SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTER SYSTEMS AND NETWORKS

Java app for network attacks concepts

تطبيق جافا لتوضيح مفاهيم الهجمات علي الشبكه

A PROJECT SUBMITTED AS ONE OF THE REQUIREMENTS FOR OBTAINING A BACHELOR OF HONOR IN COMPUTER SYSTEMS AND NETWORKS

OCTOBER 2015

بسم الله الرحمن الرحيم

SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTER SYSTEMS AND NETWORKS

Java app for network attacks concepts

A PROJECT SUBMITTED AS ONE OF THE REQUIREMENTS FOR OBTAINING A BACHELOR OF HONOR IN COMPUTER SYSTEMS AND NETWORKS

PREPARED BY

STUDENT: FATIMA AWD ALKAREEM MOHAMMED ALI

STUDENT: RASHA ABDEEN

STUDENT: SAHAR MOHAMMED ABDALRHEEM

STUDENT: SAJA MOHAMMED ALAZHARY

SUPERVISOUR: MOHAMMED OSAMA HEWITEALLA

SIGNATURE OF SUPERVISOR

DATE

OCTOBER 2015

الآيـــــة

قال تعالى:{ يرفع الله الذين امنو منكم والذين أوتو العلم درجات}

[المجادلة:11]

الحمد لله

الحمدُ لله أتـَـمَّ النـِّـعمةَ على الأمَّة و أكمل لها دِينها، و آتى الحِكْـمَة أهلَـها

و تـَـمَّـمَ بـمُحمدٍ مَـكـَـارمَ الأخلاق كـُـلـَّـها.

و أشـهـدُ أنْ لا إله إلا الله وحـدَه لا شريك له شَهادة نـَـسْـتـَـظِـلُّ بـظِـلـِّـها

و نـَـحْـيَى و نموتُ عليها و نـَـلـْـقى اللهَ بها. و أشْـهَـدُ أنَّ مُحـمـدا عبدُه و رسولـُـه،

الحمد لله أولى ما فغر النَّاطقُ به فمَه،

وافتتح كلِمَه، عَظُمت منَّته، وعمَّت رحْمتُه، وتمَّت كلِمَته، ونفذت مشيئتُه،

وسبَّح الرَّعد بِحَمده والملائكةُ من خيفتِه، نَحمدهُ بِجميع مَحامده ونُثْني عليه ببادئ الأمر وعائده،

ونشْكُره على وافر عطائِه ورافده.

DEDICATION

To all my family members whom were source of success, by giving me the confidence, my father and mother, all Brothers.

Fatima

To the one I share my soul with to my darling mother who keeps praying for me and my friends. To my colleagues who support me, to the joy of the live, my dear friends.

Rasha

To all my family members and all friends.

Sahar

Thanks all thanks to ALLAH first, and thanks to my family, all friends.

Saja

AKNOWLEDEMT

First and last thanks to ALLAH

All the regards and respect to the light of the dark roads we did across:

T. Mohamed Osama Hewait Allah, T. Ismail Ali Ibrahim

Dedicating special thanks to:

Mohamed Omer for his continues support us.

Thanks for all who help us to done this project in this way.

ABSTRACT

The idea of transfer and exchange of information is not a new idea, and the appearance of networks has become a quick and easy data transfer process, which led to the spread and frequent use at a large scale necessitating the application of procedures and techniques for security to protect the data exchanged and result of the appearance of some users who are taking advantage of the vulnerabilities of the network for data unauthorized and used for subversive goals.

Hence, data protection and network security has become an urgent need to process through the development of techniques used to protect the awareness of users and the types of attacks that may be exposed to the network and the impact on them.

The goal of this project is to help the student of computer science to understand the attacks that

May be exposed to the network using system simulation illustrates some of the concepts that are taught to him during the course of networks security.

This project was implemented using the Java language to simulate concepts of some attacks may occurs in network.

The user selects the attack which he wants, and the type of parameters necessary to execute this attack. After that he know the result of occurring that attack on the network.

We recommend that the application applies more attacks and develop algorithms of the discovery of each attack simulation and also explain how to protect them.

المستخلص

إن فكـــرة نقـــل المعلومـــات وتبادلهـــا ليســـت بفكـــرة جديـــدة ، وبظهـــور الشـــبكات أصـــبحت عمليـــة نقـــل البيانـــات ســـهلة وســـريعة ، ممـــا أدى إلـــى إنتشـــارها وكثـــرة اســـتخدامها علـــى نطاق واسع مما استلزم تطبيق إجراءات وتقنيات

أمنيـــة لحمايـــة البيانـــات المتبادلـــة وذلـــك لظهـــور بعـــض المســـتخدمين الـــذين يســـتغلون الثغـــرات الموجـــودة فـــي الشـــبكة للحصـــول علـــى بيانـــات غيـــر مصـــرح لهـــم بهـــا واســـتخدامها لأهداف تخريبية .

ومـــن هنـــا أصـــبحت عمليـــة حمايـــة البيانـــات وتـــأمين الشـــبكات ضـــرورة ملحـــة مـــن خـــلال تطـــوير التقنيـــات المســـتخدمة للحمايـــة وتوعيـــة المســـتخدمين بـــأنواع الهجمـــات التـــي قـــد تتعرض لها الشبكة والأثر المترتب عليها .

الهـــدف مـــن هـــذا المشـــروع هـــو مســـاعدة طالـــب علـــوم الحاســـوب علـــى فهـــم الهجمـــات التـــي قـــد تتعـــرض لهـــا الشـــبكة باســـتخدام نظـــام محاكـــاة يوضـــح بعـــض المفـــاهيم التـــي يـــتم تدريسها له أثناء كورس سرية الشبكات .

تـــم تطبيـــق هـــذا المشـــروع باســـتخدام لغـــة جافـــا لمحاكـــاه مفـــاهيم بعـــض الهجـــات التـــي قـــد تتعـــرض لهـــا الشـــبكه، يختـــار المســـتخدم نـــوع الهجمـــة التـــي يريـــد تطبيقهـــا ويقـــوم بإدخـــال المتغيرات اللازمة لمحاكاة لهذه الهجمة . ورؤية نتيجه حدوث الهجمه علي الشبكه.

نوصـــي بـــأن يـــتم اضـــافة المزيـــد مـــن الهجمـــات واضـــافة خوارزميـــات اكتشـــاف كـــل هجمـــه وتوضيح كيفية الحمايه منها

Table of content

Contents

Table of Figure

List of tables

Chapter 1

INTRODUCTION

1.1 Introduction

Network security has become one of the most important factors to be considered. The advantages of having computer network security are that you are keeping all files, data and personal information protected from unauthorized access from both people inside and outside the network.

The main objective of this project is to enable the student to understand and accommodate network penetrations studied during network security course.

1.2 PROBLEM

The Network security course used to concern with protection of data during their transmission through network layers, these layers exposed to be attacked.

Problem faces student in this course is the difficultness of understanding these types of attacks that can realized on network, because there is no requirements of having a sophisticated lab (servers, routers , etc.) , also they need to study this information in simplified way to get understand. Our tool make simple attacks concepts in scenarios to help student understand these attacks. It is easy, portable, does not need internet connection and thus they can make experiments whenever they want.

1.3 OBJECTIVIES

This project aim to provide a tool that helps achieving these set of objectives:

- Help students to understand the concept of network security attacks without the requirement of having a sophisticated lab (servers, routers…).
- Enable students to have inexpensive, flexible and configurable lab.
- Provide the opportunity to study large scale networks. This might help us to determine what kind of defenses we need to protect our network before creating it in real world.

1.4 SCOPE

This tool implements concepts of some attacks which could happen in OSI seven layers, these attacks are:

Denial-Of-Service (DOS overflow), Distributed Denial-Of-Service (DOSS), IP Spoofing, Man-in-Middle and SYN-Flooding attack.

1.5 METHODOLOGY

The research will use the descriptive appropriate approach to attain its goals. A tool developed to help students to digest the network attacks. To solve our problem we are going to understand each attack and represent its concept in simplifies way, we use java programming langue to develop our application which enable user to build his network

and choose among a varied attacks options. During attack scenario execution all information of sending and receiving has been written in a log file

1.6 THESIS LAYOUT

Chapter 2 discusses general introduction to the network security, simulation and some types of attacks on network layers.

Chapter 3 discusses some previous studies that related to the thesis.

Chapter 4 describes the tools and techniques.

Chapter 5 describes system analysis.

Chapter 6 describes the implementation of the system.

Chapter 7 describes result & recommendation.

CHAPTER 2

THEORETICAL BACKGROUND

2.1 Introduction to Network Security

A security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, community, nation, or organization.

The security of information felt to be valuable to an organization was provided primarily by physical and administrative means. An example of the Former is the use of rugged filing cabinets with a combination lock for storing sensitive Documents. Information Security relates to the information (owned) by an organization. Traditionally included three component parts:

1-Confidentiality:

Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

2-Availability:

Assures that systems work promptly and service is not denied to authorize users.

3-Integrity:

Assures that information and programs are changed only in a specified and authorized manner.

There are two component recently added to the security:

4-Accountability:
Someone is personally accountable and responsible for the protection of information assets.

5-Audit-ability:

Ability to explain changes to information state and ongoing audit tests [2].

2.3 Computer and network security

The idea that Computer security is primarily concerned with the protection of data stored in main memory or in secondary memory from malwares and others by techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. [2].

2.4 The importance of security

There are many important of security such as:

- It’s protecting company and its assets against theft, abuse and other forms of harm and loss.
- Estimate possible damage and potential loss through Risk analysis.
- It complies with requirements for confidentiality, integrity and availability.

- Motivate administrators and employees to maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents. [2].

2.5 Security Attacks

Most of attacks are made by hackers, the term ‘hacker’ is used to describe someone who attempts to break into computer systems. Typically, this hacker would be a proficient programmer with sufficient technical knowledge to understand the weak points in a security system.

In general, Attacks can be classified into:

2.5.1 Passive Attacks

Is the nature of eavesdropping on, or monitoring of, transmissions Figure 2-1 illustrate the passive attack

2.5.1.1 An example of the passive attack

User A transmits a file to user B. The file contains sensitive information that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a Transmission Copy of the file during its [2].

2.5.2 Active Attack

Active attacks are involve some modification of the data stream or the creation of a false stream. *Figure (2.3)* illustrate the active attack.

2.5.2.1 An example of the active attack

A network manager, D, transmits a message to a computer, E, under its Management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User F intercepts the message, alters its contents to add or delete entries, or construct his

Own message and then forwards the message to E, which accepts the message as coming from manager D and updates its authorization file accordingly.

These types of attacks are in general, but in deep there are some attacks occur in each OSI seven layers model of network which we will explain them [2].

2.6 OSI model and possible attacks

The OSI model is protocol stack where lower layers deal primarily with hardware and upper layer deal with software. The OSI model's seven layers are designed, so that control is passed down from layer to layer.

Networking is a prime concern for information security. The ubiquitous nature of Network connectivity may let us access the world from our computer, but it also lets that same world gain access back to us in ways we may not desire. No matter how well we secure our own hosts, we are still vulnerable if the parts of the infrastructure between our distant destinations and ourselves fall victim to intentional exploitation or unwitting mishap.

Data networking is a critical area of focus in the study of information security. A key area of data networking theory - The Open Systems Interconnect (OSI)

Seven Layer Network Mode. Hence that the OSI was built to allow different layers to work without the knowledge of each

Others, so if one layer is hacked, communications are compromised without the other layers being aware of the problem [3].

2.6.1 Layer One -Physical Layer

Layer one of the OSI model is known as the physical layer .Bit level communication take place at layer one. Bits have no defined meaning on the wire; however, the physical layer defines each bit loss and how it transmitted and received. Physical layer component include copper cabling, fiber cabling, wireless system components and Ethernet hubs. It's critical to data communications. It is also the most vulnerable and changeable, some Vulnerability in the physical layer [3].

2.6.1.1 Layer one attack

An attacker gaining to access physically to the telecommunication closet, or an open port in the conference room, or an unused office, could be the foothold needed to breach the network or ,even worse , gain physically access to a server or piece of equipment

Unauthorized changes to the functional environment (data connections, removable media, adding/removing resources), It's a generally accepted fact that if someone gains access physical to an item, they can control it [4].

2.6.2 Layer Two -Data Link Layer

Layer two is known as the data link layer and is focused on traffic within a single Local Area Network (LAN).The data link layer formats and organizes the data before sending it to the physical layer.

Data link layer components include: Bridges, Switches, MAC addresses and Network Interface Card (NIC) [3].

2.6.2.1 Data Link Layer attacks

1. CAM Overflow

2. MAC spoofing Attack

2.6.3 Layer Three - Network Layer

Layer three is known as the network layer. It is concerned with the global topology of the internet work. It is used to determine what path a packet would need to take to reach

a final destination over multiple possible data links and paths over numerous intermediate hosts. This layer typically uses constructs such as IP addresses to identify nodes[3].

2.6.3.1 Network layer attack

-Routing (RIP) attack.

2.6.4 Layer four -Transport Layer

Layer four is known as the Transport Layer. It is a pulsatory heart of the OSI model because it is accountable for linking between upper layers and lower layers, concerns with the transmission of data streams into the lower layers of the model, taking data streams from above and packaging them for transport, and with the reassembly and passing of incoming data packets back into a coherent stream for

The upper layers of the model. While some transport protocols are designed for high reliability and use mechanisms to ensure data arrives complete at its destination, such as the TCP, others (such as UDP) are not.

The Transport Layer is the first purely logical layer in the model. It is the primary point where multiple data conversations from or to a single host are multiplexed [3].

2.6.4.1 Transport layer attack

- UDP Flooding

2.6.5 Layer Five- Session Layer

Layer five is known as the Session Layer. Its purpose is to allow two applications on different computers to establish and coordinate a session, it's also responsible for managing the session while information and data is being moved. When a data transfer is complete, the session layer tears down the session. It includes Remote Procedure Call (RPC) which provides a different paradigm for accessing network services. And Structured Query Language (SQL) through managing multiple queries to the SQL database [3].

