

PROFESSIONAL TRAINING REPORT

at

Sathyabama Institute of Science and Technology (Deemed to be University)

Submitted in partial fulfillment of the requirements for the
award of Bachelor of Technology Degree in Information
Technology

By

BALAGANI VAMSHI
REG. NO.39120130



DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF COMPUTING

**SATHYABAMA INSTITUTE OF SCIENCE AND
TECHNOLOGY**

**JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600119, TAMILNADU**



SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)



Accredited with Grade “A” by NAAC
(Established under Section 3 of UGC Act, 1956)
JEPPIAAR NAGAR, RAJIV GANDHI SALAI
CHENNAI- 600119
www.sathyabama.ac.in

DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **BALAGANI VAMSHI (Reg. No: 39120130)** who carried out the project entitled **“DETECTION OF ADDRESS RESOLUTION PROTOCOL ATTACKS ”** under my supervision from Feb 2022 to April 2022.

Internal Guide

Dr.BEVISH JINILA

Head of the Department

Dr. R. Subhashani, M.E., Ph.D.,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I, **BALAGANI VAMSHI** hereby declare that the project report entitled **DETECTION OF ADDRESS RESOLUTION PROTOCOL ATTACKS** done by me under the guidance of **Dr. Bevish Jinila.**, is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology Degree in Information Technology

DATE:

PLACE: Chennai.

B. Vamshi

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. SUBHASHAINI, M.E., Ph.D., Heads of the Department of Information Technology** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. Bevish Jinila, M.E., Ph.D.** for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

TRAINING CERTIFICATE



ABSTRACT

Address Resolution Protocol spoofing attack is the most common type of local area network attacks. This is because the protocol packet does not contain any authentication information, which indicates the origins of reply packet. Therefore, all of the devices in Local Area Network are vulnerable to this attack. A tool like, ARPspoofer can be used to generate a forged Address Resolution Protocol reply packet to perform the attack, even without any knowledge of the details behind address resolution process. The existence of such automated tools has created a hole for the attackers to easily attack a host in a local area network. And although it is underestimated attack, this attack opens the door for much sophisticated form of attacks, such as Man-in-the-Middle attack or even domain name system spoofing and many more sophisticated forms of attacks. In this paper, we will explore different tools and methods used in detection and prevention of Address Resolution Protocol Spoofing attack. The ARP spoof tool will be used to send spoofed Address Resolution Protocol reply packet to a host in local area network to further study how a host maintains the address resolution protocol cache table with the spoofed or a fake media access control, MAC cache table. Finally, we will compare the tools and methods used in detection and prevention against Address Resolution Protocol Spoofing attack in terms of their effectiveness in detection and prevention of the attack and system performance requirements.

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE No
	ABSTRACT	i
	LIST OF ABBREVIATIONS	iv
	LIST OF FIGURES	v
1	INTRODUCTION	1
2.	AIM AND SCOPE OF THE PRESENT INVESTIGATION	4
2.1	AIM	4
2.2	PROJECT SCOPE	4
2.3	OVERALL OBJECTIVE	4
2.4	PROPOSED SOLUTION	5
3	EXPERIMENTAL OR MATERIALS AND METHODS, ALGORITHMS USED	6
3.1	MATERIAL REQUIREMENTS AND TECHNOLOGIES USED	6
3.2	IMPLEMENTATION OF ARP	7
4	RESULT AND DISCUSSION, PERFORMANCE ANALYSIS	11
4.1	RESULTS AND DISCUSSION	11
4.2	ANALYSIS AND INTERPRETATION OF RESULTS	12
5	CONCLUSIONS AND FUTURE ENHANCEMENTS	13
5.1	CONCLUSION	13
	REFERENCES	14
	APPENDIX	15
	A. SCREENSHOTS	16

