Iraqi Journal of Information and Communications Technology(IJICT)
Conference Series: The 1st Conference of Applied Researches in Information Engineering(ARIE2021), 2021

ISSN:2222-758X
e-ISSN:2789-7362

DESIGNING A SECURE NETWORK SOLUTION AGAINST DHCP ATTACKS

Ammar A. Shareef [1], Salim M. Ali [2]
[1,2] College of Information Engineering, Al-Nahrain University, Baghdad, Iraq
ammar.ali.1999.aa@gmail.com [1], salimm@coie-nahrain.edu.iq [2]
Received:5/5/2021, Accepted:19/6/2021

***Abstract*- DHCP (Dynamic Host Configuration Protocol) is an important aspect in small and large networks since it facilitates the IP configuration of computers. However, DHCP has a lot of security concerns, the most serious of which being MAC address spoofing. Furthermore, current research is still unable to guarantee a suitable level of pro-tection; therefore, DHCP is vulnerable to different attacks, thus the essential objective of this paper is to propose solutions against DHCP attacks. This paper provides a deep clarification of how DHCP can be vulnerable and presents an explanation about how DHCP works and lists a summary about DHCP attacks, how the attacks occur and affect the security of the network, which threatens the network's security. Main effective countermeasures were proposed and implemented against DHCP attacks, resulting in a successful hindrance of the attacks. Some of the countermeasures decrease the chance of attack to be implemented. The paper provides recent methods to hinder DHCP attacks and provides a complete solution to mitigate DHCP vulnerability.**

keywords: **DHCP, GNS3, Network attack.**

I. INTRODUCTION

Nowadays everything has changed, thousands, if not tens of thousands, of devices, are connected to a network using the traditional DHCP protocol. These networked devices ranging from personal digital assistants (PDAs) to laptops and desktop computers and even smart home devices that require network connectivity such as IoT applications. Network administrators can admit that manually configuring computers connected to a network is a time consuming and error-prone method; Therefore, DHCP protocol was created to handle the modern networks ex pandability. DHCP stands for Dynamic Host Configuration Protocol, which is a management protocol that assigns IP addresses automatically to users and provides them with network configurations such as default gateway and other network parameters [1]. This protocol is vulnerable to many network attacks. For example, DHCP handshake is transmitted in clear text and there is no mechanism for authentication which means clients are not sure if they got the network configuration parameters from a trusted DHCP server; therefore, it makes the DHCP protocol susceptible to DoS attacks. In this case, anyone who can access the network can launch an attack to prevent other clients from accessing a certain network resource or having a proper IP address. Since security is a top priority for businesses and companies of all types, one should build a secure network to prevent such attacks. This paper is concerned with learning the methodologies of executing attacks using some tools and testing solutions and preventing those attacks [2]. The next two sections explain the principles of DHCP, such that, how it operates in depth and how the main attacks operate. Section III, shows the implementation of the attacks by using GNS3 (Graphical Network Simulator-3) emulator, which enables the use of both virtual and physical hardware, and with the integration of VMware (Virtual Machine) workstation to run real images of operating systems as virtual machines that are necessary for the whole experiment to create a similar environment to the real world. In section IV, the methodology of countermeasures of each attack presented in Section V is explained and implemented. Lastly, the results are illustrated and verified in Section VI.

ISSN:2222-758X
e-ISSN:2789-7362

II. BACKGROUND

DHCP was first described as a policy protocol at RFC 1531 in October 1993, as an extension of the Bootstrap Protocol (BOOTP), a network protocol used by a network client to obtain an IP address in a server configuration [3]. The incentive to expand BOOTP was that BOOTP required active interventions to add configuration information to each client and did not provide a way to retrieve used IP addresses. Many have worked to clarify the protocol as it gained popularity, and in 1997 DHCP RFC 2131 was released and remains the standard for IPv4 networks [9]. As we mentioned above DHCP is a network management protocol; therefore, in any network, there is a DHCP, configured with IP addresses pool and network parameters. When a new client joins the network, it completes a four phases handshake with the DHCP server which is named DORA and it stands for 'DISCOVER' , 'OFFER' , 'REQUEST' , 'ACKNOWLEDGMENT' to get an IP [5] as shown in Fig. 1. DHCPDISCOVER, the client starts with no IP address; it sends a discovery message and broadcasts it to locate all of the available DHCP servers in the network. Each DHCP server receives the discovery message and analyses it. The server searches its address pool for an available IP address, then decides if it can give the client an IP address. When the server finds an available address, it sends a DHCPOFFER, which is an offer message that contains the IP address being offered to the client, this message is broadcasted to the network. If the server already had a lease for this client before, it would use the same previously given IP address. When the client receives the offer, it sends back a broadcast mes-sage DHCPREQUEST requesting the offered IP address. DHCPACK or DHCPNACK, the intended server will note that its lease has been chosen. It checks its databases if this lease is still available if so, it creates an entry in the database for that client and sends back a DHCPACK message that contains network configurations parameters and the allocated IP address to the client. If the lease is no longer available it sends back a DHCPNACK and the client will initiate a new handshake with the server [1] [6].