2.6.5.1 Session layer attack

-Session hijacking

2.6.6 Layer Six- Presentation Layer

Layer six is known as the Presentation Layer. The main purpose for the

Presentation layer is to deliver and present data to the Application layer. This data must be formatted so that the Application layer can understand and interpret it.

The Application layer responsible for items such as:

-Encryption and Decryption of messages.
-Compression and Decompression of message, format translation.

-Handling protocol conversion [3].

2.6.6.1 Presentation layer attacks

-SSL Stripping

2.6.7 Layer Seven- Application Layer

The Application Layer allows applications to use network services. Some of the protocols and programs that operate in the Application Layer include: FTP, Telnet, Remote Desktop, Web Browsers, HTTP, Email Clients and more [3].

2.6.7.1Application layer attacks

- DDOS attack (Distributed Denial of Service Attack)

2.7 Simulation

Although we demonstrated these types of attacks with scenarios, but still the concept of these types of attacks is not clear. So, we need to explain these attacks practically, to make users learning by doing. Simulation can do this.

Computer simulation is the discipline of designing a model of an actual or theoretical physical system, executing the model on a digital computer, and analyzing the execution output. Simulation embodies the principle of "learning by doing "to learn about the system we must first build a model of some sort and then operate the model. The use of simulation is an activity that is as natural as a child, Children understand the world around them by simulating (with toys and figurines) most of their interactions with other people, animals and objects.

Also the user wants to explore the unknown and learn things as a result of this exploration .As adults, we lose some of this childlike behavior but recapture it later on

Through computer simulation. To understand reality and all of its complexity, we must build artificial objects and dynamically act out roles with them. Computer simulation is

The electronic equivalent of this type of role playing and it serves to drive synthetic environments and virtual worlds. Within the overall task of simulation, there are three primary sub-fields: model design, model execution and model analysis. Which is mean designing a model of an actual or theoretical physical system, executing the model on a digital computer, and analyzing the execution output.

To simulate something physical, you will first need to create a mathematical model which represents that physical object. Models can take many forms including

Mathematical model properties of which are described by mathematical symbols and relations, Physical Models, properties of which are described by physical structures and relations, Process Models the process a system performs, Represents dynamic relations by mathematical and logical functions.

A multimodal is a model containing multiple integrated models each of which represents a level of granularity for the physical system. The next task, once a model has been developed, is to execute the model on a computer, we need to create a computer program which steps through time while updating the state and event variables in your mathematical model.

There is need of simulation because it allows to examine system behavior under different scenarios in virtual computational world .It can be used to identify the bottlenecks in a process, provide a safe, and relatively very cheap (in term of both cost and time) test to evaluate the side effects and to optimize the performance of system before transferring it to the real world. [1]

2.7.1 Types of Simulations

While computer simulations today are used in almost every discipline and for all sorts of purposes, the usage can be divided into three main categories: Scientific research, practical application, education and recreation. Each has somewhat different requirements and usage patterns though overlaps do exist.

1. Scientific Research

2. Practical Application

3. Education and Recreation

2.8 The suggested system

Build simple tool to make simple attacks concepts in scenarios to help student understand these attacks. It is easy, portable, does not need internet connection and thus they can make experiments whenever they want.

Therefore we tried in application to cover part of these concepts that are difficult to understand in theory.

The attacks we will cover it in our application are:

1. DOS (Denial-Of-Service)
2. DDOS (Distributed Denial-Of-Service)
3. IP Spoofing.
4. MIM (Man-In-Middle)
5. SYN Flooding.

2.8.1 DOS (Denial-Of-Service)

In a denial-of-service (DOS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, An attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer. There are two general methods of DOS attacks: flooding services or crashing services. Flood

services attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop**.**

2.8.2 Flood attacks Type

1. **Buffer overflow attack**:

The most common DOS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks

2. **ICMP flood:**

Leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.

4. **SYN Flood:**

Attacker sends a request to connect to a server, but never completes the TCP handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

In our simulator we will not cover all types of DOS method, we just limit ourselves with Buffer overflow attacks.

2.8.3 DDOS Attack

The DDOS attack uses multiple computers and Internet connections to flood the targeted resource. DDOS attacks are often global attacks.

2.8.4 MITM Attack

In MITM attack the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other.

It's a form of eavesdropping but the entire conversation is controlled by the attacker, who even has the ability to modify the content of each message. Often abbreviated to MITM, MitM, or MITMA.

2.8.5 IP Spoofing Attack

The Internet Protocol or IP is used for sending and receiving data over the Internet and computers that are connected to a network. Each packet of information that is sent is identified by the IP address which reveals the source of the information.

When IP spoofing is used the information that is revealed on the source of the data is not the real source of the information. Instead the source contains a bogus IP address that makes the information packet look like it was sent by the person with that IP address. If

you try to respond to the information, it will be sent to a bogus IP address unless the hacker decides to redirect the information to a real IP address.

2.9 CONCLUSION

This chapter has discussed the theoretical background and some of the concepts related for the research such as simulation and its types (Scientific Research, Practical Application and education and Recreation) and the end of the chapter we also discussed The suggested system.

Chapter 3

Related studies

3.1 INTRODUCTION

This chapter discuses some studies related with the thesis and table of comparison between it and our application.

3.2 studies

3.2.1 Skybox security simulator

Skybox has created a powerful tool to give IT, audit and security teams a comprehensive view of threats, as well as the ability to virtualize penetration testing through an innovative modeling scheme.

Skybox has secure tools to identify, analyze and visualize risks to your organization, and the business impact of those threats; it takes care of change policies and the compliance of your network devices [5]. Skybox work with these domains:

1. Skybox Vulnerability Control

Skybox View builds a detailed map of your network and assesses threats against it based on feeds from VA scanners (a vulnerability scanner**)** and SIMs **(**Security

Information Management), automatically evaluates risk, and prioritizes remediation activities within the context of your network.

The result is a unique and flexible approach for assessing and managing specific threats and overall risk to your digital assets.

2. **Vulnerability Assessment Using a Scan less, Rule-Driven Approach** traditionally, vulnerability assessment has relied on vulnerability scanners for vulnerability discovery. However, in today's enterprise-scale networks, there is no way for most enterprise security teams to examine prioritize, and remediate vulnerabilities fast enough to effectively reduce overall risk levels.

But security teams can take a more effective approach to vulnerability assessment. Rule-driven profiling converts the product information stored in system and security management repositories into a detailed product catalog and then accurately deduces a list of vulnerabilities in the network. With this information, more than 90 percent of the vulnerabilities in a typical enterprise network can be accurately discovered, without an active scan.

3. **Attack Simulation.**

It discovers some of attack scenarios, by all possible threats with business impact, Simulates attack scenarios to determine the impact of an attack from multiple different threat origins. It is also Scalable to large, complex networks where this analysis could not be done manual [6].

Advantages:

1- **Provides daily assessment of vulnerabilities:** continuous assessments and visibility requires less management time and delivers greater network coverage.

2- **Reduces risk exposure**: up-to-date information from highly accurate data sources shrinks risk exposure levels by shortening the time between identification of a vulnerability to remediation.

3- **Easy to deploy and manage**– connect to one or a few available data repositories, eliminating the need to touch every endpoint [13].

The operating system supported for the skybox is
-Centos.

-Windows.

-Red Hat Linux**.**

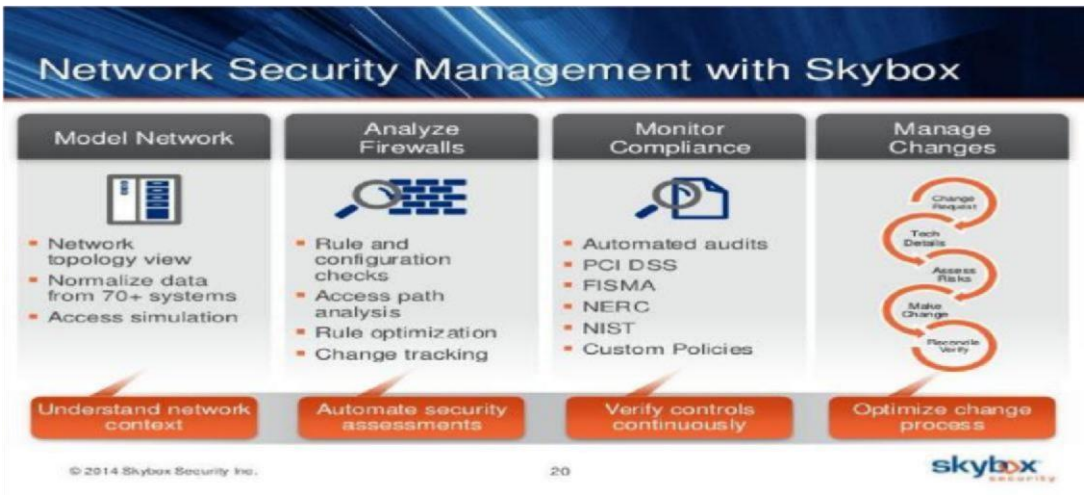

Figure 1 skybox

3.2.2 NeSSi-2 (Network Security Simulator-2)

NeSSi incorporates a variety of features relevant to network security distinguishing it from General-purpose network simulators. Its capabilities

Such as profile based automated attack generation, traffic analysis and interface Support for the plug-in of detection algorithms allow it to be used for security research and evaluation purposes.

NeSSi has been utilized for testing intrusion detection algorithms, conducting network Security analysis, and developing distributed security frameworks at the application level. NeSSi is built upon JIAC (Java Intelligent Agent Component ware). Framework, which is a service centric Middleware architecture based on the agent paradigm. Within NeSSi, agents are used for modeling and implementing the network Entities such as routers, clients, and servers. The underlying JIAC agent framework provides a rich and flexible basis for implementing and testing of various security deployments and algorithms In NeSSi.

3.2.2.1 The features of NeSSi

Attack Modeling

The simulation setup in NeSSi² is not only comprised of network creation and attachment of traffic profiles, but additionally security related settings can be configured. When a security framework composed of several detection units is to be tested, profiles can also be used in NeSSi Detection Unit API**:**

The term detection unit is to understand as an abstract term for any algorithm or tool employed for the purpose of detecting malicious activity such as intrusion or service degradation attempts. NeSSi² provides a Detection Unit API for the development of new detection algorithms as well as the integration of existing ones. Figure 3.2 illustrates the NeSSi-2 simulator workspace [7].

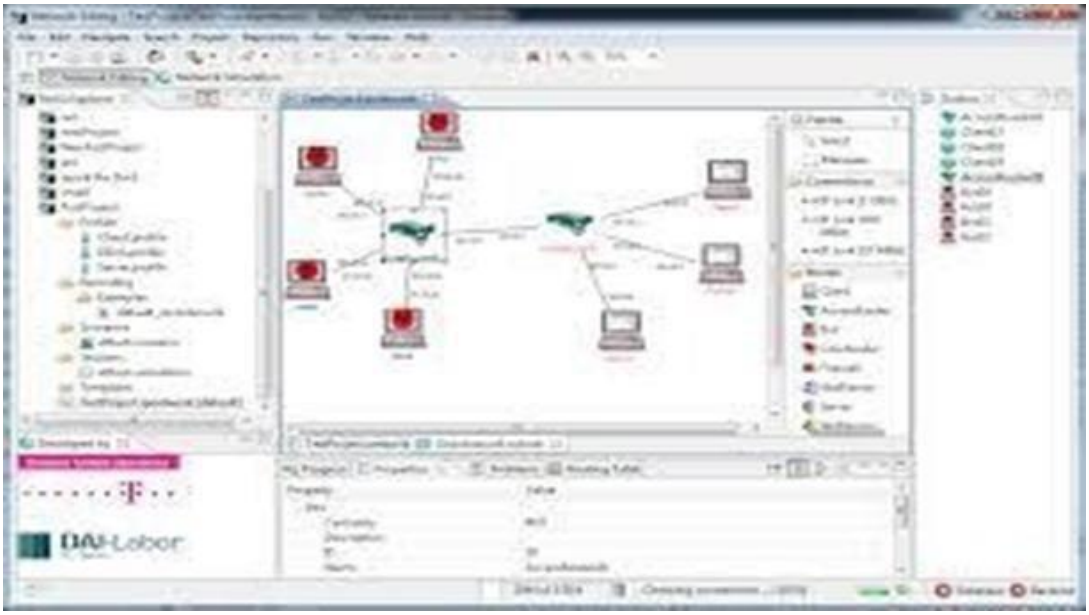

Figure 2 NeSSi

The comparison between the previous studies and our simulation NSLS (Network security lab simulator)

Previous studies	Similarities	Differences
Skybox	Simulate attack of a network.	Skybox is simulating attack by two approaches. It **Visualize threats from any origin and it Think like a hacker.** This mean it discovers possible attack scenarios and simulates those attacks to determine impact. Attack simulation uses an accurate model of an organization's network created from device configurations containing network interface information, routing rules, and access control rules[8]. In our simulation we simulate some of attack scenarios in four lower layers in network. And implements attacks manual without any supporting tool.
NeSSi2	Simulate network attacks in the OSI layers.	NeSSi2 it used to testing intrusion and it do this by create network topology. The topology can then be re-used for different scenarios .The scenario is

		comprised of elementary building blocks for each device in the network, every node profiles consists Detection mechanisms it executed on an individual node to test intrusion[7]. In our simulation we simulate some of attack scenarios in four lower layers in network. And implements attacks manual without any supporting tool not detect attack or intrusion in network.

Table 1 comparison between the previous studies and our simulation NSLS

3.3 CONCLUSION

By the end of this chapter we understand how the studies support network security against attacks and compared between these studies and our project.

Chapter 4

Tools and Techniques

4.1 INTRODUCTION

This chapter discusses the tool and technologies used in the project, they are:

Java, uml, enterprise and eclipse.

4.2Tools and Techniques

4.2.1 Java

Java is a language that is concurrent ,class-based ,object oriented ,and specifically designed to have as few implementation dependencies as possible.

It depends upon definition of best programming language, if its popularity then obviously Java out score everyone, even C. If it in terms of Job opportunities, again Java out score every one also can develop core Java based server side application, J2EE web and enterprise applications, and can even go for Android based mobile application development [9].

