Modeling Attacks on the DHCP Protocol in the GNS3 Environment and Determining Methods of Security Against Them

Tetiana Vakaliuk[1,2,3], Yelyzaveta Trokoz[1], Oleksandra Pokotylo[1], Viacheslav Osadchyi[4], and Serhii Smirnov[5]

[1] *Zhytomyr Polytechnic State University, 103 Chudnivsyka str., Zhytomyr, 10005, Ukraine*
[2] *Institute for Digitalisation of Education of the NAES of Ukraine, 9 M. Berlynskoho str., Kyiv, 04060, Ukraine*
[3] *Kryvyi Rih State Pedagogical University, 54 Gagarin ave., Kryvyi Rih, 50086, Ukraine*
[4] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str, Kyiv, 04053, Ukraine*
[5] *Central Ukrainian National Technical University, 8 University ave., Kropyvnytskyi, 25006, Ukraine*

Abstract

The article discusses various types of attacks on the DHCP protocol and the tools that can be used to implement them. Using modeling, the primary network vulnerabilities associated with dynamic address allocation were identified and methods to prevent or mitigate them were proposed. A network design close to the real one was built in the GNS3 environment. A Cisco router was used as a DHCP server. Specialized tools such as Yersinia and Ettercap were used to carry out the DHCP Starvation and Rogue DHCP server attacks. The simulation of attacks will be equally effective for different types of DHCP servers and network equipment from other companies.

Keywords

Vulnerabilities, DHCP, GNS3, attack modeling, DHCP starvation, rogue DHCP server.

1. Introduction

Network security issues are becoming increasingly relevant in today's digital environment, given its constant evolution. The number of cyberattacks is constantly growing, which, in the absence of their constant study and identification of countermeasures, can lead to problems with network availability and its safe operation. The Dynamic Host Configuration Protocol (DHCP) protocol is one of the key protocols for establishing network communication, as it provides devices with IP addresses and other network parameters. Therefore, it is important to know how attacks on this protocol are carried out and to identify methods of securing against them to take all the necessary steps to prevent attacks and ensure uninterrupted communication when administering the network.

1.1. Theoretical Background

An analysis of research on this topic has shown that there are many ways to conduct various cyberattacks on network protocols using specialized software products.

In particular, in the article [1], the GNS3 emulator was used to perform a DDoS attack and it was determined that parameters such as web server settings and security modules affect server performance during an attack and are not available in other simulators such as OPNET, NS3, and others. The study found that GNS3 provides a very realistic approach to creating network simulations, allowing you to configure a full set of parameters that are available in real computer networks. Among the disadvantages noted by the authors are the use of hardware resources to simulate the operation of all devices, limited scalability

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: tetianavakaliuk@gmail.com (T. Vakaliuk); liza.bailiuk@gmail.com (Y. Trokoz); a.a.polish4uk@gmail.com (O. Pokotylo); v.osadchyi@kubg.edu.ua (V. Osadchyi); smirnov.ser.81@gmail.com (S. Smirnov)
ORCID: 0000-0001-6825-4697 (T. Vakaliuk); 0000-0002-4961-7816 (Y. Trokoz); 0000-0002-1587-235X (O. Pokotylo); 0000-0001-5659-4774 (V. Osadchyi); 0000-0002-7649-7442 (S. Smirnov)

within the topology, and support for a small number of simulated equipment.

The paper [2] examined the DHCP Starvation attack in a wireless network and highlighted the experimental difficulties in its implementation. The authors demonstrated an easier-to-create and covert attack in this type of network using ARP Spoofing, and analyzed current methods for detecting and mitigating such threats, noting that the attack was not detected. The paper also describes a scenario using IPv6 addressing, in which similar attacks can lead to the depletion of the address pool. The review concludes with a discussion of an anomaly-based detection method for timely recognition of DHCP Starvation attacks and similar threats.

Research [3] includes the development of solutions to ensure network security against attacks on the DHCP protocol. It is noted that the presented methods should be used for all enterprises and organizations that use internal networks to minimize attacks on the network via DHCP. As a result of the study, it is determined that to prevent attacks on DHCP in the network, at least network switches must support the settings presented in the article. The presented solutions and methods can be considered based on the cost and scalability of the network.

