DETECTION AND PREVENTION OF ARP SPOOFING

Divya Samragni Nadakuditi
Dept. of Computer science
University of Bridgeport

ABSTRACT

In the initial stages of Internet existence, PC systems were utilized by college analysts for sending email and by corporate workers for sharing printers. With the advancement of society, organize innovation is additionally continually creating, and organize applications are progressively promoted. To an ever-increasing extent where clients can get to a ton of data assets of worldwide system framework at home. Web has become an essential piece of the present world. Be that as it may, arrange security additionally goes to our sight. There are huge amounts of conventions were utilized to set up these systems. During those stages no precautionary measures were considered, but now with the rapid growth of internet over years, it is time to take some measures to protect the attacks that are happening. In this paper, we do some examination and recreation about the Address Resolution Protocol (ARP) and ARP spoofing to show a few precautionary measures in ARP.

Keywords: ARP spoofing, Routing, MAC Address, Encryption, Prevention, LAN, Ettercap, IDS, Wireshark.

1. INTRODUCTION

With the improvement of the networks, a lot of administrations and applications have expanded the need of LAN. In the interim, the security of LANs likewise needs significantly more thought. Address Resolution Protocol (ARP), which is a much of the time utilized system layer convention that maps the IP address to the MAC address, is very defenseless. It expands the danger of assaults in LANs. ARP spoofing is one of the hacking methods to risk the LANs. When all is said in done, ARP spoofing is the intentional conduct of giving off base ARP communication packet. This method was initially utilized by programmers and turned into the primary technique for programmers to take information illegally. The programmer conveys an inappropriate ARP communication packet, hinders the ordinary correspondence, masks the PC that he uses to be the PC of others, so the information initially sent to different PCs is sent to the programmer's PC, to take the information. In the recent years it was noticed that ARP attacks have become more severe in terms of methods and strategies when compared to the earlier two phases. In the previous phases attack was performed using virus on WAN and DDOS attack. But because of the prevention techniques that became popular, hackers have shifted their goal to LAN. In this paper we focus on ARP spoofing and will perform simulation on ARP spoofing along with the security measures that can be taken to avoid this type of attack.

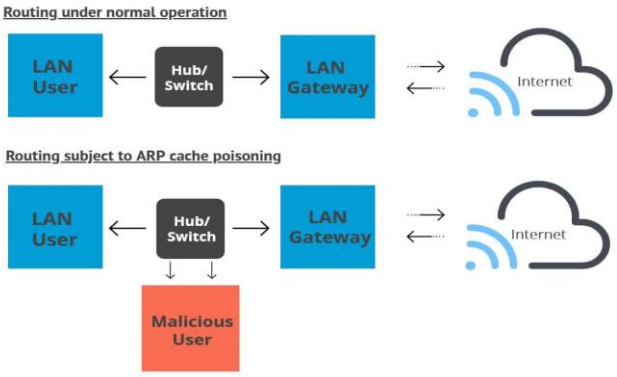

Figure1. ARP spoofing routing v/s normal routing

2. LITERATURE SURVEY

The ARP Spoofing attack depends on imitating a framework in the system, making the two parts of the communicating correspondence accept that the opposite end is the assailant's framework, capturing the traffic traded [1]. Already various techniques have been proposed to move information safely over the web. Be that as it may, none of them has given a specific answer to face the ARP spoofing [3]. Tapping into the correspondence between two has on a LAN has become very straightforward because of certain tools that can be downloaded from the Web. Such applications or tools utilize the Address Resolution

Protocol (ARP) harming strategy, which depends on has reserving answer messages despite the fact that the comparing demands were never sent. Since no message validations gave, any host of the LAN can manufacture a message containing vindictive information.[4]. S-ARP model is encryption-based security model in which each host has claim open/private key it will send it to the Authoritative Key Distribution (AKD)through which the encryption and unscrambling of information happens. One of the significant entanglements is that each time it encodes the message henceforth it requires some investment for each transmission [2].

Al zeng Qian[5] proposed a strategy to forestall ARP ridiculing by utilizing static ARP sections however the system doesn't work with dynamic systems utilizing DHCP tending to. The manager must appoint all IP addresses alongside their MAC to the server so it will be not obvious for huge scale arrangement. A strategy is recommended in [6] to tackle spoofing issue utilizing snort IDS and static ARP sections. However, it still needs the admin user to include the static mappings physically and it works only in static systems.

3. PROBLEM STATEMENT

As discussed earlier, we can see that effects and preventive measures taken so far for controlling ARP spoofing. Here, we have simulated the ARP Spoofing and tried to use Defensive tools for ARP spoofing. In previous research papers we have noticed how Encryption techniques were used for controlling ARP spoofing which had their own limitations. So, we decided to use defensive tools for prevention of ARP spoofing attacks.