4.2.2 ECLIPSE

Eclipse is an integrated development environment (IDE). It contains a base workspace and an extensible plug-in system for customizing the environment.

Written mostly in Java, Eclipse can be used to develop applications.

By means of various plug-ins, Eclipse may also be used to develop applications in other programming languages : Ada, ABAP, C, C++, COBOL, Fortran, Haskell, JavaScript, Lasso, Natural, Perl, PHP, Prolog, Python It can also be used to develop packages for

Software Mathematical Development environments include the Eclipse JDT for Java and Scala, Eclipse CDT for C/C++ and Eclipse PDT for PHP, among others [10].

4.2.3 ENTERPRISEARCHITECT

Enterprise Architect is a very powerful Visual Modeling Platform for Comprehensive UML analysis and design tool, Rich modeling for business, software and systems, Full

Traceability from requirements to deployment, Code engineering in over 10 languages, Scalable, team-based repository, Enterprise frameworks, mind maps, BPMN

4.2.4 UML

UML (unified modeling language) is an international industry standard graphical notation for describing software analysis and designs. Therefore, standardization provides for efficient communication and leads to fewer errors caused by misunderstanding [11].

4.3 CONCLUSION

This chapter has discussed the most important tools and techniques that will be used to achieve the goals of this research.

Chapter 5

SYSTEM ANALYSIS

5.1 INTRODUCTION

This chapter describe the system, related functions of system and how the system will be analysis.

5.2 SYSTEM DESCRIPTION

5.2.1 GENERAL DESCRIPTION

The architecture of the system is java classes collected to simulate some type of attacks.

5.2.2 DESCRIPE FUNCTIONS

The Basic Functions on thesis is creating, store information, view result of attack scenario and retrieve result of an existed scenario.

5.2.3 DESCRIPE USER

The project have one user (A student) .A student can create scenarios and simulate it , he can see result one or more times.

5.3 SYSTEM ANALYYSIS

This section covers how the system will work using UML Graphs. Enterprise Architect has been used to create the following UML Diagrams for theoretical analysis.

5.3.1 THE USECASE DIAGRAM

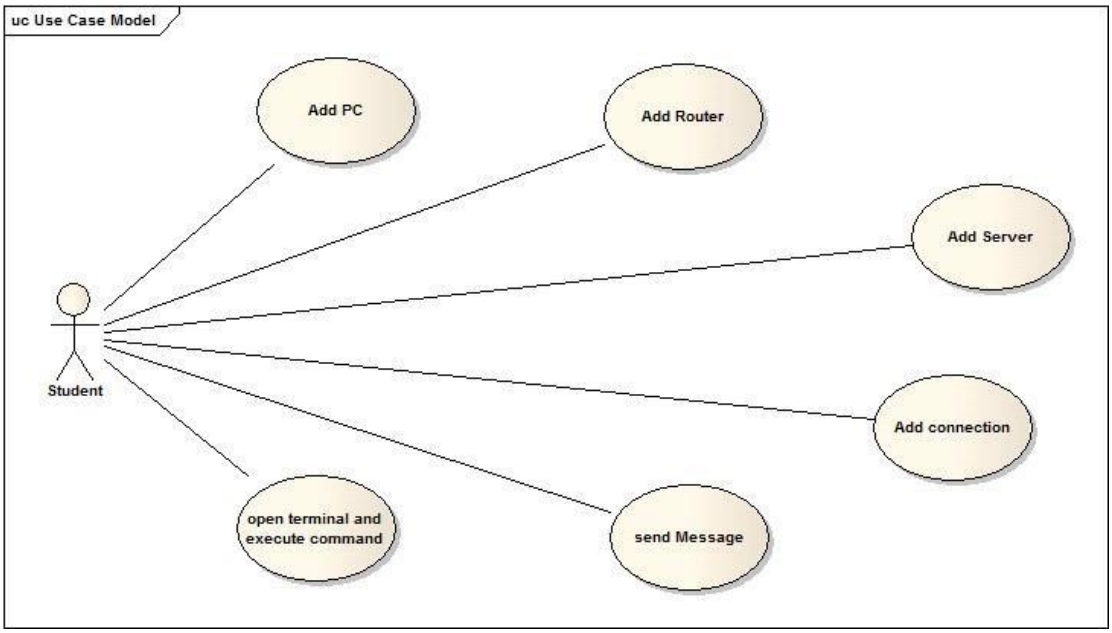

Figure 3 use case diagram

Function Name	Function Description
Add Pc	When the Student select PC, he has multi choices (Normal, Attacker, and Victim).
Add Router	To add Router.
Add server	To add Server.
Add Connection	Link Two nodes with each other.
Send Message	Student can send two types of message (DHCP, Normal Message).
Open Terminal	Student open terminal to execute command.

Table 2 Function Description

5.3.2THE SEQUENCE DIAGRAM

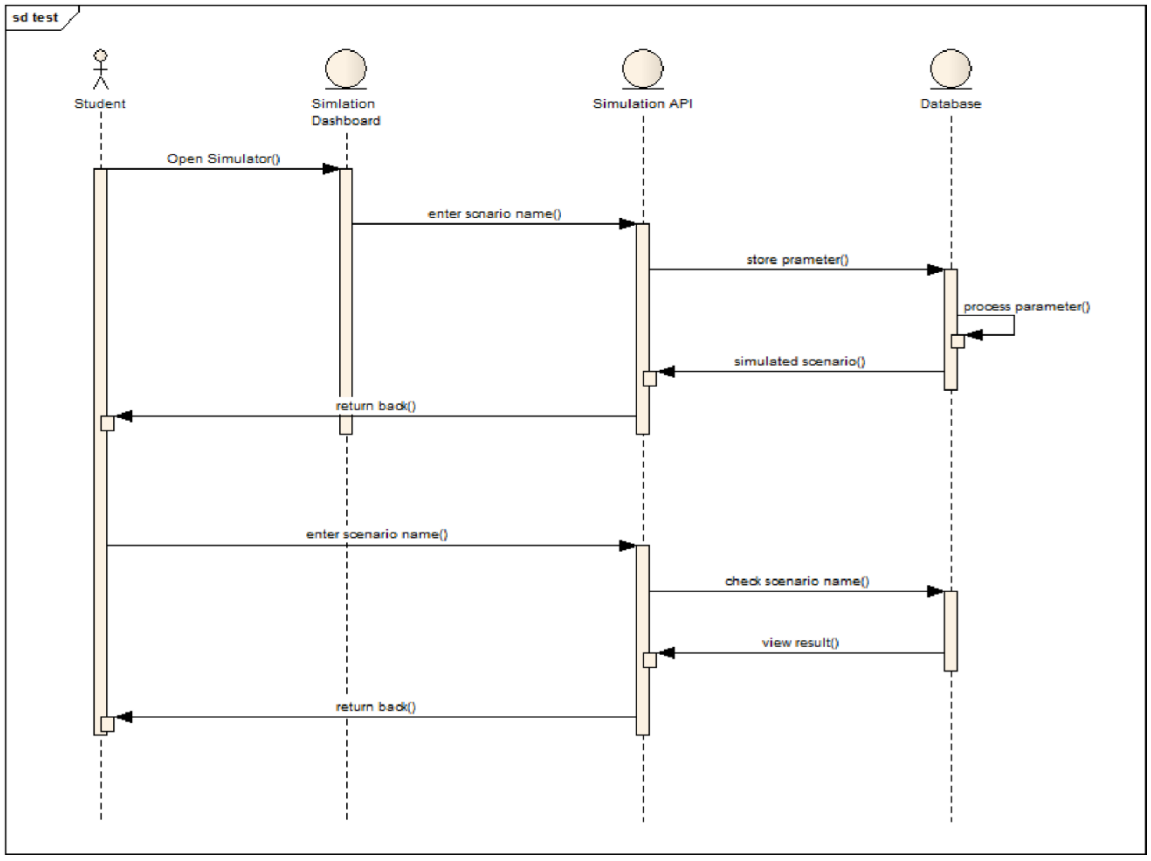

Figure 4 sequence diagram

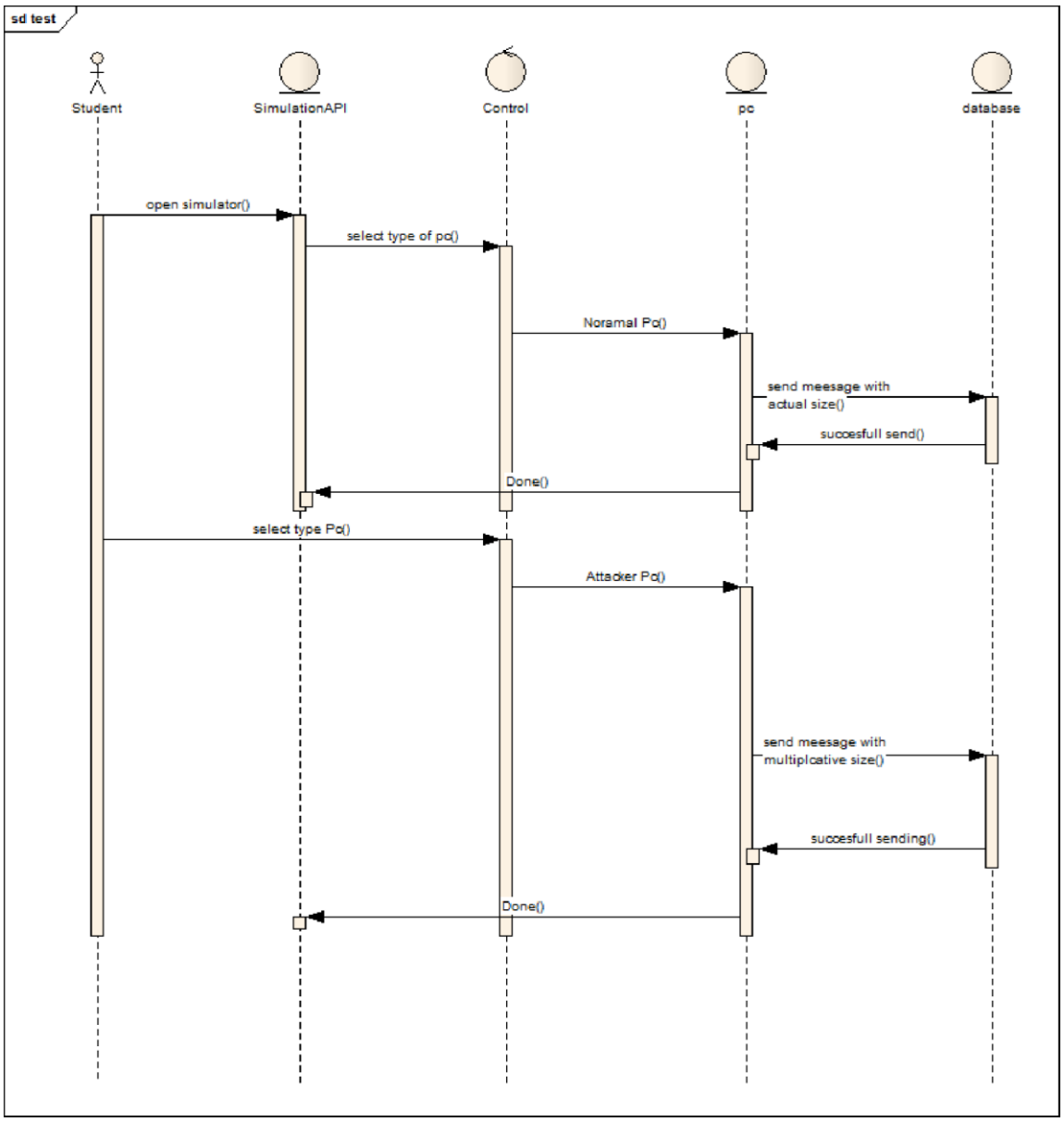

Figure 5 Dos attack

This diagram shows the sequence of actions when the student wants to simulate Denial-Of-Services and Distributed Denial-Of-Services attacks.

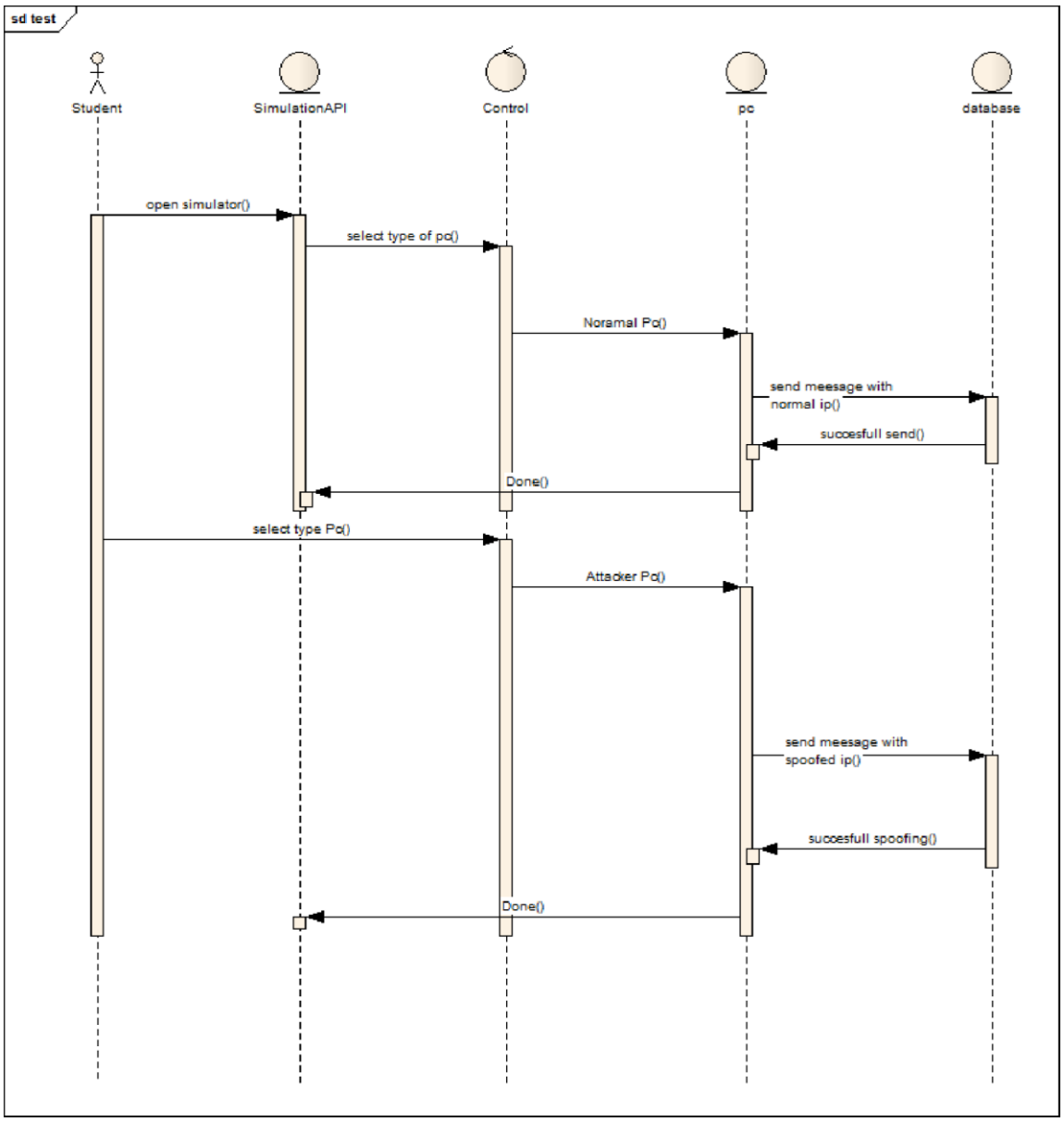

Figure 6 spoofing attack Diagram

This diagram shows the sequence of actions when the student wants to simulate Spoofing attacks.

