FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 4 No. 1, March, 2020, pp 560 – 566

MITIGATING DHCP STARVATION ATTACK USING SNOOPING TECHNIQUE

***Nuhu Abdulhafiz A., Echobu Faith O. and Olanrewaju Oyenike M.**

Department of Computer Science & Information Technology, Federal University Dutsin-Ma, Katsina, Nigeria

*Corresponding Author's email: nabdulhafiz@fudutsinma.edu.ng

ABSTRACT

Over the years, devices and the use of networks has grown by leaps and bounds thereby making the Dynamic Host Configuration Protocol (DHCP) a very important network management tool. Initially, the protocol focused more on ease of use rather than security, which made it vulnerable to attacks like DHCP starvation among others. There are techniques which have been developed over the years to mitigate attacks to the DHCP server. This research used DHCP snooping to mitigate the attack to achieve a more secured network. The experiment was done in a virtual environment using GNS3. Due to the type of malicious packets that was generated during attack, the LAN was isolated from the Internet to avoid any destruction. The experiment demonstrated how easy it was to attack and exhaust DHCP pool of address thereby prohibited the legitimate client from getting IP address. The research also demonstrated the mitigation of DHCP starvation attack by using DHCP snooping.

Keywords: DHCP, DHCP Starvation Attack, DHCP Snooping, GNS3

INTRODUCTION

Dynamic Host Configuration Protocol (DHCP) is network management protocol used to automatically allocate IP addresses and other network configuration parameters like subnet mask, default gateway and lease time to clients on a network (Tripathi & Hubballi, 2017). This of course takes the burden of manually assigning IP addresses and monitoring usage off network administrators.

Once a client machine comes up on the network, a DHCPDISCOVER message is sent to the network so that it can be assigned an IP address. The DHCP server then responds with a DHCPOFFER message, usually in unicast, containing an offered IP address. Typically, there is only one DHCP server on a network. However, there could be several on a network which could all respond to the IP address request in which case, the client sends a DHCPREQUEST message to request the offered IP address by the first DHCP server to respond, thereby declining offers from other servers. The others will be informed of the offer the client has accepted and withdraw their previous offers thereby making those addresses available for other clients. In acknowledgement, the selected server sends a DHCPACK unicast message which includes the lease time and additional network configuration information (Rooney, 2011) (Mukhtar, Salah, & Iraqi, 2012). Figure 1 displays the basic operation messages of DHCP.

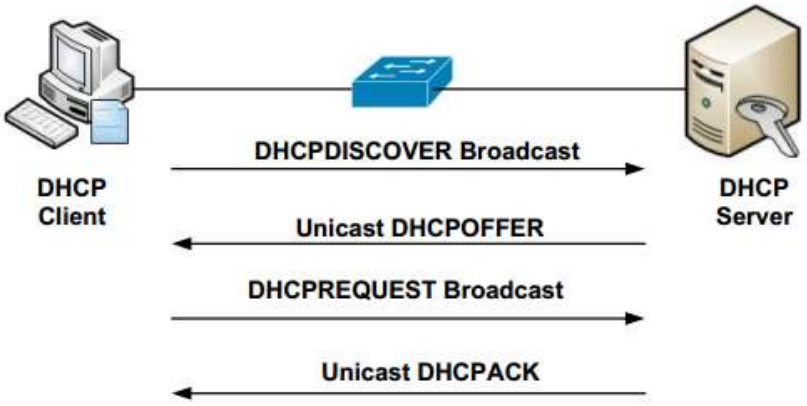

Figure 1: DHCP Process Operations

The absence of authentication of messages on the DHCP server makes it vulnerable to attacks like DHCP starvation attacks and spoofing (Hubballi & Tripathi, 2016). DHCP starvation attack occurs when attackers flood a DHCP server with IP address requests thereby making IP addresses unavailable to legitimate users. This is usually achieved through spoofed MAC addresses. When the available IP addresses become depleted on the DCHP server, the attacker then sets up a rogue DHCP server which responds to requests from other clients. This makes room for the attackers to carry out attacks such as spoofing and man-in-the-middle (Mitra, 2019). Yersinia, Gobbler, and Metasploit are some of the free hacking tools used to perform automated DHCP starvation attacks.

