A Project Report

on

ARP Poisoning and Mitigation Techniques

carried out as part of the course CC1730 Submitted by

Shubham Sanjay Sonawane

159103067

7th Semester

in partial fulfilment for the award of the degree

of

BACHELOR OF TECHNOLOGY

In

Computer & Communication Engineering

MANIPAL UNIVERSITY
JAIPUR

Department of Computer & Communication Engineering,
School of Computing and IT,
Manipal University Jaipur,

November, 2018

CERTIFICATE

This is to certify that the project entitled "***ARP Poisoning and Mitigation Techniques*** " is a bonafide work carried out as part of the course ***Network Security Lab*** , under my guidance by ***Shubham Sanjay Sonawane***, student at the Department of Computer & Communication Engineering , Manipal University Jaipur, during the academic semester ***7th semester***, in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology in Computer & Communication Engineering, at MUJ, Jaipur.

Place:

Date: Signature of the Instructor (s)

DECLARATION

I hereby declare that the project entitled **"*ARP Poisoning and Mitigation Techniques*"** submitted as part of the partial course requirements for the course ***Network Security Lab***, for the award of the degree of Bachelor of Technology in Computer & Communication Engineering at Manipal University Jaipur during the ***7th Semester, April 2018*** semester, has been carried out by me. I declare that the project has not formed the basis for the award of any degree, associate ship, fellowship or any other similar titles elsewhere.

Further, I declare that I will not share, re-submit or publish the code, idea, framework and/or any publication that may arise out of this work for academic or profit purposes without obtaining the prior written consent of the Course Faculty Mentor and Course Instructor.

Signature of the Student:

Place:

Date:

ACKNOWLEDGEMENT

The success and final outcome of this project required a lot of guidance and assistance from many people and I am extremely privileged to have got this all along the completion of my project. All that I have done is only due to such supervision and assistance and I would not forget to thank them.

I respect and thank the my professors for providing me an opportunity to do the project work in field of my interest and giving us all support and guidance which made me complete the project duly. I am extremely thankful to Mr. Gaurav Prasad for taking his time providing such a nice support and guidance, although he had busy schedule.

I owe my deep gratitude to computer and communication faculty who took keen interest in my project and guided us all along, till the completion of my project work by providing all the necessary information for developing a good system.

I heartily thank our HOD, Dr. Vijay Pal Singh Dhaka for his guidance and support during this project work. I am thankful to and fortunate enough to get constant encouragement, support and guidance from all Teaching staffs of Computer and Communication Department who helped us in successfully completing my project work.

Finally, I would like to thank my classmate who were there for me providing all the help I can get and for all the resources I ever needed. Secondly I would also like to thank my parents and friends who helped me a lot in finalizing this project within the limited time frame.

Table of Contents

Figures

Abstract

Address Resolution Protocol poisoning (ARP) poisoning is a form of attack in which an attacker changes the physical address or MAC address and attacks on network by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the packets to the hacker's computer first instead of sending it to the original destination. ARP poisoning affects the integrity and confidentiality of the data, as a result both the user's data and privacy are compromised. This technique is backbone for man in the middle attack. An effective ARP poisoning attempt is undetectable to the user as there is no way of knowing that the senders MAC address is a legit one because of incapability to perform authentication in ARP and RARP protocol. In this project we will perform passive attack using ARP poisoning to compromise data integrity and confidentiality to exploit security flaws of established network infrastructure. We will also implement various attack detection and prevention techniques against ARP poisoning. We use various packet filter tools, Anti-ARP tools and more to do so. For smaller networks, we will be using static ARP tables and static IP addresses, an effective solution against ARP poisoning.

1. Introduction

ARP stands for Address Resolution Protocol. It is used to convert IP address to physical addresses or MAC address in a network. The host sends an ARP broadcast on the network, and the recipient computer responds with its physical address or MAC Address. The resolved IP/MAC address is then used to communicate with host. ARP poisoning is sending fake ARP packets to the switch so that it can associate the fake MAC addresses with the IP address of a genuine computer on a network and hijack the traffic. ARP cache poisoning, a method of attacking an Ethernet LAN by updating the target computer's ARP cache with both a forged ARP request and reply packets in an effort to change the Layer 2 Ethernet MAC address (i.e., the address of the network card) to one that the attacker can monitor. Because the ARP replies have been forged, the target computer sends frames that were meant for the original destination to the attacker's computer first so the frames can be read. A successful APR attempt is invisible to the user.

