A Project Report
on

MAN IN THE MIDDLE ATTACK CRYPT ANALYSIS AND CYBER DEFENSE

A project report submitted in partial fulfillment of the requirements for the degree of

Bachelor of Technology in Computer Science and Engineering

by

K. DIMPLE **(2010030436)**

K. SIRISHA **(2010030438)**

Under the guidance of

Dr. GAYATHRI EDAMADAKA

Assistant Professor

KL University

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

(R.V.S Nagar, Moinabad-Chilkur Road, near AP Police Academy, Aziznagar, Telangana 500075)

KL UNIVERSITY

(R.V.S Nagar, Moinabad-Chilkur Road, near AP Police Academy, Aziznagar, Telangana 500075)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that the Project work entitled "**MAN IN THE MIDDLE ATTACK**" is carried out by **K. DIMPLE (2010030436), K. SIRISHA(2010030438),** in partial fulfillment for the award of degree of **Bachelor of Technology** in **Computer Science and Engineering**, KL University, R.V.S.Nagar, Moinabad-Chilkur Road, near AP Police Academy, Aziznagar, Telangana 500075 during the academic year 2021-22.

Dr. GAYATHRI EDAMADAKA
Internal Guide

Signature of the HOD

External Examiner

(Certificate from Industry)

DECLARATION

I hereby declare that the project titled "MAN IN THE MIDDLE ATTACK" submitted to Department of CSE, University KL, R.V.S Nagar, Moinabad-Chilkur Road, near AP Police Academy, Aziznagar, Telangana 500075 for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a result of original work carried-out in this project report. I understand that my report may be made electronically available to the public. It is further declared that the project report or any part thereof has not been previously submitted to any University or Institute for the award of degree or diploma.

Name of Student(s) : K.DIMPLE , K.SIRISHA

Hall Ticket Number(s): 2010030436 , 2010030438

Degree : Bachelor of Technology in CSE

Department : COMPUTER SCIENCE & ENGINEERING

Title of the project : MAN IN THE MIDDLE ATTACK

_____

(K.DIMPLE , K.SIRISHA)

Date: 29-11-2022

ACKNOWLEDGEMENT

First and foremost, we thank the lord almighty for all his grace & mercy showered upon us, for completing this project successfully.

We take grateful opportunity to thank our beloved Founder and Chairman who has given constant encouragement during our course and motivated us to do this project. We are grateful to our Principal **Dr. L. Koteswara Rao** who has been constantly bearing the torch for all the curricular activities undertaken by us.

We pay our grateful acknowledgement & sincere thanks to our Head of the Department **Dr. Chiranjeevi Manike** for his exemplary guidance, monitoring and constant encouragement throughout the course of the project.

We thank **Project Supervisor(s)** of our department who has supported throughout this project holding a position of supervisor.

We whole heartedly thank all the teaching and non-teaching staff of our department without whom we won't have made this project a reality. We would like to extend our sincere thanks especially to our parents, our family members and friends who have supported us to make this project a grand success.

K.DIMPLE (2010030436)

K.SIRISHA (2010030438)

ABSTRACT

Man-in-the-middle attacks (MITM) are a common type of cybersecurity attack that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen to, hence the name “man-in-the-middle.”

A man-in-the-middle attack is a type of eavesdropping attack, where attackers interrupt an existing conversation or data transfer. After inserting themselves in the "middle" of the transfer, the attackers pretend to be both legitimate participants. This enables an attacker to intercept information and data from either party while also sending malicious links or other information to both legitimate participants in a way that might not be detected until it is too late.

You can think of this type of attack as similar to the game of telephone where one person's words are carried along from participant to participant until it has changed by the time it reaches the final person. In a man-in-the-middle attack, the middle participant manipulates the conversation unknown to either of the two legitimate participants, acting to retrieve confidential information and otherwise cause damage.

Keywords: communication, legitimately, cybersecurity, eavesdrop,

TABLE OF CONTENTS

		Page
List of Figures		9
CHAPTER 1: INTRODUCTION		10
1.1	Introduction	10
1.2	Problem statement	10
1.3	Scope of research	10
1.4	Objectives	11
CHAPTER 2: LITERATURE REVIEW		12
2.1	Summary of literature review	13
CHAPTER 3: METHODOLOGY		14
3.1	Materials	15
3.2	Summary of methodology	15
CHAPTER 4: RESULTS AND DISCUSSION		16
4.1	Summary of results and discussion	16
CHAPTER 5: CONCLUSION		20
5.1	Conclusion	20
REFERENCES		21