Younes (2016) identified starvation attacks, DHCP rogue server attacks and malicious DHCP client attack as common DHCP security problems. The research proposed a cryptography based authentication and key management solution using Diffie-Hellman key exchange algorithm supported by the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP).

DHCP Snooping

DHCP Snooping is a technique used on the network to prevent DHCP starvation attacks. It is configured on a network switch and works by eavesdropping on all communications going on the network. A database, known as a DHCP binding database, is maintained and constantly populated with clients' DHCP-assigned addresses, their MAC addresses, access ports and VLAN (Harris, 2016). If the switch detects messages from any untrusted ports, or if the supplied MAC address for a packet defers from the one stored on the database, it drops the packets thereby maintaining the security of the DHCP server (Atul & Jevitha, 2017).

The rest of the article is organised as follows: Sections on materials and methods, demonstration of attack, the mitigation phase, results and discussions, then the summary of research conclusion.

MATERIALS AND METHODS

The tools used for the experiments are:

- GNS3 (Graphical Network Simulator 3): is a network simulation software. They are open source software that are free to download. It works by using real Cisco, Jupiter IOS images which are emulated by Dynamips. It is used in large companies and students use it for studies (Neumann, 2015)
- Yersinia: is a network protocol tool design to take advantage of some weakness in different layer 2 protocols.
- Cisco Router
- Cisco Switch

The experiment was done in a virtual environment using GNS3. Due to the type of malicious packets that will be generated during attack, the LAN was isolated from the Internet to avoid any destruction.

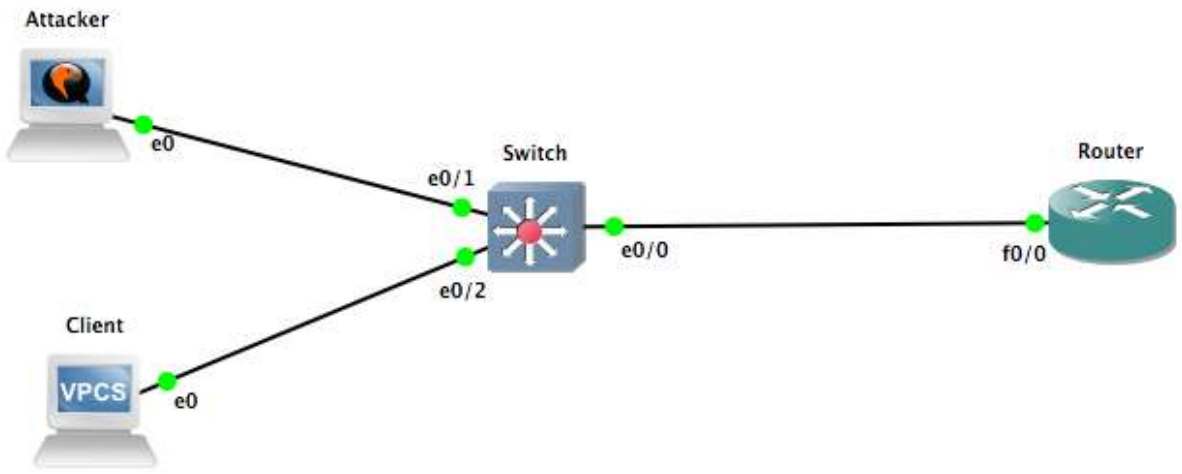

Figure 2: Network Topology

A simple LAN was used for this experiment. Figure 2 shows how the LAN was set up. The Router was set up as the DHCP server. 192.168.1.0/24 is the block of IP address that was used for the LAN. With the block of address that was used, 254 usable IP addresses can be assign to PC's and other network component within the LAN. The first usable IP address (192.168.1.1) was excluded from the pool of available IP addresses that the DHCP server can allocate. It was excluded

because it was assigned to the FastEthernet0/0 interface on the Router. The remaining 253 IP addresses can be dynamically assign to client machines when they join the network. The client machine connected to Ethernet0/1 interface on the Switch is the attacking machine. It is running Kali Linux operating system. It comes with a tool called Yersinia, which will be used to exhaust the available IP addresses on the DHCP server. The client machine connected to the Switch on Ethernet0/2 interface will be use for testing purpose to see if it can be able to get IP address from the DHCP server when attack is taking place.

