CHAPTER 1

# INTRODUCTION

In network security, one of the most predominant attacks against institutions as well as individuals is the Man-in-the-Middle (MITM) attack. Though there are many types of MITM attacks, one of the more long-standing ones is the MITM attack through ARP poisoning.

This attack makes use of the vulnerabilities in the ARP protocol in order to eavesdrop on communications over a switched LAN network. Despite its simple implementation, it is clearly an effective network penetration strategy as evident from its popularity among network security professionals.

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite. ARP was defined in 1982 by RFC 826,[1] which is Internet Standard STD 37.

The Address Resolution Protocol uses a simple message format containing one address resolution request or response. The size of the ARP message depends on the link layer and network layer address sizes. The message header specifies the types of network in use at each layer as well as the size of addresses of each. The message header is completed with the operation code for request (1) and reply (2). The payload of the packet consists of four addresses, the hardware and protocol address of the sender and receiver hosts. The principal packet structure of ARP packets is shown in the following table which illustrates the case of IPv4 networks running on Ethernet. In this scenario, the packet has 48-bit fields for the sender hardware address (SHA) and target hardware address (THA), and 32-bit fields for the corresponding sender and target protocol addresses (SPA and TPA). The ARP packet size in this case is 28 bytes.

**Address Resolution Protocol**

Communication Protocol, stateless.

Used to discover physical link layer address such as MAC address, in assign with the IPv4 address in the network layer. This mapping so critical for the internet work.

ARP operates

Request- Response protocol.

Inside the link layer protocol.

Limited to the boundary of single subset, for Ex; LAN .In cannot be routed across inter networking (network) nodes.

EXAMPLES

(192.168.0.3) B (192.168.0.4)

If needs MAC address?

MAC found! Prepare Ethernet frame.

Destination address (xx:xx:xx:xx:xx:xx)

No proper results? Broadcast

ARP request-Accepted by all the computers in the network

# CHAPTER 2

# LITERATURE SURVEY

## 2.1 REAL-WORLD MAIN-IN-MIDDLE(MITM) ATTACK IMPLEMENT USING OPEN SOURCE TOOL FOR INSTRUCTION USE

Today, networks play a vital role in everyone's life to perform a wide array of tasks including communication, finance, banking, and shopping. The massive usefulness of networks makes them continuous targets of attacks. Therefore, it is essential to understand their implementation along with the associated threats and their countermeasures. Although every institute offers courses on networks and security, the courses need to be equipped with hands-on training to enhance students' learning. To this end, we aim to develop a foundational cyber security course with in-built hands-on activities. This paper presents one such successful implementation of a popular network attack

Kali Linux is Debian derived Linux distribution designed digital forensics and penetration testing. It is one of the best security packages of an ethical hacker. Offensive Security Limited maintains and funds Kali Linux. It was developed by Mati Aharoni and Devon Kearns. Kali Linux has more than 300 penetration testing tools. Multiple languages are also supported by Kali Linux.

Man-In-the-Middle (MITM) Attack;

Man-In-The-Middle (MITM, also referred to as MIM, MiM, MitM, or MITMA in the literature) is a type of attack in which a third party in stealth takes control of the communication channel between two or more parties. In MITM attack, the attacker can intercept, modify, change, or replace target victim’s communication traffic. The victims

are not aware of the man in the middle, so, they believe that the communication channel is protected [4] Man-in-the-middle attacks allow the attacker to intercept, send and receive the data which is never meant to be for them without the outside party knowing about it.

Man-in-the-middle can be used to invoke attacks such as Distributed denial of service (DDOS) attack, DNS spoofing, port stealing and session hijacking. MITM has many consequences such as stealing someone’s online user ID and password, stealing telnet session, stealing local FTP ID, etc. Man-in-the-middle attacks can be active or passive. In a passive attack, the attacker’s presence is not detected, but he only captures the data that is being transmitted and sends it to the original person who is supposed to receive it. Whereas in an active attack, the contents are intercepted and manipulated before being sent to the expected destination. The Only difference between an active MITM attack and passive MITM attack is the attacker modifies the information to be sent in an active attack, while, in a passive attack he just records it without modification.

MITM attacks are rare on the wired internet due to lack of the spots where the attacker can insert himself between two communicating terminals and remain undetected . But for wireless connection, there is a difference in the situation. It can be effortless for the attacker to insert his information depending on the nature of the wireless link layer protocol. Figure 1 shows the difference between the flow of information or data in the regular communication and the flow of data in the man-in-the-middle kind of flow. In normal flow, the communication is taking place in between the two parties communicating with each other i.e.., the client and server and there is no intrusion or mediation of any man in the middle. Whereas, in the Man-in-the-middle flow we can see that the communication is happening between through the attacker or the man in the middle. Therefore, the attacker can spoof the victim as the server. He can affect the confidentiality, integrity, availability of the data. The storage of cryptocurrencies is also prone to a Man-In-The-Middle (MITM) attack. The most recent MITM attack exposed the vulnerability of ledger hardware wallets that were once considered safer methods to store crypto currencies. This attack would allow a cybercriminal to show the customer, a fake address of the crypto currency and use the original address to transfer to his wallet A Man-In-The-Middle (MITM) attack will transfer the crypto currency to a fraudulent address instead of the user’s wallet. This attack is accomplished by infecting the victim’s computer with malware that will accommodate the MITM attack.

## 2.2 THE DEFENSE AGAINST ARP SPOOFING ATTACK USING SEMI-STATIC

Internet becomes an important tool in our daily life. About 4.2 billion people or about 54.2% human population actively use the internet today . Most of those users use the internet for communication and sharing information. Therefore, securing the user’s data that pass through the internet is a very important challenge until today. Internet use packet switching communication model. It breaks down the data into smaller chunks then sent it in the form of a discrete packet that follows different channels in a sequence over time and rejoins at the final destination node. One of the threats to this architecture is the attacks on the data link layer such as ARP spoofing attack or ARP poisoning [2]. This attack exploits the vulnerability of ARP protocol that translates logical address to the physical address of a device.

For decades, many research proposed several approaches to mitigate the ARP spoofing attacks. There are five categories of this mitigation approaches:

 Modifying ARP using cryptographic techniques;

 Patching the operating system’s kernel;

 Securing switch ports;

 ARP spoofing attack detection and protection using external software; and

 Manually configuring static ARP cache table.

The first solution protects the ARP protocol by adding a cryptographic function. The major drawback of this approach is the incompatibility with the standard ARP protocol and affect the ARP protocol performance. The second solution adds some patches to the operating system kernel to prevent the ARP spoofing attack. However, not all operating system can implement this solution. It also may incompatible with the standard ARP protocol. The third solution prevents the ARP spoofing attack by modifying the switch devices using switch port security or Dynamic ARP Inspections (DAI). This solution is costly because the network provider should replace all old switches. The fourth solution use external software to detect and protect clients. However, some researchers argue that this solution may ineffective against the ARP spoofing attack. The fifth solution is the most basic but effective way to prevent ARP spoofing attack by manually adding the MAC address to the static ARP cache table. But this solution is a laborious job and not all network administrator willing to do it .