LIST OF FIGURES

		Page
Figure 1	ARP	16
Figure 1.1	ARP	16
Figure 1.2	ARP	17
Figure 2	Wireshark capture data	17
Figure 2.1	Wireshark capture data	18
Figure 3	DNS spoofing	18
Figure 4	Denial-of-Service	19
Figure 4.1	Denial-of-Service	19
Figure 4.2	Denial-of-Service	20
Figure 4.3	Denial-of-Service	20

CHAPTER 1: INTRODUCTION

1.1 Introduction:

A man-in-the-middle (MITM) attack is a type of cyber-attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation

1.2 Problem statement:

The main aim of our project is to perform different modules on man in the middle attack using Ettercap tool.

The modules include ARP, DNS, DOS.

1.3 Scope of research:

MITM is named for a ball game where two people play catch while a third person in the middle attempts to intercept the ball. MITM is also known as a fire brigade attack, a term derived from the emergency process of passing water buckets to put out a fire. In the year 2004, U. Meyer and S. Wetzel presented a report on Universal Mobile Telecommunication System's (UITM) security protocol where they dis-cussed about 'men-in-the-middle-attack' on mobile communication (Meyer & Wetzel, 2004). In 2006, Kish published his research in a master listed journal where he showed an encryption method of MITM using Kirchhoff-loop-Johnson (-like)-noise cipher (Kish, 2006). Hypponen and Haataja (2007), made a A. Mallik et al. / International Journal of Data and Network Science 3 (2019) 79 research on secure Bluetooth communication and showed their developed system was capable of pre-venting MITM attack (Hypponen & Haataja, 2007).

1.4 Objectives:

Our Project performs different modules on man in the middle attack using Ettercap tool.

The modules include ARP, DNS, DOS.

CHAPTER 2: LITERATURE REVIEW

2.1 Summary of literature review:

Man-in-the-middle-attack: Understanding in simple words

- Man-in-the-middle-attack' also known/abbreviated as MIM, MiM, MitM or MITMA is a type of cryp-tographic attack over a communication channel by a malicious third party where he/she takes over a confidential/personal communication channel between two or legitimate communicative points or parties.
- The MITMs interrupt interchanges between two frameworks, and this phenomenon takes place when the attacker is responsible for a switch along typical point of movement. The attacker in all cases is situated on a similar communicated domain as the victim stands. Indeed, in a HTTP exchange, a TCP protocol exists among the customer and the server. The attacker divides the TCP protocol into two connections – one between the victim and the attacker and the other between the attacker and the server.

A Survey of Man in The Middle Attacks

- In this paper, we provide a thorough survey of the MITMattack with focus on the OSI model, and on specific mobile networking technologies, i.e., GSM and UMTS. Wechose directly this scope, since classes of the MITM attack correlate with layers of OSI model; GSM is one of themost spread network, which covers more than 90% of theworld population [10], and was not designed to be MITMresistant; UMTS is a good example of technology evolutionwith legacy support. Further, in paper we classify MITMattacks based on several parameters, namely: location of

anattacker in the network, nature of a communication channel, and impersonation techniques. Next, we use the impersonation techniques classification as a reference classification and wego into details for each category providing attack algorithmsand categorising prevention mechanisms.To the best of our knowledge, this is the first extensivestudy of the MITM attack. When we compare our work withthe existing body of research, we see the following. Clark etal. [11] executed one of the most significant surveys of defenceschemes against SSL/TLS MITM attack. Authors reviewed the spectrum of issues concerning trust model between certified authorities and browsers. Similarly, in [12]–[14], researchers carried out small studies of detecting and defeating mechanisms of SSL/TLS MITM attack. Saxena et al. [15] collected proposals, which prevent MITM attack on GSM and UMTS networks. Thus, there is no previous work in the literature that covers MITM attacks across each layer of the OSI model, classifies MITM, and categorises MITM defence approaches. Our work fills this gap, by providing MITM attack survey over the period 1992-2015.

CHAPTER 3: METHODOLOGY

3.1 Materials:

- ORACLE VM VIRTUALBOX
- KALI LINUX
- ETTERCAP

3.2 Summary of methodology:

Address Resolution Protocol:

ARP is used to find out the MAC Address of a particular device whose IP address is known. ARP spoofing is a Man In The Middle (MITM) attack in which the attacker (hacker) sends forged ARP Messages. This allows the attacker to pretend as a legitimate user as it links the attacker machine's MAC Address to the legitimate IP Address.

