A Project Synopsis on

**ARP Poisoning and Mitigation**

**Techniques**

Submitted to Manipal University, Jaipur

Towards the partial fulfillment for the Award of the Degree of

**BACHELORS OF TECHNOLOGY**

In Computers and Communication Engineering

2018-2019

By

Shubham Sanjay Sonawane

159103067



Under the guidance of

Mr. Gaurav Prasad

**Department of Computer and Communication Engineering**

**School of Computing and Information Technology**

**Manipal University Jaipur**

**Jaipur, Rajasthan**

**Introduction**

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.

**Motivation**

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.

**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.

**Methodology**

1. Performing ARP packet sniffing and fake packet deployment using scapy. Scapy is a packet manipulation tool for computer networks. It can forge or decode packets, send them, capture them, and match requests and replies.
2. We will craft a packet to add a fake cached ARP entry on the target computer. This is how man-in-the-middle attacks work.
3. Once the malicious host is established between sender and receiver, try compromising the data integrity and even perform DOS attack on the server impersonating as a legit user.
4. Implement a model to prevent ARP poisoning using various techniques like packet filtering, encryption techniques, static ARP table, VPN etc.

**Facilities Required**

1. Kali Linux
2. VM Ware
3. Python 3
4. Scapy
5. Hping3
6. Wireshark
7. Ettercap

**References**

1. Jeff King, Kevin Lauerman, ARP Poisoning Attack and Mitigation Techniques, A CSSTG SE Residency Program White Paper, Jan 22, 2016
2. Goyal V., Tripathy R., An Efficient Solution to the ARP Cache Poisoning Problem. In: Boyd C., González Nieto J.M. (eds) Information Security and Privacy. ACISP 2005.
3. Address Resolution Protocol Poisoning (ARP Poisoning), https://www.techopedia.com/definition/27471/address-resolution-protocol-poisoning-arp-poisoning, viewed on Sep, 2018
4. ARP spoofing with scapy (NETLAB), https://samsclass.info/124/proj11/P13xN-arpspoof.html, viewed on Sep, 2018.
5. Learn How to Prevent ARP Spoofing the Best Way, https://www.purevpn.com/blog/prevent-arp-spoofing/, viewed on Sep 2018.