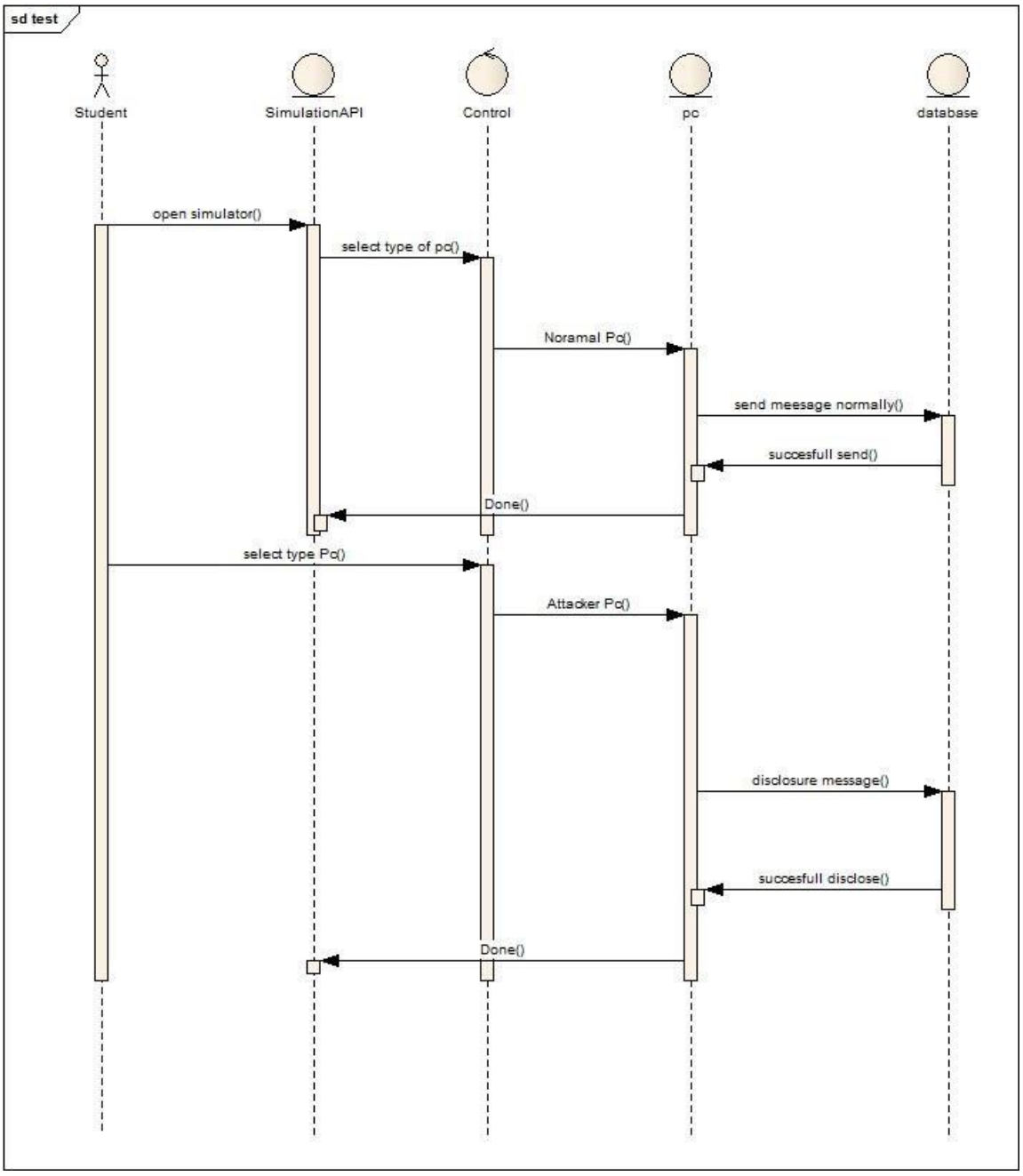

Figure 7 MITM attack

This diagram shows the sequence of actions when the student wants to simulate ManIn-Middle attacks.

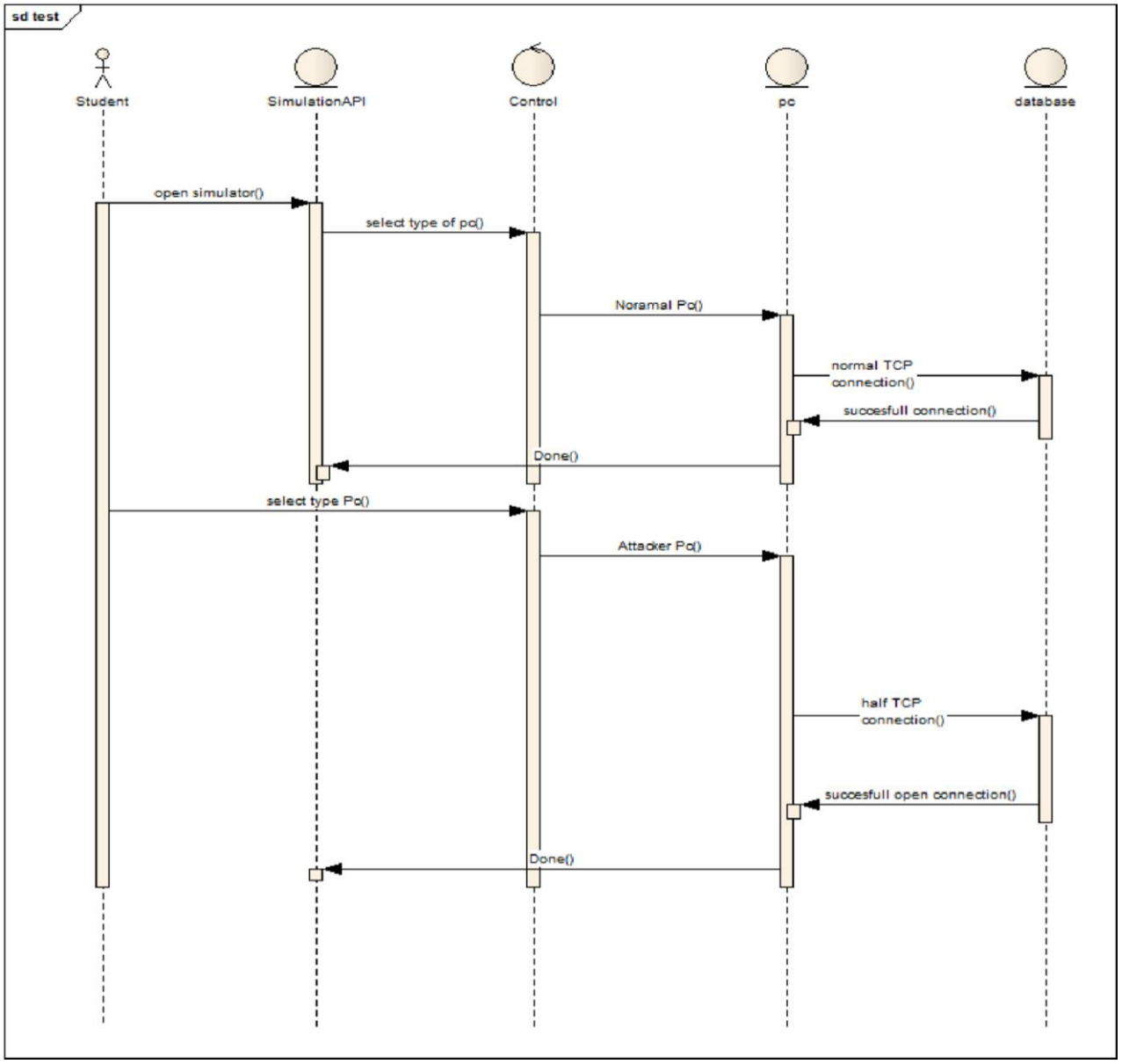

Figure 8 SYN Flooding Diagram

This diagram shows the sequence of actions when the student wants to simulate SYN Flooding attacks.

5.3.3 THE ACTIVITY DIAGRAM

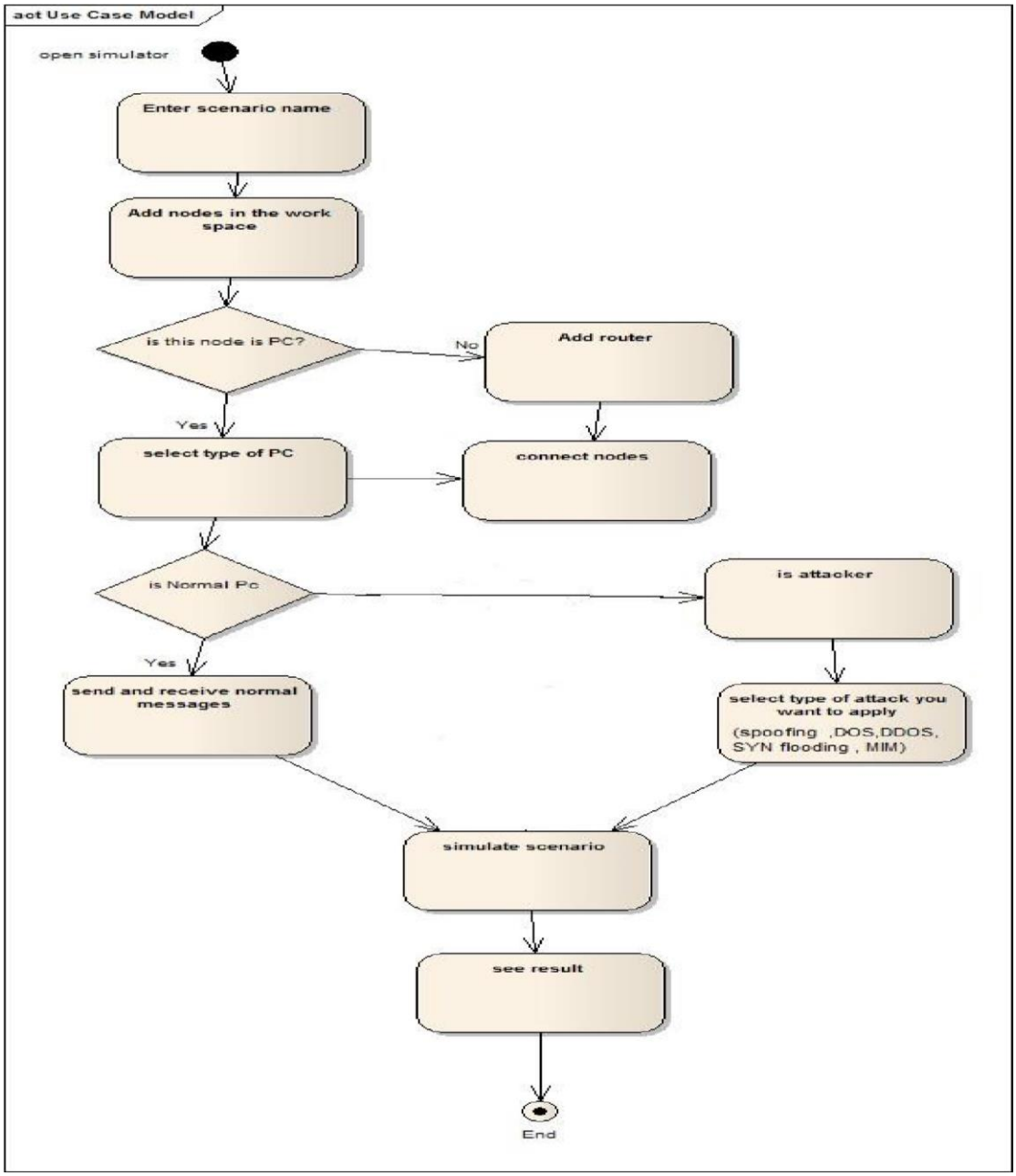

Figure 9 Activity diagram

When student open simulator he must enter scenario name to create a new scenario or import existed one, he can add nodes and connect them to send and receive

messages. After selecting attack type the student will be able to see the result of his scenario.