Attack Phase

Before the attack was initiated, DHCP server allocated IP addresses to the attacking machine and the client machine on the network. The attacking machine have the MAC address 0c2c.1a1f.2b00. From figure 3, it can be seen that the MAC address of the attacking machine was given an IP address of 192.168.1.3. The client machine on the other hand have 0100.5079.6668.00 as its MAC address. From figure 3 below, it can be seen that the MAC address of the client machine is bind to 192.168.1.2.

```
Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.2         0100.5079.6668.00       Mar 13 2020 10:28 PM    Automatic
192.168.1.3         0c2c.1a1f.2b00          Mar 13 2020 10:32 PM    Automatic
```

Figure 3: DHCP binding before attack was initiated

Yersinia is the tool that was used to attack the DHCP server. To generate the attack, the following command was entered into Kali Linux terminal;

Yersinia dhcp –attack 1

The above command generates infinite DHCPDISCOVER packets and send it as a broadcast in the network. In each of the packet that will be sent, Yersinia used a spoofed MAC address on each packet. The DHCP server will allocate IP addresses to the requests until the pool of address is exhausted.

While the attack is taking place, the IP address of the client machine was intentionally released. This was done so as to check and see if the client machine can be able to get an IP address from the DHCP server.

```
Client> ip dhcp -x

Client> ip dhcp -r
DDD
Can't find dhcp server
```

Figure 4: Client machine unable to get IP address

In figure 4, the first command (*ip dhcp -x*) on the client machine is to release the IP address allocated to it. The second command (ip dhcp -r) on the client machine from figure 4 is to renew the IP address. It can be seen that after the command, a response of "DDD" was displayed. The (D) stands for DHCPDISCOVER packet. Therefore, the 3 (D) indicate that 3 different DHCPDISCOVER packets were sent, but there was no response from the server. Finally, it states that "can't find dhcp server". It implies that the attack from the attacking machine was successful as all the IP addresses in the pool are exhausted.

```
Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.2         0122.2e69.d2cd          Mar 12 2020 11:06 PM    Automatic
192.168.1.3         0c2c.1a1f.2b00          Mar 13 2020 10:52 PM    Automatic
192.168.1.4         ee60.6f70.5d77          Mar 12 2020 11:05 PM    Automatic
192.168.1.5         0941.8555.dc33          Mar 12 2020 11:05 PM    Automatic
192.168.1.6         1ebd.df5a.9b6d          Mar 12 2020 11:05 PM    Automatic
192.168.1.7         2e42.aa49.06f4          Mar 12 2020 11:05 PM    Automatic
192.168.1.8         0699.4a51.97ce          Mar 12 2020 11:05 PM    Automatic
192.168.1.9         077e.d060.2260          Mar 12 2020 11:05 PM    Automatic
192.168.1.10        76ff.ee74.f6d4          Mar 12 2020 11:05 PM    Automatic
192.168.1.11        9ac2.310a.451d          Mar 12 2020 11:05 PM    Automatic
192.168.1.12        2c2f.f227.c299          Mar 12 2020 11:05 PM    Automatic
192.168.1.13        d25e.fa76.3dde          Mar 12 2020 11:05 PM    Automatic
192.168.1.14        b07b.2309.e245          Mar 12 2020 11:05 PM    Automatic
192.168.1.15        be24.c62a.3a80          Mar 12 2020 11:05 PM    Automatic
192.168.1.16        4fc0.e819.3c6b          Mar 12 2020 11:05 PM    Automatic
192.168.1.17        d878.2f60.32e1          Mar 12 2020 11:05 PM    Automatic
```

Figure 5: DHCP binding while attack is taking place

Figure 5 shows a portion of the DHCP binding table. Before the IP address of the client machine was released, it was assigned 192.168.1.2 by the DHCP server. After the address was released, it can be seen that 192.168.1.2 is now associated with a different MAC address. The MAC address of the client machine is 0100.5079.6668.00.

Mitigation Phase

DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch. DHCP snooping drops DHCP traffic determined to be not acceptable. DHCP snooping stores its information in a database containing the client MAC address, DHCP assigned IP address, remaining lease time, VLAN, and switch port. When DHCP snooping detects a violation, it drops the packet and logs it. The switch port involved in the violation will be disabled by the switch.

