IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Detecting and Preventing Cyber Attacks on Local Area Networks : A Working Example

Sezer YILDIZ[1], Umut ALTINIŞIK[2*]

[1]University of Beykoz, Turkey
[2]Department of Informatics, University of Kocaeli, Turkey

[*]*Corresponding Author: umuta@kocaeli.edu.tr, Tel.: +90-2623031302*

Available online at: www.ijcseonline.org

Accepted:16/Nov/2018, Published: 30/Nov/2018

Abstract— To ensure secure communication on the network, the principles of confidentiality, integrity and accessibility must be carried out in unity. To prevent external attacks on the network, many threats are eliminated by using firewalls between the external network and the internal network. However, different security scenarios need to be implemented against threats that may come from within the local area networks. For this reason, the factors that may cause security vulnerabilities in the internal network should be checked and the security should be considered. One of the most important problems encountered here is the unnecessary network traffic that occurs in internal networks, slowing the system and making it inoperable. In this article, using the GNS3 (Graphical Network Simulator) network simulation program, MAC (Media Access Control) flood, DHCP (Dynamic Host Configuration Protocol) starvation and spoofing and Arp (Address Resolution Protocol) poisoning attacks are detected and a working example has been carried out to prevent it.

Keywords— GNS3, Network Security, MAC flood, DHCP attacks, ARP poisoning

I. INTRODUCTION

To find out which categories of cyber-attacks are classified, it is necessary to find out which of the three main features of the information security are threatened. These are confidentiality, integrity, availability.

Confidentiality attacks are the attacks that users follow to learn the transactions they perform [1-2]. Integrity attacks are attacks that aim to change rather than obtain information. Confidentiality and integrity attacks can use the same method to enter the network, but their behavior on the network is different. The targets of all attack types are to leave the system out of service, or to change or retrieve the data in the system [1,3]. Availability attacks are services that enable services to become out-of-service or become vulnerable to damage from their connected systems, and to break off communication with the network [4].

Because of the attack on the secure network connections at the MITM attack, it was given to the rogue machine and it was redirected to the correct address by the applied algorithm [5]. The result of ARP poisoning in the LAN environment, the problem of MITM was eliminated by Nayak and Samaddar [6].

Ansari and Waheed presented a novel flooding attack detection and prevention method in 2017. In this method, cross layer MAC interface was added into the routing table. When an attack occurs on a node, it is marked as flooding node and is painted as blacklist [7].

Dynamic Host Configuration Protocol (DHCP) starvation attack was blocked by DHCP Server as described on the study of Tripathi and Hubballi in 2015 [8].

Aggarwal proposed a solution method to solve ARP Poisoning problems based on ARP central server (ACS) [9]. Also, Kumar and Tapaswi presented a feasible solution to the ARP cache poisoning by using ACS. They verified and corrects the poisoned ARP cache in the network [10]. Khurana and Kaur performed a MITM attack and proposed security approach to avoid ARP poisoning in 2015 [11].

In this paper, the most common LAN attacks are carried out and prevention scenario results evaluated. The rest of the paper is arranged as follows. LAN Attack types are presented in section 2. The experimental results of these attack types are analyzed in section 3. In the last section, the results of the article are included.

II. METHODOLOGY

This section presents LAN attacks which are MAC flood, DHCP spoofing and ARP poisoning implemented in the paper.

A. *Mac Flood Attacks*

Nowadays, malicious people are changing their MAC addresses or IP (Internet Protocol) addresses to hide themselves. The ports of the attacked switch keep many MAC address information in the CAM (Content Addressable Memory) table. In the MAC flood attack, the CAM table is filled with fake MAC addresses and the switch works like a hub. In Figure 1 shows learning MAC address process of Switch 1,2 and 3.