4. TOOLS USED FOR SIMULATION

4.1 Wireshark

Wireshark is an open source packet filter tool. It is utilized to analyze the system traffic. It additionally bolsters several conventions and media types. Wireshark checks all the traffic obvious on that interface. Wireshark comprehends the design of various systems administration protocols. It catches all packets that are sent and got on the system. At the point when any action occur on the Internet, for example, perusing sites, use VoIP, IRC and so forth, it goes through your system interface card (NIC) or your LAN card in which the information is constantly changed over into packets.

4.2 Ettercap

Ettercap is an effective tool for man in the middle assaults on LAN. It is answerable for sniffing live associations, content separating and numerous other intriguing stunts. It underpins dynamic and aloof division of numerous conventions (even figured ones) and incorporates numerous highlights for system and host investigation. It has a graphical interface which is anything but difficult to work. Ettercap is competent to perform assaults against the ARP convention. Ettercap can contaminate, replace and erase information in an association. It catches passwords for conventions, for example, FTP, HTTP, POP, SSH1 and some more. It goes about as Swiss armed force blade for ARP harming and organize sniffing. Ettercap have channels and modules which capable it to do a wide range of system undertakings. It has the ability to route the traffic and apply filters for modifying the data.

5. ARP SPOOFING PREVENTIVE TOOLS

XArp: XArp is a security application that uses advanced practices to detect ARP based attacks. In ARP attacks attacker silently eavesdrops all your data that is sent over the network. This includes documents, emails and VoiceIP conversations. ARP poisoning attacks are concealed by firewalls and OS security features. Firewalls don't protect against ARP based attack. XArp is built to target this problem it uses advanced techniques to detect ARP attacks and thus helps you to keep your data private[9].

6.IMPLEMENTATION

ARP poisoning is the most perilous assault on LANs, ARP protocol is a stateless convention. In this area, we have actualized Ettercap tool and Wireshark for sniffing the system traffic and performing MITM assault in kali Linux working environment. These tools are utilized for ARP poisoning and MITM attack[7].

We first launch the Linux virtual machine with Ettercap and wireshark installed. Then we check the configuration of the linux machine. We use the command ifconfig.

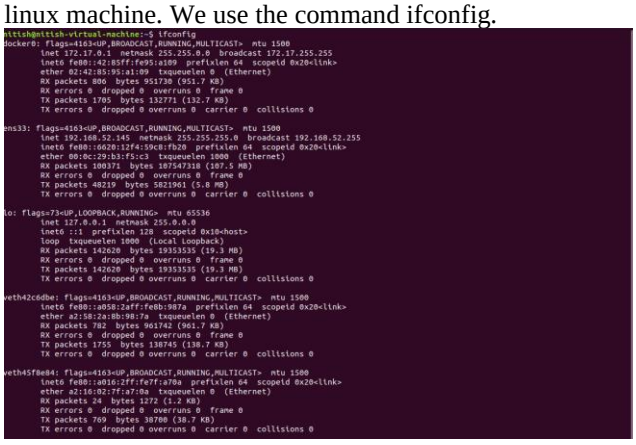

Figure1. Checking the Configuration of System

Now we launch the ettercap Graphical using the command “ettercap -G”. This command launches the ettercap.

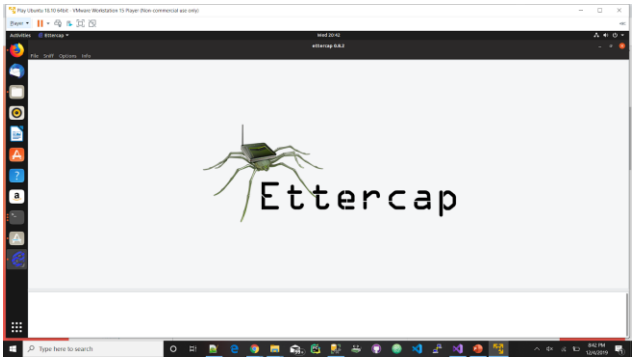

Figure 2.Launching Ettercap tool

Now Click on Sniff and select unified sniffing. It will then ask for ethernet connection which you select from the dropdown and click on OK.