This research proposed a method to improve the static ARP cache table solution. Our purposes are removing the laborious process of adding the static ARP cache table manually and adding the ARP validation function to manage the static ARP cache table automatically. This proposed method is simple and compatible with standard ARP protocol. It does not require any modification of the standard ARP protocol nor replacing old devices.

## 2.3 MAN-IN-THE-MIDDLE ATTACK DETECTION AND LOCALIZATION BASED ON CROSS-LAYER LOCATION CONSISTENCY

The proliferation of bandwidth-intensive applications, like high-deﬁnition video, virtual reality, and argument reality, has drawn pressing need for indoor mmWave communication systems. IEEE 802.11ad, which is released as a promising technology, aims to support multi-gigabit-persecond throughput through utilizing 60GHz unlicensed frequency, and thus to support the aforementioned applications. Compared with other IEEE 802.11 standards [1], the introducing of mmWave communication in IEEE 802.11ad has many desirable characteristics, including wide available spectrum range and large information capacity; achieving narrow be a mand high gain antenna easily; higher solution and strong directivity; strong ability to penetrate plasma; high transmission rate and completely free spectrum resources .

However,IEEE802.11adstillfacesdiversesecuritythreats,as revealed recently in , especially the man-in-the-middle (MITM attack), in which an attacker could hijack the information exchanged between two victims through establishing a relay path between them.

Steinmetzer et al. have shown the feasibility of utilizing the beam-training period for launching MITM attacks in An attacker located between the transmitter and the receiver kept listening to the channel tries to establish a relay path between the two ends; then all the transmitted packets between two victims need to be received, analyzed, and relayed by the attacker. MITM attacks could degrade legitimate communications in three aspects: ﬁrst , the original legitimate communication path is changed after the attack, which will introduce extra communication delays; second, the attacker will intercept and steal the original data when the attack is performed; third, the data content may be modiﬁed by the attacker.

Detecting and locating MITM attacks accurately in a timely manner is critical for restoring network service and preventing privacy leakage. Steinmetzer etal have proposed four schemes that can be used to detect MITM attacks:detection of frequent of beam switching, detection of change of signal strength, detection of beam gap length, beacon value detection. However, in general, the above methods all need to determine a threshold in advance before conducting MITM detection, which requires a long training, and the algorithm proposed by the author can only detect whether there is a MITM attack, while it cannot locate the attacker. Weietal. have proposed allocation consistency-based MITM attack detection algorithm from the perspective of MAC. However, on the one hand, the algorithm proposed by the author can only determine whether there is a MITM attack, and it cannot achieve positioning, on the other hand, the success of their proposal relieson three ideal assumptions: ﬁrst, a legitimate node can accurately estimate the distances to it sneighbors; second,there a reat least two commonn eighbors between the victims for checking location in consistency; third, legitimate nodes’ coordinate systems are synchronized in advance. These assumptions limit the applicability of the algorithms presented in .

In this back drop,this paper aims attacking these problems utilizing the physical-layer as well as MAC layer knowledge. On the one hand, the algorithm proposed in this paper can detect the MITM attack; on the other hand, the algorithm can also locate the attacker at the same time, which is not considered by previous works. Therefore, this paper solves the problem of simultaneous detection and localization in the MITM attack research. Firstly,with the help of physical layer information, we establish a multi-path channel propagation model and a directional multi-sector antenna propagation model, and proposed a positioning algorithm so that the distance and relative angle between any two transceivers can be determined. Secondly,we complete the sector consistency check with the help of MAC layer information to determine the existence of a MITM attack. Thirdly, a MITM attack detection and localization algorithm based on cross-layer location consistency is put forward.

The remaining of this paper is organized as follows. Section II introduces the background and related work. In Section III, we present the MITM detection and localization algorithm. In Section IV, a series of experiments are conducted to verify the feasibility and effectiveness of the algorithm. Finally, abrief conclusion of this work is provided in section V.

## 2.4 A SOLUTION FOR ARP SPOOFING: LAYER-2 MAC AND PROTOCOL FILTERING AND ARP SERVER

## Nowadays Ethernet is the most common protocol used at layer-2 of Local Area Networks (LANs). Ethernet protocol is implemented on the Network Interface Card (NIC). On top of Ethernet, Internet Protocol (IP), Transmission Control/User Datagram Protocols (TCP/UDP) are employed respectively. In this protocol stack for a packet to reach its destination IP and MAC of destination have to be known by the source. This can be done by ARP which is a protocol running at layer-3 of Open System Interface (OSI) model. ARP is designed without considering security issues like all other TCP/IP protocol stack. Malicious people can use these protocols for their own use.

**Source Attacker Destination**

ARP finds the MAC address of destination computer by using the IP address of destination computer. ARP spoofing forces the destination computer to send packets to the attacker instead of source. Attacker can tap into the communication by forcing source and destination computers to send packets to itself at the same time. When it comes to this situation it is called MITM. In this situation the attacker can read packets of source and destination computers, save them and may change packet content or inject new packets. Figure 1 is showing MITM.

## 2.5 A DETAILED SURVEY FOR DETECTION AND MITIGATION TECHNIQUES AGAINST ARP SPOOFING

In today’s era, the internet has become a crucial part of our lives and are entirely inclined towards it. Every sector of our country (both public and private) requires a well-functioned network to work efficiently. With this increasing usage of internet, many issues have come into the picture, security being the major issue in networking. Many researchers are working to find solutions to prevent such attacks and to provide network security. This paper focusses on one such issue called ARP Spoofing which facilitates many attacks discussed later in this paper.

ARP (Address Resolution Protocol)

Every device on a wireless network consists of two different addresses called the IP address and the MAC (Media Access Control) address. Although the actual communication takes place over the hardware address called MAC address, many computer applications transmit or receive data with IP addresses. Because of this, it is required to find the corresponding MAC address for IPv4 communication. So, to get the destination MAC address, Address Resolution Protocol [1] is required. It is a protocol which links or maps the consequent MAC address (48 bits) with the IP address (32 bits).

Working Of ARP

ARP also maintains an ARP cache table that stores information about which MAC address is linked with which IP address. So whenever one device sends a packet to an IP address, first it checks the cache table to find if the required MAC address already exists or not. If it does, ARP is not used and the address found is used to transmit the packet. But if it does not exist in the table, then the device broadcasts ARP request over the network to know which device is using the required IP address. Being a broadcast packet, it is transmitted with a destination MAC address as FF:FF:FF:FF:FF:FF. After receiving the ARP request, all the devices check if their IP address matches with the one in the ARP request. If it does not match, the device will drop the packet without any action. The one whose IP address matches sends a unicast ARP reply which includes the destination MAC address. After this both the devices update their cache table for future references .

ARP Spoofing

ARP does not authenticate whether the reply is from the desired device or not. So, if the reply is not sent by the desired user, but instead by a malicious user then the network becomes prone to ARP spoofing . To sum up, ARP spoofing also called ARP cache poisoning is a technique in which a malignant user links its own MAC address with the legitimate IP address as a means to poison the ARP table within the network. As a consequence, all the data meant for the intended IP address is sent to the attacker’s MAC address instead. From here, the attacker can conduct various attacks and can damage the data in future. Many detection and prevention techniques exist to detect and prevent such false mappings. This survey conducts a deep comparative analysis of those strategies bringing out their advantages and disadvantages.