LIST OF ABBREVIATIONS

S.NO	SHORTCUT	ABBREVIATION
1	ARP	Address Resolution Protocol
2	MAC	RANDOM FOREST Media access control
3	LAN	Local area network
4	VM	Virtual Machine

LIST OF FIGURES

FIGURE NO.	FIGURE NAME	PAGE NO.
1.1	flow dig for Arp poisoning	2
	Man in the middle attack	3
		1.2

CHAPTER 1

INTRODUCTION

The Address Resolution Protocol is the portion of TCP/IP protocol set used for associating Media Access Control destination to the Internet Protocol destination for physical reachability between devices in a network. The Ethernet next hop must be discovered before data encapsulation is accomplished and Ethernet Frame is forwarded to hosts in a local area network. In order to take place communication in local area network, the lower layer address should be mapped to higher layer address. To make this association, an Address Resolution Protocol is used. Moreover, to avoid unnecessary generation of additional broadcast network traffic and to improve network performance an Address Resolution Protocol is required. Data link forwarding relies on the knowledge of the MAC address of the data link destination. The source must be aware of the target MAC address to which data should be transmitted. To transmit data at a data link layer, the forwarding host should have information of the lower layer address of the destination device to which Ethernet frame is to be forwarded. If the ARP cache table of a device is empty, then the device has to learn or resolve the upper layer address to lower layer address to physically reach the destination of the device [1, 2, 3]. The device learns the Media Access Control address through the Address Resolution Protocol process. Address Resolution Protocol process is required to resolve the Media Access Control address, to the internet protocol address. When a device needs to transmit any network traffic to another device for the very first time, the address resolution process is required. The device broadcasts an Address Resolution Protocol packet to every other device in the network. Upon receiving the Address Resolution Protocol broadcast traffic, a device whose Internet Protocol address matches with the destination header in the broadcasted Address Resolution Protocol packet, reply's to the sender. This reply packet contains the hardware address of the device. Through this process a device learns the hardware address of all devices in the network [4]. The Address Resolution Protocol is very important for physical reachability between devices in Local Area

Networks. This protocol does not support validation, and this is often used as part of other serious attacks such as Resolution Protocol spoofing, Distributed Denial of Service (DDoS) attack. In Resolution Protocol process spoofing, the spoofer can capture the packets between devices in the network. In Denial of Service violence, the invader marks a target device reject communication with other device. Due to this reason Address Resolution Protocol spoofing remains a bad attack in the local area network [5, 6]. a network [5, 6]. In Address Resolution Protocol spoofing the attacker marks Media Access Control table as its target. In local area networks, a device may connect with another device such as a router, to do so; the device transmits a Media Access Control address. In transmission of the lower layer address, reaching the intended destination relies on firstly resolving the Media Access Control address to the Internet Protocol address of a device. There is no verification or authentication procedure for the Address Resolution Protocol. Any device that needs to reach another device on a local area network creates an Address Resolution Protocol packet with destination address of broadcast Media Access Control which is FF-FF-FF-FF-FF-FF [7-10].