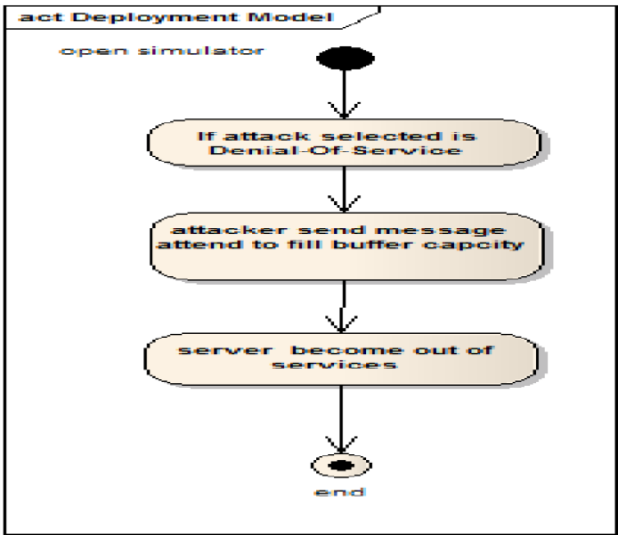

Figure 10 illustrate when student select DOS or DDOS Attacks

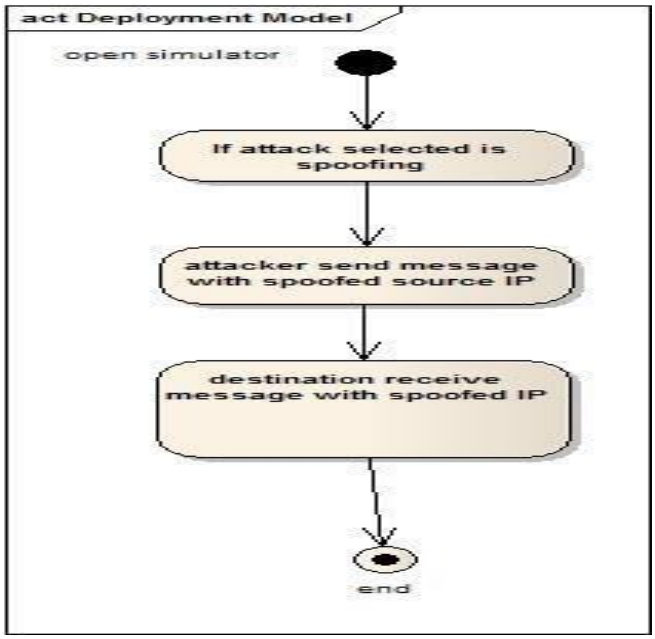

Figure 11 illustrate when student select Spoofing Attacks

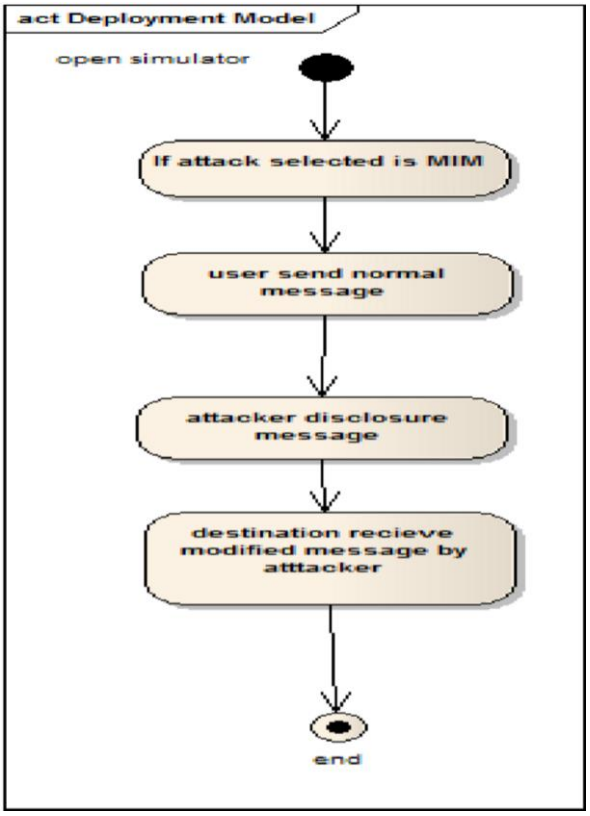

Figure 12 illustrate when student select MIM Attacks

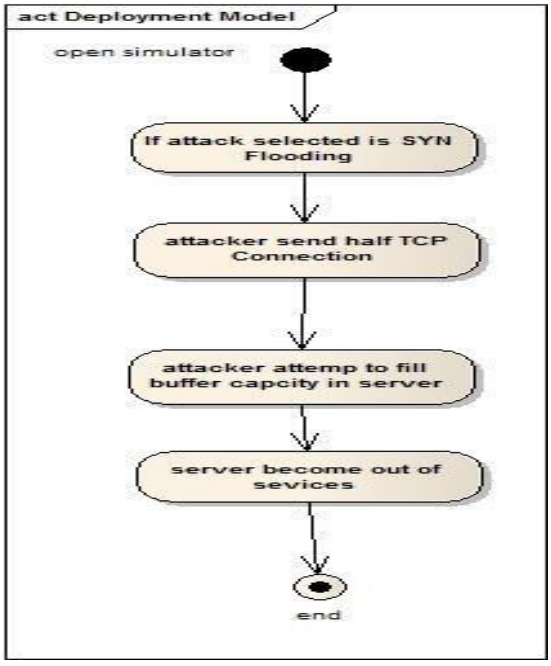

Figure 13 illustrate when user select SYN Flooding attack

5.3 CONCLUSION

This chapter has discussed a general description of the proposed system and its functions and the analysis of the system operations using UML diagrams.

Chapter 6

Implementation

6.1 INTRODUCTION

This chapter discusses the implementation steps, the test scope and the results we get after run the application.

6.2 IMPLEMENTATION

6.2.1 Application component

In this screen student can be able to select application component.

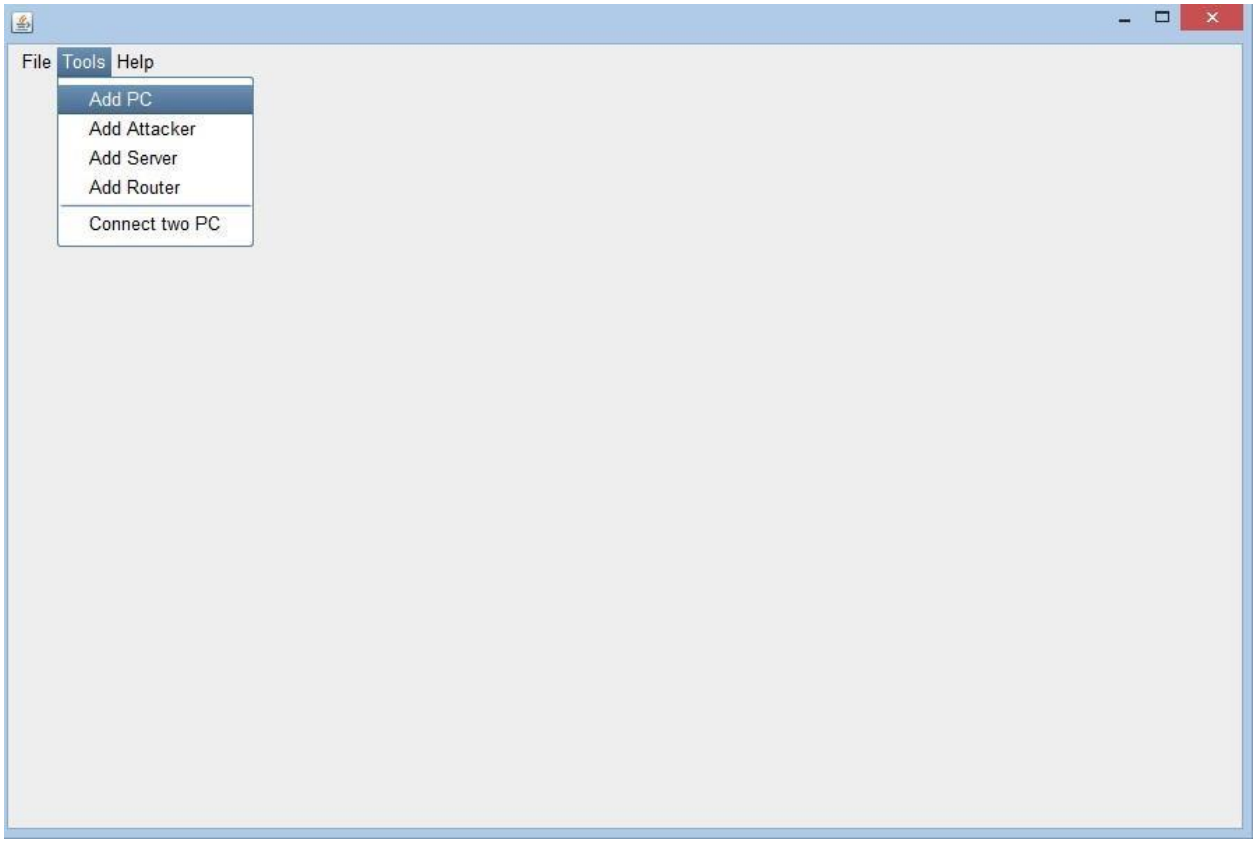

Figure 14 application component

The type of component can be added in simulator to simulate attacks scenarios:

- PC's:

Students can simulate the normal user.

- Attacker:

The student can choose any of the attacks scenarios that can be occur in the network.

- Router:

To connect between computers in the network.

- Server:

Provides service to the clients.

- Connection:

To link between the other components.

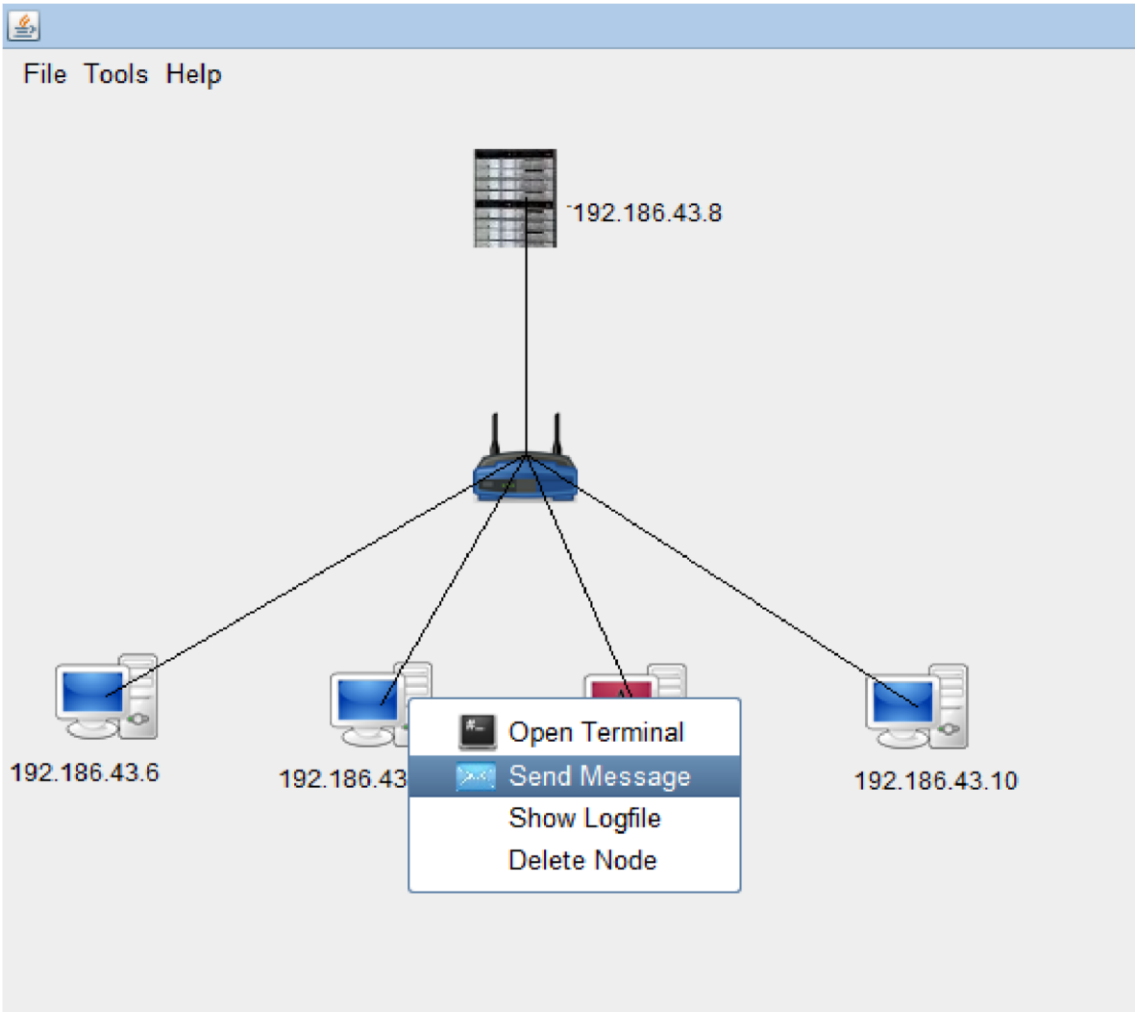

Figure 15 PC Option

The normal user has many options such as:

1- Open Terminal:

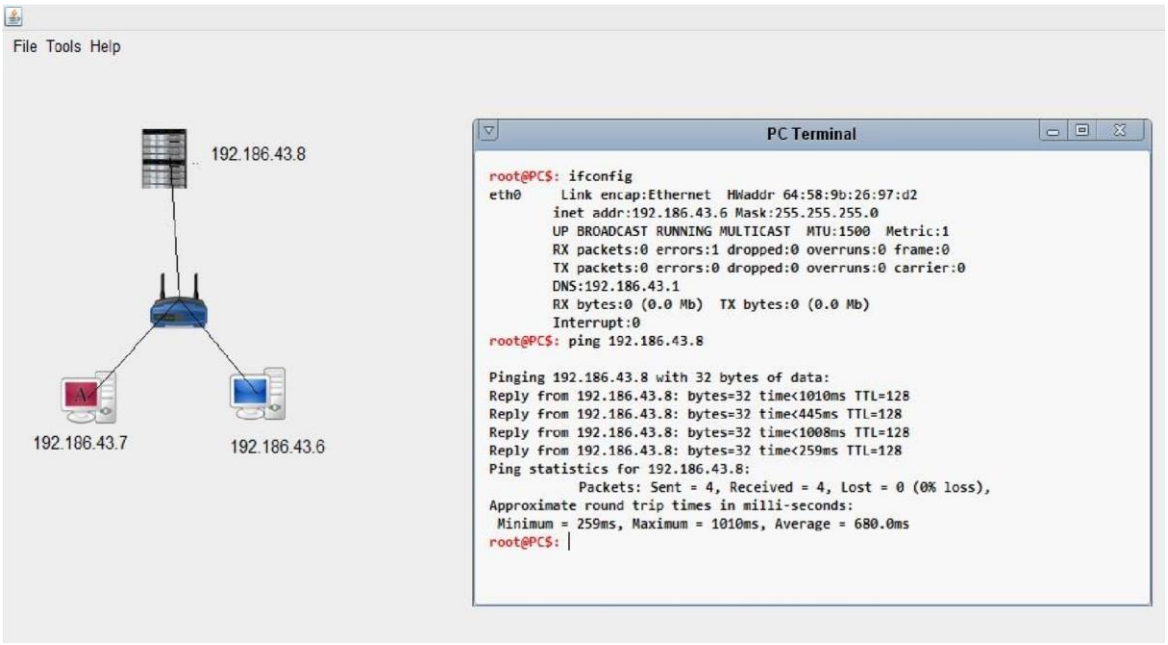

Figure 16 Open Terminal

Student execute ifconfig to know the ip address of pc (source or destination). And it has ping which is a utility to determine whether a specific IP address is accessible or not.