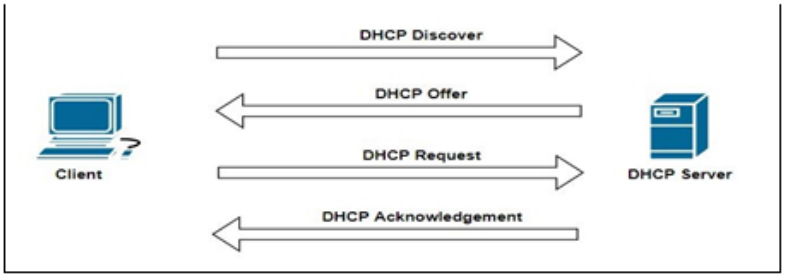


Figure 1: DHCP handshake

In [7] , an introduction to two DHCP protocol security improvement strategies based on digital certificates for DHCP clients was proposed. However, the suggested methodology is compatible with DHCP clients which do not have digital certificates. In [2] , a DHCP attack detection approach based on fingerprint and behavioural markers was proposed. In [3], a technique for authenticating "DHCP servers" and "DHCP server Replies" using public-key cryptography and digital certificates was proposed to prevent rogue DHCP server attacks in this way. In [8] , DHCPAuth, which is a technique, was proposed that uses two trust models: PGP (Pretty Good Privacy) and PKI (Public Key Infrastructure) to authenticate

ISSN:2222-758X
e-ISSN:2789-7362

DHCP packets. In [9] , proposes a novel approach that uses an OTP sent to a mobile OTP DHCP to authenticate DHCP clients and servers, therefore increasing the security.

III. DHCP VULNERABILITY

This section shows the two main methods that exploit the vulnerability of DHCP and defines the mechanism of each attack.

A. DHCP Starvation Attack

The DHCP starvation attack is a widespread attack that targets network DHCP servers, it floods the DHCP server with DHCPDISCOVER messages, and each message is different in MAC address. The DHCP server will respond to all of the requests and not knowing this is a DHCP starvation attack, by assigning avail-able IP addresses to the fake requests resulting in the depletion of DHCP pool and therefore, it is considered as a DoS attack. This attack is equally successful for wired and wireless networks [7] as shown in Fig. 2.

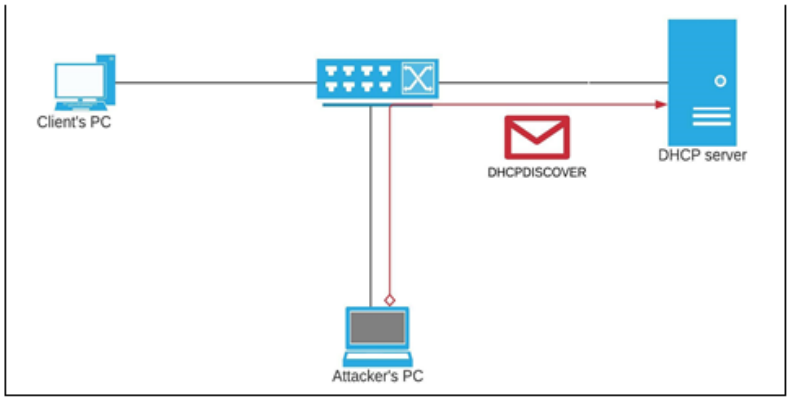


Figure 2: DHCP starvation attack

B. DHCP Spoofing Attack

In a DHCP spoofing attack, a rogue DHCP server, which is a non-legitimate DHCP server, is installed on a network by an unauthorized person who has access to the LAN or an authorized user who wants to sabotage the network that is not within the control of network administrators. The attacker responds to the DHCPDIS-COVER message from the client and supplies its IP address as the default gateway, this is done by the installa-tion of a rogue DHCP server on the network thus, a man in the-middle attack occurs as shown in Fig. 3 [10].