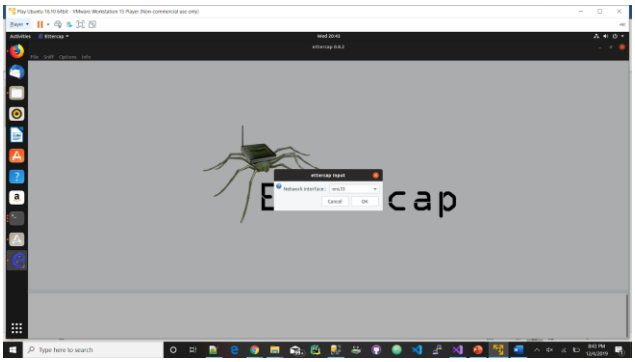

Figure 3.Configuring Ethernet Connection

Now select the Host tab in menu bar and Scan the host. It will scan the whole network and get the hosts that are available[8]

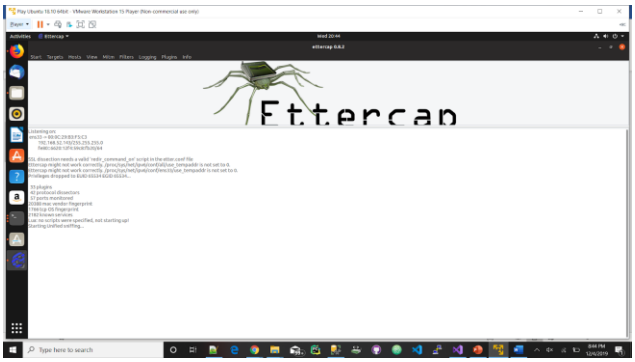

Figure 4.Scanning the Hosts

Now Click on the Host tab and select Host list. This will show you the number of hosts that are available in the network.

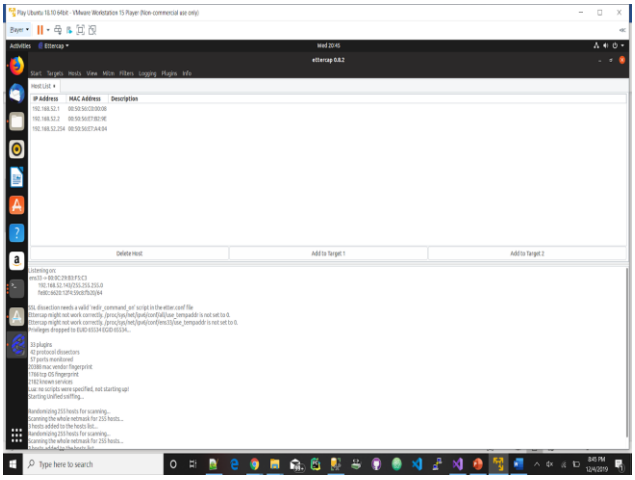

Figure 5. Available Hosts in the Network

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

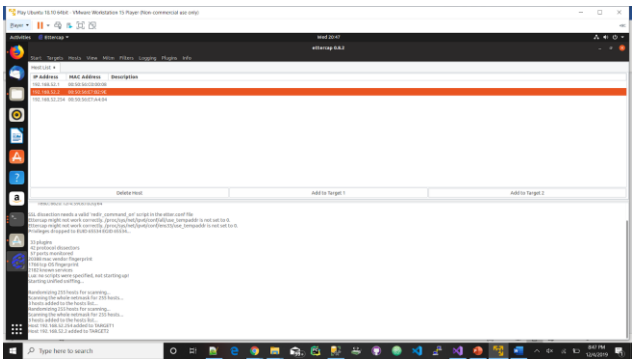

Figure 6. Selecting the Victim Network

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

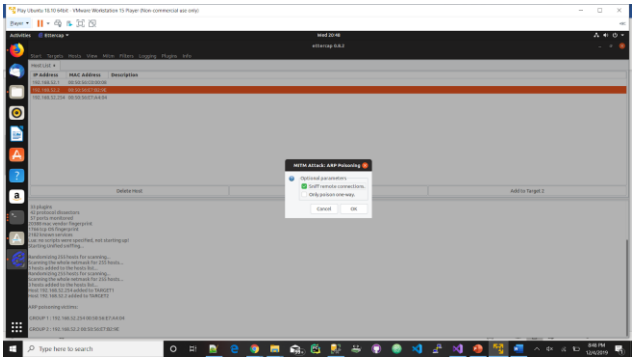

Figure 7. Sniffing Remote Connections using EtterCap

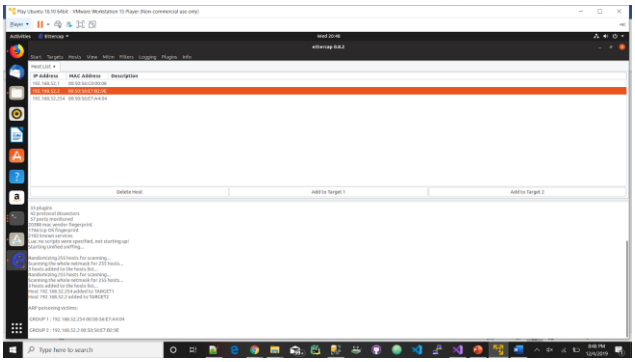

Figure 8. Sniffed Host and Target Network

Now launch wireshark and select the lan connection from the list of connections. It will display the packets that go through the network. Before doing that we select the connection in the capture interface. Then the packets transferring in the network in between the connections is shown. We filter it based on the IP of victim. here we can see the packets being transferred and can see what the victim does. Now if the victim enter something to the page and we can see what details that he entered.