Paper [4] identified the main types of attacks on the DHCP protocol and studied the process of detecting them using Python scripts. The authors used Python, Scapy, and GNS3 to model a real network architecture and study the impact of DHCP flooding and Rouge DHCP attacks. This article proposes a method for detecting the DHCP Starvation attack using the Offer packet of the DHCP protocol itself.

The study [5] analyzed the vulnerabilities of the DHCP protocol that can be used in various attacks, including Rogue DHCP server, DHCP starvation, and others. The authors also summarize the existing countermeasures to neutralize or mitigate them and identify the advantages and disadvantages of each of them.

The article [6] describes a new method of implementing the DHCP starvation attack, which is effective in both wired and wireless networks. The authors note that it uses a pre-query performed by a DHCP server, as described in RFC 2131, and checks the IP address offered for exploitation for accidental use by other network clients. The research demonstrates that an attacker can send fake responses to these requests to implement address exhaustion in different types of networks.

In [7] analyze the types of attacks on the network, including Rogue DHCP Server, DHCP starvation, MAC-spoofing, ARP Spoofing, and DOS. The authors also consider ways to secure against each of them.

The study [8] presented a method for detecting and neutralizing potential DHCP Rogue Servers attacks. This paper focuses on developing a method to provide active security for a node running the GNU/Linux operating system. Unauthorized DHCP servers can be located on the same local network as the main one, and thus have the ability to intercept network information and send incorrect routing information to devices. Therefore, the purpose of the study is to prevent this situation by identifying unreliable DHCP servers.

During the analysis of publications on this topic, it was found that they pay little attention to the tools themselves for implementing threats to the DHCP protocol, which is an important element in security networks from attacks. This article, in addition to analyzing the vulnerabilities of the DHCP protocol, provides a step-by-step implementation of the DHCP Starvation and Rogue DHCP Server attacks in a simulated network and demonstrates the reactions of devices before and after their implementation, which makes it possible to understand the weaknesses of the network and choose the right method to eliminate them.

The **purpose** of the article is to study different types of DHCP vulnerabilities and to simulate DHCP Starvation and Rogue DHCP Server attacks on a network created in the GNS3 environment using specialized tools Yersinia and Ettercap.

1.2. Methods

To achieve this goal, we chose the methods of analysis and simulation. The analysis was used to identify the vulnerabilities of the DHCP protocol and their possible consequences. In addition, attacks were simulated using tools such as Yersinia and Ettercap in the GNS3 environment, which allowed us to conduct practical research in a network similar to a real

one, determine the impact on it and, using the results obtained, choose a method of security. The object of research is the DHCP protocol and its vulnerabilities to attacks. The subject of research is methods and tools for modeling attacks on the DHCP protocol in the GNS3 simulation/emulation environment.

2. Results

The DHCP plays a key role in a network because it provides efficient and automated configuration of network settings for connected devices. DHCP allows you to automatically allocate unique IP addresses, which simplifies network management, especially if you have a large number of connected devices and manual configuration is impractical.

When configuring a DHCP server, administrators can easily manage and make changes to the network configurations of devices, not only desktop PCs, but also mobile phones, tablets, and guest devices on the network [9].

In Internet of Things environments, DHCP attacks can play an important role in remotely gaining network access or even affecting the functioning of physical devices [10].

DHCP is an integral part of the network infrastructure, so the growing number of threats in the field of network security necessitates a detailed study of attacks on this protocol and the identification of methods to detect, eliminate, or prevent them.