1.1 Scope of Work

This project we will guide us in performing attack using ARP poisoning to compromise data integrity and confidentiality to exploit security flaws of established network infrastructure. We will also implement various attack detection and prevention techniques against ARP poisoning. We use various packet filter tools, Anti-ARP tools and more to do so. Man in the middle attack using ARP poisoning will be used to remote sniff a connection within a network.

ARP poisoning is very effective against both wireless and wired local networks. By triggering an ARP poisoning attack, hackers can steal sensitive data from the targeted computers, eavesdrop by means of man in the middle techniques, and cause a denial of service on the targeted computer. In addition, if the hacker modifies the MAC address of a computer that enables Internet connection to the network, access to Internet and external networks may be disabled. ARP being a commonly used IP to MAC protocol, compromising its security becomes a large scale threat. Hence, demanding the requirement for necessary security protocols against the ARP poisoning becomes genuine.

2. Methodology

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

2.1 ARP Spoofing

ARP spoofing attacks typically follow given progression. The steps to an ARP spoofing attack usually include:

1 The attacker opens an ARP spoofing tool and sets the tool's IP address to match the IP subnet of a target. Examples of popular ARP spoofing software include Arpspoof, Cain & Abel, Arpoison and Ettercap. We will be using scapy-python3 for this operation.

2 The attacker uses the ARP spoofing tool (scapy-python3) to scan for the IP and MAC addresses of hosts in the target's subnet.

3 The attacker chooses its target and begins sending ARP packets across the LAN that contain the attacker's MAC address and the target's IP address.

4 As other hosts on the LAN cache the spoofed ARP packets, data that those hosts send to the victim will go to the attacker instead. From here, the attacker can steal data or launch a more sophisticated follow-up attack.

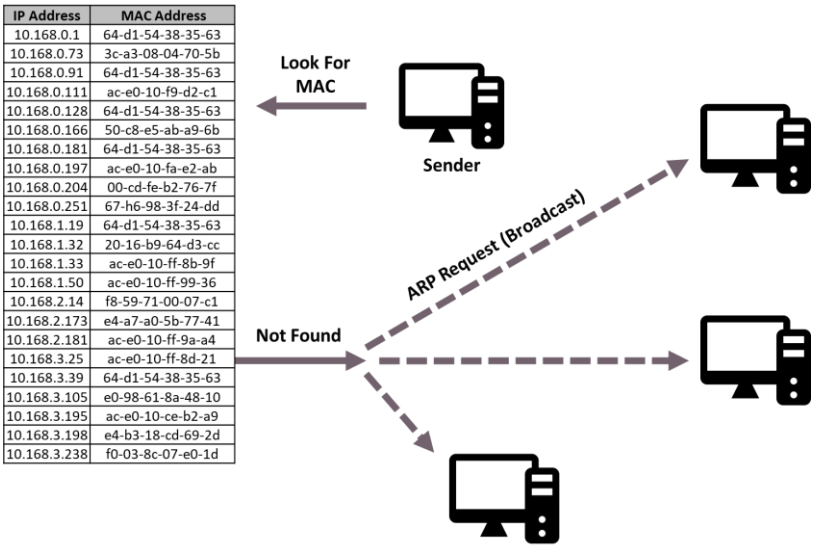

Fig 1. ARP Working

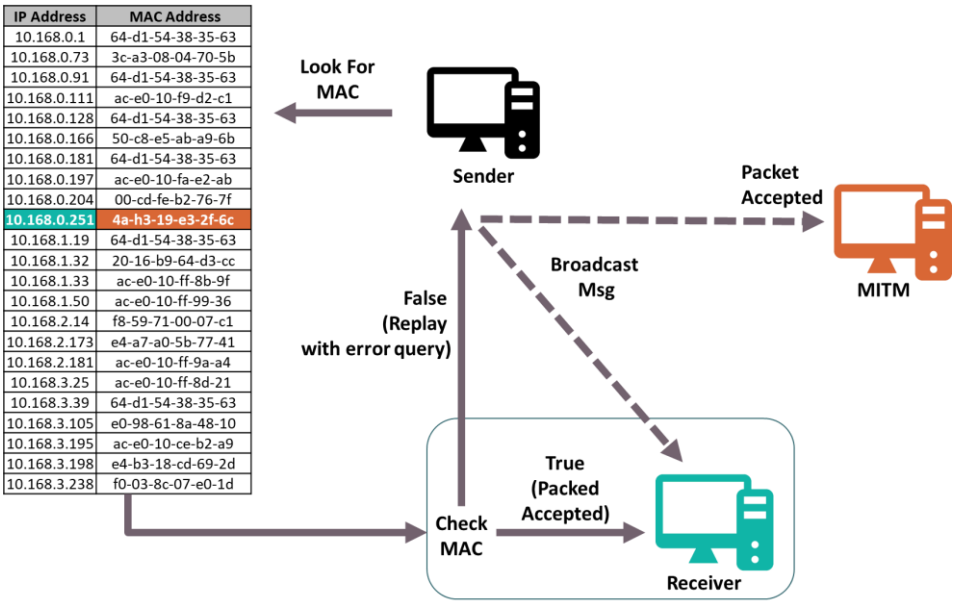

Fig 2. ARP Poisoning in Local Area Network

2.2 ARP Spoofing Detection, Prevention and Protection

The following methods are recommended measures for detecting, preventing and protecting against ARP spoofing attacks:

Packet filtering: Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in ARP spoofing prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).

Avoid trust relationships: Organizations should develop protocols that rely on trust relationships as little as possible. Trust relationships rely only on IP addresses for authentication, making it significantly easier for attackers to run ARP spoofing attacks when they are in place.

Use ARP spoofing detection software: There are many programs available that help organizations detect ARP spoofing attacks. These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.

Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster ARP spoofing attack prevention by encrypting data prior to transmission and authenticating data when it is received.

Static ARP entries: these can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets. The disadvantage of this method is, it's difficult to maintain on large networks. IP/MAC address mapping has to be distributed to all the computers on the network.

2.3 ARP Spoofing Attacks

The effects of ARP spoofing attacks can have serious implications for enterprises. In their most basic application, ARP spoofing attacks are used to steal sensitive information. Beyond this, ARP spoofing attacks are often used to facilitate other attacks such as:

Denial-of-service attacks: DoS attacks often leverage ARP spoofing to link multiple IP addresses with a single target's MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target's MAC address, overloading the target with traffic.

Man-in-the-middle attacks: MITM attacks can rely on ARP spoofing to intercept and modify traffic between victims.

3. Statement of Problem

ARP poisoning is a long standing problem which is known to be difficult to solve without compromising efficiency. The cause of this problem is the absence of authentication of the mapping between IP addresses and MAC addresses. Due to lack of the required authentication, any host on the LAN can forge an ARP reply containing malicious IP to MAC address mapping causing ARP cache poisoning. In fact, there are a number of tools freely available on the internet using which, anyone can launch such an attack.

4. Implementation

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.

4.1 Working

ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. It works in following manner:

- When one machine needs to communicate with another, it looks up its ARP table.
- If the MAC address is not found in the table, the ARP_request is broadcasted over the network.
- All machines on the network will compare this IP address to MAC address.
- If one of the machines in the network identifies this address, then it will respond to the ARP_request with its IP and MAC address.
- The requesting computer will store the address pair in its ARP table and communication will take place.

4.2 Attack Implementation

The attack is performed by a python3 script on a Local Area Network. We have used scapy module of python3 to do so.

4.2.1 Scapy

Scapy is a powerful interactive packet manipulation program. It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, match requests and replies, and much more. It can easily handle most classical tasks like scanning, tracerouting, probing, unit tests, attacks or network discovery. It also performs very well at a lot of other specific tasks that most other tools can't handle, like sending invalid frames, injecting your own 802.11 frames, combining technics.

4.3 Attack Detection and Prevention

4.3.1 Duplicate Entries

Arp Poisoning often results in duplicate entries. This entries are analysed by a JAVA based programme to detect attack via ARP Table.

4.3.2 Hop count

Increase in hop count from gateway can be a reason for ARP poisoning. We are using tracert command in windows to determine route and hop count. The tracert command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify.

4.3.3 Static ARP entries

These can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets. The disadvantage of this method is, it’s difficult to maintain on large networks. IP/MAC address mapping has to be distributed to all the computers on the network.