Domain Name Server:

DNS spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination. Once there, users are prompted to login into (what they believe to be) their account, giving the perpetrator the opportunity to steal their access credentials and other types of sensitive information. Furthermore, the malicious website is often used to install worms or viruses on a user's computer, giving the perpetrator long-term access to it and the data it stores.

Denial-of-Service:

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

CHAPTER 4: RESULTS AND DISCUSSION

4.1 Summary of results and discussion:

ARP:

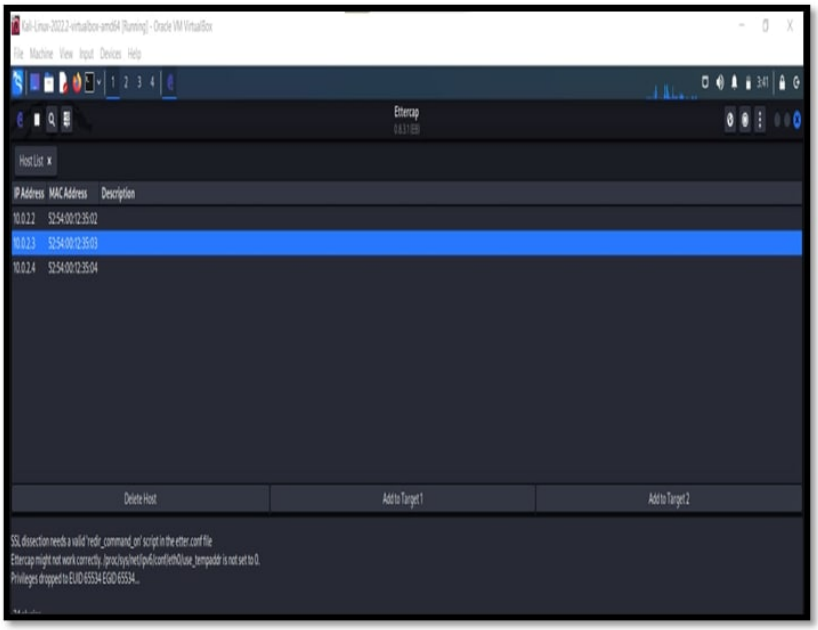

Fig:1

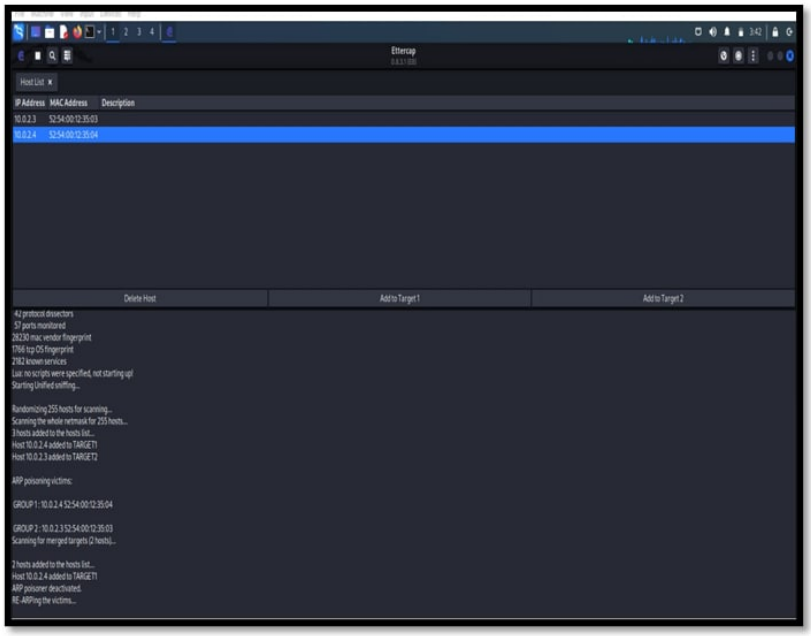

Fig: 1.1

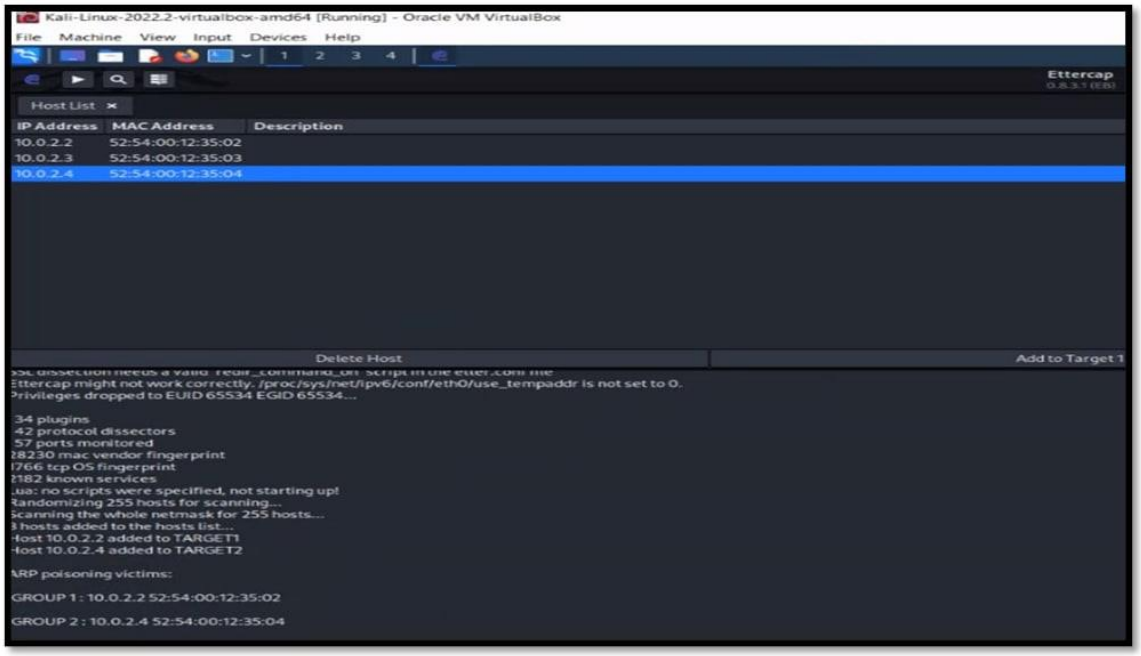

Fig: 1.2

Wireshark capture data:

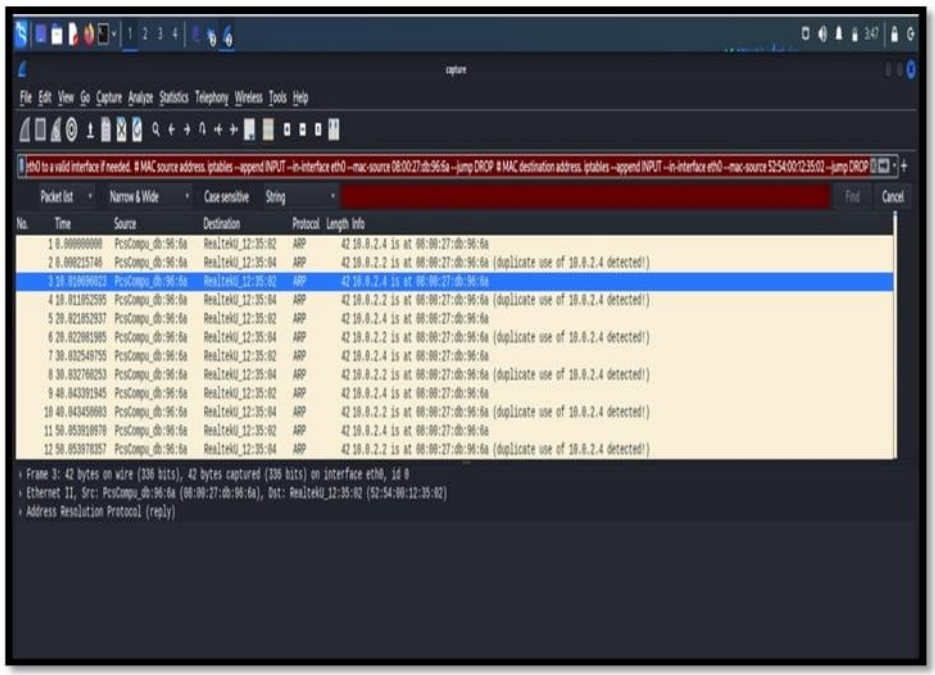

Fig: 2

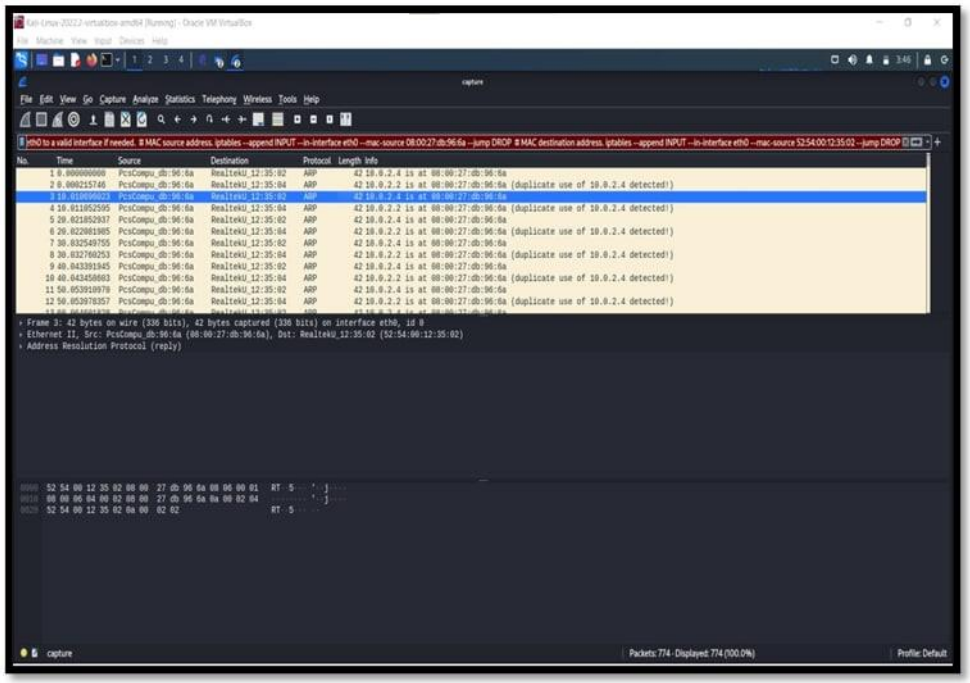