IV. DHCP ATTACKS

In this section, two attacks were presented by the use of GNS3 and VMware Workstation:

1) Attack I:

This scenario shows how to execute a DHCP spoofing attack. A small network that consists of a cisco switch, windows

ISSN:2222-758X
e-ISSN:2789-7362

7 and kali-Linux is used refer to Fig. 4. Attacker's pc contains Ettercap tool which is pre-installed by default, this tool is used for man in the middle attacks and it's a good demonstration for this attack. When the attack is started, the attacker's pc listens for DHCPDISCOVER messages in the network. The client sends a DHCPDISCOVER first to discover the available DHCP servers and since there are two servers in the network one is fake and one real server, both of the servers get the request and reply for the client, but the server that replies with a DHCPOFFER first is the one that completes the full DHCP hand-shake with the client, in this case, the attacker's server replied first as shown in Fig. 5 by Using Wireshark. The time difference can be seen between the two responses which indicate the attacker's server was faster. When the handshake is completed, the client's pc receives a fake IP address and other network configurations from the attacker.

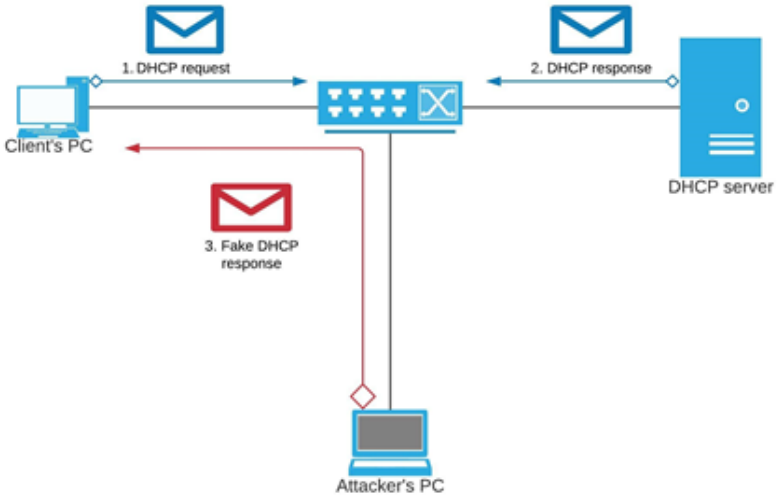


Figure 3: DHCP spoofing attack

2) Attack II:

The second attack shows DHCP starvation attack is executed by flooding the network with fake DHCPDISCOVER messages to take all of the available leases in the DHCP server. Starting with the same network as above see Fig. 4. Yersinia is the used tool for this attack, it provides a list of different attacks to deal with. When the attack is started by this tool, it generates thousands of fake DHCPDISCOVER packets each second, with each packet is different in MAC address from the other. The network and DHCP server are flooded by these packets; therefore, the server replies for all of these flooding requests and make an en-try in its database for each request and assign all of the available IP address for those packets, as a result of a depletion in the address pool of the DHCP server occurs. Clients are unable to join the network as shown in Fig. 6. Fig. 7 shows the minimal time between each packet and the destination IP address which is a broadcast address, this indicates that this attack doesn't only affect the DHCP server but it also affects the switch and other devices in the network because the switch has to process all of these packets and

ISSN:2222-758X
e-ISSN:2789-7362

for-wards them to all ports except the port that packets came from, thus, this would affect the performance of the switch and the network because it creates unnecessary traffic and allocates more bandwidth.