## 2.6 A SECURE MECHANISM TO PREVENT ARP SPOOFING AND ARP BROADCASTING IN SDN

New technologies appeared in this decade such as cloud services, Internet of Things IoT, Voice over IP VoIP, multimedia, big data, etc. enforce requirements such as high bandwidth, scalability, higher accessibility and dynamic management [1]. In order to implement the network policies, each network device must be configured separately by the network operators using low-level and often vendorspecific commands. Besides, they must manually input these commands using the command line or graphical user interfaces. In case of any failure to a section of network or adopting load changes, there must be automatic reconfiguration and response mechanisms which are very hard to be performed in current IP networks. In addition to the management difficulties, the vertical integration of the existing network devices makes it a more complicated architecture. In the absence of a unified control unit for currently distributed control networks, the network management becomes a very challenging task, and the problematic configuration process leads to many errors, security gaps and network faults.

New protocol designing may take several years to be fully matured and deployed. Therefore, a new paradigm to change the network architecture instead of the current IP network is considered as a difficult task and impractical . Furthermore, with the growth of the network and its traffic, operational expenses of running an IP network has increased rapidly. The idea of a solution for the current network infrastructures limitation was started with the emergence of Software-Defined Networking SDN. SDN is a new networking paradigm that gives hope for changing the inertia of the existing network model . It moves the network model to be an open, programmable, reliable, secure and manageable infrastructure .

Some spoofing attacks such as IP spoofing, Domain Name System DNS spoofing and Address Resolution Protocol ARP spoofing etc. are still a big concern for SDN architecture since a plain SDN controller cannot mitigate them. Usually, an ARP spoofing attack is the first step in other threats such as Denial of Services DoS and Man in the Middle attack, where an attacker can steal vital information regarding the network user. ARP is used by the host in the network to get the physical address of hosts willing to communicate with. The mechanism of ARP is designed to search for the device’s MAC address in the network, and mapping its MAC address with its IP address. In the network, every single device has an ARP table or ARP cache. The primary function of this table is to temporarily store the IP and MAC addresses that have previously communicated. However, this table is vulnerable to alteration by an attacker, and its data can be poisoned with a wrong entry. By doing this, the attacker can falsify the IP-MAC of ARP table of a host, making them send data to the wrong or a malicious destination instead of the original destination. ARP protocol is a stateless and non-authenticated protocol, and that is why most network attacks are caused by ARP . In other words, ARP does not have either an authentication mechanism to ensure the validity of the sender nor integrity to ensure that it is from a real source. Therefore, it is critical to have a mechanism for validating ARP protocol for detecting and preventing ARP spoofing by malicious hosts.

2.7 MAN-IN-THE-MIDDLE ATTACK IN WIRELESS AND COMPUTER NETWORKING

One of the most discussed attacks in computer security is Man-In-The-Middle attack and it is a serious concern for many security professionals. The attackers target the actual data flowing between the endpoints and also compromise the integrity and confidentiality of the data. Adversary can compromise the confidentiality by eavesdropping and the integrity by message modification by communication interception. Adversary can also intercept, modify or destroy the messages to cause end of communication for one of the parties thereby leading to compromise of availability issue. In this paper, we present an extensive review on MITM to categorize and analyse the MITM attacks scope. We considered OSI reference model and two basic networking technologies such as GSM and UMTS. MITM attacks are classified based on various parameters such as attacker location, impersonation techniques and nature of channel. The existing countermeasures are surveyed. The paper categorize MITM attacks into four categories namely spoofing based MITM, TLS/SSL MITM, BGP MITM and false base station based MITM attack. Finally we present prevention mechanisms for all such attacks and also identify few future research directions.

Nowadays, every aspect of our daily life is based on the use of cellular networks or internet. Few applications such as online home banking, social networks, online shopping and so on involve usage of cellular networks or internet. These online services are the primary target for hackers as these involves transfer of user’s sensitive information. Hackers target organizations and enterprises leading to huge economical loss. Man-In-The-Middle (MITM) is the most successful attack that is launched for gaining control over the transferred sensitive end-users data. This is one of the primary threats against wireless network security.

The common MITM attack scenario involves victims (the two endpoints) and the attackers (a third party). The attacker accesses the communication channel and manipulates the messages between the two endpoints. Thus, in MITM attacks, the malicious third party attacker can intercept, change, replace or modify the data being transmitted in the communication channel between the endpoints. Victims believe the communication channel to be protected as they are unaware of these intruders. These MITM attacks can be launched in various communication channels including GSM, long term evolution, UMTS, Bluetooth and Wi-Fi. The attackers target the actual data flowing between the endpoints and also compromise the integrity and confidentiality of the data. Adversary can compromise the confidentiality by eavesdropping and the integrity by message modification by communication interception. Adversary can also intercept, modify or destroy the messages to cause end of communication for one of the parties thereby leading to compromise of availability issue.

CHAPTER 3

# SYSTEM ANALYSIS

## 3.1 EXISTING SYSTEM:

Cyber security is becoming more significant with the increased reliance on the internet; and wireless networks like Bluetooth and Wi-Fi. There are many vulnerabilities in the cyber world which the attackers are exploiting. One such attack is Man -In-The-Middle (MITM) attack. Man-In-The-Middle (MITM) is one of the primary attacks employed in computer-based hacking. In this paper, we will discuss how the attacker performs the Man-in-the middle (MITM) attack using the open source Ettercap tool in Kali Linux environment. Ettercap tool is a sniffing tool available in the Kali Linux operating system. It is used to perform sniffing, using Man-in-the-middle attack and other attacks like DDOS attack, packet filtering, DNS spoofing, etc. This paper attempts to implement this attack for instructional use in an academic setup for teaching a foundational cybersecurity course.

Man-In-The-Middle (MITM, also referred to as MIM, MiM, MitM, or MITMA in the literature) is a type of attack in which a third party in stealth takes control of the communication channel between two or more parties. In MITM attack, the attacker can intercept, modify, change, or replace target victim’s communication traffic. The victims are not aware of the man in the middle, so, they believe that the communication channel is protected Man-in-the-middle attacks allow the attacker to intercept, send and receive the data which is never meant to be for them without the outside party knowing about it.

Man-in-the-middle can be used to invoke attacks such as Distributed denial of service (DDOS) attack, DNS spoofing, port stealing and session hijacking. MITM has many consequences such as stealing someone’s online user ID and password, stealing telnet session, stealing local FTP ID, etc. Man-in-the-middle attacks can be active or passive. In a passive attack, the attacker’s presence is not detected, but he only captures the data that is being transmitted and sends it to the original person who is supposed to receive it. Whereas in an active attack, the contents are intercepted and manipulated before being sent to the expected destination. The Only difference between an active MITM attack and passive MITM attack is the attacker modifies the information to be sent inan active attack, while, in a passive attack he just records it without modification.

MITM attacks are rare on the wired internet due to lack of the spots where the attacker can insert himself between two communicating terminals and remain undetected . But for wireless connection, there is a difference in the situation. It can be effortless for the attacker to insert his information depending on the nature of the wireless link layer protocol.