Fig: 2.1

DNS spoofing:

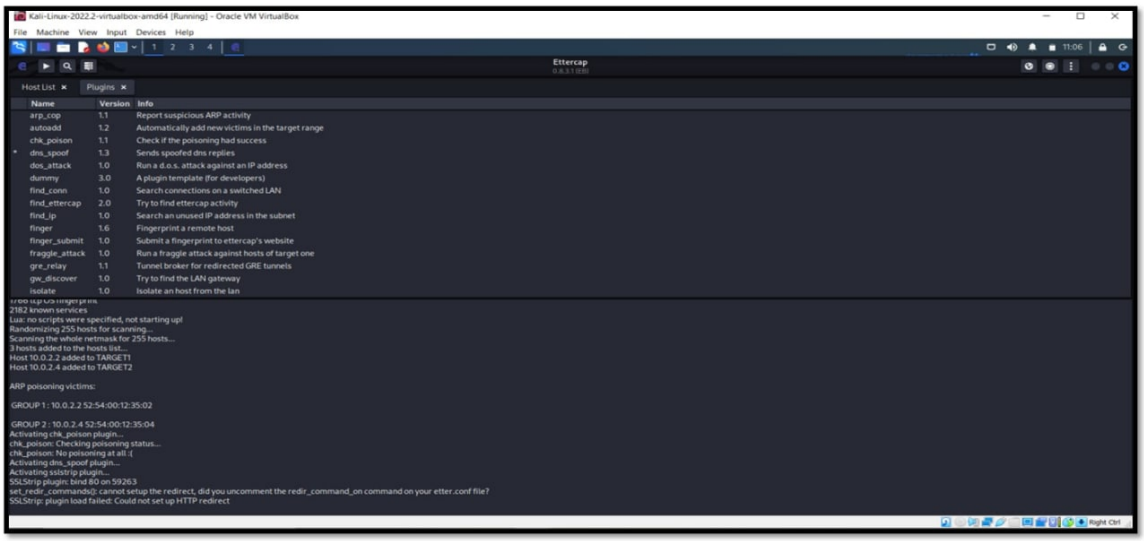

Fig: 3

Denial-of-Service:

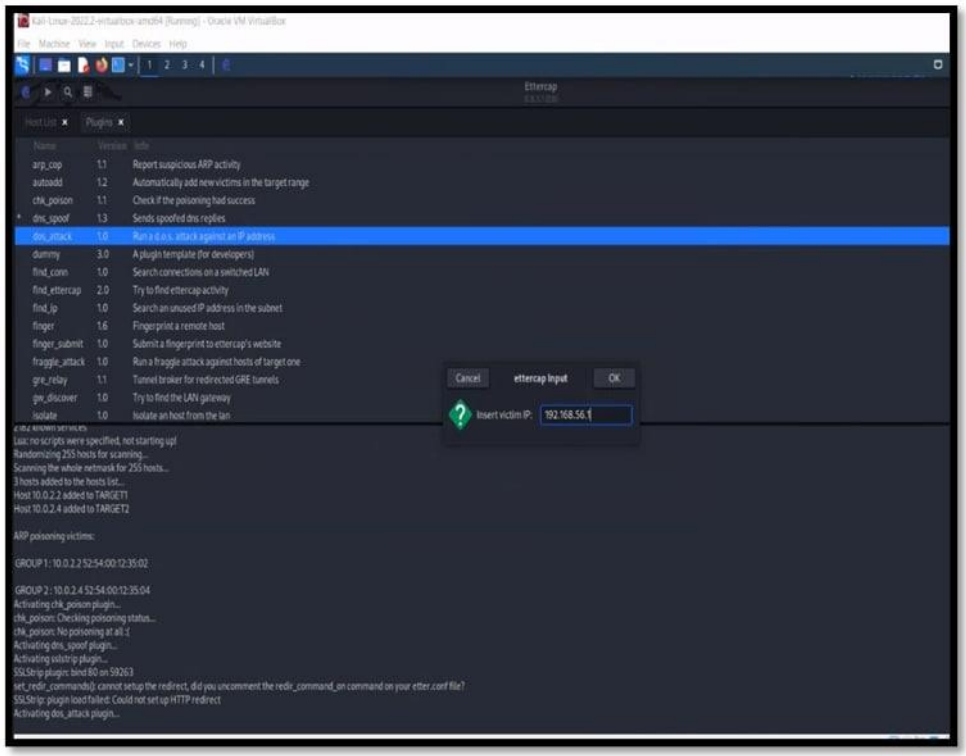

Fig: 4

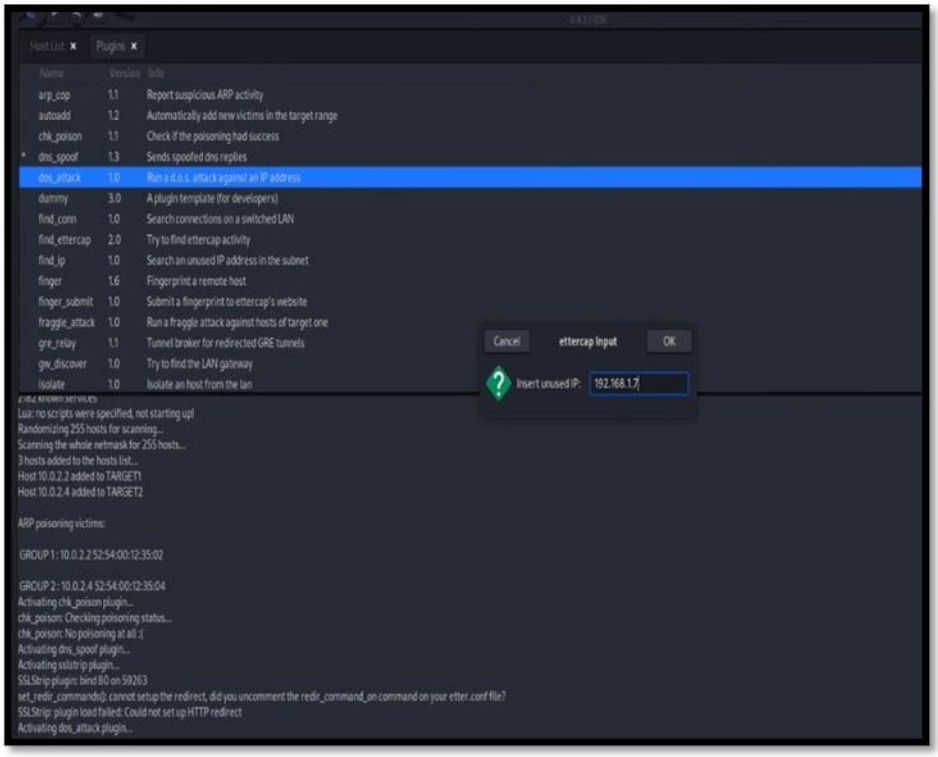

Fig: 4.1

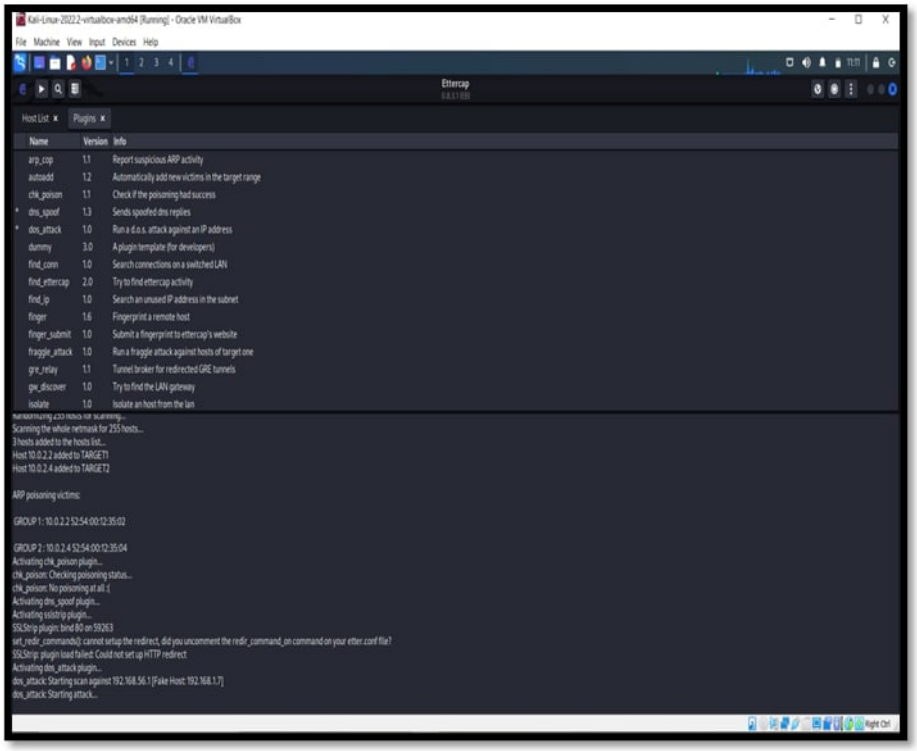
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ettercap
Host List
Plugins
Name Version Info
arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
dns_spoof 1.3 Sends spoofed dns replies
dos_attack 1.0 Run a d.o.s. attack against an IP address
dummy 3.0 A plugin template (for developers)
find_conn 1.0 Search connections on a switched LAN
find_ettercap 2.0 Try to find ettercap activity
find_ip 1.0 Search an unused IP address in the subnet
finger 1.6 Fingerprint a remote host
finger_submit 1.0 Submit a fingerprint to ettercap's website
fraggle_attack 1.0 Run a fraggle attack against hosts of target one
gre_relay 1.1 Tunnel broker for redirected GRE tunnels
gw_discover 1.0 Try to find the LAN gateway
isolate 1.0 Isolate an host from the lan
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 10.0.2.2 added to TARGET1
Host 10.0.2.4 added to TARGET2
ARP poisoning victims:
GROUP 1 : 10.0.2.2 52:54:00:12:35:02
GROUP 2 : 10.0.2.4 52:54:00:12:35:04
Activating chk_poison plugin...
chk_poison: Checking poisoning status...
chk_poison: No poisoning at all :(
Activating dns_spoof plugin...
Activating sslstrip plugin...
SSLStrip plugin: bind 80 on 59263
set_redir_commands(): cannot setup the redirect, did you uncomment the redir_command_on command on your etter.conf file?
SSLStrip: plugin load failed: Could not set up HTTP redirect
Activating dos_attack plugin...
dos_attack: Starting scan against 192.168.56.1 [Fake Host: 192.168.1.7]
dos_attack: Starting attack...
Right Ctrl