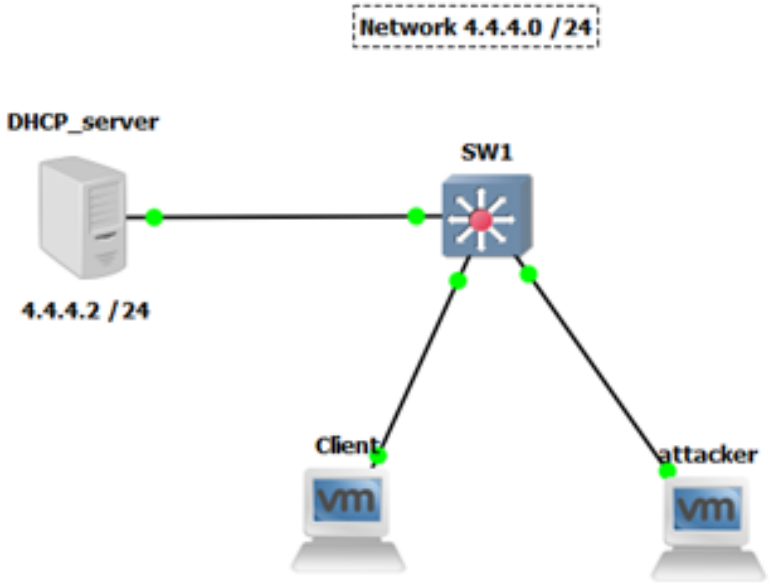


Figure 4: Simple network design

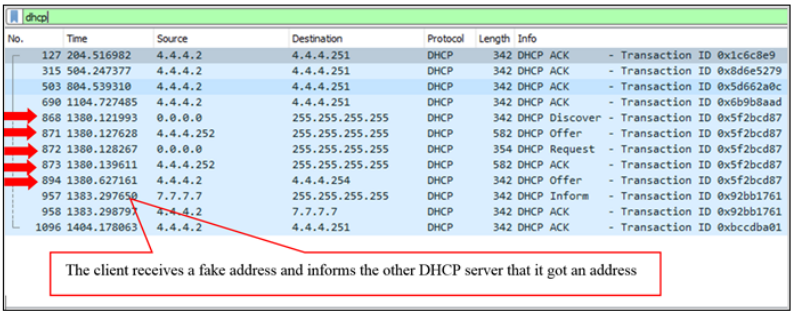


Figure 5: Wireshark capture

V. METHODOLOGY

This section shows the Different countermeasures that are considered, such as configurations in the networking device that can prevent the attack and others can eliminate the probability of an attack happening. These are listed below:

1) Activation of DHCP Snooping:

   DHCP snooping can be applied on switches that support this configuration. Its function is to prevent malicious rogue servers from sending malicious DHCP traffic, it categorizes ports as trusted ports and untrusted ports. The trusted port is the only port that DHCP messages from the server side are allowed. The untrusted port is the port that discards

ISSN:2222-758X
e-ISSN:2789-7362

all of the ingress DHCP server-side messages and drops them see Fig. 8. First, the switch is accessed and DHCP snooping is enabled to a specific VLAN since all of the devices on the network are on the same VLAN, but if it's enabled globally without specifying it to a certain VLAN has no effect see Fig. 9. The switch port that is directly connected to the real DHCP server is accessed and enabled as a trusted port see Fig. 10.

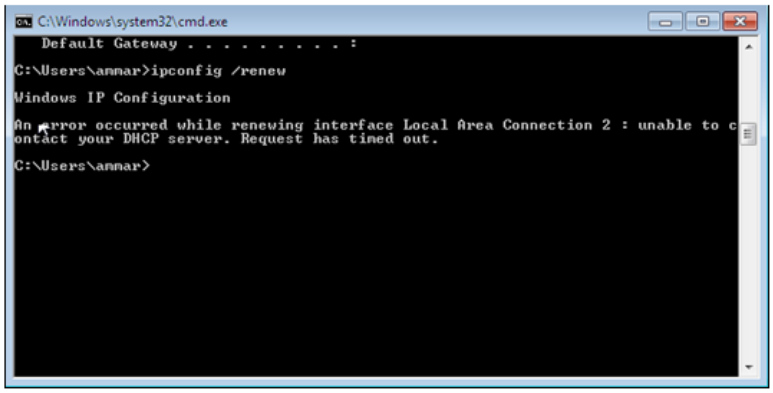


Figure 6: The client is unable to join the network

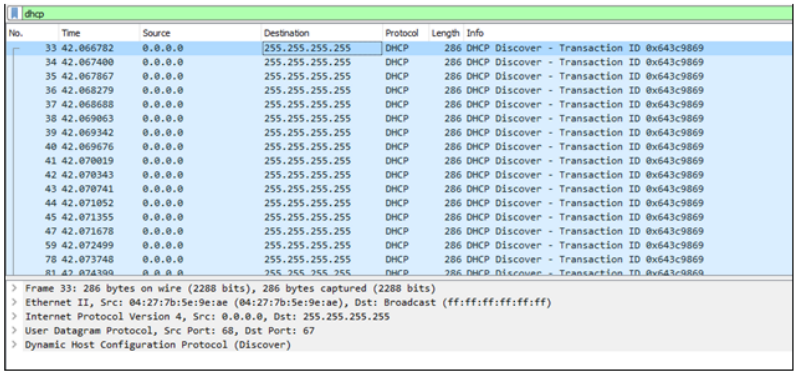


Figure 7: Packets flooding in wireshark capture

2) Port Security:

This method mitigates the DHCP starvation attack, it limits the number of MAC addresses on the port or configures a certain address on the port to be the only allowed address, as shown in Fig. 11.a. some cases cause switch port violation If the MAC addresses received on a port exceeds the limit or the address that is received is different from the address that is configured on the port; therefore, the port shuts down automatically and needs to be re enabled manually based on the selected violation type in the configuration, or when a MAC address seen on a switch port and has already been seen on another port. For cisco switch-es, there are three switch port violation types which one of them is enabled by default and these types are:

ISSN:2222-758X
e-ISSN:2789-7362

- Protect: When you use this mode, frames from known MAC addresses are allowed to continue sending traffic while frames from unknown MAC addresses are dropped. The switch keeps logs for all of the discarded frames.
- Restrict: The frames form known MAC addresses are permitted to pass but unknown addresses are discarded and unlike protect the type, the switch sends an alert message informing the administrator that a certain violation has occurred.
- Shutdown: In this mode, the switch port is disabled and needs to be re enabled manually and generates an alert message. To enable this method, the untrusted switch port is accessed and switch port security is enabled then the number of MACS is limited, as shown in Fig. 11: b).

