IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

Command line and Graphical interface comparative analysis for ARP Poisoning through Ettercap

S. Prudhviraj[1*], C. Sudha[2]

[1,2]Dept. of Computer Science, Mahatma Gandhi Institute of Technology, Hyderabad, India

Corresponding Author: prudhvi193@gmail.com *Tel:* +91 9502630591

Available online at: www.ijcseonline.org

Accepted: 19/Oct/2018, Published: 31/Oct/2018

Abstract--- There has been many changes taking place in the recent arena of Address Resolution Protocol (ARP) Poisoning from the command line interpretation to the graphical interfaces that are developed. The process of ARP Poisoning is one of the famous techniques amongst present Man in The Middle (MITM) attacks. It is applicable to access the various unsecured websites authentication details which can be captured by the attacker and can be visualized on both the command line and graphical user interface (GUI). The entire process or communication takes place through the ethernet or local area network (LAN) and the result of the poisoned address is the physical address of the LAN which acts as a common interface between both the attacker and victim's machine. This paper, there by explains the entire mechanism of ARP Poisoning that takes place through the LAN by both the command line interpretation (CLI) and the GUI Ettercap which shows the differences amongst both the methods and determines the best method which has the least complexity.

Keywords--- Address Resolution Protocol (ARP), ARP Poisoning, Man in The Middle Attack, Ettercap, Attacker, Victim, Ethernet or Local Area Network (LAN).

I. INTRODUCTION

The Address Resolution Protocol (ARP) [1] runs using the Internet Protocol which is the IPv4 or its extended version IPv6, for mapping different IP network IP addresses to MAC address which operates through the data link layers protocol.

This protocol plays its role in between the physical and network layer as a portion of the Open System Interconnection (OSI) model. It runs over the Ethernet or the Local area network (LAN) using IPv4 protocol.

This definition of ARP is used to find address of any computer that is hosted on a particular network. This address can be found out by using a protocol through which a part of information is sent by the client host process executing on the other remote machine. This required information obtained by the server allows the server to distinctively identify the network system for which the address was necessary and thereby to ensure the required address. This process is completed when the required client achieves a response from the server which is followed by the necessary address.

An Ethernet or local area network (LAN) [2] utilizes two hardware addresses which identify the source and destination resulted addresses for each frame dispatched by the Ethernet. Broadcasting of packets which is distributing address to all connected computers is been satisfied by the destination address which are all 1's. The hardware address which is referenced to as the Medium Access Control (MAC) address, with inference to all the standards which define the LAN. For every single computer network interface card (NIC) is assigned universally distinct 6-byte link address when the factory produces the card which are likely to be deposited in a PROM. [2] The intermediate uses this for hosting the source or client's address. Observing this scenario, the source computer posts all packets which it generates with its possessed hardware source link address, and receives all packets which peer the equivalent hardware addresses in the destination field or their constituted broadcast/multicast addresses.

This paper thereby gives the brief summary of both the command line, the graphical interface methodologies for performing ARP Poisoning in sections 3 and 4, and their outcome and drawbacks in section 5 respectively.

II. BACKGROUND

A. ARP Poisoning

ARP Poisoning is the same term as ARP Spoofing where in a malevolent actor forwards a counterfeited ARP messages over the Ethernet. This will out-turn in the linking of an attacker's Ethernet hardware address (EHA) with the IPv4 address of an authorized server or computer hosted on the

network. [3] The data is received by the attacker through the intended IP address only when the attacker's Ethernet hardware address is bridged to an authentic IP address. The operations such as intercepting, modifying or even stopping data en routing can be done by the malevolent actors through ARP poisoning. These attacks can only occur on ethernet or local area networks that uses the address resolution protocol.

B. Types of ARP Poisoning Attacks

Various insights for organizations can have serious ARP poisoning attacks. [3] Stealing of most useful or sensitive information is one of the basic most application for performing ARP Poisoning. Various other attacks that can be achieved through ARP Poisoning can be classified as follows:

Denial of Service attacks (DOS): DOS attacks, hold ARP poisoning to bind several IP addresses with a single target's ethernet hardware address. As a reaction, traffic which is much intentional for multiple different IP addresses will be rechannelled to the quarry IP Ethernet physical address, by encumbering the destination target with traffic. [3]

Session Hijacking: The attackers exclusives or personals for systems and data can be stolen by using the session IDs (unique identification number) through the ARP Spoofing mechanism.