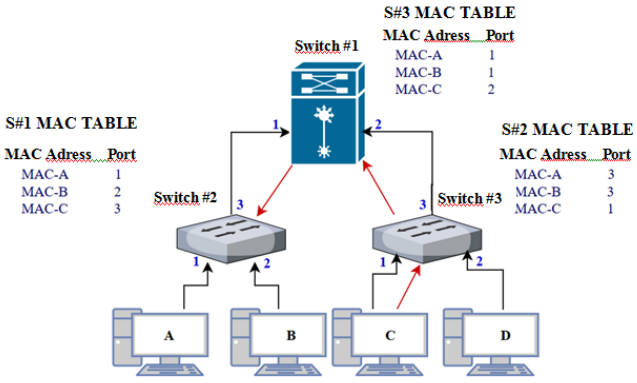

Figure 1: MAC flood attack process

B. *DHCP Attacks*

In the DHCP starvation attack, huge number of DHCP requests are broadcasted with the fake source MAC addresses generated by the attacker. The DHCP Server on the network responds to all these fake DHCP request messages and the IP Addresses in the server pool run out in a very short time. When the IP addresses on the server are exhausted, a fake server is installed by network attackers. Once the dummy server is set up, it can distribute IP addresses and TCP / IP configuration settings to DHCP clients on the network. This replaces the default gateway IP address with its own IP address. Then, traffic data are sent by network clients to the attacker's computer. Thus, important data is obtained by the attacker and the man in the middle attack (MITM) is performed. This is called the DHCP spoofing attack. An attacker can also set up a fake DNS server, leading to phishing attacks by redirecting client traffic to fake websites [5-6,12-13].

Figure 2 illustrates the response of fake DHCP response to the victim computer A by the rogue computer A.

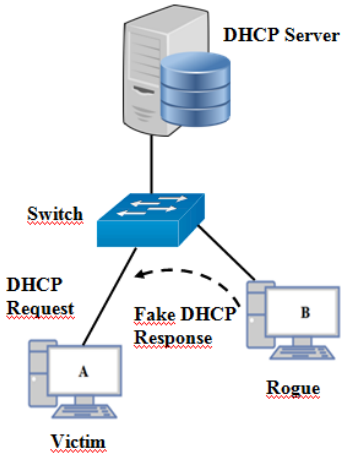

Figure 2: DHCP attack process

C. *Arp Poisoning Attacks*

A type of LAN attack is performed by placing fake ARP request and reply packets on the target computer's ARP cache by replacing MAC addresses on the network by an attacker. In this attack, the MAC address is changed by the attacker. Thus, the target computer is sent to the attacker's computer instead of sending the data to the original destination. As a result, both the user's data and the privacy are compromised. An effective ARP poisoning attempt cannot be detected for the user. Figure 3 illustrates the ARP poisoning attack to the victim computer A by the rogue computer A.

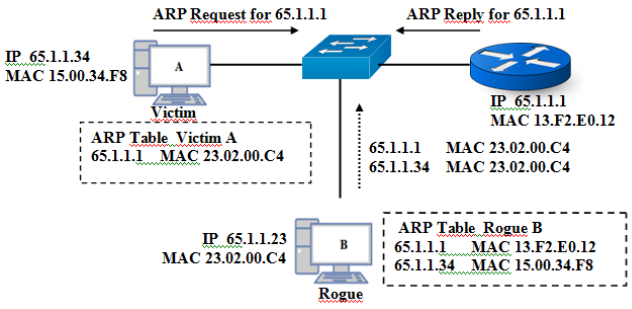

Figure 3: ARP poisoning attack process

III. EXPERIMENTAL STUDY

In the experimental studies, Mac Flood, DHCP Starvation and Spoofing and Arp Poisoning attack are implemented by GNS3 network simulation program. The GNS3 is an open source simulation program used in cyber security and networking applications. A real network with GNS3 can be run on the Cisco operating system IOS [14]. The GNS3 network design allows you to design and test without the use of physical network devices. Network design and desired measurements can be made with minimum cost with GNS3.

In the study, a sample network scenario for cyber-attacks were implemented by integrating VMware and Kali Linux with GNS3. In the study, MAC flooding, DHCP starvation and ARP spoofing attacks were applied at the network and the results were analyzed.

A. Mac Flood Attacks Implementing

The network topology designed to detect the MAC flood attack is presented in Figure 4.

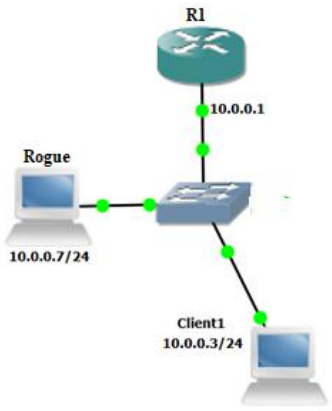

Figure 4. Network topology

Network traffic before the MAC flood attack is performed is shown in Figure 4 by using the Wireshark program. As shown in Figure 5, there don't send any packets to the rogue computer.