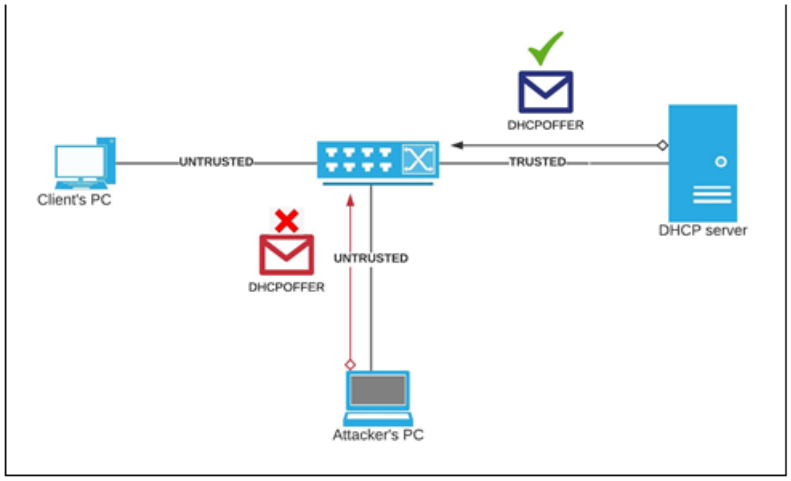


Figure 8: DHCP snooping's solution functionality

```
sw1#
sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw1(config)#
sw1(config)#ip dhc
sw1(config)#ip dhcp snoopi
sw1(config)#ip dhcp snooping ?
  database     DHCP snooping database agent
  information  DHCP Snooping information
  verify       DHCP snooping verify
  vlan         DHCP Snooping vlan
  <cr>

sw1(config)#ip dhcp snooping vlan 1
sw1(config)#
```

Figure 9: DHCP snooping enabled globally

3) Authentication server:

Authentication is the determination of whether someone or something is actually who or what they claim to be. When a new user connects to the network, a unique username and password for each user that is stored in a database are all needed to identify the user through an authentication server see Fig. 12; therefore, Authentication is used in large companies with many employees to control the large number of persons access-ing the network and limiting the

ISSN:2222-758X
e-ISSN:2789-7362

access for the employees only. Thus, the need for an authentication server (RADIUS) is important, RADIUS stands for Remote Authentication Dial in User Service, The RADIUS server doesn't prevent DHCP attacks at all but its main function is to authenticate users joining the network and non employees are not able to access the network because they don't have a unique username and password; therefore, outsiders cannot execute DHCP attacks because they don't have an access to the network. Encryption is one of the good features that RADIUS supports since, all messages transferred between the client and the server are encrypted. RADIUS server needs a database to store user profiles there. In this case, Microsoft windows server 2016 is added to the network see Fig. 13. The switch is added to the radius server as a RADIUS client which is responsible for transmitting messages between the server and the client. The user enters his credentials in the window prompt and sends them to the switch see Fig. 14. When the user enters his username and password, the switch forwards the user information to the RADIUS server for authentication. A Wireshark capture shows the communication process between the switch and the server to grant access for the user see Fig. 15, the server sends multiple challenges and the user computer must pass all of these challenges to get authenticated.

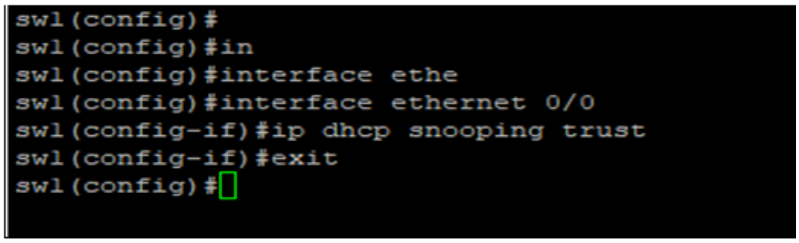
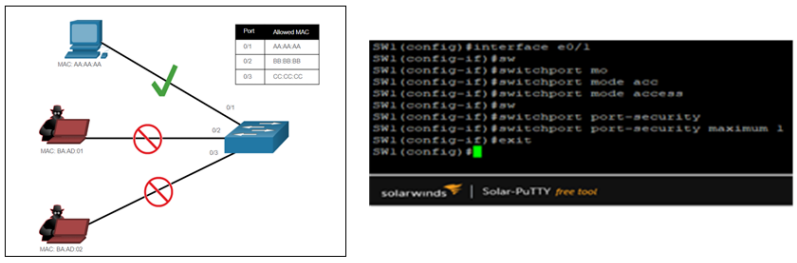