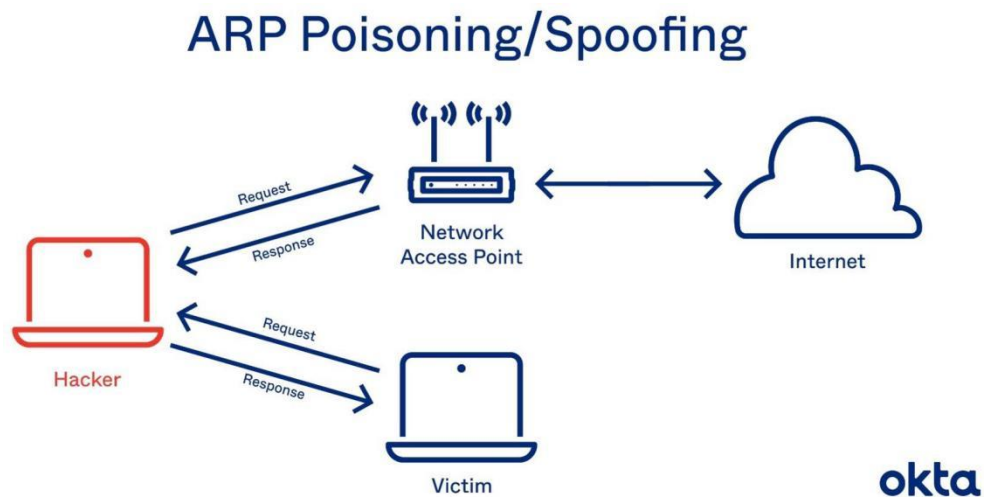


fig 1.1:flow dig for Arp poisoning

The Address Resolution Protocol process request/reply between two hosts is shown in figure 1 and is discussed in detail in the upcoming sections. When the host-1 needs to communicate with the host-2 which is in the same network, does the following:

1. Sends ARP request to host-2 with upper layer protocol address, MAC address as a source, the upper layer protocol address and a broadcast MAC address as destination address.
2. The host compares the upper layer address in the received frame with the upper layer address. Since, the frame was destined to this host, the frame is processed and ARP reply packet is sent as a unicast frame with the host1 MAC address as destination and host-2 MAC address as source in the frame.
3. Upon receiving this frame, host-1 will associate the new MAC received in frame in step 2 to upper layer protocol address and updates the ARP cache.

Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines' MAC addresses. ARP Poisoning is also known as ARP Spoofing

What is MITM?

The Man-in-the-Middle attack (abbreviated MITM, MitM, MIM, MiM, MITMA) implies an active attack where the adversary impersonates the user by creating a connection between the victims and sends messages between them. In this case, the victims think that they are communicating with each other, but in reality, the malicious actor controls the communication.

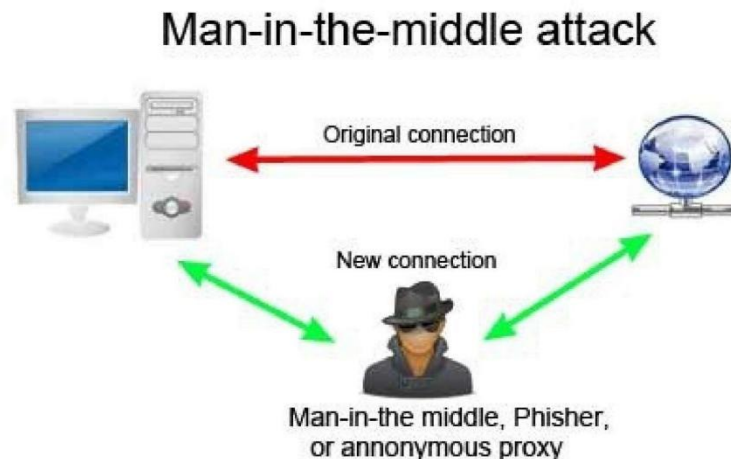


fig 1.2 : Man in the middle attack

A third person exists to control and monitor the traffic of communication between two parties. Some protocols such as SSL serve to prevent this type of attack.

CHAPTER 2

AIM AND SCOPE OF THE PRESENT INVESTIGATION

2.1 AIM :

The main aim of the project is to detection of Address resolution protocol attack.

2.2 PROJECT SCOPE :

we will focus on the methods used in detection and prevention of Address Resolution Protocol spoofing attacks, such as XARP, Wireshark, ARPalert, ARPon and static inspection. One of the best methods to deal with Address Resolution Protocol spoofing attack is static inspection. In this method, media access control address, MAC is statically mapped to specific Internet Protocol address and the mapping is controlled by administrator manually. Using this method, highest level of Local Area Network security can be achieved but, it is not feasible in larger network with hundreds of hosts. Hence, automated tools are required to prevent the Address Resolution Protocol Spoofing attack in Local Area Networks

2.3 OVERALL OBJECTIVE :

The ARP protocol is the only protocol which gives the solution to the Mac address for the communication. Once a system knows an ip address of the communication system it will broad cast ip address to know the Mac address of the system but because of this volatile catch mechanism hacker can easily hack any system by sending its Mac address as the pair of ip address broadcast and can spoof his data.

