Detection and Prevention of ARP poisoning Attacks Based on Scripts

Neel Raval[1], Payal Chaudhary[2]

[1] *PG Student, Network Security, Gtu Pg School, Ahmedabad, Gujarat, India*
[2] *Assistant Professor, CE & IT, LDRP, Ahmedabad, Gujarat, India*

ABSTRACT

Address Resolution Protocol (ARP) been working under the network layer as per The Open Systems Interconnection model (OSI model). ARP is used to map Internet Protocol (IP) address or Media Access Control (MAC) address. Arp protocol is vulnerable so its weakness leads attacks like sniffing, man in the middle (MITM) attack by poisoning ARP cache\cite{c}. By detecting Arp cache poisoning we can minimize the attack. This paper present the different attack and prevention mechanism.

Keyword: - *Address Resolution Protocol, ARP poisoning, MITM;*

1. INTRODUCTION.

The Address Resolution Protocol (ARP) is used by Internet Protocol (IP), which bind the logical addresses with the hardware access or you can say IP address with the MAC addresses which is used in local area network (LAN). ARP works between the network and data link layer. Using this protocol we get idea or we figure out how many hosts are connected in our network. We also discover hosts MAC address and IP address in LAN environment. ARP have to packets, first one is ARP request and the other one is ARP reply. When anyone want to communicate in LAN network they require sender require receiver IP address so packets travels from source to destination.it is also possible to communicate with other host using there mac address. If any Alice and Bob wants to communicate with each other first Alice send ARP request to the Bob. ARP request generally used to request to get the mac address and same way ARP reply packet for respond corresponding to the request.

1.1 ARP Poisoning

ARP spoofing, ARP cache Poisoning, or ARP Poison is a technique where ARP reply packet sent to victim with senders IP address as target IP address and sender MAC address as attacker's MAC Address\cite{a}. Victim when process the ARP reply packet will add or change the ARP table entry for Target IP address with attacker's MAC address\cite{a}.

1.2 Snort

Snort is an Intrusion Detection System (IDS). We can use it as a Network Base IDS or else Host base IDS. it is open source and capable of real time packet analysis.

2. RELATED WORK.

In this chapter we discuss the literature review about our interested domain.

A Centralized Detection and Prevention Technique against ARP Poisoning. In this paper author maintain ARP table by providing algorithms as below,

1) Client Side Implementation
2) ACS Implementation
3) ACS Antidote Implementation

Detection of ARP Spoofing: A Command Line Execution Method. Here authors check the file if mac id mismatched then they find corresponding IP & thus they detect Arp spoofing

Stealth and Semi-Stealth MITM Attacks, Detection and Defense in IPv4 Networks. In this paper authors clarify MITM techniques. Techniques like Stealth and Semi-Stealth MITM.

1) Stealth MITM

Here, an attacker use sniffer to get copy of communication between Alice & Bob as shown in fig. 1.

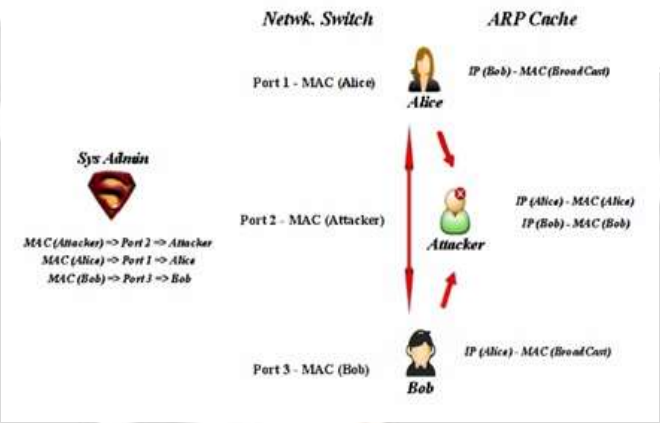

Fig. 1. Stealth MITM Attack

2) Semi Stealth MITM

Here Alice and bob communicate through the Attacker so one way interruption of message possible by the attacker as shown in fig. 2.

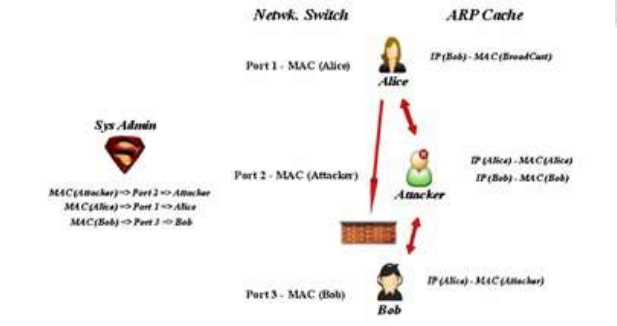

Fig. 2. Semi Stealth MITM Attack

Implementation of a SNORT's Output Plug-In in reaction to ARP Spoofing's attack. In this paper author monitor if the sender hardware address is not the same addressee in the configuration file then an alarm message is generated.

3. ASSUMPTION.

a. We're focusing on small topology.
b. Each machine node connected in LAN environment.