By default, DHCP snooping is disabled on Cisco switches. The switch is configured to enable DHCP snooping to mitigate the attack. The commands added in the switch global configuration mode are as follows;

ip dhcp snooping

ip dhcp snooping vlan 1

interface ethernet0/0

ip dhcp snooping trust

interface ethernet0/1

ip dhcp snooping limit rate 5

interface ethernet0/2

ip dhcp snooping limit rate 5

Table 1 below describes the function of each command that was used in mitigating DHCP starvation attack in the experiment.

Table 1: Command descriptions

COMMAND	DESCRIPTION
ip dhcp snooping	Enables DHCP snooping on the switch
ip dhcp snooping vlan 1	Enables DHCP snooping for vlan 1
interface ethernet0/0	Enters into the interface configuration mode connecting the switch to the DHCP server for configuration
ip dhcp snooping trust	When executed in interface configuration mode, it tells the switch to trust any DHCP server responses coming from the configured interface
interface ethernet0/1	Enters into the interface configuration mode for interface connecting the switch to the attacking machine for configuration
ip dhcp snooping limit rate 5	Limits the number of DHCPDISCOVER to 5 per second
interface ethernet0/2	Enters into the interface configuration mode for interface connecting the switch to the client machine for configuration
ip dhcp snooping limit rate 5	Limits the number of DHCPDISCOVER to 5 per second

RESULTS AND DISCUSSION

The only way to know if the mitigation technique works is when the client machine on our LAN is able to get an IP address from the DHCP server when an attack is taking place. After the DHCP snooping was enabled and all necessary configurations were made on the switch, the attacking machine was used again to attack the DHCP server to try and exhaust the pool of IP address.

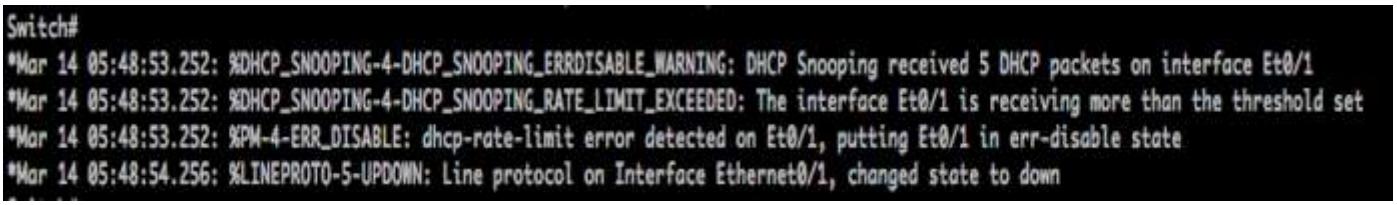

Figure 6: DHCP snooping showing rate limit exceeded

As soon as the attacking machine start sending the DHCPDISCOVER packets, within the first second of the attack starting, DHCP snooping was able to detect the attack. From figure 6 above, it can be seen that 'DHCP snooping received 5 DHCP packets on interface E0/1'. Interface E0/1 (Ethernet0/1) is the interface the attacking machine connects to the switch. The second line is displaying a log that the threshold that was set on interface E0/1 is exceeded. Therefore, in the subsequent lines, its saying that Et0/1 interface is been put into err-disable state. Err-disable is a feature that automatically disables a port on Cisco switch. When the port is disabled, no packet will be able to reach the switch from the attacking machine. Likewise, no packet can be able to reach the attacking machine from the network.