Potential vulnerabilities that can be exploited by attackers to disrupt the normal operation of the network in which the DHCP server operates include the following:

1. DHCP Starvation is an attack that consists of the attacker sending many more requests for new IP addresses than the DHCP server can process. As a result, the server is overloaded, and legitimate clients connecting to the network cannot receive network parameters. The main goal of the attacker is to overwhelm the server with requests and prevent the normal assignment of IP addresses.
2. DHCP Flood—an attack in which an excessive number of requests (ICMP, UDP, TCP, etc.) are sent to the server to occupy all its resources and prevent it from processing legitimate requests. As a result, the server may respond with long-time delays or even be unavailable for proper processing. This type of attack can cause a Denial of Service (DoS).
3. Rogue DHCP server—an attack that is implemented by installing a malicious DHCP server in the network without the knowledge and permission of the administrator to assign its IP addresses to unauthorized devices and perform various malicious actions (DNS spoofing, man-in-the-middle attack) [11].
4. Disclosure or confidential information—During the exchange of data between the client and the DHCP server, confidential information such as IP addresses, hostnames, etc. may be disclosed. If this data falls into the hands of an attacker, it can create privacy and security issues.

These threats are especially dangerous in corporate networks that need to run smoothly and be secure at all times. Therefore, it is important to understand all the stages of these attacks to see what the impact of such actions will be on the network and determine what needs to be done to secure it [12].

Among the specialized programs and utilities that can be used to implement attacks on the DHCP protocol are the following: Yersinia, Ettercap, DHCPig, dhcpstarv, DHCPwn, and others. They have different functionality and purpose and support different operating systems and protocols. The choice of a particular tool depends on what kind of attack is planned to be implemented and for what purpose [13]. Table 1 shows a comparison of the above-mentioned tools by their main characteristics and capabilities. All tools are free and open source.

In this study, the Yersinia and Ettercap programs were chosen to carry out the DHCP Starvation and Rogue DHCP Server attacks, as they allow working with both Linux and Windows operating systems, although the latter has some limitations.

The next step is to choose a modeling environment. Several options are suitable for the task at hand: Graphical Network Simulator-3 (GNS3), Cisco Packet Tracer, ns-3, OMNeT++. After analyzing the advantages and disadvantages of these simulators/emulators, it was decided to choose GNS3.

Table 1
Main characteristics of tools for implementing attacks on the DHCP protocol

Program	Functionality and usage	OS support	Protocol support
Yersinia	• Emulation of attacks on network protocols • Vulnerability demonstration and analysis • Pentesting	Windows Linux	DHCP, ARP, ICMP, CDP, HSRP, STP
Ettercap	• Network traffic analysis • MITM attack on	Windows Linux	DHCP, ARP, DNS
DHCPig	• Generating DHCP requests to overload the server • DoS testing • vulnerability analysis	Linux	DHCP
dhcpstarv	• Simulation of the DHCP Starvation attack • training and demonstration	Linux	DHCP
DHCPwn	• Generating attacks on the DHCP protocol • Pentesting, testing DoS	Linux	DHCP
Hyenae	• Emulation of network protocol attacks (DoS) • Testing resistance to attack • network traffic analysis	Linux	DHCP, ICMP, UDP, ARP, DNS, TCP
Gobbler	• DHCP and ARP request generation • DoS testing • vulnerability analysis	Linux	DHCP, ARP

GNS3 is a network modeling tool that allows you to create virtual network topologies and emulate the operation of switches, routers, servers, and other devices. An important factor in choosing this environment was its ability to use real operating system images, which allows us to recreate the most realistic network operation possible.

To simulate attacks on the DHCP protocol, a real network topology will be created in GNS3, network devices will be added, their operation will be configured, and Yersinia and Ettercap will be used to launch DHCP starvation and Rogue DHCP Server. The next step is to observe their impact on the network and determine security methods [14–15].

To demonstrate this, it is enough to build a small network consisting of a Cisco router that acts as a DHCP server, a switch, a DNS server, and three workstations: two legitimate ones running Windows and Linux, and one malicious one with tools for carrying out attacks (Fig. 1).