2.4 PROPOSED SOLUTION :

This method achieves complete detection and prevention to ARP spoofing with a minimal burden by involving three significant proposed modules a (1) Host perspective model (2) Server perspective model and (3) Server to server authentication. In our first module every communicating host has to send his ipMac pair to the centralized server at the time of DHCP itself and regular IP-Mac match checking is done by broadcasting a packet with its own ip and Mac in the source field and its own ip and ff:ff:ff:ff in the Mac of destination field. If any hacker is found

by getting a reply for the above message. Then the destination host will send the hacker information udp/tcp message to the centralized server. In server perspective module in which a centralized server is installed to the LAN which collects all the systems ip-mac pair at the time of DHCP itself ,generate and maintain a tabled database of an legitimate users and hackers if any information is came from the host that intimating about the hacker as a formal udp message. It will verify the information with the database and will send an udp/tcp message to the source. The final module is the server to server authentication module in which if two information messages has came to the source then the source will forward that to the centralized system of that LAN. Initially every host in a LAN has a detail of centralized server information through the authentication procedure. The centralized servers in each LAN have some sort of secured network with other LAN servers through public key encryption and decryption algorithm. If a server conflict occurs on the source host it resolves the conflict by sending a message to the trusted centralized server in that LAN, which check the database for finding the legitimate server matching and inform that to the source host.

CHAPTER 3

3 MATERIALS AND IMPLEMENTATION OF ARP,

3.1 MATERIAL REQUIREMENTS AND TECHNOLOGIES USED :

- VM ware workstation
- Kali Linux or Linux Operating system
- Ettercap Tool
- LAN Connection
- Xarp Tool

XARP is an application used for Address Resolution Protocol Spoofing attack detection. This runs on windows, Mac or UNIX systems. It requires very limited memory space and processing time. It is valuable easily usable software to screen the Address Resolution Protocol table of a computer. The XARP sends instant packets to a computer Address Resolution Protocol table on the computer on which it is running. If any change occurs with the previously stored address resolution table of the computer and received address resolution protocol reply packet, it notifies the

change in matching Address Resolution Protocol reply packet to the previous one. Thus, XARP is required for detecting Address Resolution Protocol spoofing attack. The fake address resolution protocol replay detected by XARP is shown in Figure 7. XARP raises alert in cases where Address Resolution Protocol spoofing attack is attempted. In figure 1, we have sent Address Resolution Protocol frame replay to a host with Internet Protocol address 10.0.0.1 as a target or victim.

ARP spoof detection and System Resource

prevention tools	requirement	Detection and inspection
Wireshark	High	Powerful in detection but, requires manual inspection
ARP watch	Medium	Powerful in detection but, requires manual inspection
XARP	Moderate	Powerful in detection but, requires manual inspection
ARP Alert	Low	Powerful in detection and does not, require manual intervention

3.2 IMPLEMENTATION OF ARP:

This attack is possible in wired and wireless networks. You can perform this attack in local LAN.

Step 1– Install the VM ware workstation and install the Kali Linux operating system.

