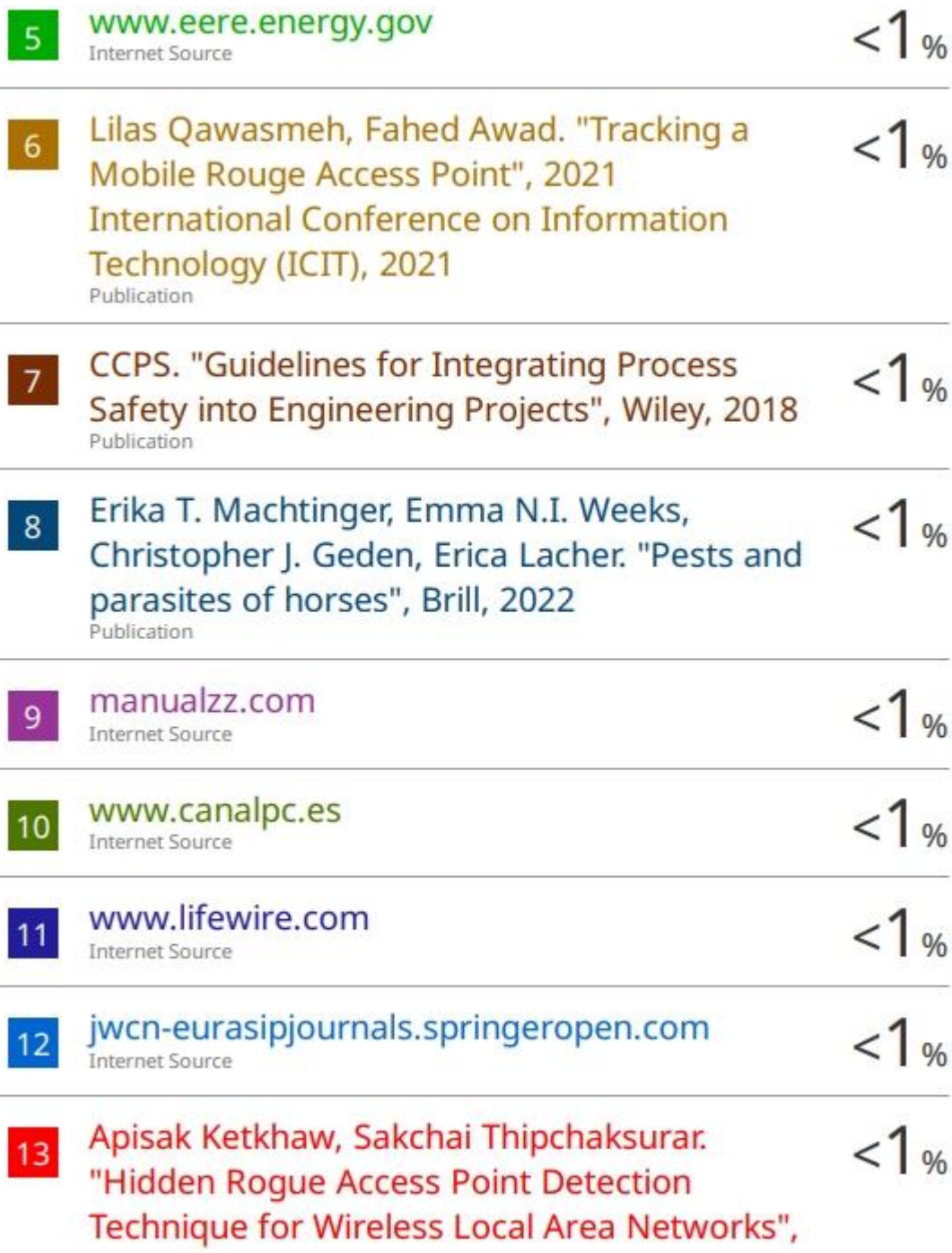
ORIGINALITY REPORT

7%	3%	6%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Qinghua Luo, Kexin Yang, Xiaozhen Yan, Jianfeng Li, Chenxu Wang, Zhiquan Zhou. "An Improved Trilateration Positioning Algorithm with Anchor Node Combination and K-Means Clustering", Sensors, 2022 Publication	1%
2	Somayeh Nikbakhsh. "A Novel Approach for Rogue Access Point Detection on the Client-Side", 2012 26th International Conference on Advanced Information Networking and Applications Workshops, 03/2012 Publication	1%
3	"Security, Privacy, and Anonymity in Computation, Communication, and Storage", Springer Science and Business Media LLC, 2017 Publication	<1%
4	Otasowie Owolafe, Gbenga Moses Adediran, Olaniyi Abiodun Ayeni. "chapter 20 Rogue Access Detection Using Multi-Parameter Dynamic Features on WLAN", IGI Global, 2023 Publication	<1%