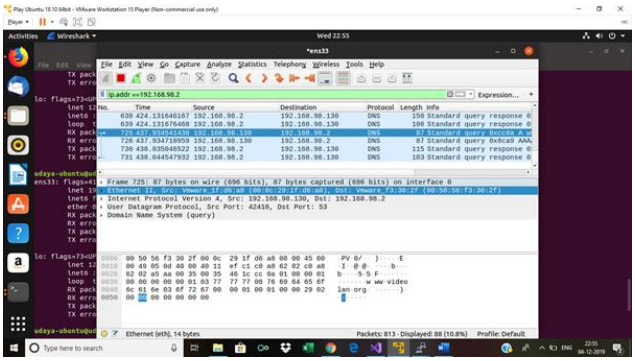

Figure 9.Filtering the Packets using Victim IP Address in Wireshark

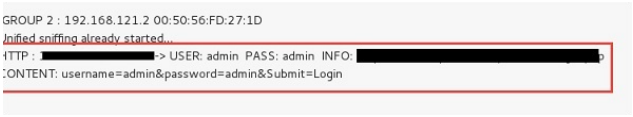

Figure 10.Packets Captured using WireShark.

8.CONCLUSION

As a part of this project, we have performed a simulation of ARP Spoofing using a linux machine with ettercap, wireshark. We have used MITM ARP Spoofing in Ettercap for the implementation.We implied tools like ettercap and wireshark for sniffing the traffic and give defensive countermeasures for securing our system from being poisoned. ARP spoofing and attack problems are the culprits of enterprise networks. The discussion on this issue has been very thorough. After our simulation, the mechanism of ARP attacks has been thoroughly understood and various preventive precautions have been introduced. But the question is that is it really bothering you to get rid of ARP problems now. As we known, although various methods have been tried, this problem has not been fundamentally solved. There are three reasons that we conclude. First, the preventive ability of the solution measures is limited, and it is not the most fundamental method. The second is that the network management is very constrained, inconvenient and impractical, and has no operability. Third, some measures have a loss in the efficiency of network transmission, slower network speed, and wasteful bandwidth which is also undesirable.

9.REFERENCES

[1] Pandey,P. “Prevention of ARP spoofing: A probe packet based technique”, IEEE Conference on Advance Computing, pp.147-153, 2013

[2] Bruschi,D., Ornaghi,A. and E. Rosti, “S-arp: a secure address resolution protocol,” IEEE Conference on Computer Security Applications Conference, pp. 66 – 74, 2003.

[3] AmitKumar,T., SurendraKumar and PrafullKumar Singh, “ A Novel Approach to Detect and Defense against Address Resolution Protocol(ARP) Spoofing Attack”, International Conference on Advance Development in Engineering and Technology, 2014

[4] Nam,S., Kim,D. and Kim,J. “Enhanced Arp: preventing arp poisoning based man-in-the-middle attacks,” IEEE Communications Letters, Vol. 14, No. 2, pp. 187–189, 2010.

[5] Ai-zeng Qian., "The Automatic Prevention and Control Research of ARP Deception and Implementation," WRI World Congress on

Computer Science and Information Engineering, No. 2(1), pp. 555-558, 2009.

[6] Boughrara, A. and Mammar, S., "Implementation of a SNORT's output Plug-In in reaction to ARP Spoofing's attack," International Conference on Sciences of Electronics Technologies of Information and Telecommunications , pp.643,647, 2012.

[7] Satya P Kumar Somayajula, Yella. Mahendra Reddy,HemanthKuppili and Tamaram, Visakhapatnam, "A New Scheme to Check ARP SpoofingPrevention of MAN-IN-THE-MIDDLE Attack" International Journal of Computer Science and Information Technologies, Vol. 2 no.4 , 2011.

[8] https://www.researchgate.net/deref/http%3A%2F%2Fwww.arppoisoning.com%2Fhow-does-arp-poisoning-work%2F.

[9] http://www.arpalert.org