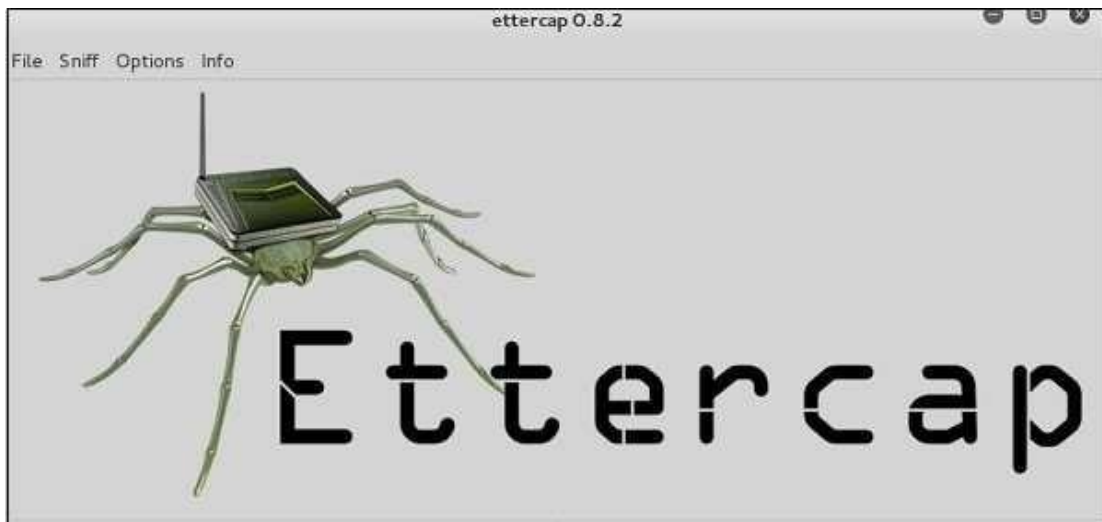
Step 2– Login into the Kali Linux using username pass “root, toor”.

Step 3– Make sure you are connected to local LAN and check the IP address by typing the command **ifconfig** in the terminal.

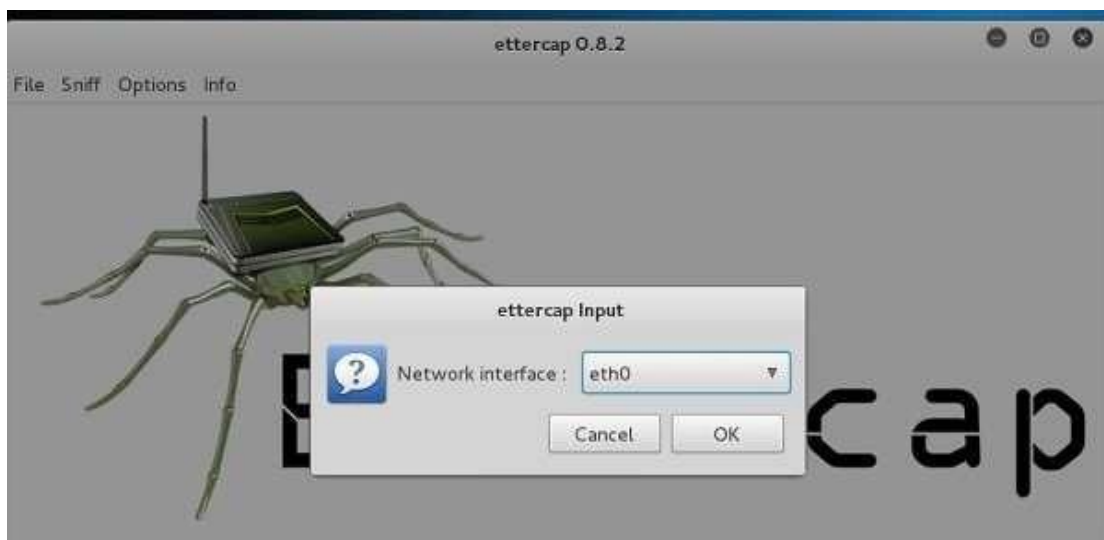
```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:cf:f8:e7
          inet addr:192.168.121.128  Bcast:192.168.121.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fecf:f8e7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4963 (4.8 KiB)  TX bytes:8868 (8.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:960 (960.0 B)  TX bytes:960 (960.0 B)
```

Step 4– Open up the terminal and type “Ettercap –G” to start the graphical version of Ettercap.