Man In The Middle attacks (MITM): These attacks depend on ARP Spoofing to interpret and alter traffic occurrence between victims. [3]

C. Ettercap

Ettercap is a graphical interface tool developed by Aberto Ornaghi (ALoR) and Macro Valleri (NaGA) and primarily is a suite for man in the middle attacks over the Ethernet. [4] To overcome the complexities in writing the commands in the Command Line Interface (CLI), it is being replaced by the easiest method for accessing and performing the attacks with the Ettercap graphical interface.

This interface is also enabling to perform attacks against the spoofing of ARP by placing oneself as the man in the middle and once positioned by this role will be able to:

- Various data manipulation operations such as, deleting, replacing, infecting data in a connection can be done.
- POP, HTTP, SSH1 and other related protocol passwords can be located.
- The supply of falsified SSL and SSH certificates in the HTTPS sections can be transmitted to the victim.

III. COMMAND LINE ARP POISONING

Before the development of graphical interfaces there was use of Command line interface (CLI) which allows to perform the task of ARP Poisoning. [5] It follows a sequence of steps that are as follows:

1. Enable IP Forwader

Determining which passage a packet or datagram will be sent is known as IP forwarding. The decisions are taken based upon the routing information and is outlined to forward a packet over multiple networks. It must be enabled, as it is evident to redirect traffic through attacker PC.

Disable=0 Enable=1

#echo "1" > /proc/sys/net/ipv4/ip_forward

2. IPTables NAT

The procedure of recasting addresses on a packet as it passes through a routing device is called network address translation (NAT). There are far reaching consequences on protocol compatibility and network design every time NAT is plied. [6]

#iptables -t nat -A PREROUTING -p tcp -destination port 80 -j REDIRECT -to-port 8880

Request coming on port 80 will be redirected to user define port number. With the IPTable NAT rule the attacker PC will provide internet services to the victim PC. [6]

3. ARP Poisoning Attack

Address Resolution Protocol (ARP) spoofing is a type of attack in which a hostile actor sends fake ARP messages over the ethernet.

Syntax: arpspoof -i interface -t target-ip target-gateway-ip

ARP spoof attacks on victim PC and associated IP gateway. [5]

#arpspoof -i eth0 -t 192.168.1.254 192.168.0.189

192.168.1.254 - Victim PC IP address
192.168.0.189 - IP Gateway address

4. Packet sniffing through Ettercap

Ettercap is the tool used for ARP spoof attack under Window or Linux operating system. [5]

#ettercap -i eth0 -T -w /root/file.txt -M 192.168.1.254

-i Defines specific interface
-T To launch command execution over the terminal
-M Man in the middle mode
-w Writes sniffed data to a file

To overcome this command line arguments there has been an introduction of various graphical interfaces that makes the process of ARP Poisoning easy compared to the

traditional method and reduces the complexity of an attacker to memorize the IP addresses that are connected over the same LAN.

IV. ARP POISONING THROUGH ETTERCAP GUI

Various graphical interfaces have been developed in order to reduce the time efficiency and perform tasks easily and efficiently. [9] There are a series of steps that are followed to prove how this task is being performed. [7]

A. Ensuring same LAN connection
The initial phase to be ensured by the attacker is
that the poisoning of system is being performed under the same local area network.

B. Launching the Ettercap Interface
Here we use the command line interface initially to pop up the Ettercap graphical menu.

