Bit-Tech (Binary Digital - Technology)
Vol.6, No.3, April 2024
Available online at: http://jurnal.kdi.or.id/index.php/bt

Implementation of DHCP Snooping Method to Improve Security on Computer Networks

Andi Purnomo[1]

[1]Sekolah Tinggi Ilmu Manajemen dan Ilmu Komputer ESQ / Computer Science Department
[1]TB Simatupang, Jakarta Selatan, Indonesia
[1)]andi.purnomo@esqbs.ac.id

Article history:

Received 04 March 2024;
Revised 07 March 2024;
Accepted 19 March 2024;
Available online 30 April 2024

Keywords:

Computer Network
DHCP Snooping
Network Security
Trusted Port
Untrusted Port

Abstract

This research proposes the DHCP Snooping method which is used to increase security on computer networks because Dynamic Host Configuration Protocol (DHCP) is a potential target for computer network attacks, one of the attack gaps that can occur in DHCP is the DHCP Rogue attack which is the simplest hacking method in which the attacker creates a fake DHCP connected to the core network allowing the hacker to set up a fake DHCP Server with full access to distribute IP addresses to clients. To address security gaps in computer networks in this research, researchers applied the DHCP Snooping method, which is a series of techniques to improve DHCP network security. When the DHCP server allocates IP addresses to clients on the LAN, DHCP Snooping can be configured on the LAN switch to allow only clients with certain IP and MAC addresses to have access to the network. By implementing the DHCP Snooping method you can increase security on computer networks where DHCP Snooping can distinguish which ports can be trusted (Trusted Port) and which ports cannot be trusted (Untrusted Port) so that the security of data and information in the computer network is maintained properly. Based on the results of this research, DHCP Snooping can prevent clients from getting DHCP IPs from DHCP Rouge because it has determined Trusted Port and Untrusted Port.

I. INTRODUCTION

The development of information technology is currently growing very rapidly, marked by the existence of various types of computers that are connected to each other so that they can provide convenience for users. Every computer definitely needs a computer network which has become a critical infrastructure that supports communication and information exchange throughout the world. The rapid growth in use of Computer Networks, including increases in the number of connected devices and the volume of data transmitted, has encouraged ongoing research in various aspects of computer networks.

A computer network is a collection of devices connected to each other, allowing users to exchange information in the form of sound, video, images and Internet connections [2]. According to APJII (Association of Indonesian Internet Service Providers), in 2023 the number of Indonesian people connected to the internet will reach 215.62 million people out of a total population of 275.77 million Indonesians, meaning that 78.19% of Indonesia's population is connected to the internet. In recent years, computer networks have become an important component in various fields, including business, education, health, and communications. The rapid growth of information and communication technology has encouraged the development and use of increasingly complex computer networks.

Computer networks are very important for an agency because they really support the process of exchanging information and communication. In this process, of course you need a network service to get an Internet Protocol (IP) Address. Handling IP addresses will waste a lot of time and energy because you have to configure them one by one, therefore we need a technology that can distribute IP addresses to users automatically. The technology that can support automatic IP address sharing is Dynamic Host Configuration Protocol (DHCP)[2]. The DHCP IP provided is a Dynamic IP, whereas if the IP is assigned manually it is called a Static IP[15].

However, DHCP is a potential target for network attacks, one of the attack gaps that can occur on a DHCP server is a DHCP Rogue attack which is the simplest hacking method where the attacker creates a fake DHCP that is connected to the core network, allowing the hacker to set up a fake DHCP Server with access. full to distribute IP addresses to clients, and not just IP Addresses, the attacker also replaces the original Gateway IP and Domain

ISSN 2622-2728 (online) 2622-271X (print)
doi: 10.32877/bt.v6i3.1174

Name Server (DNS) IP with a Gateway IP and DNS IP that he created himself to then distribute to clients who make IP Address requests to DHCP Server[1].

Therefore, there is a need to increase network security to prevent attacks on computer networks because the main goal of computer network security is to protect information on the network. According to (Lede et al, 2022) if a client gets a DNS IP from a fake DHCP, the attacker can carry out an attack called phishing by sending a fake website, so that the client's computer fills in real data, then the data entered will be recorded for use by the attacker. Internet access on the network often experiences difficulties caused by attacks on servers run by unauthorized users due to poor network security.