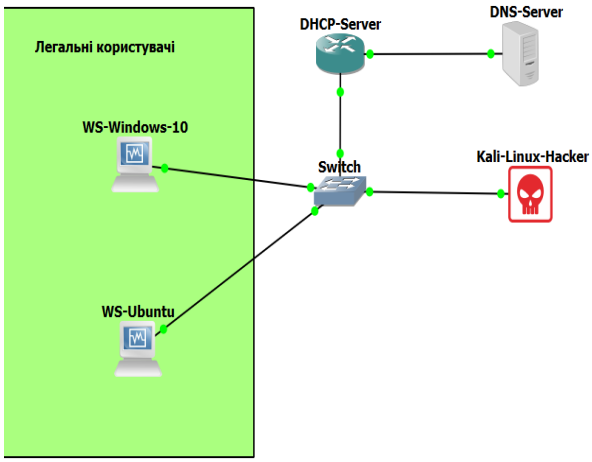
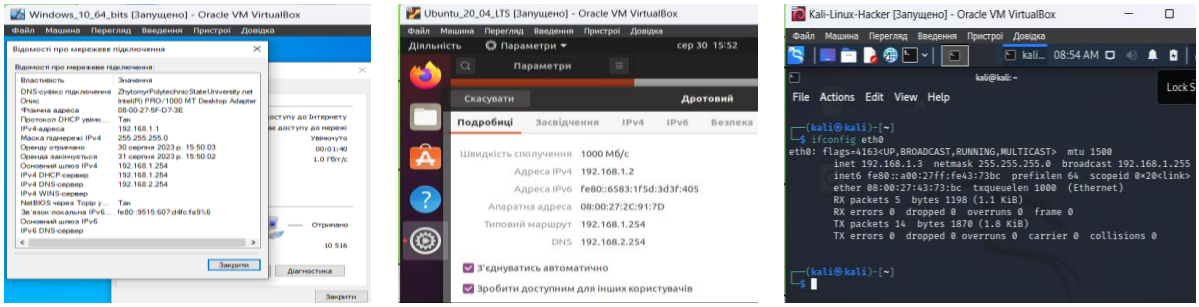


Figure 1: Design of the built network

Set up a DHCP server on the router with addresses from the 192.168.1.1-192.168.1.252 pool. The last address in the range will be assigned to the router interface to which the switch is connected and excluded from the distribution. The test shows that the three workstations have successfully received IP addresses dynamically (Fig. 2). The diagnostic command on the router confirms that the server only issued three addresses to these particular workstations, which is confirmed by the MAC addresses of their network adapters (Fig. 3).

Let's start with the DHCP Starvation attack. The main idea of this attack is to deplete the pool of addresses provided by the DHCP server by

sending a large number of DHCPDISCOVER packets to obtain an IP address with different sender MAC addresses. To do this, launch Yersinia, select the DHCP protocol, and specify “sending DISCOVER packet”. This will result in sending false requests to the server (Fig. 4).



a) b) c)

Figure 2: Dynamic address retrieval by workstations

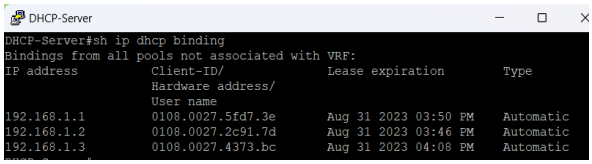
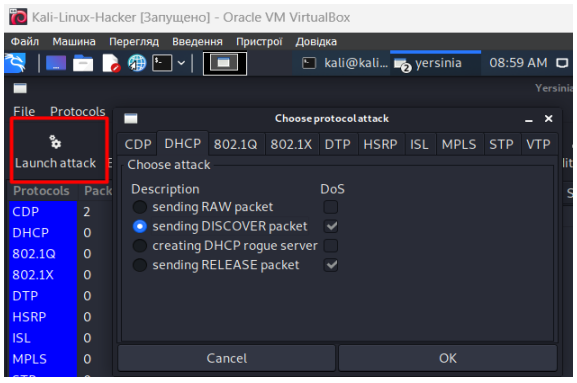
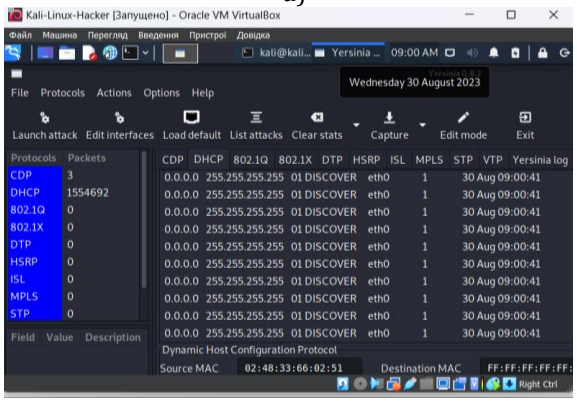