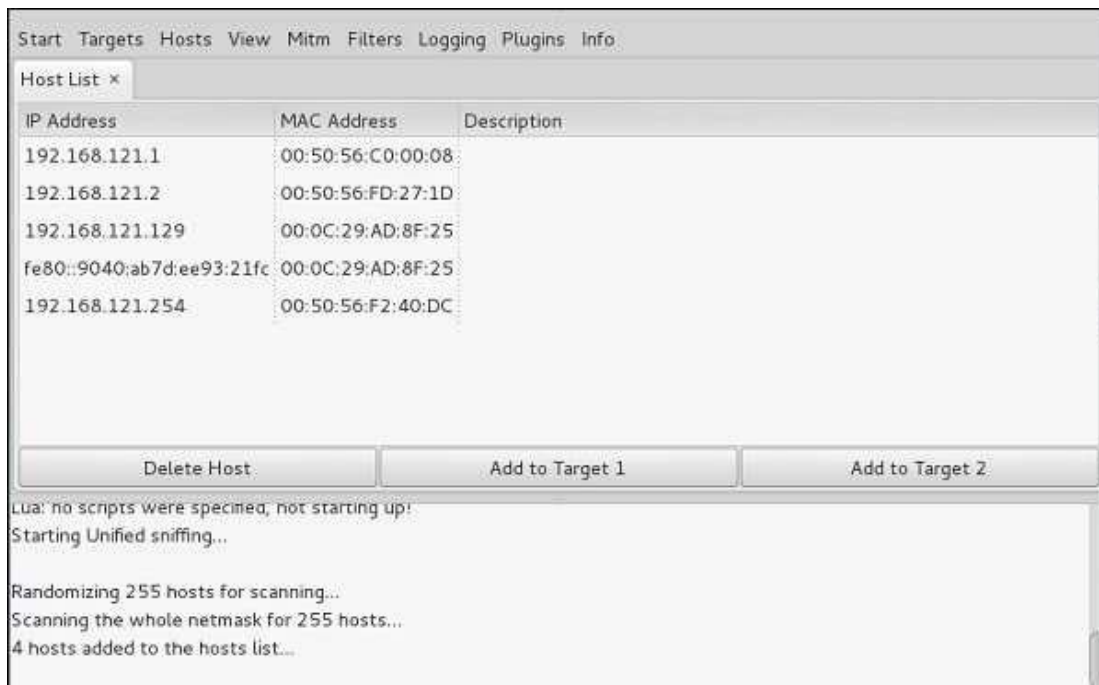


Step 5– Now click the tab “sniff” in the menu bar and select “unified sniffing” and click OK to select the interface. We are going to use “eth0” which means Ethernet connection.



Step 6– Now click the “hosts” tab in the menu bar and click “scan for hosts”. It will start scanning the whole network for the alive hosts.

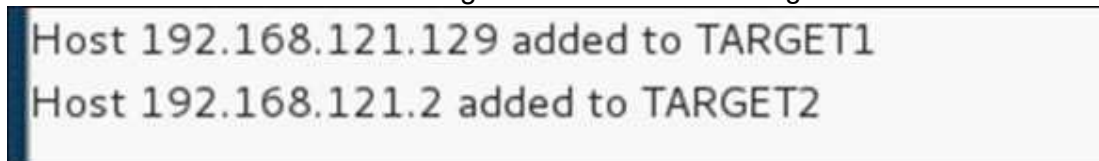
Step 7– Next, click the “hosts” tab and select “hosts list” to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.



Step 8– Now we have to choose the targets. In MITM, our target is the host machine, and the route will be the router address to forward the traffic. In an MITM attack, the attacker intercepts the network and sniffs the packets. So, we will add the victim as “target 1” and the router address as “target 2.”

In VMware environment, the default gateway will always end with “2” because “1” is assigned to the physical machine.