Researchers want to use the DHCP Snooping technique on LAN switches in this study to address security flaws in computer networks and enhance network security. A set of methods called "DHCP Snooping" is used to increase the security of DHCP networks. DHCP snooping can be set up on the LAN switches to restrict network access to clients with specific IP and MAC addresses when the DHCP Server assigns IP addresses to LAN clients. IP addresses and their related MAC addresses are recorded in a switch database through DHCP snooping [8].

Researchers hope that the application of the DHCP Snooping method can improve security on computer networks where DHCP Snooping can distinguish which ports can be trusted (Trusted Port) and which ports cannot be trusted (Untrusted Port) so that the security of data and information in computer networks is maintained properly.

II. Related Works/Literature Review

A service called Dynamic Host Configuration Protocol (DHCP) gives a computer or client that requests one an IP address automatically. A DHCP Server is a computer that distributes IP addresses, and a DHCP Client is a computer that requests IP addresses. In this manner, network managers can configure TCP/IP by just providing a reference to the DHCP Server instead of manually providing IP addresses [4].

DHCP snooping is a term used to describe a collection of methods used in computer networking to increase a DHCP network's security. DHCP snooping can be set up on the LAN switches to restrict network access to clients with particular IP and MAC addresses when a DHCP server assigns IP addresses to clients on a LAN. In Layer 2 switched domains, IP integrity can be guaranteed using DHCP snooping. [6]. DHCP Snooping works like a firewall where its main function and task is to distinguish between trusted IP sources and untrusted sources[11].

A layer 2 security mechanism called DHCP Snooping can stop rogue DHCP servers from giving clients on the network harmful information. When DHCP Snooping is used at every network layer, it can be a very helpful tool for safeguarding sensitive data and preventing assaults on the network architecture. In order to control access to IP addresses that have been registered on the router and stop attackers from accessing or entering the network, DHCP Snooping is primarily used. More generally, ARP Man in the Middle attacks, DHCP packet flooding attacks, IP/MAC spoofing attacks, and unauthorized DHCP server assaults can all be avoided with DHCP snooping [10]. DHCP starvation attack and setting up a rogue DHCP server, the attacker can start distributing IP addresses and other TCP/IP configuration settings to the network DHCP clients. TCP/IP configuration settings include Default Gateway and DNS Server IP addresses[14].

Unlike LANs, which are restricted to a certain physical location, VLANs allow for virtual network configuration, independent of a device's physical location. By using VLANs, the network configuration can be divided into departments or organizations rather than relying just on the workstation's location[16].

Cisco Packet Tracer is an application produced by the San Francisco, California-based Cisco company. Cisco was founded in 1984. Cisco Packet Tracer is a simulation tool for learning computer networks, especially those related to Cisco products. With the Cisco Packet Tracer tool, simulated network data can be used to provide information about the connection status of a machine in a network in the event that an issue with the connections occurs [9].

There are various kinds of threats to the network security of an institution which can result in the loss of valuable information held by the institution. The following are several threats to network security according to [4].

Interruption It is a threat to the availability of information, the data in the computer system is damaged or deleted so that if the data or information is needed, the owner will have difficulty accessing it, the information may even be lost. An example is damage/modification to hardware or network channels.

Interception it is a threat to confidentiality. Information is intercepted so that unauthorized people can access the computer where the information is stored. An example is tapping data on a network.

Modifications it is a threat to integrity. An unsuccessful person intercepts the information traffic that is being sent and then changes it according to that person's wishes. Examples include changing values in data files, modifying programs so that they run incorrectly, and modifying messages that are being transmitted on a network.

Fabrication it is a threat to integrity. Unauthorized people succeed in imitating or falsifying information so that the person receiving the information thinks that the information comes from the person the recipient of the information wants. An example is sending fake messages to other people.

III. METHODS

Research requires clear, orderly and systematic stages, so that the research can be achieved in accordance with its objectives.

1. Identify the Problem
   In the initial stage, it begins with determining the topic of discussion by looking for problems that occur in the surrounding area and that can be solved using methods that have been studied in computer science. After determining the topic to be researched, the background to the problem needs to be identified and stated in the problem formulation. Carrying out this stage aims to ensure that this research focuses on the main problem only. At this stage, the objectives and benefits obtained from the results of this research will also be explained.
2. Literature Study
   Literature study, which is carried out by looking for theoretical references, previous research and methodology that are relevant to the case or problem found.
3. Topology Design
   Topology Design functions to get an idea of how devices on a computer network are connected to each other. Topology design uses Cisco packet tracer, the topology design used in this research can be seen in Figure 1.