ARP spoofing

If an attacker (a compronisedhost or a computer in network)broadcasts

Spooffed (fake) response(or)broadcast message into a LAN, we call this ARP spoofing.

Purpose ? Idea is to associate attackers MAC address to IP of another host(victine).

ARP vulnerabilities

To communicate among LAN, Mac has to be known. If it is not known & not available in ARP cache, a authentication has broadcast request is sent, we cache this ARP request.

By sending fake broadcast response the computers in network will save the spoofed IP:MAC in this cache.

Since it cannot with ,we cannot prevent this.

### 3.1.1DISADVANTAGES:

* In addition, threat actors could use Man-in-the-Middle attacks to harvest personal information or login credentials.
* Further, attackers could force compromised updates that install **malware** can be sent on users' mobile devices instead of legitimate ones.
* MITM attacks are a common cyber security threat, but what exactly are they, and what cyber risk do they present to you and your business.

3.2 PROPOSED SYSTEM:

ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses

### ARP poisoning of a network leads to MITM Attack, to prevent that our project will check the ARP Request from the router and if we get ARP request from the router in very less interval, i.e ARP request will be sent from router to the machine only once, if it is sent continoulsy we can conclude that our network has been afftected by arp poisoning

### 3.2.1 ADVANTAGES:

Packet filters are useful in ARP spoofing prevention because they are capable of filtering out and blocking packets with conflicting source address information .

ARP helps in knowing the MAC address of the destination Last will see the this protocol. This is easy to helps to provide the router network.

CHAPTER 4

# SYSTEM DESIGN

In network security, one of the most predominant attacks against institutions as well as individuals is the Man-in-the-Middle (MITM) attack. Though there are many types of MITM attacks, one of the more long-standing ones is the MITM attack through ARP poisoning.

System design concentrates on moving from problem domain to solution domain. This important phase is composed of several steps. It provides the understanding and procedural details necessary for implementing the system recommended in the feasibility study. Emphasis is on translating the performance requirements into design specification.

The design of any software involves mapping of the software requirements into Functional modules. Developing a real time application or any system utilities involves two processes. The first process is to design the system to implement it. The second is to construct the executable code.

Software design has evolved from an intuitive art dependent on experience to a science, which provides systematic techniques for the software definition. Software design is a first step in the development phase of the software life cycle.

Before design the system user requirements have been identified, information has been gathered to verify the problem and evaluate the existing system. A feasibility study has been conducted to review alternative solution and provide cost and benefit justification. To overcome this proposed system is recommended. At this point the design phase begins.

The process of design involves conceiving and planning out in the mind and making a drawing.

4.1 INPUT DESIGN

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering.

Input Design is the process of converting a user oriented description of the inputs to a computer-based business system into a programmer-oriented specification.

* Input data were found to be available for establishing and maintaining master and transaction files and for creating output records
* The most suitable types of input media, for either off-line or on-line devices, where selected after a study of alternative data capture techniques.

4.2 INPUT DESIGN CONSIDERATIONS

* The field length must be documented.
* The sequence of fields should match the sequence of the fields on the source document.
* The data format must be identified to the data entry operator.
* These specify what the product does, focusing on its operational capabilities and the processing of inputs and resultant outputs.

4.3 OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs.

In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system’s relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

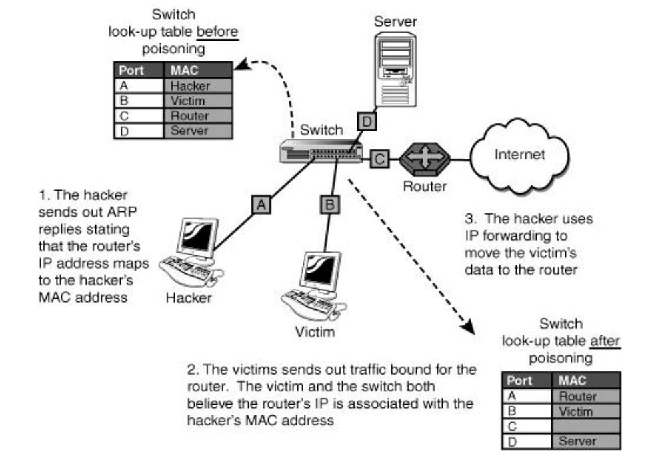
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

* Convey information about past activities, current status or projections of the
* Future.
* Signal important events, opportunities, problems, or warnings.
* Trigger an action.

Confirm an action.

4.4 ARCHITETURE DIAGRAM:



**Figure4.4 Architecture Diagram**

## 4.5 UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

**Goals:**

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.

2. Provide extendibility and specialization mechanisms to extend the core concepts.

3. Be independent of particular programming languages and development process.

4. Provide a formal basis for understanding the modeling language.

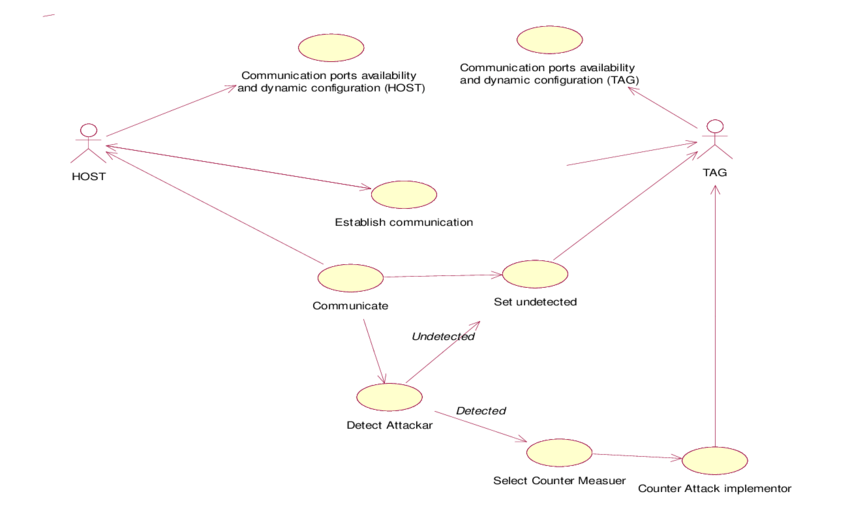
5. Encourage the growth of OO tools market.

6. Support higher level development concepts such as collaborations, frameworks, patterns and components.

7. Integrate best practices.

### 4.5.1 Use Case Diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

 Figure 4.5.1 use case diagram

4.5.2 Data Flow Diagram:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

3. DFD shows how the information moves through the system and how it is modified by a series of transformations.

4. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

5. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

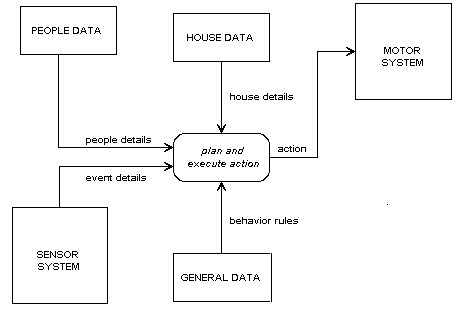


Figure4.5.2: Data Flaw Diagram

# CHAPTER 5

# SYSTEM REQUIREMENTS

## 5.1 HARDWARE REQUIREMENTS:

## Hardware is the collection of physical element that constitutes a computer system. Computer hardware refers to the physical parts or component of a computer such as monitor , keyboard ,computer data storage etc.