4. ARP POISONING ATTACKS BASED ON SCRIPT.

According to survey, attacks done by the attacker so for that various analysis have been done to perform attacks in different ways.

A. MITM for Credential Sniffing

Consider a Scenario Where Victim node is trying to log in with his credential and Attacker node performing MITM by ARP Poisoning.

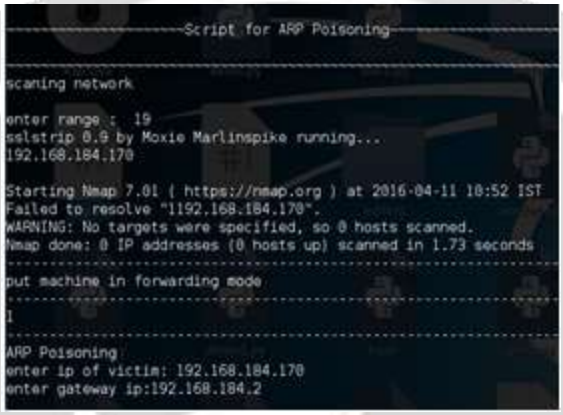

Fig.3. MITM Attack Credential Sniffing

1) Run ./arp.sh
2) Enter IP for Scanning
3) Enter Victim IP to Perform Attack

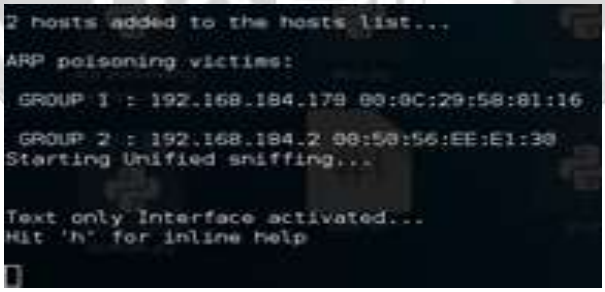

Fig.4. Victim Added

Fig.5. Sniffed Credential of Victim

B. MITM for URL Sniffing

After execution of arp.sh now we have to execute url.py for URL sniffing.

Fig.6. URL sniffing Script.

Fig.7. Sniffed URL

C. DOS Attack

We have to execute dos1.py to perform DOS Attack

Fig.8. DOS Attack

As shown in Fig.8 ARP reply packets continuously travels to the victim node. At the end victim is not able to access service this is consider as a DOS attack.

5. PROPOSED WORK.

In our work we created one sensor machine node. And for traffic monitoring purpose or to detect malicious activity we configure snort. When any malicious activity regarding to ARP Poisoning take place it will generate alert.

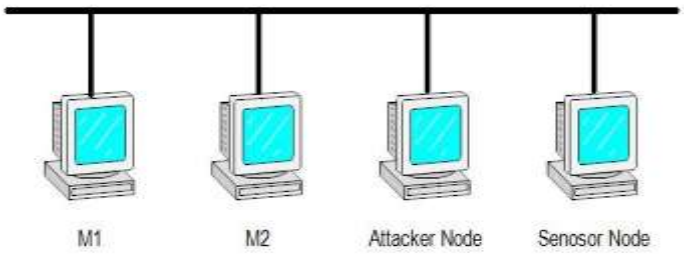

Fig.9. Topology of Network

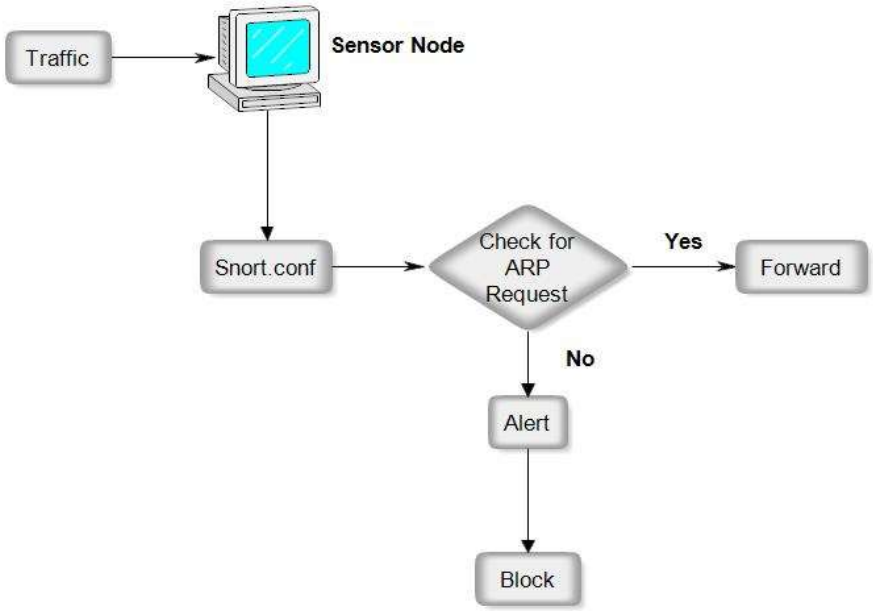

Fig.10. Proposed Architecture

A. Algorithm and Flow Diagram

a. Input: ARP Packets.

b. Output: Identifying Attacker Hosts.