Figure 3: List of addresses issued by the DHCP server



a)



b)

Figure 4: Launching a DHCP Starvation attack with Yersinia’s help

Let’s check how many addresses the DHCP server issued in response to the false requests generated by the attacker. As you can see, all free addresses in the range were reserved (Fig. 5). As long as this activity continues, i.e. as long as DHCPDISCOVER packets are received from the attacker’s workstation, new clients will not be able to receive addressing parameters and will not have access to the network.

To confirm the effectiveness of the attack, let’s try to connect a new workstation and get an IP address for it. The existing workstations will retain the addresses they were originally assigned since the minimum lease time was set to 1 day when the DHCP server was configured.

A new user will not receive an address upon request (Fig. 6a). If, after the attack is stopped, the new user makes another request to the DHCP server from the same workstation after some time, the addressing parameters will be successfully received (Fig. 6b). As you can see, for an attacker to obtain a successful result, the attack must be carried out continuously.

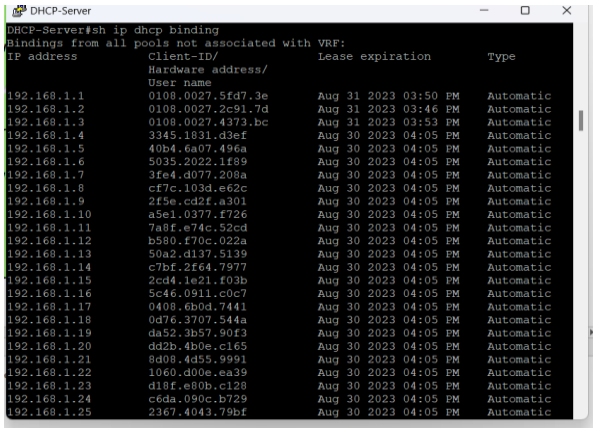
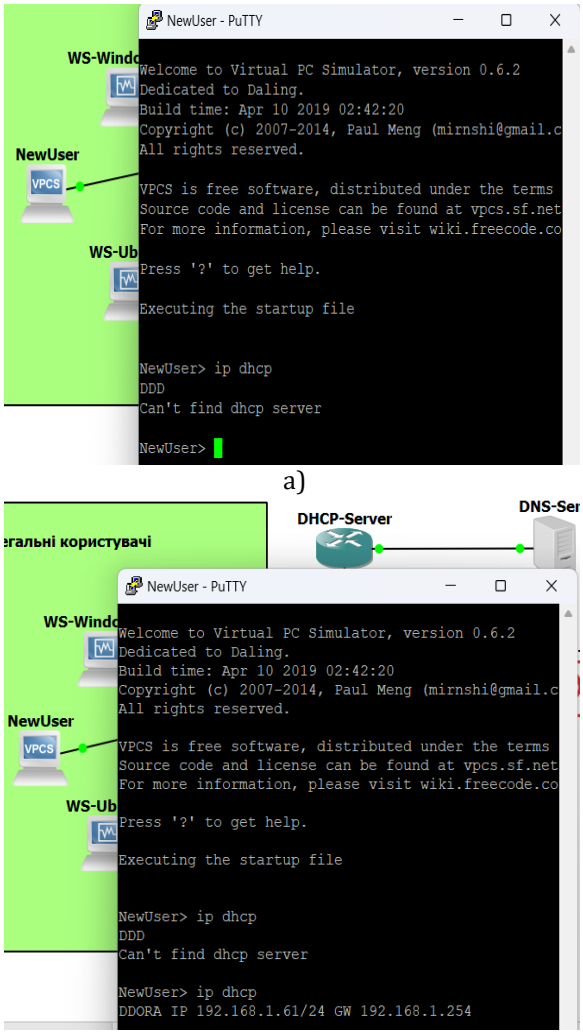