2- Send Message:

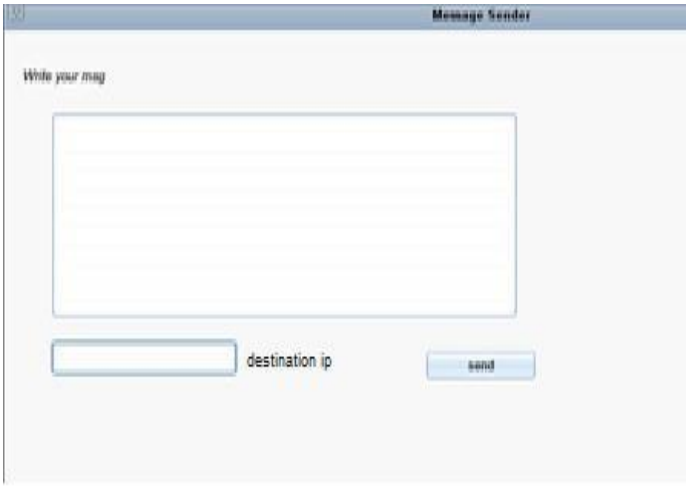

Figure 17 Send Message

User writes the content of message and identify destination IP which will receive the message.

3- Show log file:

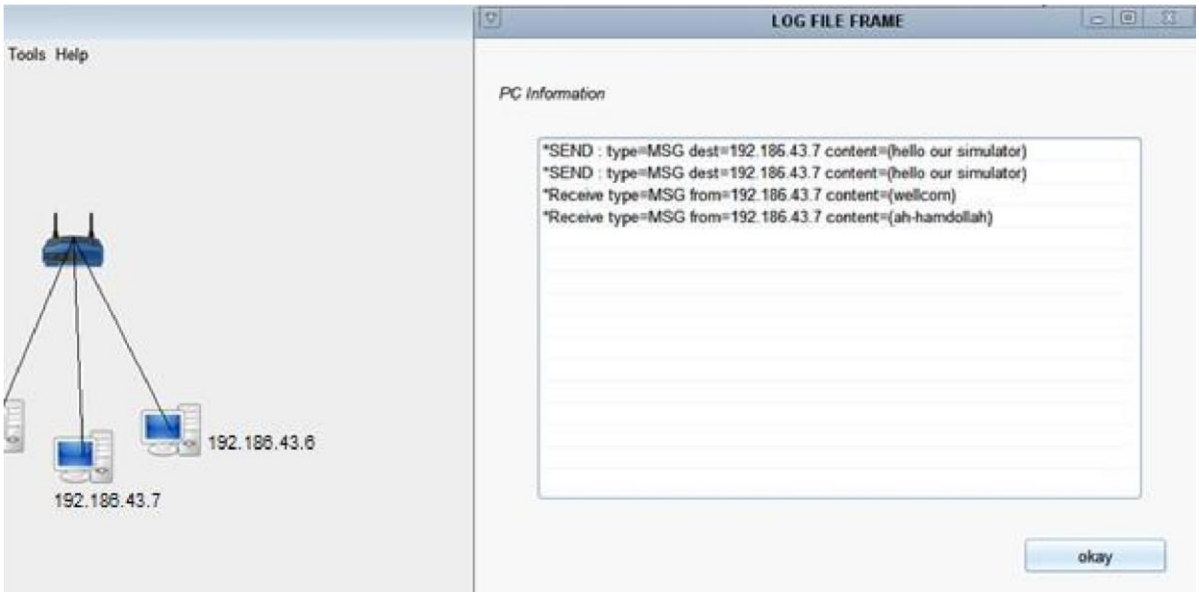

Figure 18 Show log file

All PC's has log files to allow the users to see the details of sending and receiving messages.

Server pc:

The server duty is to serve pc's existed in network, and it has additional service (configure DHCP service) which is responsible to assign ip addresses to clients within specific range.

Figure 19 Server pc

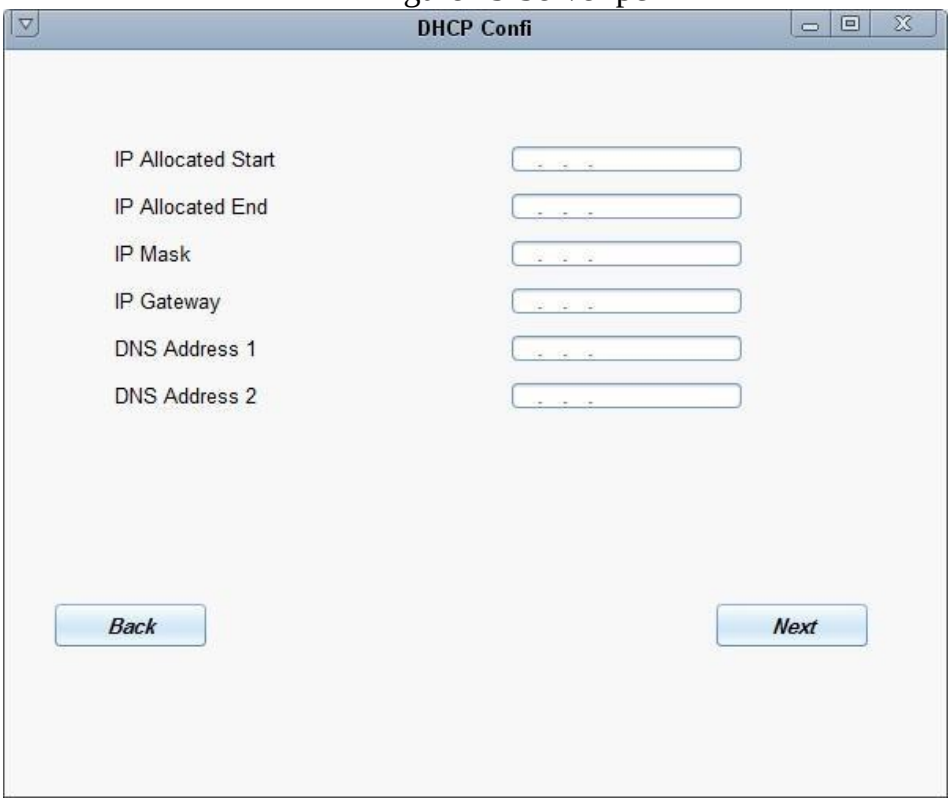

Figure 20 DHCP Config **Attacker**

PC:

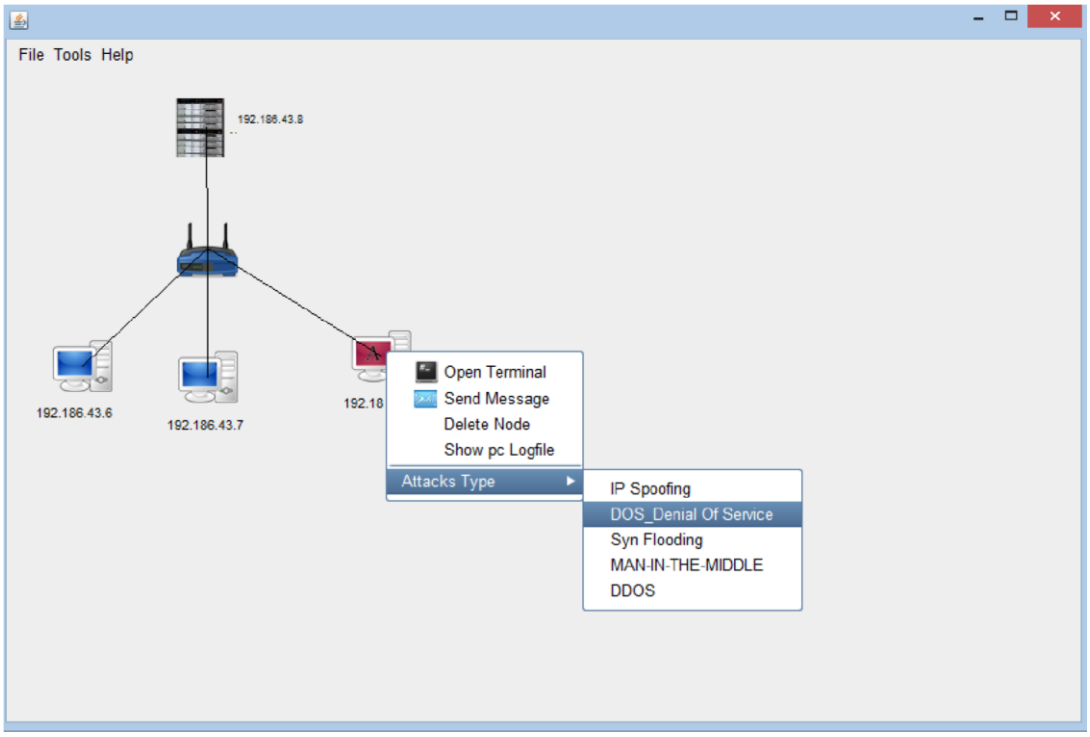

Figure 21 Attacker PC

The Attacker pc has the ability to choose type of attack In addition to the normal PC features.

Types of attacks can be selected:

- IP Spoofing attack:

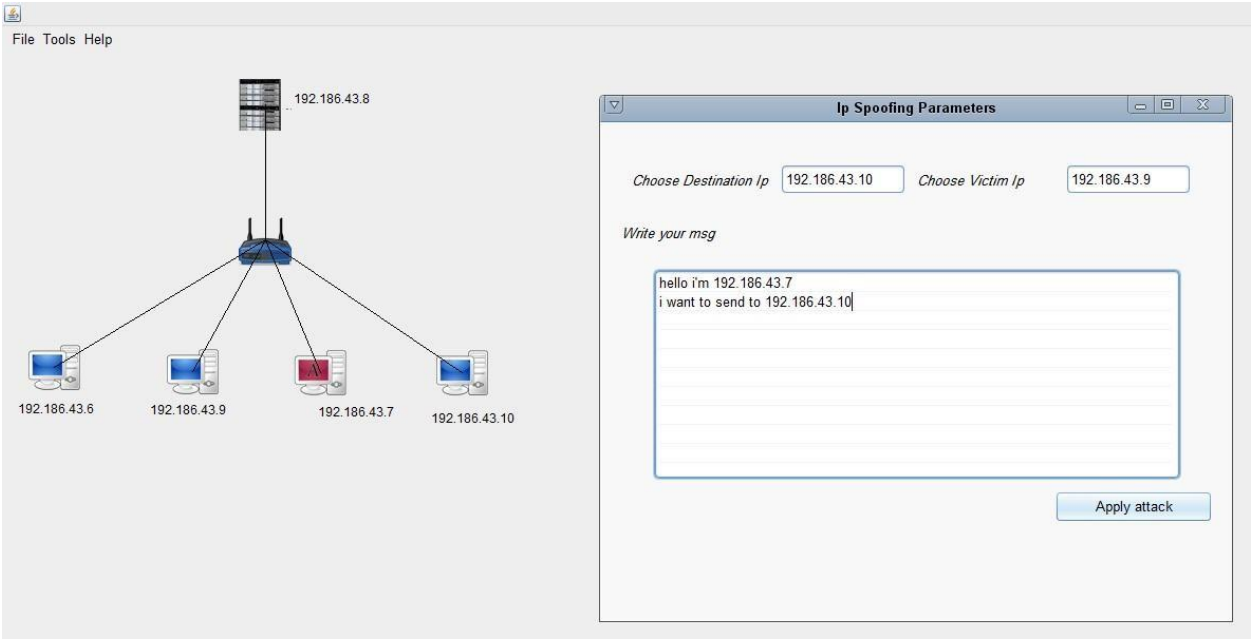

Figure 22 IP Spoofing Parameter

The attacker writes the content of message and identifies victim IP and destination IP which will receive the message with spoofed IP (by the victim IP).