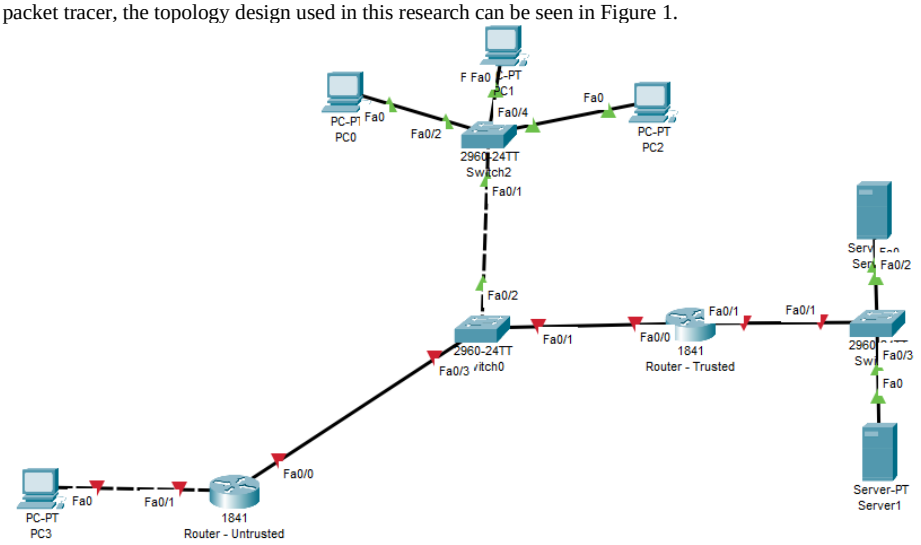

Fig *1*. Network Topology

4. Configure Switch and Router Devices
   In the topology design which can be seen in Figure 3, the Switch will be configured with VLAN without DHCP Snooping and the Router will be configured with a DHCP Server to provide IP to the PC and Server.
5. Configure DHCP Snooping
   After carrying out the basic configuration, the next step will be to configure DHCP Snooping on the Switch.
6. DHCP Snooping Testing
   After DHCP Snooping has been configured, the next step will be to test whether the PC and server can still get IP distribution from DHCP Server – Untrusted.

From the topology design which can be seen in Figure 1, each device will have an IP address configured, along with the distribution of IP addresses which can be seen in Table 1.

TABLE 1
IP ADRESS CONFIGURED

Device	Port	IP Address	Subnetmask	Gateway
Router – Trusted	FastEthernet0/0	192.168.1.1	255.255.255.0	192.168.1.1
	FastEthernet0/1	192.168.2.1	255.255.255.0	192.168.2.1
PC		DHCP	255.255.255.0	192.168.1.1
Server		DHCP	255.255.255.0	192.168.2.1
Router – Untrusted	FastEthernet0/0	192.168.10.1	255.255.255.0	192.168.10.1
	FastEthernet0/1	192.168.20.1	255.255.255.0	192.168.20.1
PC		DHCP	255.255.255.0	192.168.10.1

IV. RESULTS

A. Configure DHCP Server on Router – Trusted

Configure DHCP Server on Router - Trusted, on FastEthernet port 0/0 with Network IP 192.168.1.0 & Gateway IP 192.168.1.1 which will later provide DHCP IP to PC0, PC1 & PC2 will get an IP address between 192.168.1.2 – 192.168.1.254 as follows.

```
Router#configure terminal
Router(config)#service dhcp
Router(config)#ip dhcp pool pool1
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.1
Router(dhcp-config)#exit
```

After configuring the DHCP Server on FastEthernet port 0/0, a test will be carried out on PC0 to see whether it is successful in getting a DHCP IP originating from the Trusted Router which can be seen above.

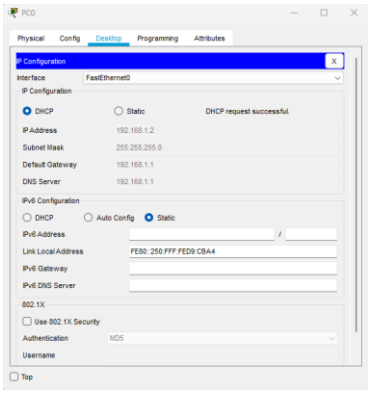

Fig 2. PC0 Server DHCP Testing

After testing the DHCP Server on PC0, it gets the IP Address 192.168.1.2, then after getting the IP Address, then carry out the test by pinging the gateway 192.168.1.1. If the result of pinging the gateway is a reply, then the test is successful, which can be seen in Figure 3.