* I5 hexa core processor.
* 8 GB Ram.
* LAN network.

## 5.2 SOFTWARE REQUIREMENTS:

Software is any set of machine-readable instructions that directs a computers processor to perform specific operations. Software is usually written in high level programming languages that are easier and more

* Ubuntu operating system.
* 64 bits.
* 3GHz dual core processor

## 5.3 SOFTWARE ENVIRONMENT:-

Ubuntu operating system

Ubuntu is a popular operating system for cloud computing, with support for OpenStack. Ubuntu's default desktop has been GNOME, since version 17.10.  Ubuntu is developed by Canonical, and a community of other developers, under a meritocratic governance model.

Ubuntu operating system is based on the Linux kernel and its development was led by UK-based Canonical Ltd. a company owned by South African entrepreneur Mark Shuttleworth. The Ubuntu operating system is primarily designed for desktop computers, smart phones and tablets. Since Ubuntu is an open source it has become one of the fastest growing Linux based operating system. This work is to measure the Sentiments level of Ubuntu Operating System; Customer Satisfaction is a measure of how products and services supplied by a company meet customer prospect. Customer satisfaction is critical if a company is to benefits from high sales profits.

The work was done to know, how much a consumer is satisfied about the Ubuntu Operating System and current market scenarios of Ubuntu Operating System and what additional features should company introduce to increase the potential customer.

This study is based on both primary and secondary data sources. Primary data was collected through questionnaire using a sample space 120 out of which 100 responded given a response rate of 83.33%. The sample was purposefully selected using a sample space of Students and Lectures drawn from University of Energy and Natural resources-Sunyani, University of Education- Kumasi Campus, Christian Service University College-Kumasi, and Catholic University College-Sunayni. The researchers can conclude that even though the Ubuntu OS has not been in existing for long but its growth in the market has been tremendous especially among computer science and IT students. The simplicity of use coupled with convenience and customization factor have been the influential features of this technology. Ghanaians are now appreciating and moving towards to usage of Ubuntu OS as a good number of them are using the OS.

In present era of technology advancement, the usage of desktop computers and other forms of computers such as smart phones which also called as is increasing day by day throughout the world. The same trend is also happening in Africa and for that matter Ghana. There are various technologies are introduced into desktop computers day by day. According to a survey conducted by the internetlivestats.com in 2014, about 19.56% of Ghanaians are were accessing the internet for various purposes when our total population was around 26,442,178 .Per this analysis the researchers can conclude that this 19.56% of the of Ghanaians who were using the internet were also using computer in different forms thereby using Operating Systems (OS). There are so many marketers/ companies that are producing various computers with different operating system and technologies. The main popular OS used in Ghana are Windows, Android, Ubuntu and Apple OS.

A survey has been taken among OS users in Ghana. Ubuntu operating system is one of the most widely used desktop and laptop Operating System among students, lecturers and others users these days. Since Ubuntu is an open source it has become one of the fastest growing operating system. Due to its open nature it has become favorite for many consumers and developers. Moreover software developers can easily modify or customized and add enhanced feature in it to meet their individual requirements of the computer technology. Ubuntu Powerful development framework allow users as well as software engineers to be able to create their own applications for wide range of devices.

Ubuntu, originally with its pronunciation as /ʊˈbuːntʊ/ uu-BOON-tuu, according to the company website /ʊˈbʊntuː/ uu-BUUN-too is an African language that roughly referred to the 'humanity towards others' and comes from the Zulu and Xhosa African languages. If the name is connected with the fact that this is a Linux distribution based on the Debian distribution, that is free to the satisfaction of all who wish to use it, from whom is inherited all of its qualities, it's no wonder that Ubuntu and its variants more popular distributions, although 2004 year is presented as discussed elsewhere .

Debian distribution based on a fully voluntary work of members of the FSF Association (The Free Software Foundation), whose key objective is to develop the software for free to anyone, which is currently in the development of this type of software involved more than 1000 people. Ubuntu is a different project than Debian, but in both projects included people from both teams, and it is therefore very similar in important characteristics .

This spring's latest update to Ubuntu is a landmark release. That's not just a way of saying that Ubuntu 14.04 marks a turning point for the popular Linux operating system, for this is a Long Term Support edition. See all software reviews.

As such, it will be supported by developer Canonical for a full five years, making it particularly attractive for businesses and organizations that need a stable platform to roll out for their end users.

# CHAPTER 6

# SYSTEM IMPLEMENTATION

## 6.1 MODULE DESCRIPTION

6.1.1 ARP (Address Resolution Protocol)

Every device on a wireless network consists of two different addresses called the IP address and the MAC (Media Access Control) address. Although the actual communication takes place over the hardware address called MAC address, many computer applications transmit or receive data with IP addresses. Because of this, it is required to find the corresponding MAC address for IPv4 communication. So, to get the destination MAC address, Address Resolution Protocol is required. It is a protocol which links or maps the consequent MAC address (48 bits) with the IP address (32 bits).

### 6.1.2 Working Of ARP

ARP also maintains an ARP cache table that stores information about which MAC address is linked with which IP address. So whenever one device sends a packet to an IP address, first it checks the cache table to find if the required MAC address already exists or not. If it does, ARP is not used and the address found is used to transmit the packet. But if it does not exist in the table, then the device broadcasts ARP request over the network to know which device is using the required IP address. Being a broadcast packet, it is transmitted with a destination MAC address as FF:FF:FF:FF:FF:FF. After receiving the ARP request, all the devices check if their IP address matches with the one in the ARP request. If it does not match, the device will drop the packet without any action. The one whose IP address matches sends a unicast ARP reply which includes the destination MAC address. After this both the devices update their cache table for future references .

### 6.1.3 ARP Spoofing

ARP does not authenticate whether the reply is from the desired device or not. So, if the reply is not sent by the desired user, but instead by a malicious user then the network becomes prone to ARP spoofing . To sum up, ARP spoofing also called ARP cache poisoning is a technique in which a malignant user links its own MAC address with the legitimate IP address as a means to poison the ARP table within the network. As a consequence, all the data meant for the intended IP address is sent to the attacker’s MAC address instead. From here, the attacker can conduct various attacks and can damage the data in future. Many detection and prevention techniques exist to detect and prevent such false mappings. This survey conducts a deep comparative analysis of those strategies bringing out their advantages and disadvantages..

### 6. 1 .4 Man in the middle attack (MITM)

In this attack, the hacker intercepts the communication of two genuine devices. It receives the data from the transmitter and then forwards it to the target device to remain undetected. With this, they can steal the crucial data and can then use it for various purposes without distorting the communication. Keeping the hosts unaware, the hacker becomes a part of their communication and sniffs passwords or hijacks the secured internet sessions .