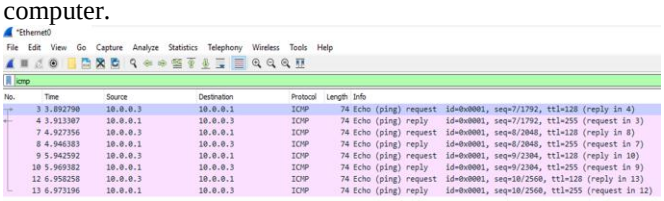

Figure 5. Network traffic before the attack

The MAC addresses of the computers are registered in the ports of the switch before the attack. It is concluded that there are registered MAC addresses and communication is unicast. The screenshots before and after the attack are shown in Figures 6 and 7 respectively.

```
----------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000c.2958.8b9c    DYNAMIC     Gi0/0
   1    000c.29f7.c34c    DYNAMIC     Gi0/1
   1    0050.56c0.0003    DYNAMIC     Gi0/1
   1    0050.56c0.0004    DYNAMIC     Gi0/0
   1    ca01.3114.0008    DYNAMIC     Gi0/3
Total Mac Addresses for this criterion: 5
```

Figure 6: MAC table of the switch before the attack

```
   1    fa83.1f0c.d76a    DYNAMIC     Gi0/3
   1    fb02.ff4d.7877    DYNAMIC     Gi0/3
   1    fb2c.6b5c.4547    DYNAMIC     Gi0/3
   1    fdfe.2658.1aa8    DYNAMIC     Gi0/3
   1    febb.ab31.f84b    DYNAMIC     Gi0/3
   1    fee7.3866.6921    DYNAMIC     Gi0/3
Total Mac Addresses for this criterion: 292
```

Figure 7: MAC table of the switch after the attack

As seen in Figure 6, CAM table of a switch is flooded after the attack. Client2 host added to the network topology for testing MAC flood attacks as shown in Figure 8.

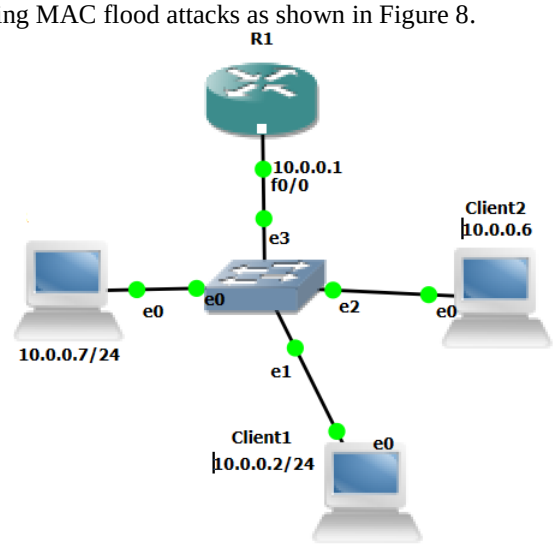

Figure 8: Network topology after adding client2

The ping packet is sent from the Client2 computer on the network topology in Figure 1 to the Client1 computer. The Figure 9 shows that the Kali machine has received this sent package. Although the sent ICMP package has nothing to do with it, it has been determined that it has received this package and it is not possible to make single point communication. Thus, it has been seen that the switch starts to work like a hub.

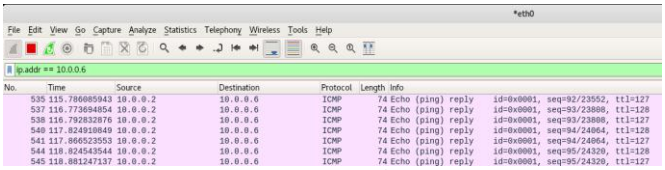

Figure 9: Ping result of the router

To prevent unauthorized or malicious users from being included in the network, traffic is not increased unnecessarily, and MAC is not changed continuously, MAC flood is prevented by ensuring the security of the ports to which the computers are connected. To include only certain machines on the network in the network, the MAC address must be registered to the corresponding port. Sticky command or static MAC address is entered to perform the registration. This allows recording of the number of MAC addresses to the corresponding port. Protect, Restrict and Shutdown

commands are used in cases of attack. The usage of these commands is shown in Figure 10.

```
SW1>enable
SW1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#interface fa0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security maximum 1
SW1(config-if)#switchport port-security mac-address sticky
SW1(config-if)#exit
SW1(config)#

SW1>enable
SW1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#interface fa0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security maximum 3
SW1(config-if)#switchport port-security violation restrict
SW1(config-if)#exit
SW1(config)#
```

Figure 10: Port security command

B. DHCP Attacks Implementing

A lab environment was prepared by using the GNS3 simulator program for attacks on the DHCP service. In figure 11, R1 is authorized DHCP server. In the case study, cyber-attack was started on the Kali Linux machine. The fact that the port security feature was active could not prevent the attack. The purpose of the attack is to ensure that the authorized DHCP server is out of service. The ability to remain out of service depends on the completion of the IP pool of the authorized DHCP server.