APPENDIX


5
www.eere.energy.gov
Internet Source
<1%
6
Lilas Qawasmeh, Fahed Awad. "Tracking a Mobile Rouge Access Point", 2021 International Conference on Information Technology (ICIT), 2021
Publication
<1%
7
CCPS. "Guidelines for Integrating Process Safety into Engineering Projects", Wiley, 2018
Publication
<1%
8
Erika T. Machtinger, Emma N.I. Weeks, Christopher J. Geden, Erica Lacher. "Pests and parasites of horses", Brill, 2022
Publication
<1%
9
manualzz.com
Internet Source
<1%
10
www.canalpc.es
Internet Source
<1%
11
www.lifewire.com
Internet Source
<1%
12
jwcn-eurasipjournals.springeropen.com
Internet Source
<1%
13
Apisak Ketkhaw, Sakchai Thipchaksurar. "Hidden Rogue Access Point Detection Technique for Wireless Local Area Networks",
<1%

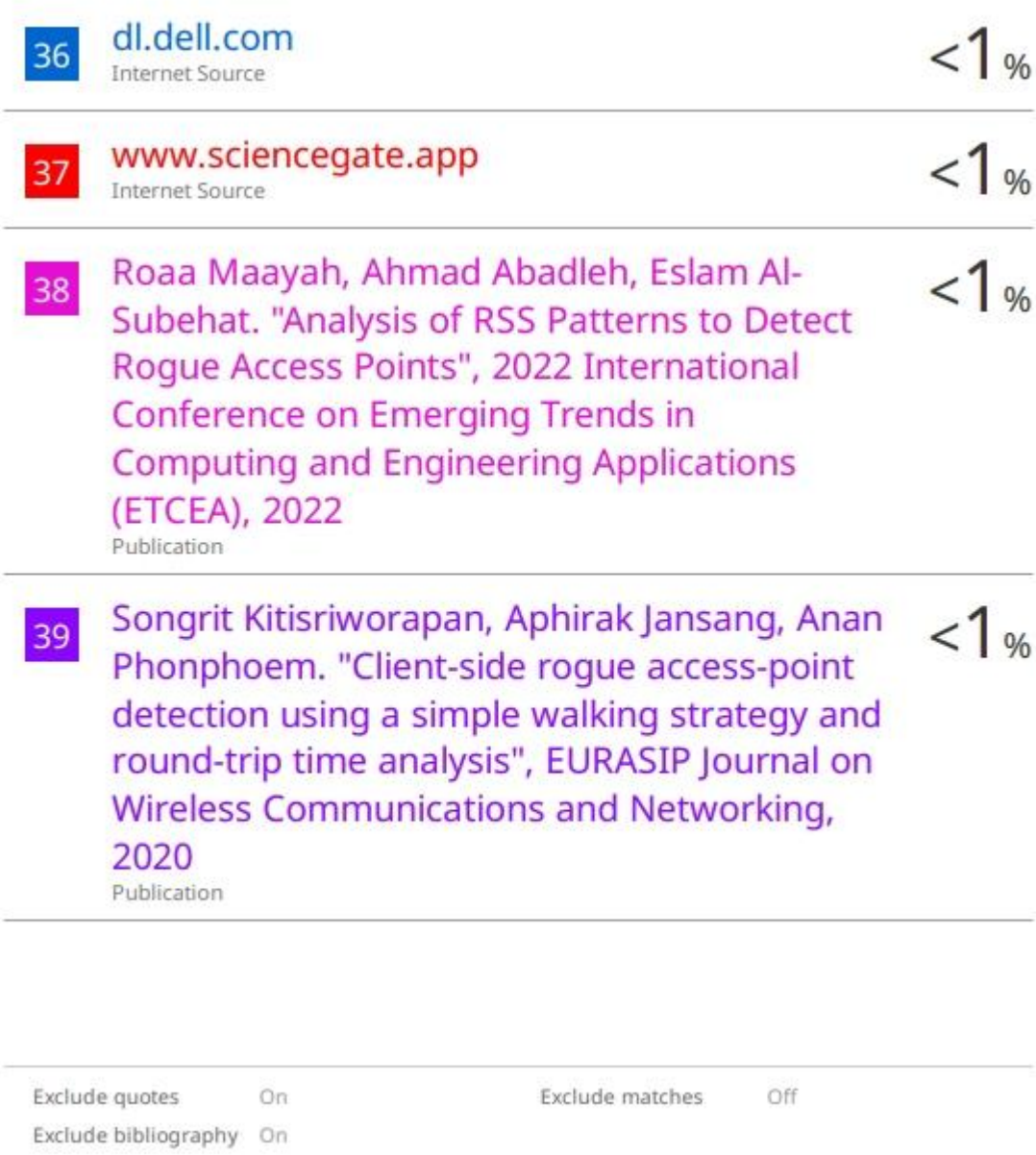
2017 21st International Computer Science and Engineering Conference (ICSEC), 2017
Publication