Figure 1. Enabling Ettercap Graphical interface

Ettercap -G is a Linux based graphical command that pops up the interface required to perform the different type of man in the middle attacks. [7]

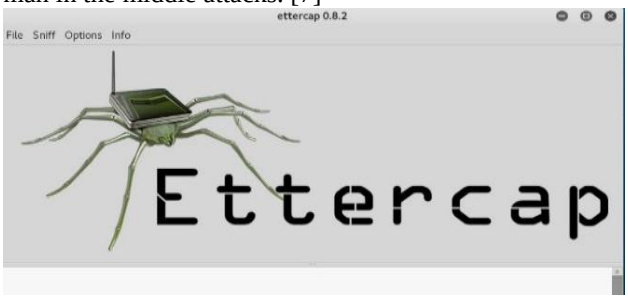

Figure 2. Ettercap Interface

C. Performing Unified Sniffing and choosing the network interface

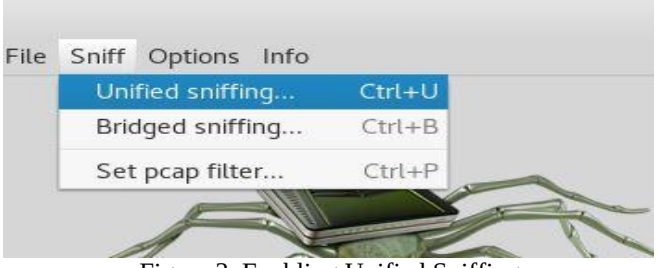

Figure 3. Enabling Unified Sniffing

Unified Sniffing is the base for all attacks. The kernel IP forwarding is always disabled and this task is accomplished by Ettercap itself. Packet that needs to be forwarded are packets with the destination mac address equal to the attacker's one, but with different IP address. Those packets are re-sent back to the wire to the real destination. This way, you can plug in carious MITM attacks at a time. You can even use external attacker/poisoner, then only have to redirect packets to Ettercap's host and the game is over. Thereby this process enables an Ettercap input to choose the network interface. [8]

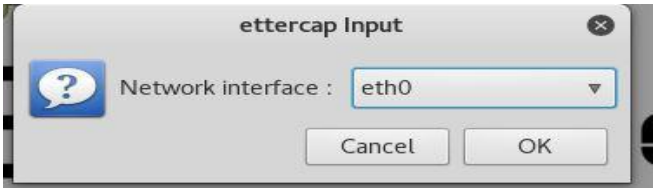

Figure 4. Choosing the network Interface

Here the network interface is ethernet (LAN) that is an initial phase that allows us to perform ARP Poisoning.

Figure 5. Visualizes processing of Unified Sniffing

This figure shows us that the process of unified sniffing has been started.

D. Scanning for hosts on the network and display the host lists.
The hosts are to be initially identified by scanning them along the network being opted i.e. ethernet.

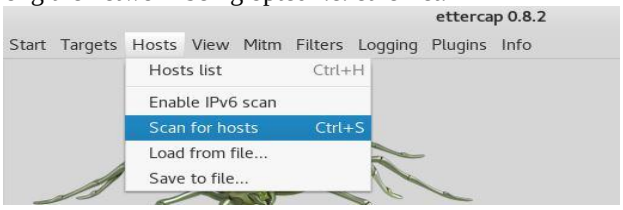

Figure 6. Scanning for hosts available on LAN

Now on scanning the hosts we can see a description which shows the number of hosts added to the host list that are being randomized for scanning. [9]

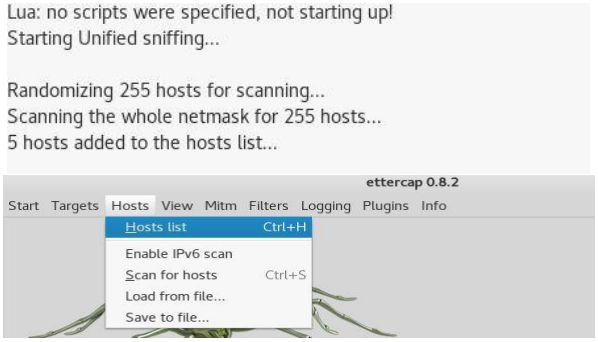

Figure 7. Depicts number of hosts added and to menu to show added hosts

The figure shows, how can we display the host list through the hosts menu.