Figure 10: DHCP snooping trusted port



(a) (b)

Figure 11: a) MAC address limitation b) Limitation of MAC addresses rate to 1

4) VLANS:

VLAN is a virtual network created from the same local network, it allows a group of devices from different networks to be grouped into a single virtual network. VLAN is useful because it improves network stability, management and security. VLAN separates broadcast domains; therefore, DHCP attacks remain on the virtual LAN that the attacker connected to and not broadcasted to all of the switches in the network. Thus, the probability of attacks will be lowered

ISSN:2222-758X
e-ISSN:2789-7362

[7] , the implementation of this method is left as future work.

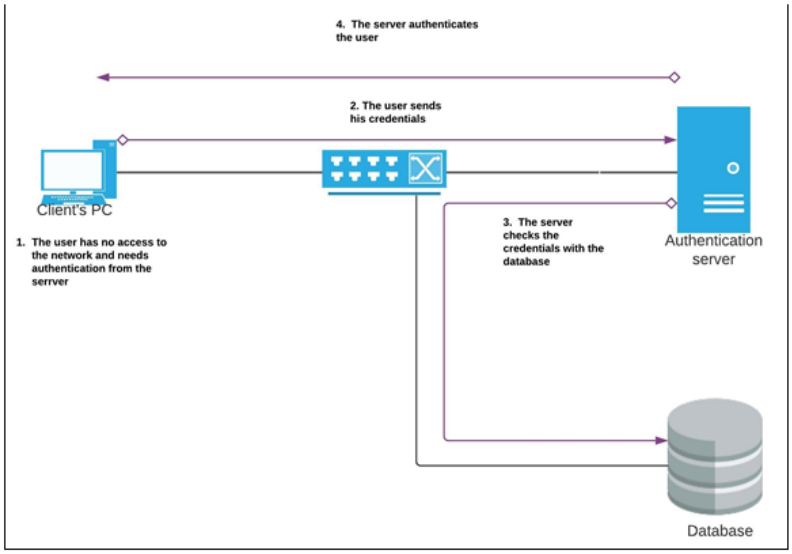


Figure 12: Authentication process

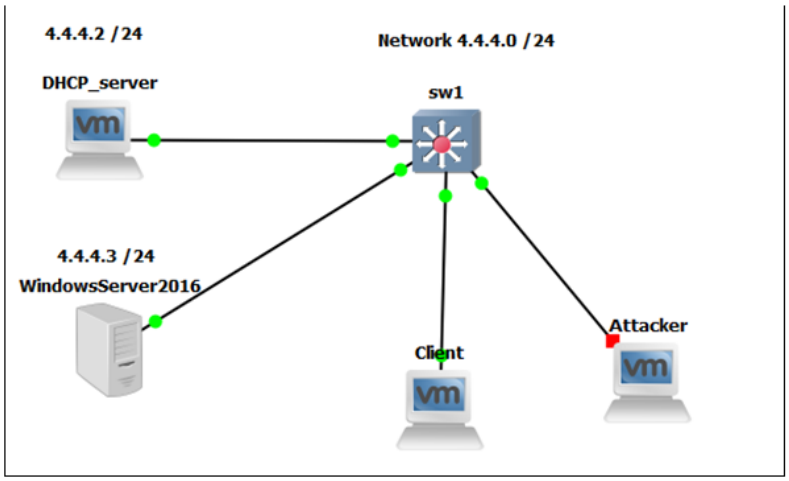


Figure 13: Radius network

VI. RESULTS

It is important to check whether the proposed methods above work and deny DHCP attacks successfully. For the authentication server, the client is authenticated and granted access from the server successfully. By this method, the attacks are not prevented but the probability for the attacks to occur is lowered. Fig. 16 shows a logged event in the server that contains information about the authentication request and if it's accepted or rejected. The MAC limitation method is

ISSN:2222-758X
e-ISSN:2789-7362

effective against DHCP starvation attack, Fig. 17, Fig. 18 show that the switch port exceeded the MAC address limit and the port sends an alert to the network administrator; therefore, the switch port goes down based on the configuration of the switch port violation.