Figure 5: List of addresses issued by the DHCP server after a DHCP Starvation attack



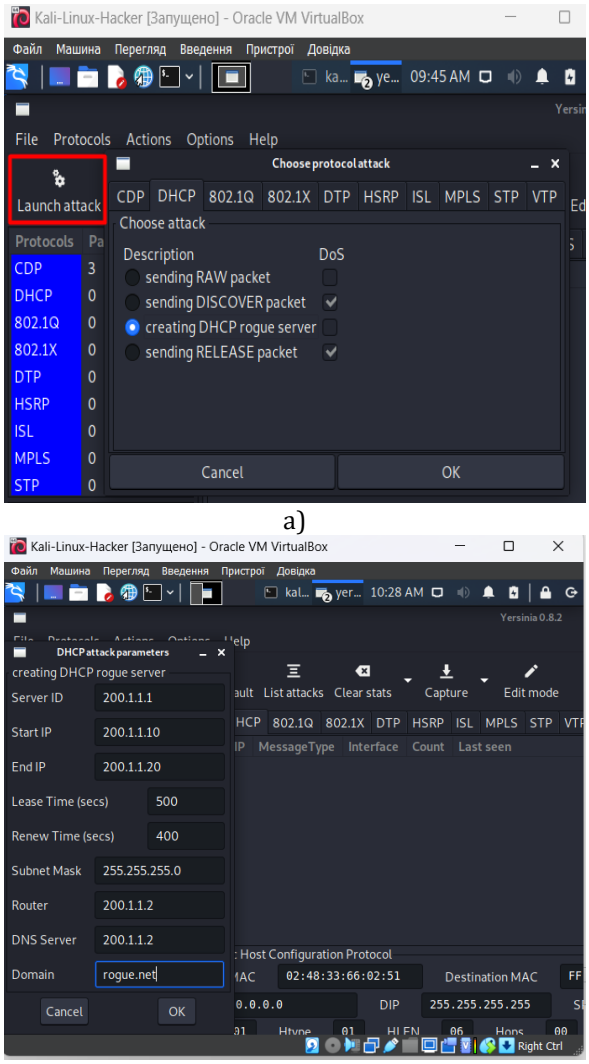
a)

b)

Figure 6: Attempting to obtain an address during the attack(a) and after the attack(s) have ceased(b)

The next attack to be simulated is the Rogue DHCP server. It can be performed either with Yersinia or with Ettercap. Let's try both options. The main goal of this attack is to create a malicious DHCP server that will issue fake addressing parameters to clients. For address requests to be sent to the offender's server, and not the main one, it is enough to simply cause a DoS by overloading it with artificial requests.

For our study, we will statically assign the attacker's workstation the address 200.1.1.1/24. Next, let's run Yersinia (Fig. 7) and Ettercap (Fig. 8), and configure the parameters of the fake DHCP server of the network, on behalf of which offers with IP addresses will be sent to devices.

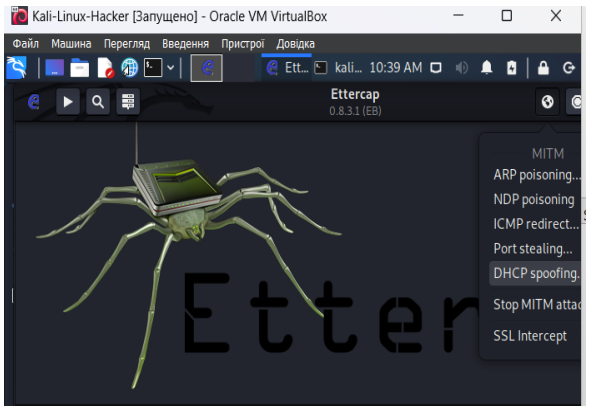


a)