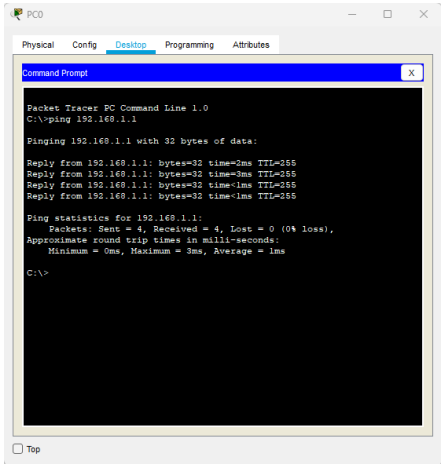

Fig 3. PC0 Connection Testing to gateway

After configuring the FastEthernet 0/0 port, the next step will be to configure the DHCP Server on the FastEthernet 0/1 port with Network IP 192.168.2.0 & Gateway IP 192.168.2.1 to provide a DHCP IP to Server0 & Server1, which will then get an IP address between 192.168.2.2 – 192.168.2.254 which can be seen below.

```
Router(config)#ip dhcp pool pool2
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 192.168.2.1
Router(dhcp-config)#exit
```

After configuring the DHCP Server on FastEthernet port 0/1, a test will be carried out on Server0 to see whether it is successful in getting the IP Address 192.168.2.2 which comes from the Router - Trusted which can be seen in figure 4.

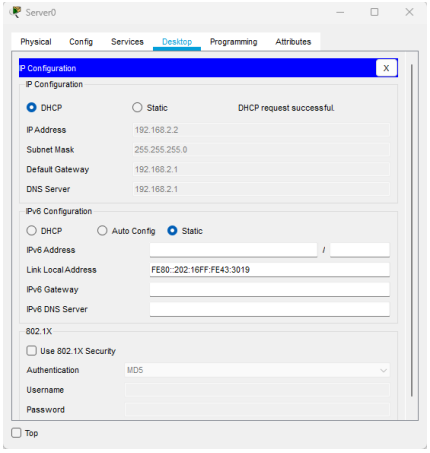

Fig 4. DHCP Server0 Testing

After testing the DHCP Server on the Server, it gets the IP Address 192.168.2.2, then after getting the IP Address, then carry out the test by pinging the gateway 192.168.2.1. If the result of pinging the gateway is a reply then the test is successful which can be seen in Figure 5.

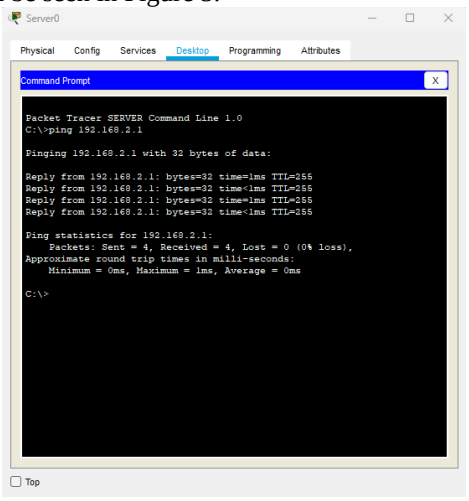

Fig 5. Server0 Connection Testing to the gateway

B. DHCP Server Router Configuration - Untrusted

Configure router-untrusted on FastEthernet port 0/0 with Network IP 192.168.10.0 & Gateway IP 192.168.10.1, which will later be used to carry out DHCP Snooping testing to see whether it can detect giving fake IP addresses to PCs 0,1 and 2 with IP range 192.168 .10.2 – 192.168.10.254 which can be seen below.

```
Router(config-if)#service dhcp
Router(config)#ip dhcp pool poolfalse
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 192.168.10.1
Router(dhcp-config)#exit
```

After configuring DHCP Server False on FastEthernet port 0/0, a test will be carried out on PC0 to see whether it is successful in getting the IP Address 192.168.10.2 which comes from the Router - untrusted which can be seen above.