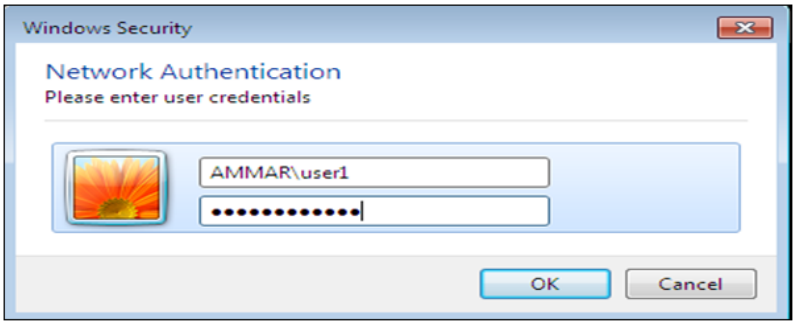


Figure 14: Window prompt for credentials

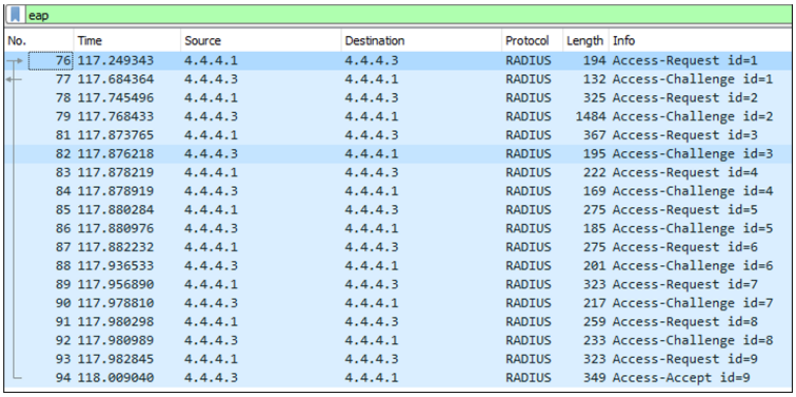


Figure 15: A wireshark capture of the user authentication process and switch to server communication

DHCP snooping in ports stops the DHCP spoofing attack, Fig. 19 shows that the switch sends an alert with the MAC address of the attacker indicating an attack attempt has occurred. the switch creates DHCP snooping binding table by getting information from DHCP messages, it contains the MAC address, lease time, IP address from the DHCP server and the port that the client is connected to, this is useful since, the MAC address from the alert mes-sage is compared to the table to find on which port the attacker is connected to, as shown in Fig. 20. As a result, the client gets an IP address from the correct DHCP server as shown in Fig. 21.