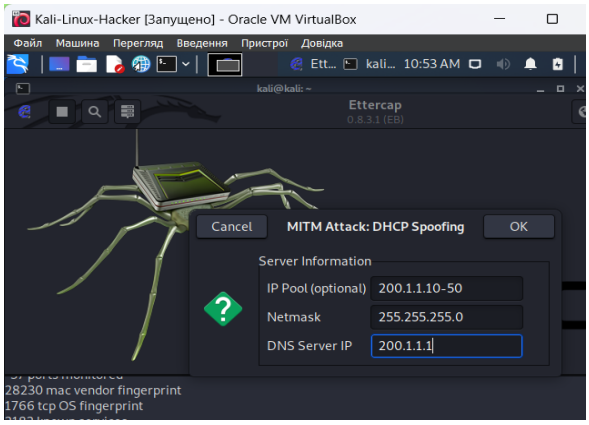
b)

Figure 7: Creating a fake DHCP server in Yersinia

Confirm the settings wait for the first device to connect and send an address request. In the first case, the interface of the new router will receive a fake address, and in the second—a new workstation (Fig. 9).

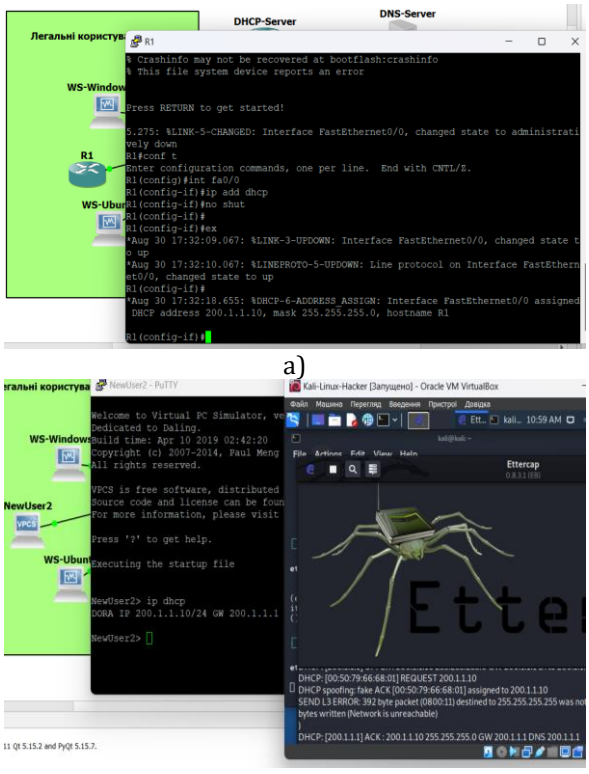


a)



b)

Figure 8: Creating a fake DHCP server in Ettercap



a)

b)

Figure 9: Receiving fake addresses from fake servers created using Yersinia and Ettercap

After the above steps, the attacker can carry out a Man-in-the-Middle attack or other violations using these fake addresses. For example, it is possible to distribute malware among devices in the network or use fake addresses to intercept network traffic containing confidential data.

Having modeled attacks on the DHCP protocol, it is determined that their consequences can be DoS and network unavailability due to excessive server load, security breaches, and loss of control, opening up a potential opportunity for a Man-in-the-Middle attack.

Knowing the vulnerabilities of your network, you can take the following steps to help improve network security:

1. Enable DHCP Snooping on the switches, which allows you to check the legitimacy of DHCP requests and responses in the network.
2. Limit the number of DHCP requests from a single device and configure the DHCP server to allocate addresses only to legitimate clients (for example, by filtering MAC addresses).
3. Install a network monitoring system to detect unusual activity from DHCP servers and a firewall to control Traffic between different parts of the network.
4. Use authentication to prevent untrusted clients from connecting and set up static addressing for important devices.
5. Perform regular updates and install patches to security against known vulnerabilities.

Following these simple recommendations will minimize the possibility of attacks on the DHCP protocol and create a more secure network infrastructure.