Step 9– In this scenario, our target is “192.168.121.129” and the router is “192.168.121.2”. So we will add target 1 as **victim IP** and target 2 as **router IP**.



Step 10– Now click on “MITM” and click “ARP poisoning”. Thereafter, check the option “Sniff remote connections” and click OK.



Step 11– Click “start” and select “start sniffing”. This will start ARP poisoning in the network which means we have enabled our network card in “promiscuous mode” and now the local traffic can be sniffed.

Step 12– Now it's time to see the results; if our victim logged into some websites. You can see the results in the toolbar of Ettercap.

A screenshot of the Ettercap toolbar interface. It shows a list of sniffed packets. The first packet is highlighted with a red border. The text of the packet is: GROUP 2 : 192.168.121.2 00:50:56:FD:27:1D, Unifed sniffing already started..., HTTP: [REDACTED] -> USER: admin PASS: admin INFO: [REDACTED], CONTENT: username=admin&password=admin&Submit=Login. The toolbar has a light gray background and a red border around the selected packet.

```
GROUP 2 : 192.168.121.2 00:50:56:FD:27:1D
Unifed sniffing already started...
HTTP: [REDACTED] -> USER: admin PASS: admin INFO: [REDACTED]
CONTENT: username=admin&password=admin&Submit=Login
```

This is how sniffing works. You must have understood how easy it is to get the HTTP credentials just by enabling ARP poisoning.

CHAPTER 4 RESULTS AND DISCUSSION, PERFORMANCE ANALYSIS

This section consists of outputs and tables of features selection and different classification approaches which have been discussed in chapter 3.

4.1 Results And Discussion :

Address Resolution Protocol spoofing attack which is the most underestimated attack, can be a base for more sophisticated attacks. Although poisoning the Address Resolution Protocol table of a host will do nothing when it is in the inactive state, this kind of attack may lead to loss of sensitive data, disclosure of confidential information to the intruder as the Address Resolution Protocol spoofing is the basis for other advanced attack. To mitigate this attack different software tools were developed. Among these we have discussed the most popular open source Address Resolution Protocol spoofing attack detection and prevention tools such as XARP, and the static method. Those all methods may be useful based on the level of security requirement and the nature of a company network. For example in a network consisting of three or four computer or in small workgroup the static method may be preferred than all other methods. The main solutions that are proposed to detect Address Resolution Protocol spoof attacks are XARP, static method and ARPwatch. In this section we have discussed different Address Resolution Protocol spoof detection and prevention methods such as XARP software tool for detection of Address Resolution Protocol spoofing. we conducted an extensive work to know which security solutions are able to detect a very dangerous MAC layer attack called ARP spoofing. It is to be noted that ARP spoofing constitutes the beginning of many attacks, one of which is, the destructive MiM attack. We were able to show throw testing and experimentation that the current security solutions have many shortcomings and defects when it comes to detecting ARP Spoofing. XArp 2 tool was the most efficient available security solution that can cope with ARP spoofing attacks. However, it needs minor improvements, compared to the other security solutions, by adding mechanisms to detect ARP request storm and ARP scanning. As a conclusion of our study, we suggested 6 basic and crucial requirements that any algorithm should follow in order to detect ARP spoofing sufficiently on switched LANs.

4.2 Analysis and Interpretation of Results:

As illustrated in figure 6, a command line arpspoof tool was used to send address resolution protocol reply packet to a host destined at upper layer protocol address which is the Internet Protocol address of 10.0.0.2. Upon receiving this packet, the host maintains its media access control address with the received MAC address in the arpspoof attack option.

inspection is required by the network administrator. Another perfectly performing tool is ARPalert which is applicable to small high security networks, such as Wireless Local Area Networks with two or more dozen machines. Compared to Wireshark and ARPalert, XARP has a better performance, it is a lightweight program yet very powerful in detection of Address Resolution Protocol spoofing attack. Unlike, the ARP alert which runs only on UNIX, XARP is platform independent and runs on UNIX and Windows systems. The other most important tool used in Address Resolution Protocol spoofing attack is the ARPWatch tool. This tool runs on UNIX system. It can be configured on UNIX system to automatically detect any spoofed Address Resolution Protocol reply packet. This tool is more powerful in detection and can be automated so that once configured it does not need human intervention to deal with Address Resolution Protocol spoofing attack.