### 6.1.5 MAC flooding

MAC flooding does not attack any host machine rather it attacks the network switches. Switches maintain a table of MAC addresses known as CAM table which allows the switches to send data only to the intended user whereas the hub broadcasts the data to the entire network. In this attack, the perpetrator uses ARP poisoning to takedown the CAM table by overloading it with a huge amount of ARP replies.

### **CHAPTER 7**

# SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

## 7.1 TYPES OF TESTS

### 7.1.1 Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

### 7.1.2 Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

### 7.1.3 Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted

Invalid Input : identified classes of invalid input must be rejected

Functions : identified functions must be exercised

Output : identified classes of application outputs must be exercised

Systems/Procedures: interfacing systems or procedures must be invoked

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

### 7.1.4 System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

7.1.5 White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

### 7.1.6 Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

#### Unit Testing:

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach

Field testing will be performed manually and functional tests will be written in detail.

Test objectives

* All field entries must work properly.
* Pages must be activated from the identified link.
* The entry screen, messages and responses must not be delayed.

Features to be tested

* Verify that the entries are of the correct format
* No duplicate entries should be allowed
* All links should take the user to the correct page.

#### Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results**:** All the test cases mentioned above passed successfully. No defects encountered

Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results**:** All the test cases mentioned above passed successfully. No defects encountered.

# CHAPTER 8

**CONCLUSION**

Cyber security is growing in its importance. It is a requirement for every individual to be knowledgeable of attacks and follow certain safety measures when on the internet. Privacy and data protection have become the needs of the hour. The sensitive data like the username and password can easily be sniffed if the user does not follow the security principle when on the internet. We have seen that the user credentials are easily sniffed using the ARB tool. The user can observe some safety precautions which might prevent his data from getting stolen. To train the next generation of workers in this area, it is necessary for students to learn cyber security and related attacks/concepts using actual real world attack and protection implementation. Additionally, the user needs to be aware of best practices in safeguarding them self against popular cyber-attacks.

## FUTURE ENHANCEMENT

This study is carried out to check the economic impact that the system will have

on the organization. The amount of fund that the company can pour into the research and

development of the system is limited. The expenditures must be justified. Thus the

developed system as well within the budget and this was achieved because most of the

technologies used are freely available. Only the customized products had to be

purchased.

# APPENTIX 1: CODING

#include <stdio.h>

#include <string.h>

#include <stdlib.h>

#include <pcap.h> // To invoke the libpcap library and use its functions.

#include <errno.h>

#include <sys/socket.h>

#include <netinet/in.h>

#include <arpa/inet.h>

#include <time.h>

#include <netinet/if\_ether.h>

#include <unistd.h>

//#include <libnotify/notify.h>

#define ARP\_REQUEST 1 //ARP Request

#define ARP\_RESPONSE 2 //ARP Response

typedef struct \_arp\_hdr arp\_hdr;

struct \_arp\_hdr

{

uint16\_t htype; //Hardware type

uint16\_t ptype; //Protocol type

uint8\_t hlen; //Hardware address lenght (MAC)

uint8\_t plen; //Protocol address length

uint16\_t opcode; //Operation code (request or response)

uint8\_t sender\_mac[6]; //Sender hardware address

uint8\_t sender\_ip[4]; //Sender IP address

uint8\_t target\_mac[6]; //Target MAC address

uint8\_t target\_ip[4]; //Target IP address

};

void alert\_spoof(char \*ip, char \*mac){

printf("\nAlert: Possible ARP Spoofing Detected. IP: %s and MAC: %s\n", ip, mac);

}

int print\_available\_interfaces(){

char error[PCAP\_ERRBUF\_SIZE];

pcap\_if\_t \*interfaces, \*temp;

int i = 0;

if(pcap\_findalldevs(&interfaces, error) == -1){

printf("Cannot acquire the devices\n");

return -1;

}

printf("The available interfaces are: \n");

for(temp = interfaces; temp; temp=temp->next){

printf("#%d: %s\n", ++i, temp->name);

}

return 0;

}

void print\_version(){

printf(" / | / \_\_ \\/ \_\_ \\ \n");

printf(" / /| | / /\_/ / /\_/ / \n");

printf(" / \_\_\_ |/ \_, \_/ \_\_\_\_/ \n");

printf("/\_/\_\_|\_/\_/ |\_/\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \n");

printf(" / \_\_\_// | / / \_/ \_\_\_\_/ \_\_\_\_/ \_\_\_\_/ \_\_ \\ \n");

printf(" \\\_\_ \\/ |/ // // /\_ / /\_ / \_\_/ / /\_/ /\n");

printf(" \_\_\_/ / /| // // \_\_/ / \_\_/ / /\_\_\_/ \_, \_/ \n");

printf("/\_\_\_\_/\_/\_|\_/\_\_\_/\_/ \_\_/\_/ /\_\_\_\_\_/\_/ |\_| \n"); printf("\n ARP Spoof Detector v0.1\n");

printf("\nThis tool will sniff for ARP packets in the interface and can possibly detect if there is an ongoing ARP spoofing attack. This tool is still in a beta stage. \n");

}

void print\_help(char \*bin){

printf("\nAvailable arguments: \n");

printf("----------------------------------------------------------\n");

printf("-h or --help:\t\t\tPrint this help text.\n");

printf("-l or --lookup:\t\t\tPrint the available interfaces.\n");

printf("-i or --interface:\t\tProvide the interface to sniff on.\n");

printf("-v or --version:\t\tPrint the version information.\n");

printf("----------------------------------------------------------\n");

printf("\nUsage: %s -i <interface> [You can look for the available interfaces using -l/--lookup]\n", bin);

exit(1);

}

char\* get\_hardware\_address(uint8\_t mac[6]){

char \*m = (char\*)malloc(20\*sizeof(char));

sprintf(m, "%02X:%02X:%02X:%02X:%02X:%02X", mac[0], mac[1], mac[2], mac[3], mac[4], mac[5]);

return m;

}

char\* get\_ip\_address(uint8\_t ip[4]){

char \*m = (char\*)malloc(20\*sizeof(char));

sprintf(m, "%d.%d.%d.%d", ip[0], ip[1], ip[2], ip[3]);

return m;

}

int sniff\_arp(char \*device\_name){

char error[PCAP\_ERRBUF\_SIZE];

pcap\_t\* pack\_desc;

const u\_char \*packet;

struct pcap\_pkthdr header;

struct ether\_header \*eptr; //net/ethernet.h

arp\_hdr \*arpheader = NULL;

int i;

u\_char \*hard\_ptr;

char \*t\_mac, \*t\_ip, \*s\_mac, \*s\_ip;

int counter = 0;

time\_t ct, lt;

long int diff = 0;

pack\_desc = pcap\_open\_live(device\_name, BUFSIZ, 0, 1, error);

if(pack\_desc == NULL){

printf("%s\n", error);

print\_available\_interfaces();

return -1;

} else {

printf("Listening on %s...\n", device\_name);

}

while(1){

packet = pcap\_next(pack\_desc, &header);

if(packet == NULL){

printf("Error: Cannot capture packet\n");

return -1;