 MITM (Man-In-The-Middle):

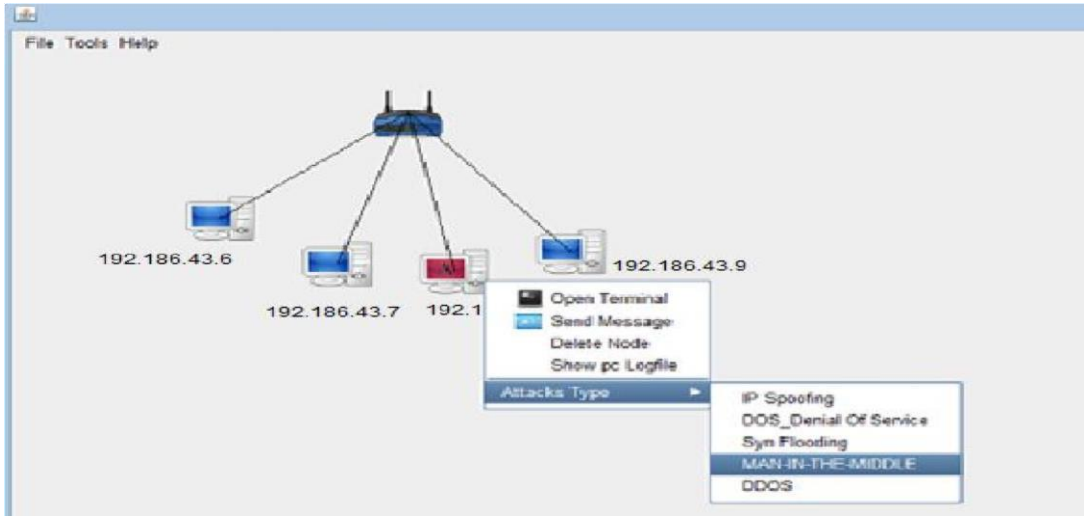

Figure 23 User Select MITM (Man-In-The-Middle) attack

User select Man-In-The-Middle attack from menu of attacks.

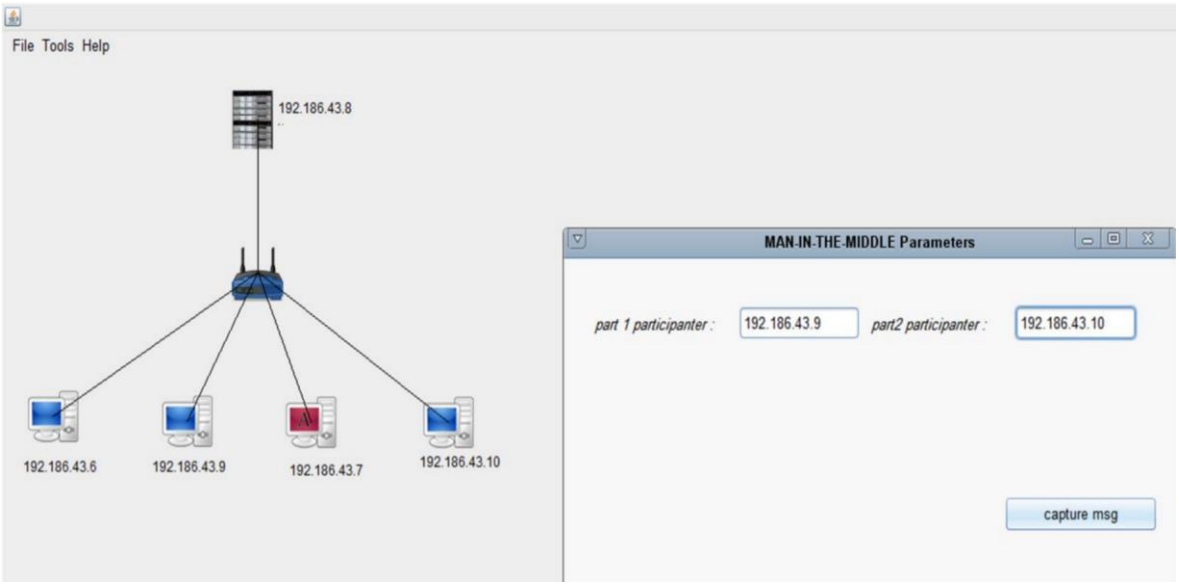

Figure 24 MITM (Man-In-The-Middle) Parameter

The attacker choose the two participants that he want to listen to their connection and captures any messages exchanged between them. As shown below

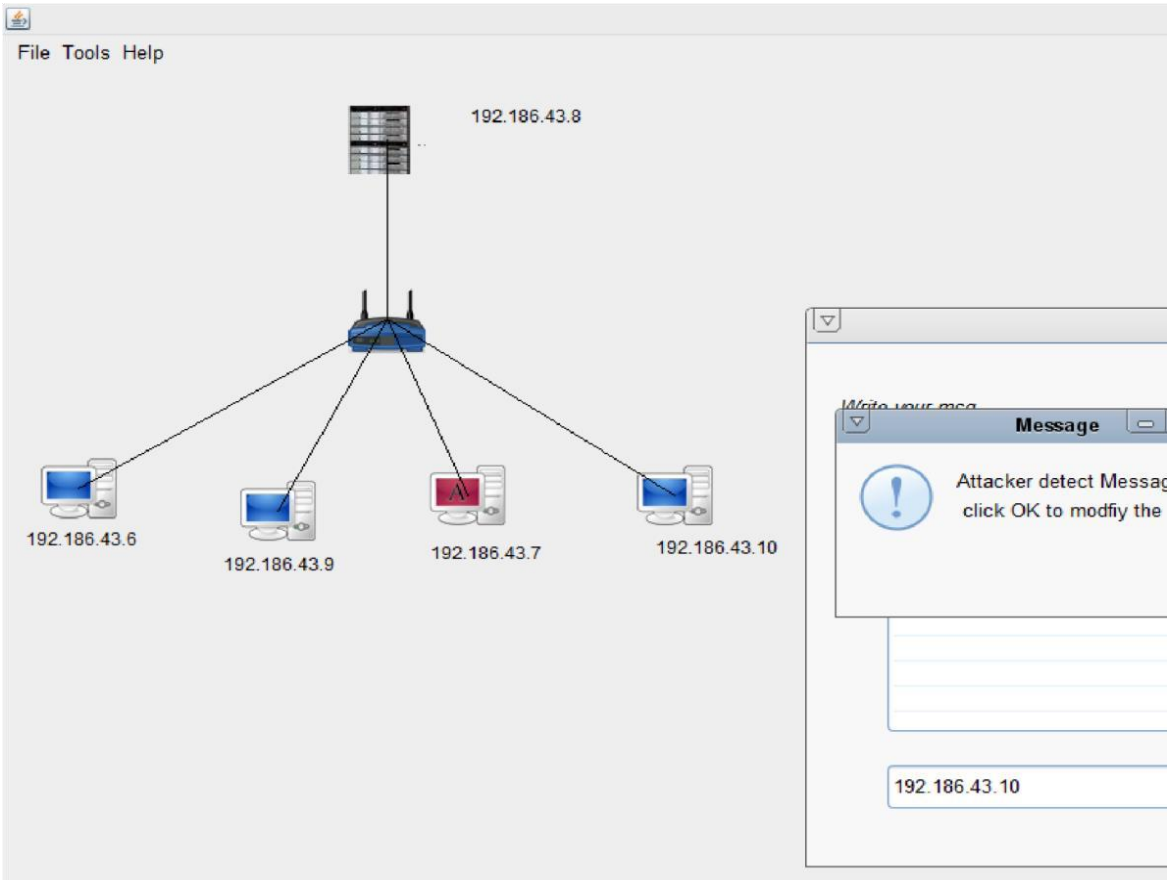

Figure 25 MITM (Man-In-The-Middle) attack

DOS attack

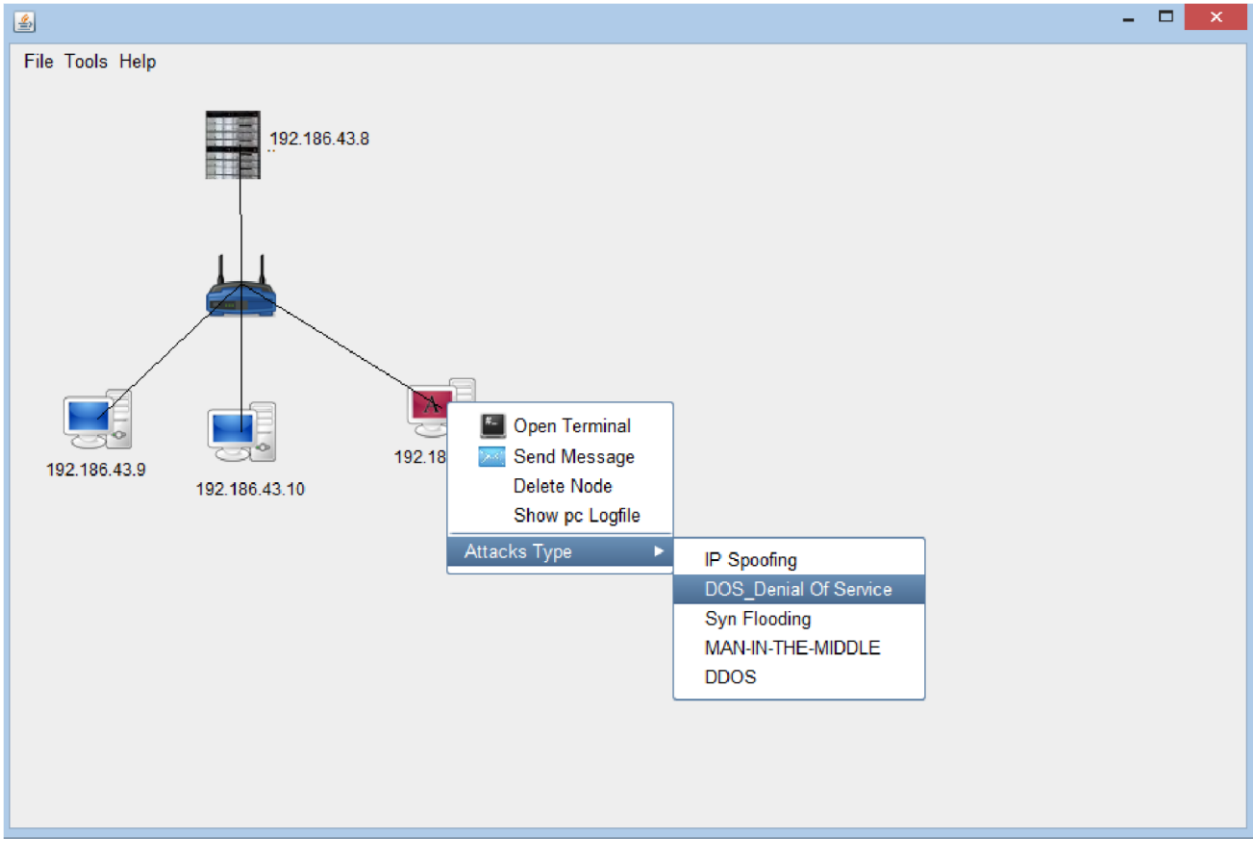

Figure 26 DOS attack

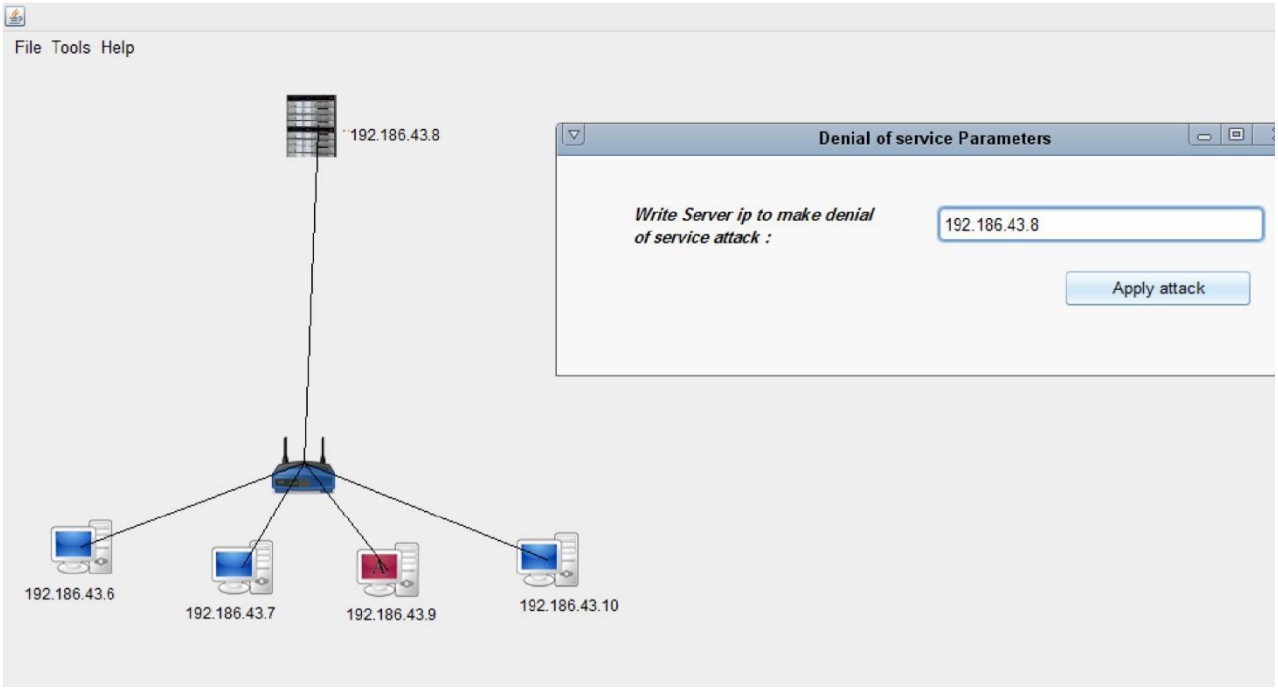

Figure 27 DOS attack Parameter

After the attacker applies the DOS attack and identifies the server IP, this will exhaust the server with lots of pinging requests until it stops servicing legitimates users in the network so that every request of pinging to the server from any pc in the network will result in Request time out and the server will be non-reachable to get the service from it again. As shown in figure 6.15 below before and after applying dos attack.