ISSN:2222-758X
e-ISSN:2789-7362

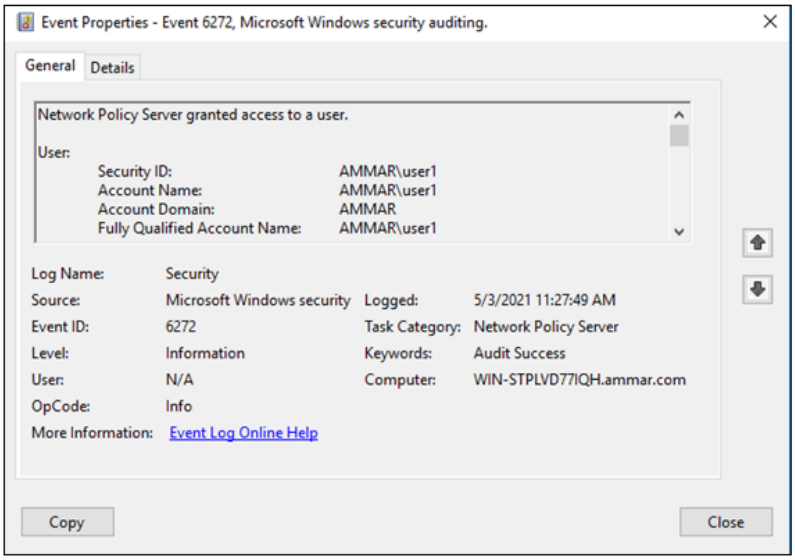


Figure 16: User's request from the event viewer in the radius

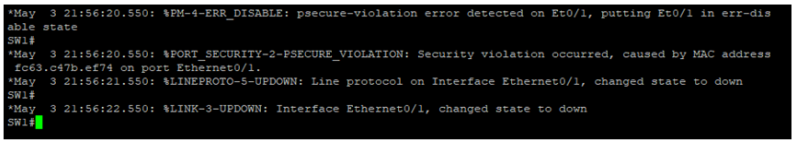


Figure 17: Port violation due to an attempt for DHCP starvation attack

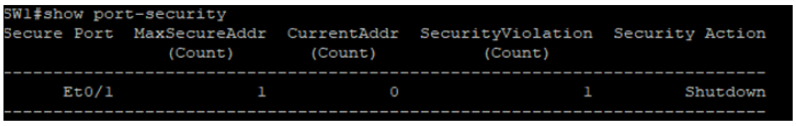


Figure 18: Port security description

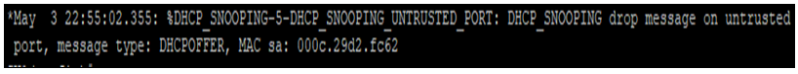


Figure 19: Alert messages show an attempt for DHCP snooping attack

As a comparison to previous related works in [2], [3], [7], [8] and [9], our research contribution can be listed as:

- The research addresses almost all the attacks that can be applied to DHCP protocol.
- The implementation of the experiments and tests were accomplished by using the most updated software such as GNS3, VMware 15, Windows Server 2016, Kali Linux etc.

ISSN:2222-758X
e-ISSN:2789-7362

- The presented solutions can be implemented without further modification of a working network, while what is presented in the related work requires lots of changes in network configuration and devices.
- The solutions presented requires low-cost devices and can be scalable based on the network complexity.
- No protocol modifications were made, which means all devices are compatible with the presented solutions.

```
SW1#show ip dhcp snooping bin
SW1#show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
00:0C:29:D2:FC:62   4.4.4.254       549         dhcp-snooping   1     Ethernet0/1
00:0C:29:BB:DA:52   4.4.4.253       406         dhcp-snooping   1     Ethernet2/0
Total number of bindings: 2
```

Figure 20: DHCP binding table in the switch

```
C:\Windows\system32\cmd.exe
Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d892:c7f4:787:aab0%13
   IPv4 Address. . . . . . . . . . . : 4.4.4.253
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 4.4.4.1

Tunnel adapter isatap.{95A50F80-CE7F-4748-88E9-23FC6FC6777B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter 6TO4 Adapter:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Reusable Microsoft 6To4 Adapter:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2002:404:4fd::404:4fd
   Default Gateway . . . . . . . . . :

C:\Users\ammar>
```

Figure 21: The client got an IP address from the real DHCP server

VII. CONCLUSION

In a conclusion, internal network DHCP attacks put any network at risk of losing network resources. This paper shows the currently available techniques to avoid DHCP attacks. The network solutions presented benefit all enterprises and offices that use internal networks by keeping DHCP network attacks as low as possible. As a result, to prevent DHCP attacks in a network, there must be at least network switches that support configurations present-ed in the paper to hinder DHCP attacks. The various solutions and methods, which are presented, can be considered based upon the cost and the scalability of the network. Finally, this paper documents thoroughly the vulnerability of DHCP protocol and the available current solutions that should be considered to provide a safe network.

ISSN:2222-758X
e-ISSN:2789-7362

REFERENCES

[1] S. A. Alabady, "Design and Implementation of a Network Security Model Using Static VLAN and AAA Server" , in 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications, Damascus, Syria, 2008.
[2] M. Aldaoud, D. Al-Abri, A. Al Maashri and F. Kausar, "DHCP Attacking Tools: An Analysis" , Journal of Computer Virology and Hacking Techniques, pp. 1-11, 01 2021.
[3] Dumitru, Dinu, Togan and Mihai, "DHCP Server Authentication Using Digital Certificates" , in 2014 10th International Conference on Communications (COMM), Bucharest, Romania, 2014.
[4] A. Shete, A. Lahade, T. Patil and R. Pawar, "DHCP Protocol Using OTP Based Two-Factor Authentication" , in 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2018.
[5] C. Kozierok, "The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference" , No Starch Press, 2005.
[6] T. Rooney, "Dynamic Host Configuration Protocol (DHCP) " , in Introduction to IP Address Management , IEEE, 2010, pp. 53-68, doi: 10.1002/9781118073810.ch3.
[7] S. Duangphasuk, S. Kungpisdan and S. Hankla, "Design and Implementation of Improved Security Protocols for DHCP Using Digital Certificates" , Singapore, 2011.
[8] D. D. Dumitru and M. Togan, "DHCPAuth: A DHCP Message Authentication Module" , in 2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics, Timisoara, Romania, 2015.
[9] A. Shete, A. Lahade, T. Patil and R. Pawar, "DHCP Protocol Using OTP Based Two-Factor Authentication" , in 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2018.
[10] N. Tripathi and N. H, "A Closer Look Into DHCP Starvation Attack in Wireless Networks" , Computer security, Vol. 65, pp. 387-404, 2017.