14	Suwadi, Wirawan, Mike Yuliana. "Performance Enhancement of Multi-User Key Extraction Scheme (MKES) Based on Imperfect Signal Reciprocity", 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2020 Publication	<1 %
15	Guangjie Han, Chenyu Zhang, Tongqing Liu, Lei Shu. "MANCL: a multi-anchor nodes collaborative localization algorithm for underwater acoustic sensor networks", Wireless Communications and Mobile Computing, 2016 Publication	<1 %
16	Submitted to Universiti Teknologi Malaysia Student Paper	<1 %
17	iris.unica.it Internet Source	<1 %
18	Suwadi, Mike Yuliana, Wirawan. "Discrete Cosine Transform-Based Key Generation Scheme for Indoor Environment", 2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2021 Publication	<1 %

19	orca.cf.ac.uk Internet Source	<1 %
20	Sweta Anmulwar, Shalvi Srivastava, Shrinivas P. Mahajan, Anil Kumar Gupta, Vinodh Kumar. "Rogue access point detection methods: A review", International Conference on Information Communication and Embedded Systems (ICICES2014), 2014 Publication	<1 %
21	Manesh Thankappan, Helena Rifà-Pous, Carles Garrigues. "A Signature-Based Wireless Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks", IEEE Access, 2024 Publication	<1 %
22	link.springer.com Internet Source	<1 %
23	Submitted to Holmesglen Institute of TAFE Student Paper	<1 %
24	ore.exeter.ac.uk Internet Source	<1 %
25	Submitted to Bournemouth University Student Paper	<1 %
26	Submitted to Glasgow Caledonian University Student Paper	<1 %

27	Submitted to University of Northumbria at Newcastle Student Paper	<1%
28	dspace.uevora.pt Internet Source	<1%
29	escholarship.org Internet Source	<1%
30	a.cs.uiuc.edu Internet Source	<1%
31	mdpi-res.com Internet Source	<1%
32	Hanoi National University of Education Publication	<1%
33	wrap.warwick.ac.uk Internet Source	<1%
34	"Innovative Mobile and Internet Services in Ubiquitous Computing", Springer Science and Business Media LLC, 2020 Publication	<1%
35	Thejdeep. G, Shiva Sagar. B, Siddartha. L. K, B. R. Chandavarkar. "Detecting Rogue Access Points using Kismet", 2015 International Conference on Communications and Signal Processing (ICCSP), 2015 Publication	<1%

APPENDIX


36
dl.dell.com
Internet Source
<1%
37
www.sciencegate.app
Internet Source
<1%
38
Roaa Maayah, Ahmad Abadleh, Eslam Al-Subehat. "Analysis of RSS Patterns to Detect Rogue Access Points", 2022 International Conference on Emerging Trends in Computing and Engineering Applications (ETCEA), 2022
Publication
<1%
39
Songrit Kitisriworapan, Aphirak Jansang, Anan Phonphoem. "Client-side rogue access-point detection using a simple walking strategy and round-trip time analysis", EURASIP Journal on Wireless Communications and Networking, 2020
Publication
<1%
Exclude quotes On
Exclude bibliography On
Exclude matches Off

Universiti Tunku Abdul Rahman			
Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	Lee Chiew Min
ID Number(s)	20ACB003861
Programme / Course	CN
Title of Final Year Project	Rogue Access Point Detection and Tracking in UTAR Campus

Similarity	**Supervisor's Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)**
Overall similarity index:7**%** **Similarity by source** Internet Sources:3% Publications: 6% Student Papers:1%	
Number of individual sources listed of more than 3% similarity: 0	

Parameters of originality required and limits approved by UTAR are as Follows:
- **(i) Overall similarity index is 20% and below, and**
- **(ii) Matching of individual sources listed must be less than 3% each, and**
- **(iii) Matching texts in continuous block must not exceed 8 words**

Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

Signature of Supervisor

Name: Nor 'Afifah Binti Sabri

Date: 19/04/2024

Signature of Co-Supervisor

Name: _____

Date: _____

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF INFORMATION & COMMUNICATION TECHNOLOGY (KAMPAR CAMPUS)

CHECKLIST FOR FYP2 THESIS SUBMISSION

Student ID	20ACB03861
Student Name	Lee Chiew Min
Supervisor Name	Puan Nor 'Afifah Binti Sabri

TICK (√)	DOCUMENT ITEMS Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
√	Title Page
√	Signed Report Status Declaration Form
√	Signed FYP Thesis Submission Form
√	Signed form of the Declaration of Originality
√	Acknowledgement
√	Abstract
√	Table of Contents
√	List of Figures (if applicable)
√	List of Tables (if applicable)
√	List of Symbols (if applicable)
	List of Abbreviations (if applicable)
√	Chapters / Content
√	Bibliography (or References)
√	All references in bibliography are cited in the thesis, especially in the chapter of literature review
√	Appendices (if applicable)
√	Weekly Log
√	Poster
√	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)
√	I agree 5 marks will be deducted due to incorrect format, declare wrongly the ticked of these items, and/or any dispute happening for these items in this report.

*Include this form (checklist) in the thesis (Bind together as the last page)

I, the author, have checked and confirmed all the items listed in the table are included in my report.

Lee Chiew Min

(Signature of Student)
Date: 19/04/2024