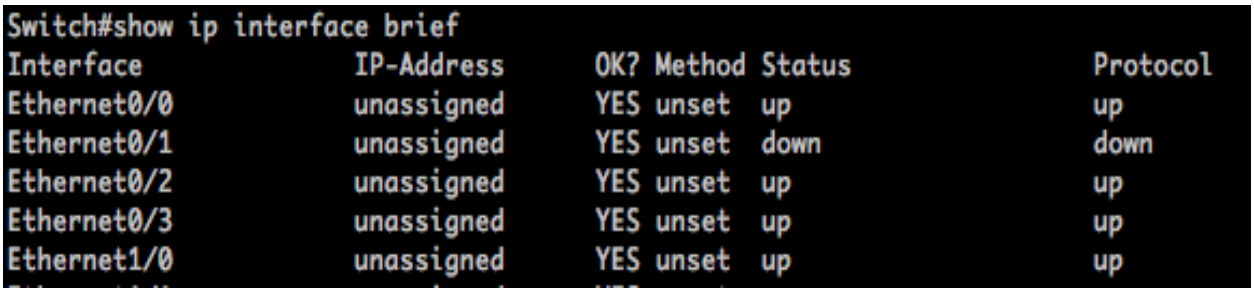

Figure 7: Interfaces status

When an interface in disabled, it shutdown. The network administrator has to configure the shutdown interface for it to be able to come up. From figure 7, Ethernet0/1 can be seen as down.

The client machine has no IP address because it was earlier released. Now we will try to get an IP address from the DHCP server.

```
Client> show ip

NAME        : Client[1]
IP/MASK     : 0.0.0.0/0
GATEWAY     : 0.0.0.0
DNS         : 8.8.8.8
DHCP SERVER : 192.168.1.1
DHCP LEASE  : 85615, 86400/43200/75600
MAC         : 00:50:79:66:68:00
LPORT       : 10004
RHOST:PORT  : 127.0.0.1:10005
MTU         : 1500

Client> ip dhcp -r
DDORA IP 192.168.1.2/24 GW 192.168.1.1
```

Figure 8: Client machine renewing IP address

From figure 8 above, after a show ip command, it can be seen that the client machine has no IP address assign to it. The command ip dhcp –r was used to renew IP address. It was able to get an IP address from the DHCP server. 192.168.1.2 was assign to it by the server. The DDORA before the IP address in figure 8 indicates that the first (D) which stands for DHCPDISCOVER packet was unsuccessful. The client had to send another DHCPDISCOVER packet before it got a response from the DHCP server with a DHCP OFFER (O) packet. The client sent a DHCPREQUEST (R) to the DHCP server and finally the server sent a DHCPACK (A) packet.

CONCLUSION

In this study, the experiment demonstrated how easy it is to attack and exhaust DHCP pool of address thereby making legitimate clients unable to get IP address in other for them to be able to have access to the network and Internet at large. The experiment also show how to mitigate DHCP starvation attack by using DHCP snooping. By default, it is disabled in a Cisco switch, network administrators should always enable it. As a feature study, such mitigation technique will be applied to wireless network.

REFERENCES

Atul, K., & Jevitha, K. (2017). Prevention of PAC File Based Attack Using DHCP Snooping. *Security in Computing Communications* (pp. 195–204. DOI: 10.1007/978-981-10-6898-0_16). Springer Nature Singapore Pte Ltd.

Harris, M. (2016, February 9). *DHCP Snooping: Basic Concepts and Configuration*. Retrieved from Pearson IT Certification: https://www.pearsonitcertification.com/articles/printerfriendly/2474170

Hubballi, N., & Tripathi, N. (2016). A Closer Look into DHCP Starvation Attack in Wireless Networks. *Computers & Security*, DOI: 10.1016/j.cose.2016.10.002.

Mitra, A. (2019, October 25). *What is DHCP Starvation attack and how does it work?* Retrieved from The Security Buddy: https://www.thesecuritybuddy.com/network-security/what-is-dhcp-starvation-attack-and-how-does-it-work/

Mukhtar, H., Salah, K., & Iraqi, Y. (2012). Mitigation of DHCP starvation attack. *Computers and Electrical Engineering 338(5)*, 1115–1128; DOI: 10.1016/j.compeleceng.2012.06.005.

Neumann, J. C (2015). *The book of GNS3: build virtual network labs using Cisco, Jupiter, and more.* San Francisco: No Starch press.

Rooney, T. (2011). *Introduction to IP Address Management.* John Wiley & Sons; pp55.

Tripathi, N., & Hubballi, N. (2017). Detecting Stealth DHCP Starvation Attack using Machine. *Journal of Computer Virology and Hacking Technique*, 1-12; DOI: 10.1007/s11416-017-0310-x.

Younes, O. S. (2016). A Secure DHCP Protocol to Mitigate LAN Attacks. *Journal of Computer and Communications, 4*, 39-50. . http://dx.doi.org/10.4236/jcc.2016.41005.