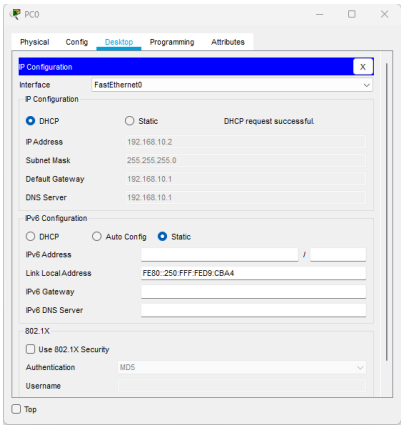

Fig *6*. Testing DHCP Server False to PC0

Can be seen in table 2, PC0 initially got the IP DHCP from the trusted router after configuring the untrusted router for the dhcp server, PC0 got the IP address from the untrusted router which PC0 should have gotten the DHCP IP from the trusted router

TABLE 2
CONFIGURE IP-ADDRESS BEFORE USING DHCP-SNOOPING

Device	Port	IP Adress	Subnetmask	Gateway
Router-Trusted	FastEtehernet0/0	192.168.1.1	255.255.255.0	192.168.1.1
	FastEtehernet0/1	192.168.2.1	255.255.255.0	192.168.2.1
Router-Untrusted	FastEtehernet0/0	192.168.10.1	255.255.255.0	192.168.10.1
	FastEtehernet0/1	192.168.20.1	255.255.255.0	192.168.20.1
PC0		192.168.10.1	255.255.255.0	192.168.10.1
Server0		192.168.2.2	255.255.255.0	192.168.2.1

C. DHCP Snooping Configuration

DHCP Snooping configuration is carried out on switch 0, with the aim that later PC0, PC1 and PC2 will only get IP from Router - Trusted with the IP Address range 192.168.1.2 - 192.168.1.254 which can be seen below.

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#int fa 0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config)#int fa 0/2
Switch(config-if)#ip dhcp snooping trust
```

V. DISCUSSION

In the configuration below, it is used to determine that the FastEthenet 0/0 port and FastEtheher 0/1 port on switch 0 are trusted ports, where the path passed by FastEthernet 0/1 and FastEthernet 0/2 is a trusted interface that can provide IP DHCP and FastEtehernet 0/3 cannot provide IP DHCP which can be seen in figure 7.