REFERENCES:

- [1] Zhang Chao-yang, DDOS attack analysis and study of new measures to prevent ARP Spoofing attack (Communications Magazine, IEEE, 40(10), pp.42-51, Oct (2012).
- [2] Jami Manzoor, Avinash Kumar, Sweetie Kumari, ARP SPOOFING AND MANIN THE MIDDLE ATTACK, , International Journal of Computer Engineering and Applications, Volume X, Special Issue, ICRTCST -2016.
- [3] D Raviya Rupal, Dhaval Satasiya, Hires Kumar, Archit Agrawal, Detection and prevention of ARP poisoning in dynamic IP configuration, IEEE, 2016.
- [4] J. David Brown, Tricia J. Willink, A new look at: ARP spoofing to create routing loops in Ad Hoc networks, IEEE, 2018.
- [5] Ahmed M. AbdelSalam, Wail S. Elkilani, Khalid M. Amin, An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014.
- [6] Andre P. Ortega, Xavier E. Marcos, Luis D. Chiang and Cristina L. Abad, "

Preventing ARP cache poisoning attacks: A proof of concept using OpenWrt," Latin American Network Operations and Management Symposium. (LANOMS), pp. 1- 9, Oct. 2009.

APPENDIX:

A. SCREENSHOTS:

1.

```
PC>arp -a

Internet Address      Physical Address      Type
10.0.0.2              54-89-98-52-23-F6    dynamic
```

```
tt@ubuntu:~/Desktop$ sudo arpon arpalert.darpi -i ens33 -y 1 -D
[sudo] password for tt:
```

```
07:26:01 WAIT LINK on ens33...
```

```
07:26:01 DARPI on
```

```
DATE = <09/27/2018>
```

```
DEV = <ens33>
```

```
HW = <0:c:29:79:e1:8b>
```

```
IP = <10.128.0.0>
```

```
07:26:04 ARP cache, ACCEPT
```

```
src HW = <0:50:56:f8:84:5c>
```

```
src IP = <10.0.0.2>
```

```
07:26:59 ARP cache, ACCEPT
```

```
src HW = <0:50:56:c0:00:08>
```

```
src IP = <10.0.0.1>
```

```
07:27:11 ARP cache, ACCEPT
```

```
tt@ubuntu:~/Desktop$ sudo arpon arpalert.sarpi -i ens33 -S
```

```
07:33:25 WAIT LINK on ens33...
```

```
07:33:25 SARPI on
```

```
DATE = <09/27/2018>
```

```
DEV = <ens33>
```

```
HW = <0:c:29:79:e1:8b>
```

```
IP = <10.128.0.0>
```

```
CACHE = </etc/arpon.sarpi>
```

```
07:33:29 ARP cache, IGNORE
```

```
src HW = <0:50:56:f8:84:5c>
```

```
tt@ubuntu:~$ sudo arp -s 10.0.0.2 00:50:56:f8:84:5c
```

```
tt@ubuntu:~$ ip neighbour show
```

```
10.0.0.1 dev ens33 lladdr 00:50:56:c0:00:08 STALE
```

```
10.0.0.2 dev ens33 lladdr 00:50:56:f8:84:5c PERMANENT
```

```
10.255.255.254 dev ens33 lladdr 00:50:56:ee:ff:b9 STALE
```

```
PC>arp -a
```

Internet Address	Physical Address	Type
10.0.0.1	54-89-98-C5-6C-F9	dynamic