4.3.4 MAC Filtering

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

5. Results

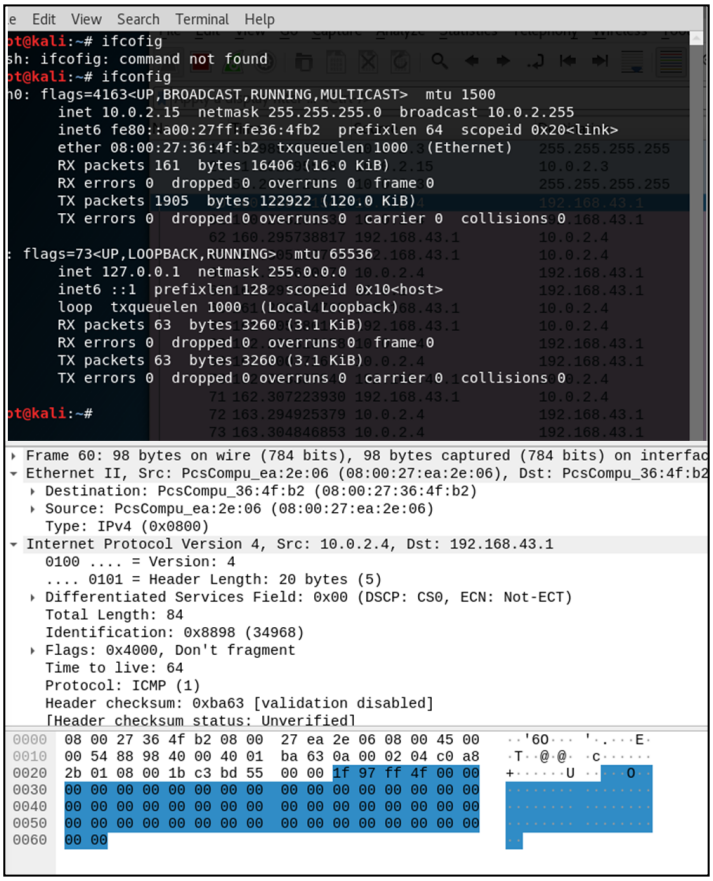

Fig 3. Change in addresses after attack

Fig 4. Sniffing HTTP Requests

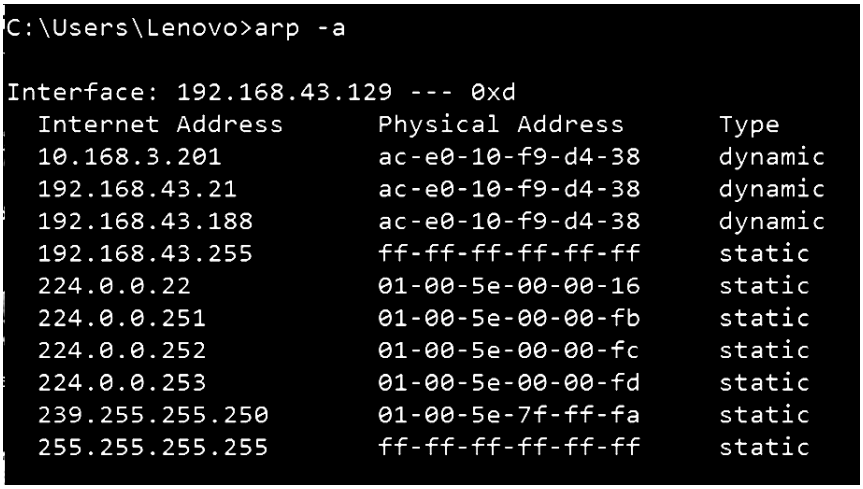

Fig 4. Duplicate entries in ARP table

6. Conclusion

We have successfully implemented the working tool for ARP poisoning attack and its required mitigation tools. Although today router are powerful enough to prevent ARP poison on their own it still is a dangerous attack done within the network. Hence resulting in requirements of respective counter measures. We have seen and implemented how sniffing works. We also have understood how easy it is to get the HTTP credentials just by enabling ARP poisoning. ARP Poisoning has the potential to cause huge losses in company environments. This is the place where ethical hackers are appointed to secure the networks. Like ARP poisoning, there are other attacks such as MAC flooding, MAC spoofing, DNS poisoning, ICMP poisoning, etc. that can cause significant loss to a network.

References

[1] Address Resolution Protocol Poisoning (ARP Poisoning), https://www.techopedia.com/definition/27471/address-resolution-protocol-poisoning-arp-poisoning, viewed on Nov, 2018

[2] ARP spoofing | Veracode, https://www.veracode.com/security/arp-spoofing, Viewed on Nov, 2018.

[3] ARP spoofing with scapy (NETLAB), https://samsclass.info/124/proj11/P13xN-arpspoof.html, viewed on Nov, 2018.

[4] Enable IP Forwarding on Ubuntu 13.04, http://www.networkinghowtos.com/howto/enable-ip-forwarding-on-ubuntu-13-04/, viewed on Nov 2018

[5] Learn How to Prevent ARP Spoofing the Best Way, https://www.purevpn.com/blog/prevent-arp-spoofing/, viewed on Nov 2018.

[6] Jeff King, Kevin Lauerman, ARP Poisoning Attack and Mitigation Techniques, A CSSTG SE Residency Program White Paper, Jan 22, 2016

[7] How to add static ARP entry in windows 2008 or Windows 7, http://www.gkhan.in/how-to-add-static-arp-entry-in-windows-2008-or-windows-7/, viewed on Nov 2018.