Fig: 4.2

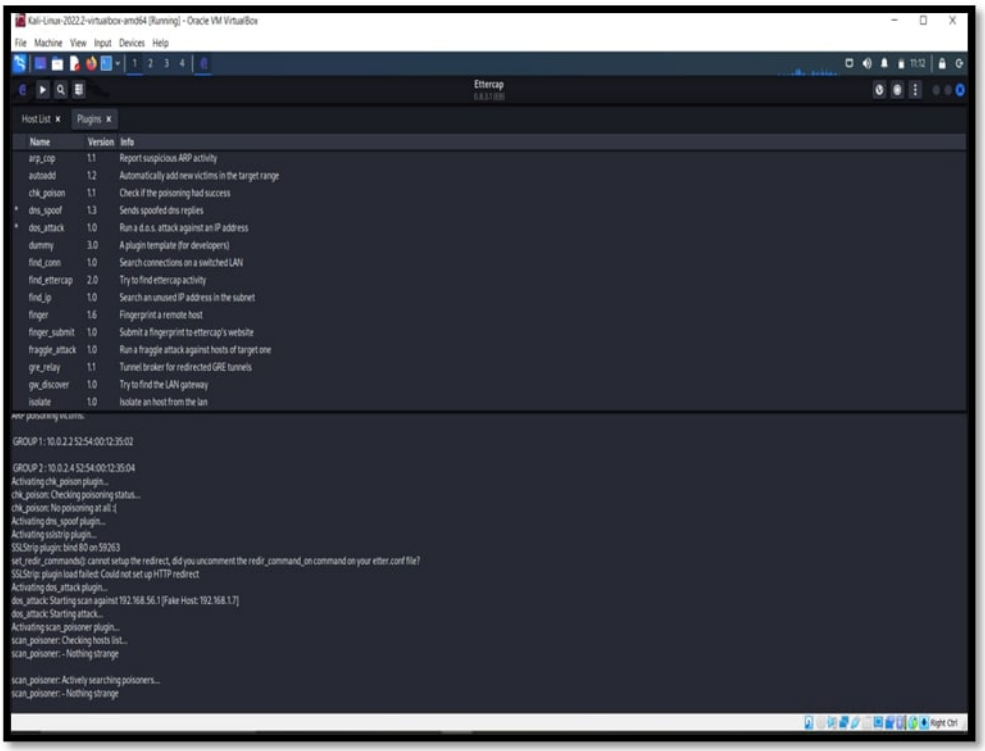
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ettercap
Host List
Plugins
Name Version Info
arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
dns_spoof 1.3 Sends spoofed dns replies
dos_attack 1.0 Run a d.o.s. attack against an IP address
dummy 3.0 A plugin template (for developers)
find_conn 1.0 Search connections on a switched LAN
find_ettercap 2.0 Try to find ettercap activity
find_ip 1.0 Search an unused IP address in the subnet
finger 1.6 Fingerprint a remote host
finger_submit 1.0 Submit a fingerprint to ettercap's website
fraggle_attack 1.0 Run a fraggle attack against hosts of target one
gre_relay 1.1 Tunnel broker for redirected GRE tunnels
gw_discover 1.0 Try to find the LAN gateway
isolate 1.0 Isolate an host from the lan
GROUP 1 : 10.0.2.2 52:54:00:12:35:02
GROUP 2 : 10.0.2.4 52:54:00:12:35:04
Activating chk_poison plugin...
chk_poison: Checking poisoning status...
chk_poison: No poisoning at all :(
Activating dns_spoof plugin...
Activating sslstrip plugin...
SSLStrip plugin: bind 80 on 59263
set_redir_commands(): cannot setup the redirect, did you uncomment the redir_command_on command on your etter.conf file?
SSLStrip: plugin load failed: Could not set up HTTP redirect
Activating dos_attack plugin...
dos_attack: Starting scan against 192.168.56.1 [Fake Host: 192.168.1.7]
dos_attack: Starting attack...
Activating scan_poisoner plugin...
scan_poisoner: Checking hosts list...
scan_poisoner: - Nothing strange
scan_poisoner: Actively searching poisoners...
scan_poisoner: - Nothing strange
Right Ctrl

Fig: 4.3

CHAPTER 5: CONCLUSION

5.1 Conclusion:

MITM attacks has been well explained with its defensive mechanism. The main problem with the current work related the Man in the middle attacks comprise circulation through a middleman, however still annotative MITM procedure is not obtainable so this can be totally a different research direction. Man in the middle attacks can be combined with plentiful cryptographic approaches such as key dissemination and elliptic curve cryptography. As in the future work we aim to extend this research in order to evaluate the impact of such attack in different background of VANET by the flexibility

REFERENCES

- C. L. Abad, R. I. Bonilla, "An analysis on the schemes for detecting and preventing ARP cache poisoning attacks", Proc. 27th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW'07), pp. 60, 2007.
- [2] S. Shukla, I. Yadav, "An innovative method for detection and prevention against ARP spoofing in MANET", Int. J. Comput. Sci. Inf. Technol. Secur., vol. 5, 2015.
- https://www.veracode.com/security/man-middle-attack
- https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html
- Feher, B., Sidi, L., Shabtai, A., Puzis, R., & Marozas, L. (2018). WebRTC security measures and weaknesses. In-ternational Journal of Internet Technology and Secured Transactions, 8(1), 78-102.
- Hypponen, K., & Haataja, K. M. (2007, September). "Nino" man-in-the-middle attack on bluetooth secure simple pairing. In Internet, 2007. ICI 2007. 3rd IEEE/IFIP International Conference in Central Asia on (pp. 1-5). IEEE