E. Adding Targets on the attacker's system

Now as all the available hosts over the LAN are visible in the hosts list (attacker), thereby the attacker can add the victim which is needed to be poisoned as one of the targets and then the network address (eth0) which is common both to the victim and attacker. [9]

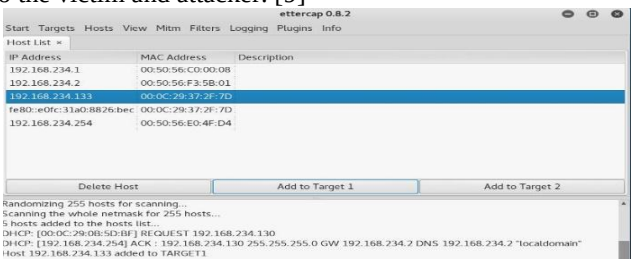

Figure 8. Adding victim's IP address as 1st target

The figure depicts us the victim's IP address that the host (attacker) needed to perform poisoning on.

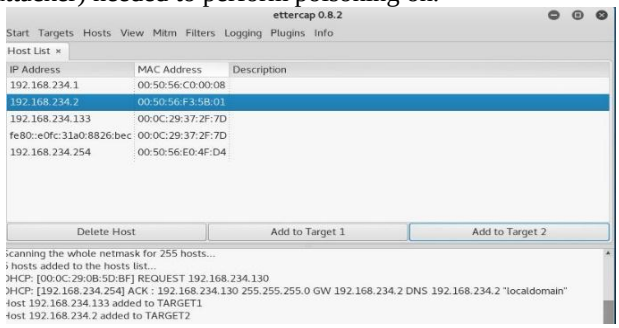

Figure 9. Adding the network's IP address as the second target

Here the network address (eth0) is added at the end as to notify prior about the victim machine that is to be poisoned. [9]

F. Performing MITM attack using ARP Poisoning and its activation on both the targets.

Now as the targets are added the host (attacker) can perform ARP Poisoning through Ettercap and thereby opt for the optional parameters required
according to the hosts choice.

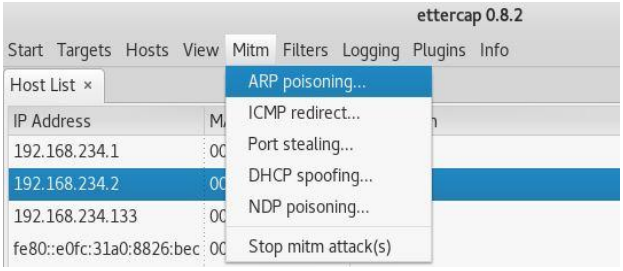

Figure 10. ARP Poisoning through MITM

Now on choosing ARP Poisoning the window requests an optional parameter to be chosen that is whether the attack to be performed on remote connections or on the host itself. [9]

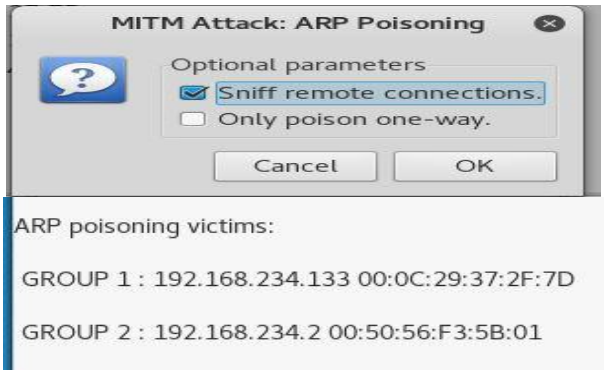

Figure 11. Optional parameters list and groups of ARP Poisoned victims

Now finally, the process of ARP Poisoning is being achieved without performing any traditional operations on the command line interface as discussed in section III. Thereby the victim's system is poisoned and can be attacked over any of the victim's operations that are performed over their (victim's) local machines. [9]

G. Verification of poisoned ARP Packet

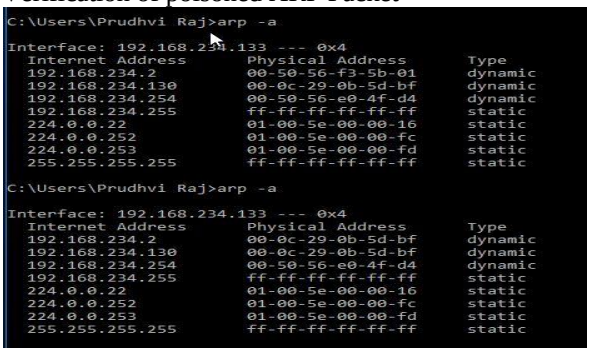

Figure 12. Verifying ARP Poisoning on victim's Windows machine

This verification is not known to the host (attacker) but this can be checked by knowing ARP lists on the victim's machine before and after poisoning.