1. Monitor Traffic.
2. Take ARP packets.
3. If (ARP type= known)
   Forward
   EndIf
   Loop
4. Take Next ARP packet
5. If (Next ARP type= Unknown)
   Raise Alarm
   If (Alert Message = Misc Activity)
   Get IP of Attacker and Victim
   Block Attacker

EndIf

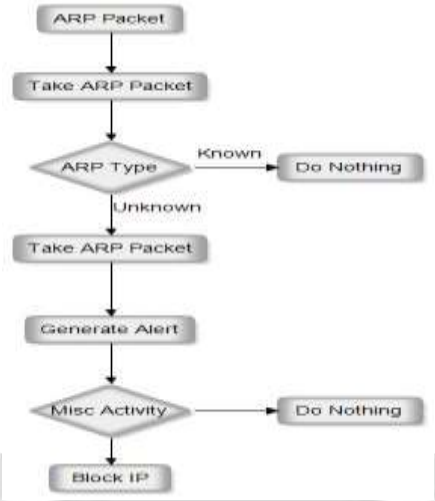

Fig.11. Flow Chart

B. Installation and Configuration of snort

1. To install snort in sensor node, root@kali:~#Sudo aptitude install snort
2. After that it will ask for ip Range provide ip range like 192.168.0.0/24.
3. Now we have to configure snort.conf file to monitor traffic.now we have to open file for edit, root@kali:~#nano /etc/snort/snort.conf
4. After that we have to look for " ipvar HOME_NET any " here in place of any we have to put range " 192.168.0.0/24 "
5. To detect arp attack we have to insert ip address and mac address in snort.conf file for that, Preprocessor arpspoof_detect_host: IP MAC
6. Save snort.conf now.
7. Open Terminal and follow command to start snort root@kali:~#/etc/init.d/snort start
8. Now give following command snort -A console -q -i eth0 -c /etc/snort/snort.conf

If any malicious activity is going on then it will generate alarm.

6. PREVENTION MECHANISM AND FUTURE WORK.

When sensor node detected IP after that by executing arp_block.py we are able to stop MITM Attack. You can block attack two ways first one is based on host by executing this file and another one is network base.
As shown in Fig.12 after execution of this script you have to enter ip of attacker.

Fig.12. Attack Prevention by Host

As shown in Fig.13 here we executed script for blocking attacker through sensor node. We have to enter attacker ip and victim ip which we observed by the alerting message using Snort IDS.

Fig.13. Attack Prevention by Sensor Node

As Show in Fig.14 this is the out put screen short of attacker node. it's shows that attacker is trying to attack by script ./arp.sh but here victim machine blocked the attacker or else when attack is being in progress sensor node can also block the attacker so victim node is not added here so now victim is safe from being attacked by the attacker.

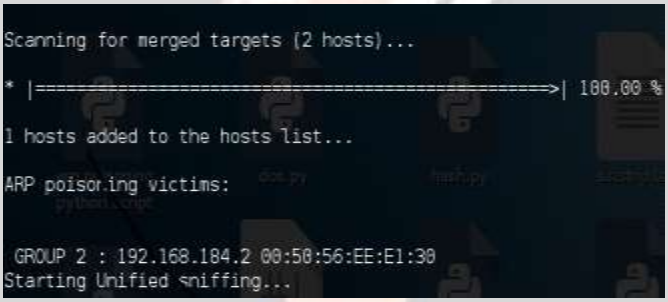

Fig.14. Attack Prevention

7. CONCLUSION.

ARP is used to get provided MAC address of the IP address. ARP cache position done by the attacker to perform MITM attack so to secure the network and network host from the attack, Snort IDS helps us to detect the malicious activity in the network. We can Implement snort mechanism for ARP to secure network.

8. REFERENCES

1. Kumar, Sumit, and Shashikala Tapaswi. "A centralized detection and prevention technique against ARP poisoning", Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on. IEEE, 2012.
2. Sharma, Divya, Oves Khan, and Nidhi Manchanda. "Detection of ARP Spoofing: A command line execution method." , 2014 International Conference on Computing for Sustainable Global Development (INDIACom) 2014.
3. Samineni, Naga Rohit, Ferdous A. Barbhuiya, and Sukumar Nandi" Stealth and semi-stealth MITM attacks, detection and defense in IPv4 networks", Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on. IEEE, 2012.
4. Boughrara, Asmaa, and Said Mammar. "Implementation of a SNORT's output Plug-In in reaction to ARP Spoofing's attack" , Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on. IEEE, 2012.

5. Goldendeep Kaur, Dr. Jyoteesh Malhotra. "ARP Spoofing Detection Algorithm: An Effective Approach." , International Association of Scientific Innovation and Research (IASIR), USA
6. Nath Nayak and S. Ghosh Samaddar. Different flavours of manin- themiddle attack, consequences and feasible solutions,Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, vol. 5. IEEE, 2010.
7. Z. Trabelsi and K. Shuaib. "Man in the middle intrusion detection. In Globeco m.", IEEE, 2006
8. Snort implementation: https://snort.org/