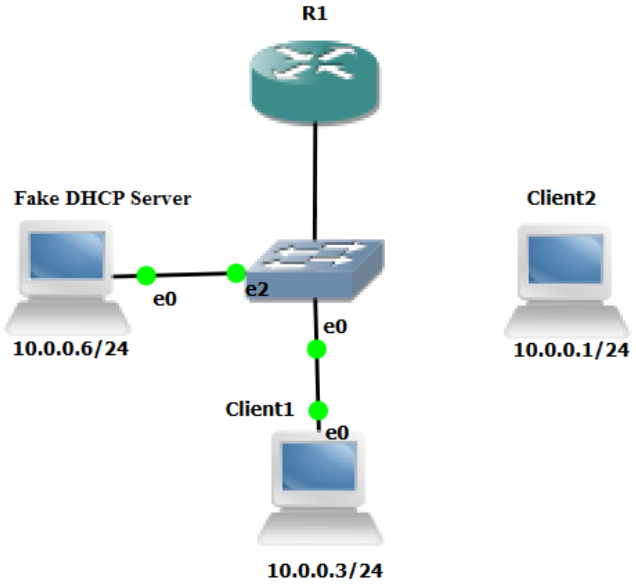

Figure 11: Network topology for fake DHCP server

After successfully completing this attack, a rogue can set up a fake DHCP server so that clients can make the gateway information for the IP address of this Fake DHCP server and make the man in the middle attack on a larger scale. Figure 12 shows the statistical data of the DHCP Packages before the DHCP starvation attack was performed.

```
R1#show ip dhcp server statistic
Memory usage          48824
Address pools         1
Database agents       0
Automatic bindings    3
Manual bindings       0
Expired bindings      0
Malformed messages    0
Secure arp entries    0

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          4
DHCPREQUEST           5
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             3
DHCPACK               3
DHCPNAK               0
R1#
```

Figure 12: DHCP server statistic before the attack

The statistics of the DHCP server because of the attack by a rogue DHCP server are shown in Figure 13.

```
R1#show ip dhcp server statistic
Memory usage          29201244
Address pools         1
Database agents       0
Automatic bindings    3449
Manual bindings       0
Expired bindings      0
Malformed messages    0
Secure arp entries    0

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          3451
DHCPREQUEST           10
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             3449
DHCPACK               8
DHCPNAK               0
R1#
```

Figure 13: DHCP server statistic after the attack

It is seen that the shutdown of the attacked port is prevented from making the DHCP starvation attack from the same port again. Since the DHCP server does not have an IP in the IP pool, it is seen that the client2, which is going to be

connected in Figure 11, cannot receive service from this network. The DHCP snooping limit rate second command is used for other ports where the authorized DHCP server is not connected. Thus, Client2 can get an IP from DHCP but it does not block the attack.

C. Arp poisoning

When Arp attack is performed, all movements of the victim computer can be monitored by the rogue computer. The ARP table of the victim computer before the Arp poisoning attack is shown in Figure 14. In Figure 15, the ARP table after the rogue attack is performed is shown.

```
C:\Users\IEUser>arp -a

Interface: 10.0.0.2 --- 0x5
  Internet Address      Physical Address      Type
  10.0.0.1              ca-01-06-b7-00-00     dynamic
  10.0.0.3              00-0c-29-58-8b-9c     dynamic
  10.0.0.4              00-50-79-66-68-00     dynamic
  10.255.255.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 14: ARP table before the ARP poisoning

```
C:\Users\IEUser>arp -a

Interface: 10.0.0.2 --- 0x5
  Internet Address      Physical Address      Type
  10.0.0.1              00-0c-29-58-8b-9c     dynamic
  10.0.0.3              00-0c-29-58-8b-9c     dynamic
  10.0.0.4              00-50-79-66-68-00     dynamic
  10.255.255.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 15: ARP table after the ARP poisoning

To avoid this situation, the DHCP snooping feature must be turned on. Thus, it is possible to know which IP is used on the port. Providing a gateway security by using ARP inspection

IV. CONCLUSION AND FUTURE SCOPE

In the article, methods used in LAN network are performed. Port security, DHCP security, and ARP control methods have been tested to prevent local network traffic from being disabled. It has been observed that these methods respond to the need and the method of port security does not respond to DHCP attacks on its own. It is concluded that the port security feature for DHCP starvation attack does not prevent the attack from being performed. Using the port security, the port where the attack occurred was closed so that no DHCP starvation attack could be made from the same port. Therefore, all the protection methods must be applied from Layer-2 attacks.