} else {

eptr = (struct ether\_header\*) packet;

if (ntohs(eptr->ether\_type) == ETHERTYPE\_ARP){

ct = time(NULL);

diff = ct - lt;

printf("ct: %ld; Diff: %ld; Counter: %d\n",ct, diff, counter);

if(diff > 20){

counter = 0;

}

arpheader = (arp\_hdr\*)(packet+14);

printf("\nReceived an ARP packet with length %d\n", header.len);

printf("Received at %s", ctime((const time\_t\*) &header.ts.tv\_sec));

printf("Ethernet Header Length: %d\n", ETHER\_HDR\_LEN);

printf("Operation Type: %s\n", (ntohs(arpheader->opcode) == ARP\_REQUEST) ? "ARP Request" : "ARP Response");

s\_mac = get\_hardware\_address(arpheader->sender\_mac);

s\_ip = get\_ip\_address(arpheader->sender\_ip);

t\_mac = get\_hardware\_address(arpheader->target\_mac);

t\_ip = get\_ip\_address(arpheader->target\_ip);

printf("Sender MAC: %s\n", s\_mac);

printf("Sender IP: %s\n", s\_ip);

printf("Target MAC: %s\n", t\_mac);

printf("Target IP: %s\n", t\_ip);

printf("--------------------------------------------------------------");

counter++;

lt = time(NULL);

if(counter > 10){

alert\_spoof(s\_ip, s\_mac);

}

}

}

}

return 0;

}

int main(int argc, char \*argv[]){

if(access("/usr/bin/notify-send", F\_OK) == -1){

printf("Missing dependencies: libnotify-bin\n");

printf("Please run: sudo apt-get install libnotify-bin");

printf("\n");

print\_version();

exit(-1);

}

if(argc < 2 || strcmp("-h", argv[1]) == 0 || strcmp("--help", argv[1]) == 0){

print\_version();

print\_help(argv[0]);

} else if(strcmp("-v", argv[1]) == 0 || strcmp("--version", argv[1]) == 0){

print\_version();

exit(1);

} else if(strcmp("-l", argv[1]) == 0 || strcmp("--lookup", argv[1]) == 0){

print\_available\_interfaces();

} else if(strcmp("-i", argv[1]) == 0 || strcmp("--interface", argv[1]) == 0){

if(argc < 3){

printf("Error: Please provide an interface to sniff on. Select from the following.\n");

printf("--------------------------------------------------------------------------\n");

print\_available\_interfaces();

printf("\nUsage: %s -i <interface> [You can look for the available interfaces using -l/--lookup]\n", argv[0]);

}

else

{

sniff\_arp(argv[2]);

}

}

else

{

printf("Invalid argument.\n");

print\_help(argv[0]);

}

return 0;

}

**APPENTIX 2**

**SCREENSHOTS**

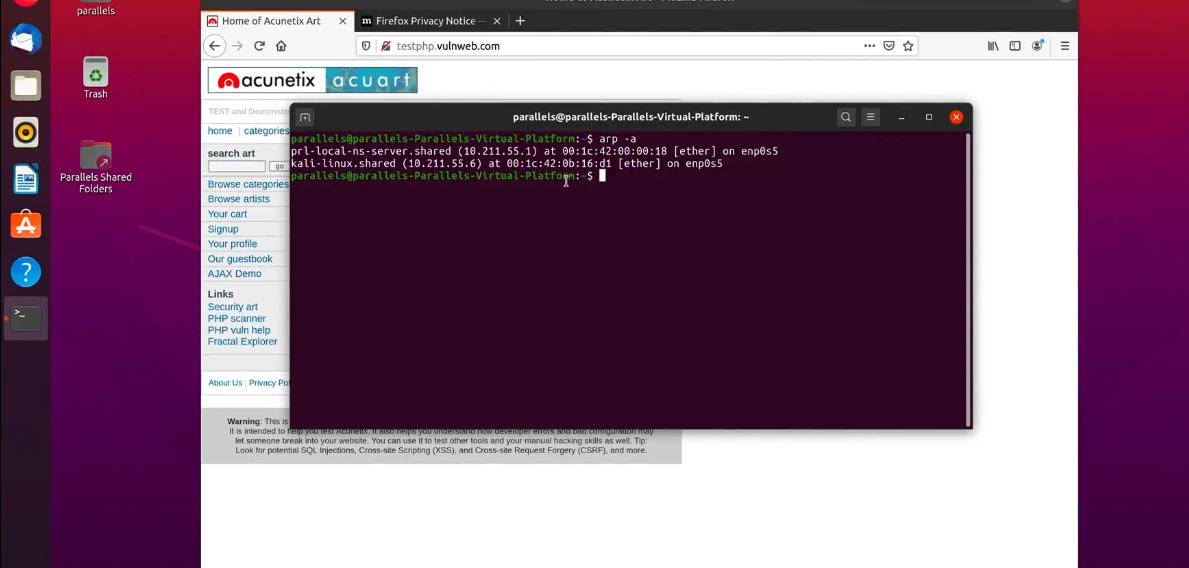
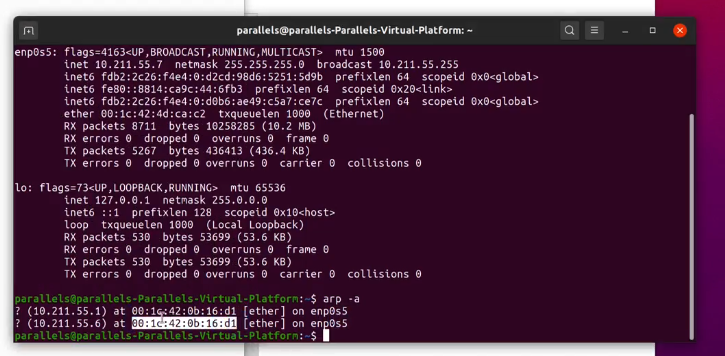
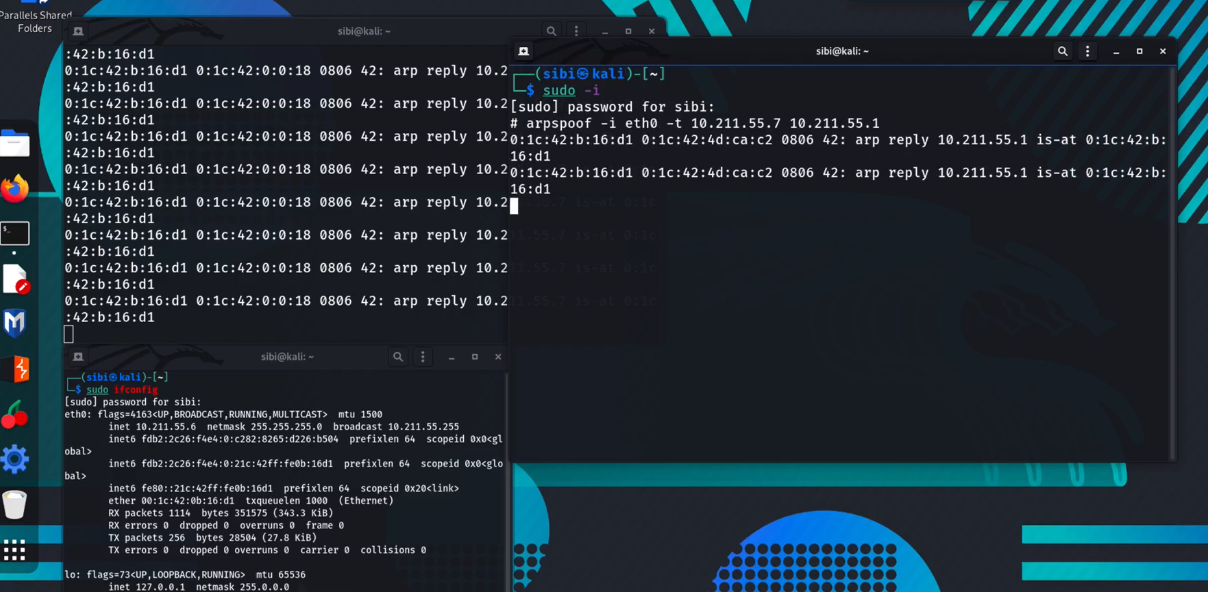
****