Syntax: arp -a
Here from the figure the LAN address (Internet Address) is 192.168.234.2 which holds the physical address before poisoning as [00-50-56-f3-5b-01] and after poisoning its physical address changes which is [00-0c-29-0b-5d-bf].

It is been easily identified by checking the Physical address of the LAN which acts as a common interface between both the hosts (victim and attacker) and shows us the poisoned MAC address after performing MITM attack over victim's local machine. [9]

This completes the understanding of how the process of ARP Poisoning takes place using the Ettercap interface and enable these entire operations.

V. OUTCOME AND DRAWBACKS

There is lots of information that can be captured by the host (attacker) from the victim's machine, which can be varied as, allowing to access any unsecured (http) websites authentication credentials, causing vulnerabilities to victim's machine through malwares and any form of virus injections.

The major drawback of this technique is they are restricted to capture information on unsecured websites but not on the secured one's, but this can be achieved by the DNS (Domain Name System) Poisoning which deals with handling of different security certificates, files operated through and perform high end operations on the victim's machine.

VI. CONCLUSION AND FUTURE SCOPE

After having a detailed knowledge on Address Resolution Protocol, its functionality and mechanism in both the interpretations through command line and GUI Ettercap we can conclude that amongst both the mechanisms, the GUI approach is a better one as there is a reduced time complexity for identifying the attacker hosts. As it is a stateless protocol and attackers use this vulnerable point to spoof the ARP reply packets to impersonate the presence to victim so performing attack becomes easy which is best possible through GUI approach. Thereby the time complexity for scanning the hosts is reduced and poisoning of ARP packets become an easy and efficient method.

The limitations to be taken for preventing ARP Poisoning are generating alerts when unsolicited replies are discovered, sending verification messages when ARP requests or replies are received to build a validated resolved IP and MAC table. Apart from Ettercap there are other graphical interfaces such as sslstrip, driftnet, urlsnarf that are used to perform ARP Poisoning which are in the further development and other flavours of man in the middle attacks such as Domain Name System (DNS) Poisoning, Dynamic Host Configuration Protocol are also in development which can help in performing attacks similar to ARP Poisoning with extended features.

REFERENCES

[1] Mauro Conti, Nicola Dragoni, Viktor Lesyk, "A Survey of Man In The Middle Attacks", Communication surveys & Tutorials IEEE, vol. 18, no. 3, pp. 2027-2051, 2016.
[2] Navid Behboodian, "ARP Poisoning attack: "An introduction to attack and mitigations", vol.1, 2 Jan 2012.
[3] Sudhakar, R.K. Aggarwal, A Survey on Comparative Analysis of Tools for detection of ARP Poisoning, International Conference on Telecommunication and Networks, 2017.
[4] C. Hornig, Standard for the transmission of IP datagrams over Ethernet networks, Internet Engineering Task Force, RFC 826, November 1982.
[5] D. Plummer, An ethernet address resolution protocol, Nov.2010, RFC 826
[6] Kyokyedk Kwon, Seongjin Ahn, Jinwook Chung, "Network Security Management Using ARP Spoofing", pp. 142-149, 2004.
[7] Behrouz A. Forouzan, "Data Communications and Networking" in, Mc Graw Hill, pp. 678-680, 2007.
[8] D. Bruschi, A. Ornaghi, and E. Rosti, S-arp: a secure address resolution protocol in Computer Security Applications Conference, 2003. Proceed-ings. 19th Annual. IEEE, 2003, pp. 66 -74.
[9] S. Jadhav and Mandal," A survey on network security for open source," IEEE International Conference of Current Trends in Advanced Computing (ICCTAC), pp. 1-6,2016.

.