It is seen that the differences in the communication status of two different networks established for the MAC flood attack are since the MAC address information continues to be kept in the CAM table if there is data flow in the corresponding port.

Because of the security vulnerabilities experienced in the local area networks, the bandwidth of these networks expires due to heavy traffic and this negatively affects the processor performance of the network devices. Therefore, it has been determined that the nerve lines that provide the flow of local network traffic are disabled.

In future studies, network applications need to be secured with an information security program as the applications used on the network to bring too much load to the network because of the lack of awareness of the end users and the design of the network design is complex.

REFERENCES

[1] Singer, P. W., Friedman, A, Cybersecurity: What everyone needs to know. Oxford University Press. pp.102-104, 2014.

[2] Bella, G., Bistarelli, S. , "Soft constraints for security protocol analysis: Confidentiality. In International Symposium on Practical Aspects of Declarative Languages". Springer, Berlin, Heidelberg,pp. 108-122, 2001.

[3] Heberlein, L. T., Dias, G. V., Levitt, K. N., Mukherjee, B., Wood, J., Wolber, D, "A network security monitor. In Research in Security and Privacy", Proceedings., IEEE Computer Society Symposium on, pp. 296-304,1990.

[4] Wullems, C., Tham, K., Smith, J., Looi, M., "A trivial denial of service attack on IEEE 802.11 direct sequence spread spectrum wireless LANs", In Wireless Telecommunications Symposium, pp. 129-136, 2004.

[5] Chordiya, A. R., Majumder, S., Javaid, A. Y., "Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools.", In 2018 IEEE International Conference on Electro/Information Technology (EIT), pp. 438-443, 2018.

[6] Nayak, G. N., Samaddar, S. G., "Different flavours of man-in-the-middle attack, consequences and feasible solutions.", In Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, Vol. 5, pp. 491-495, 2010.

[7] Ansari, A., Waheed, M. A., "Flooding attack detection and prevention in MANET based on cross layer link quality assessment.", In Intelligent Computing and Control Systems (ICICCS), International Conference on IEEE, pp. 612-617,2017.

[8] Tripathi, N., Hubballi, N. , "Exploiting DHCP server-side ip address conflict detection: A dhcp starvation attack.", In Advanced Networks and Telecommuncations Systems (ANTS), International Conference on IEEE, pp. 1-3, 2015.

[9] Aggarwal, R. K., "A Security Approach and Prevention Technique against ARP Poisoning.", In International Conference on Information and Communication Technology for Intelligent Systems, Springer, Cham, pp. 39-49, 2017.

[10] Kumar, S., & Tapaswi, S., "A centralized detection and prevention technique against ARP poisoning.", In Cyber Security, Cyber

Warfare and Digital Forensic (CyberSec), International Conference on IEEE, pp. 259-264, 2012.
[11] Khurana, S., Kaur, R.: A security approach to prevent ARP poisoning and defensive tools. Int. J. Comput. Commun. Syst. Eng. (IJCCSE), 2(3), 431–437, 2015.
[12] Guha, R. K., Furqan, Z., Muhammad, S., "Discovering man-in-the-middle attacks in authentication protocols.", In Military Communications Conference, MILCOM, IEEE, pp. 1-7, 2007.
[13] Conti, M., Dragoni, N., Lesyk, V., "A Survey of Man In The Middle Attacks.", IEEE Communications Surveys & Tutorials, pp. 2035, 2016.
[14] Yılmaz, T., Karaarslan, E., Akın, G., "GNS3 Tabanlı Ağ Emülasyonlarının Bilgisayar Ağları Eğitiminde Kullanımı: Senaryolar ve Öneriler", Researchgate, 2013.

Authors Profile

Sezer YILDIZ received his M.S. degree in Computer Engineering from İstanbul University, İstanbul, Turkey in 2010. He is currently a lecturer in Beykoz University. His research interests are cyber security, computer network, game programming.

Dr. Umut Altınışık received his M.S. degree in Electronics-Computer Education from Kocaeli University, Kocaeli, Turkey in 2006 and Ph.D. degree in Electronics-Computer Education from Kocaeli University in 2012. He is currently an Assist Professor in Informatics Department, Kocaeli University. His research interests are image steganography, computer vision, data mining, control systems and distance education.