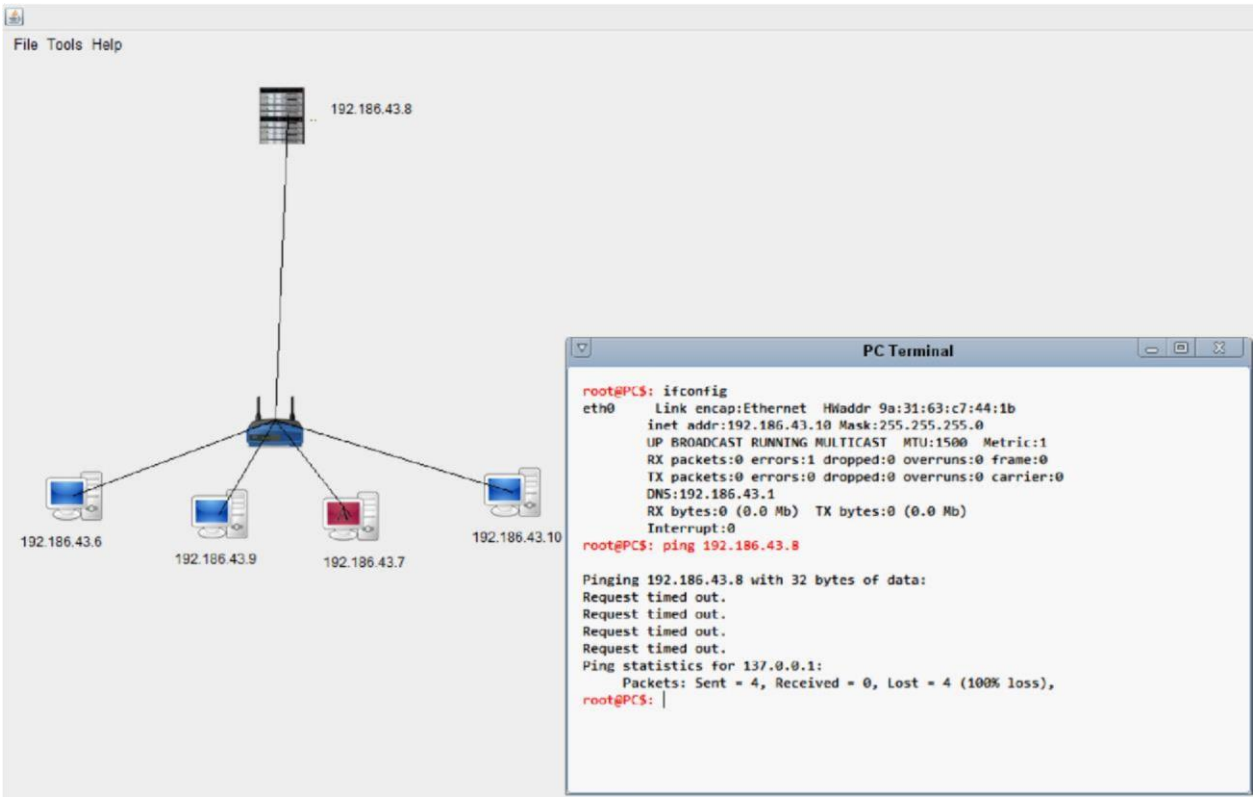

Figure 28 DOS attack

Ip spoofing result

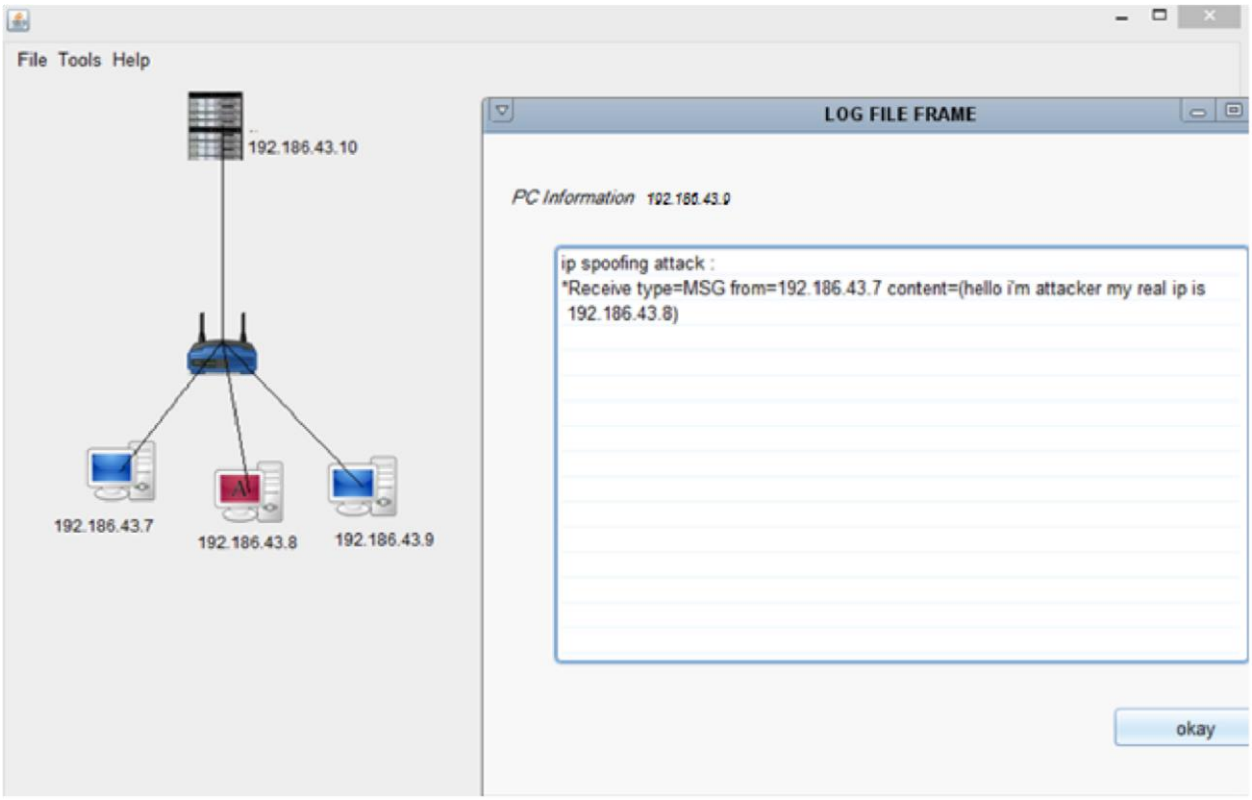

Figure 29 Ip spoofing result

Man-In-The-Middle result:

After implement Mitm attack, the attacker is able to define the two participant that will capture the messages between them, then any exchanging of messages and data will be captured by attacker who is able to modify, delete, and add to the message and resend it again to the destination.

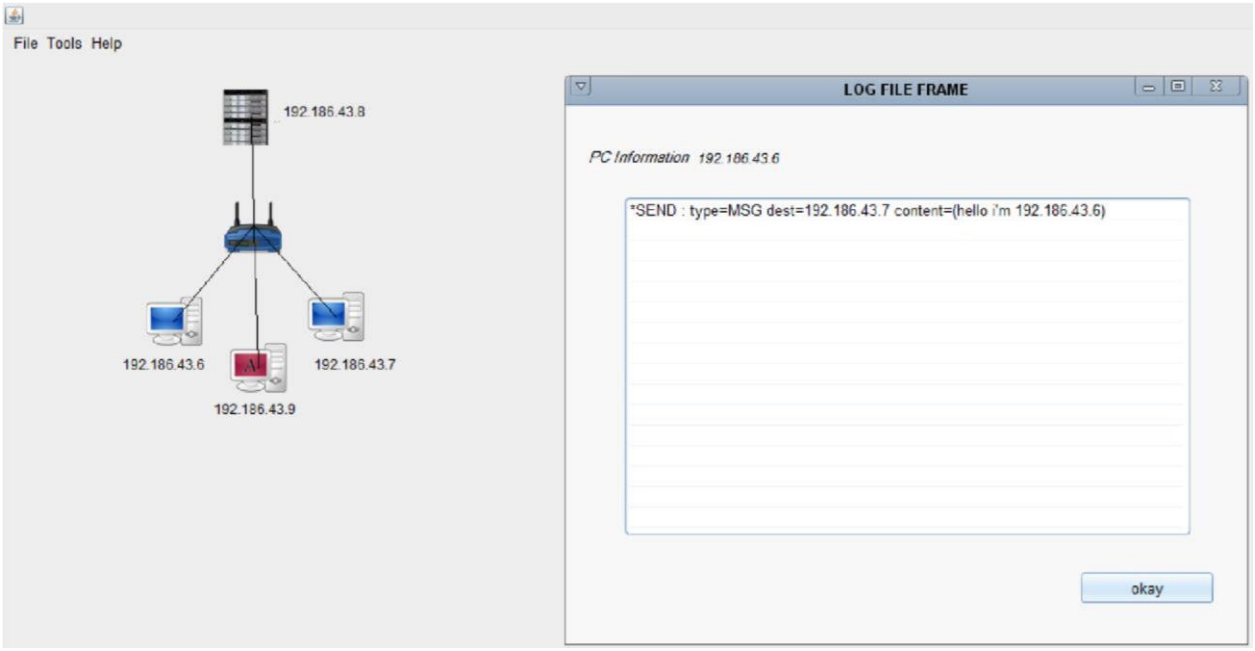

Figure 30 Send Man-In-The-Middle

Figure 31 Capture Message

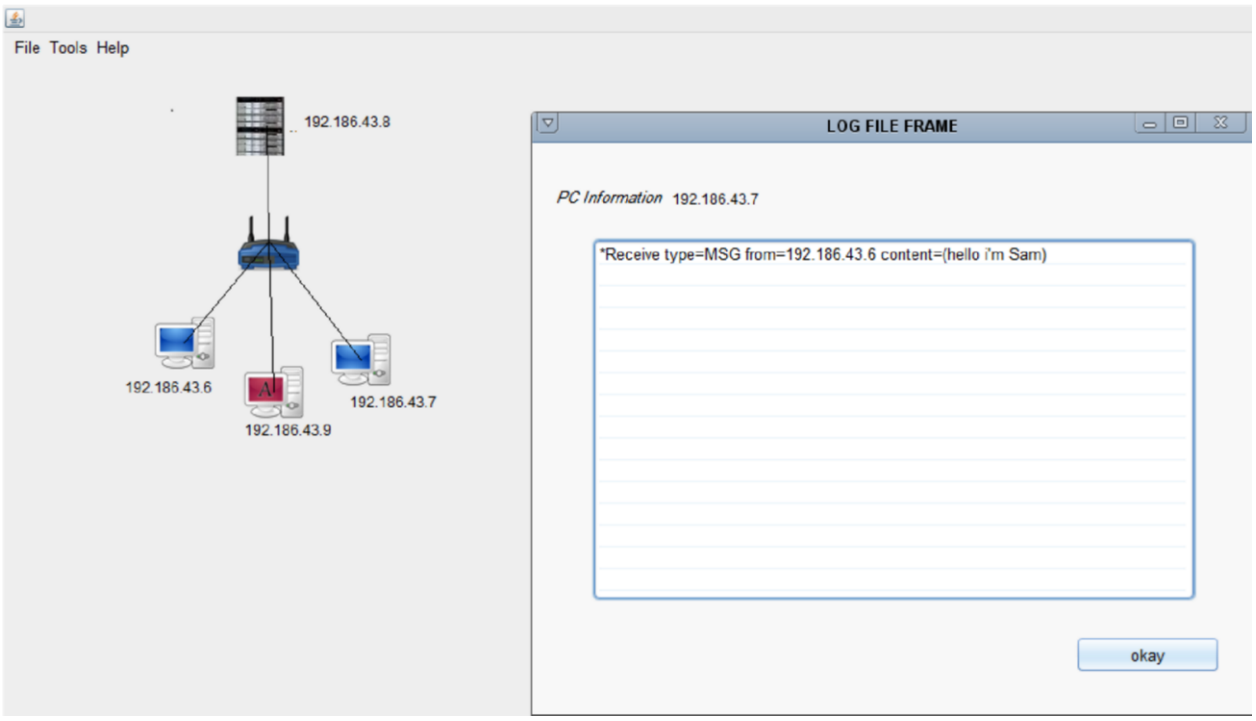

Figure 32 Receive Man-In-The-Middle

6.3 Conclusion

In this chapter we explained in details each attack scenario from the student creates network and chooses the attack, which wants to implement. The students simulate attacks supported by the simulator. Which are: (IP spoofing, MITM and DoS) attacks based on parameters that have been entered. The student understands the result of implementation by referring to the log file that contains all the details of send and receive with existing PCs in the network.

Chapter 7

Result & recommendations

7.1 Result

The result is project aim to provide a tool that helps achieving these set of objectives:

- Help students to understand the concept of some network security attacks without the Requirement of having a sophisticated lab (servers, routers…).
- Enable students to have inexpensive, flexible lab.

7.2 recommendations

There are improvement can be added to this project, so we recommend to:

- Add more attacks.
- Add protection feature to make understand of how to protect network against attacks.
- Add demonstration of detection mechanism to detect the possible attacks.

7.3 CONCLUSION

By the end of the project we have reached a solution to the problem of the research, program has been used to understand and execute some of the attacks on the network (IP spoofing, Dos, DDos, MIM, and SYC flooding).

Reference

1- Retrieved from http://www.examiner.com/article/what-iscomputer-network-and-why-is-it-important.html. [accessed at 2015, march 10].

2- Stallings, W. (2011). *Network security essential.*

3- Rodriguez, K. (n.d.). An Analysis of Security Mechanisms in the OSI Model.

4- Retrieved from http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html. [Accessed at2015, March 20].

5- Retrieved from http://www.techworlnce isd.com/review/security software/skybox-view- assure-and-skybox-view-secure-review-3230391/

6- Retrieved from http://www.skyboxsecurity.com/news%2526events/press%20releases/skyboxsecurity-introduces-next-generation-vulnerability-management-solut.html . .[accessed at 2015, june 29].

7- Stephan Schmidt, R. B. (n.d.). *Application-level simulation for network security.*

8-Retrieved from http://www.skyboxsecurity.com/products/vulnerabilitycontrol#.Vdcg-aFgm1t.html. [accessed at 2015, 7 10].

9- Java™ How to Program, Seventh Edition. (n.d.).

10- Retrieved from http://www.eclipse.org/ , http://projects.eclipse.org. [accessed at 2015, 7 30]

11- 11- Retrieved from http://sparxsystems.com/products/ea_editions.html