3. Conclusion

As a result of detailed modeling of attacks on the DHCP protocol using Yersinia and Ettercap, it was found that the built network has certain vulnerabilities related to insufficient control and security of the internal network infrastructure, and it can be easily accessed by unauthorized persons [16]. Having the ability to connect to the network, an attacker can cause disruption of the legitimate DHCP server or even become a new DHCP server itself and then perform malicious actions. Therefore, to avoid the threat of unauthorized access, you should consider the above recommendations both when building a network and before implementing any changes to network settings. The choice of additional methods depends on the existing network infrastructure and available equipment.

Prospects for further research include a more in-depth analysis of network vulnerabilities related to other protocols and

the development of effective methods of security against them.

References

[1] A. Balyk, et al., Using Graphic Network Simulator 3 for Ddos Attacks Simulation, Int. J. Comput. 16(4) (2017) 219–225.

[2] N. Hubballi, N. Tripathi, A Closer Look into DHCP Starvation Attack in Wireless Networks, Comput. Secur. 65 (2017) 387–404. doi:10.1016/j.cose.2016.10.002.

[3] S. Ali, A. Shareef, DESIGNING A SECURE NETWORK SOLUTION AGAINST DHCP ATTACKS, Iraqi J. Inf. Commun. Technol. 1(1) (2021) 45–57. doi:10.31987/ijict. 1.1.175.

[4] P. Shrestha, T. Sherpa, Dynamic Host Configuration Protocol Attacks and its Detection Using Python Scripts, Int. Conf. Artif. Intell. Knowl. Discov. Concurr. Eng. (2023) 1–5. doi:10.1109/ICECONF5712 9.2023.10084265.

[5] A. AbdulGhaffar, S. Paul, A. Matrawy, An Analysis of DHCP Vulnerabilities, Attacks, and Countermeasures, Bienn. Symp. Commun. (2023) 119–124. doi:10.1109/bsc57238.2023. 10201458.

[6] N. Tripathi, N. Hubballi, Exploiting DHCP Server-Side IP address Conflict Detection: A DHCP Starvation Attack, IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (2015) 1–3. doi:10.1109/ants.2015. 7413661.

[7] A. Savchenko, A. Efimenko, T. Vakaliuk, Varieties of Attacks on the Network and Methods of Protection, Abstracts of the IV All-Ukrainian Scientific and Technical Conference “Computer Technologies: Innovations, Problems, Solutions”, Zhytomyr Polytechnic, Zhytomyr (2021) 27–28.

[8] M. Makarova, A. Maksutov, Methods of Detecting and Neutralizing Potential DHCP Rogue Servers, IEEE Conf. Russian Young Res. Electr. Electron. Eng. (2021) 522–525. doi:10.1109/elconrus51938. 2021.9396106.

[9] Y. Sadykov, et al., Technology of Location Hiding by Spoofing the Mobile Operator IP Address, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 22–25. doi: 10.1109/UkrMiCo52950.2021.9716700

[10] N. Lobanchykova, I. Pilkevych, O. Korchenko, Analysis and Protection of IoT Systems: Edge Computing and Decentralized Decision-Making, J. Edge Comput. 1(1) (2022) 55–67. doi:10.55056/jec.573.

[11] A. Mikhailov, Attacks on the DHCP Protocol: DHCP Starvation, DHCP Spoofing, and Protection Against These Techniques. URL:https://hackmag.com/ security/dhcp-hacking/

[12] M. Vladymyrenko, et al., Analysis of Implementation Results of the Distributed Access Control System. in: 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (2019). doi: 10.1109/picst47496.2019.9061376

[13] Infosavvy Cyber Security & IT Management Trainings, Sniffing Technique: DHCP Attacks (2020). URL: https://infosavvy.home.blog/2020/03/ 02/sniffing-technique-dhcp-attacks/

[14] I. Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, vol. 11660 (2019) 16–27. doi: 10.1007/978-3-030-30859-9_2

[15] P. Anakhov, et al., Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 169–176.

[16] P. Anakhov, et al., Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network, Journal of Theoretical and Applied Information Technology 100(22) (2022) 6635–6644.