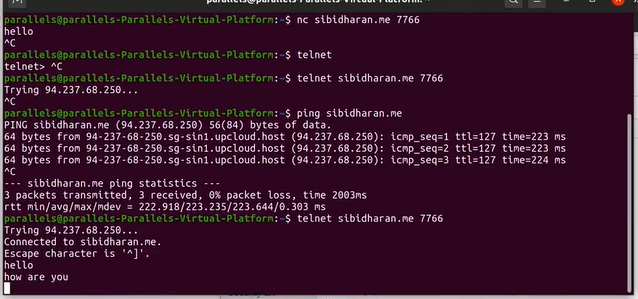
Figure2:1 ARP Sniffer

****

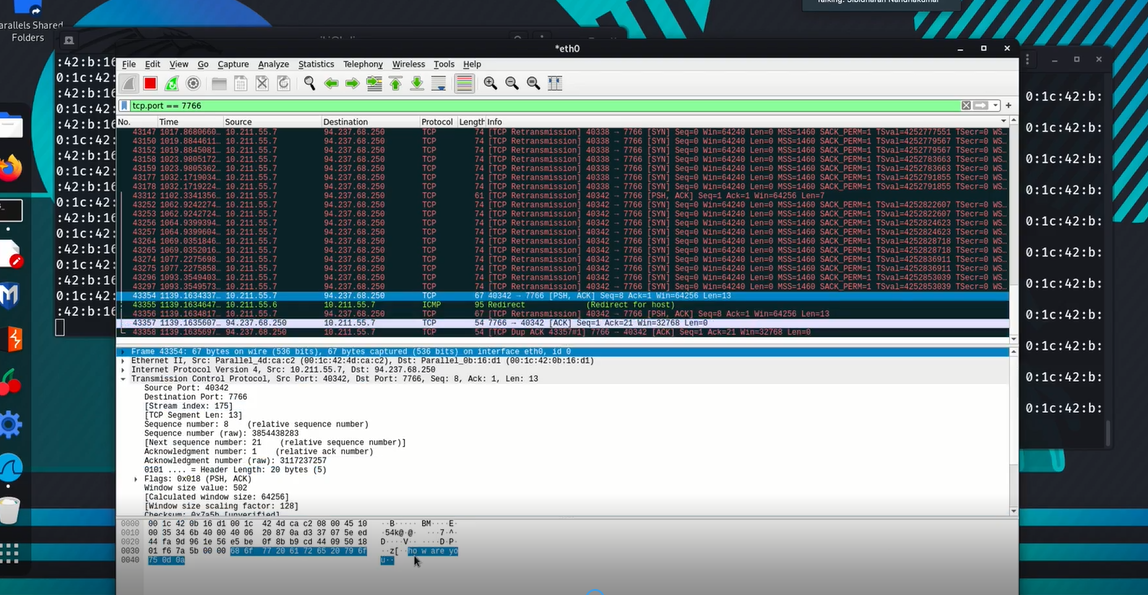
**Figure2:2 IP Spoofing**

****

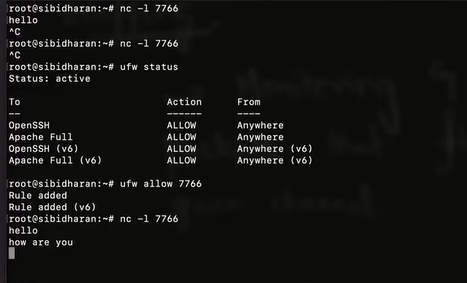
**Figure2:3 Packet Sniffing**

****

**Figure2:4 Source of data from packet transfer**

****

**Figure2:5 Analysis the packet to sniffing**

****

**Figure 2:6 Destination of data from packet receiving**

**REFFERENCE**

[1] A. Ornaghi, “Ettercap project,” [Online]. Available: http://ettercap.sourceforge.net/. [Accessed 10 Feb 2018].

[2] D. Norton, “sans.org,” sans institute, [Online]. Available: https://www.sans.org/reading-room/whitepapers/tools/ettercapprimer-1406. [Accessed 10 Feb 2018].

[3] J. Elks, “grin.com,” [Online]. Available: https://www.grin.com/document/170676. [Accessed 10 Feb 2018].

[4] M. Conti, D. Nicola, and V. Lesyk. "A survey of man in the middle attacks." IEEE Communications Surveys & Tutorials 18, no. 3 (2016): 2027-2051.

[5] N. Du Paul, “veracode.com,” CA technologies, [Online]. Available: https://www.veracode.com/security/man-middle-attack. [Accessed 08 Feb 2018].

[6] P. Smith, “bitcoinist.com,” 09 Feb 2018. [Online]. Available: https://bitcoinist.com/ledger-hardware-wallets-vulnerable-manmiddle-attacks/. [Accessed 10 Feb 2018

[7] “iugaza.edu.ps,” [Online].Available:http://site.iugaza.edu.ps/nour/files/lab4MITM1.pdf. [Accessed 05 Feb 2018].

[8] xinlwang,“mtu.edu,”[Online].Available:http://pages.mtu.edu/~xinl wang/itseed/labs/Spoof\_MiTM.pdf. [Accessed 09 Feb 2018].

[9] G. N. Nayak, “Different Flavours of Man-In-The-Middle attack, Condequences and Feasible solutions,” IEEE, pp. 491-495, 2010.

[10] D. D. Yogesh Joshi, “Mitigating Man in the middle attack over Secure socket layer,” in IEEE, Bangalore, 2009.].

[11] S. T. Sumit kumar, “A Centralized Detection and prevention Technique against ARP poisoning,” pp. 259-264.

[12] S. Y. Nam, “Enhanced ARP: Preventing ARP poisoning-Based Man-in-the-Middle Attacks,” IEEE COMMUNICATIONS LETTERS,, vol. 14, pp. 187-189, 2010.

[13] h. R. Faheen Fayyaz, “Using JPCAP to prevent man-in-the-middle attacks in a local area network environment,” 2012.

[14] “virtualbox,” or, [Online]. Available: https://www.virtualbox.org/. [Accessed 14 04 2018]