```
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/3            no         unlimited
FastEthernet0/2            yes        unlimited
FastEthernet0/1            yes        unlimited
Switch#
```

Fig 7. Trusted Port determination results

Next, we carried out another test on PC0 which previously got a DHCP IP from the untrusted router which can be seen in Table 3. After configuring DHCP Snooping, PC0 currently only gets IP addresses from ports that have been declared Trusted, namely FastEthernet 0/1 and FastEthernet ports. 0/2 which can be seen in Figure 8 that PC0's DHCP IP comes from Router-Trusted.

TABLE 3
CONFIGURE IP-ADDRESS AFTER USING DHCP-SNOOPING

Device	Port	IP Adress	Subnetmask	Gateway
Router-Trusted	FastEtehernet0/0	192.168.1.1	255.255.255.0	192.168.1.1
	FastEtehernet0/1	192.168.2.1	255.255.255.0	192.168.2.1
Router-Untrusted	FastEtehernet0/0	192.168.10.1	255.255.255.0	192.168.10.1
	FastEtehernet0/1	192.168.20.1	255.255.255.0	192.168.20.1
PC0		192.168.1.1	255.255.255.0	192.168.10.1
Server0		192.168.2.2	255.255.255.0	192.168.2.1

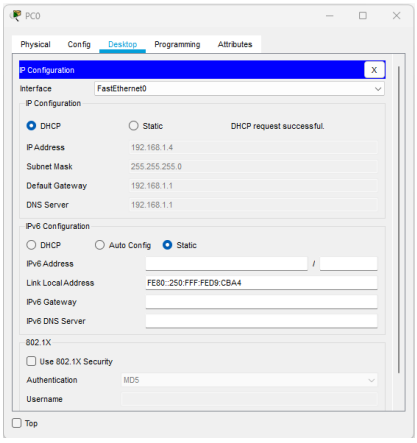

Fig 8.DHCP Snooping Testing on PC0

VI. CONCLUSIONS

Based on the tests carried out in chapter IV, it can be concluded that DHCP Snooping can improve computer network security by distinguishing Trusted ports and Untrusted Ports which have been determined in the switch configuration port FastEthernet 0/1 and port FastEthernet 0/2 as Trusted port and port FastEthernet 0/3 as Not Trusted port which can be seen in Figure 7. After configuring DHCP Snooping, testing is carried out on PC0 which can be seen in table 2, before configuring DHCP Snooping PC0 can still get the IP Address from the Router-Untrusted , while PC0 should only get the IP Address from the Router-Trusted. However, after DHCP Snooping configuration which can be seen in table 3, PC0 has received an IP Address from Router-Trusted. DHCP Snooping on layer 2 switches in the future can still be further developed and the DHCP Snooping method applied to strengthen the security of layer 2 switches.

REFERENCES

[1] Dara YC, Hariadi F, Lede PA. Analisis Penerapan Sistem Keamanan Jaringan Menggunakan Metode Dhcp Snooping Dan Switch Port Security. JURNAL TEKNIK INFORMATIKA INOVATIF WIRA WACANA. 2023 May 16;1(3):187-96.

[2] Ariyadi T, Riyansyah AN, Agung M, Ikrar MA. Analisis ANALISIS SERANGAN DHCP STARVATION ATTACK PADA ROUTER OS MIKROTIK. JURNAL ILMIAH INFORMATIKA. 2023 Mar 10;11(01):85-93.

[3] Sulaiman OK. Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security. CESS (Journal Of Computer Engineering, System And Science). 2016 Jan;1(1):9-14.

[4] Tamsir Ariyadi T. Desain keamanan DHCP snooping untuk mengurangi serangan Local Area Network (LAN). Jurnal Sistem Komputer Musi Rawas (JUSIKOM). 2017;2(01):28-36.

[5] ANOM, I. G. K. SISTEM AUTENTIKASI PROVISIONING JARINGAN WIRELESS MELALUI DHCP SERVER DENGAN MENGGUNAKAN LAYANAN PESAN.

[6] Tarkaa NS, Iannah PI, Iber IT. Design and simulation of local area network using cisco packet tracer. The International Journal of Engineering and Science. 2017;6(10):63-77.

[7] Marcus RD, Rosyadi HE, Pamuji FY, No JT, Klojen PC. Prototype Sistem Administrasi Dan Keamanan Jaringan Komputer Berbasis DHCP Server Mikrotik. Briliant: Jurnal Riset dan Konseptual. 2021 Aug 31;6(3):685-95.

[8] Puspasari L, Rasmila R. IMPLEMENTASI DHCP SNOOPING TRUST DAN LIMIT RATE DENGAN METODE ACTION RESEARCH. InProsiding Seminar Hasil Penelitian Vokasi (Semhavok) 2019 (Vol. 1, No. 1, pp. 87-94).

[9] Miftah Z. Simulasi keamanan jaringan dengan metode DHCP SNOOPING dan VLAN. Faktor Exacta. 2018;11(2):167.

[10] Pradana DA, Budiman AS. The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack. IJID (International Journal on Informatics for Development). 2021;10(1):38-46.

[11] Medianto, Medianto. "Analisis Keamanan Jaringan Local Area Network yang Menggunakan DHCP Server Berbasis Cisco dengan metode Penetration Testing." *Journal of Information System and Technology (JOINT)* 1.1 (2020): 100-124.

[12] Buamona, Nur Qamar, Mustamin Hamid, and Erwin Gunawan. "Analisis Dan Implmentasi Keamanan Jaringan Menggunakan Metode DHCP Snooping dan Swirch Port Security." *Jurnal Teknik Informatika (J-Tifa)* 6.1 (2023): 23-31.

[13] Akashi, Shigeo, and Yao Tong. "Classification of DHCP spoofing and effectiveness of DHCP Snooping." *Proceedings on 2018 International Conference on Advances in Computer Technology, Information Science and Communication, edited by Wen-Bing Horng and Yong Yue*. 2019.

[14] Alsaadi, Rawya Raed, and Dalael Saad Abdul-Zahra. "SECURITY DHCP SERVER ON LAN NETWORK." *Turkish Journal of Physiotherapy and Rehabilitation* 32: 3.

[15] Bayu, Teguh Indra, and Nurhanif Nurhanif. "Model Keamanan pada Virtual Local Area Network (VLAN) untuk Mengatasi DHCP Rogue." *Indonesian Journal of Computing and Modeling* 1.2 (2018): 55-60.

[16] Rominton, Muhamad Agung, Ahmad Heryanto, and Adi Hermansyah. "Perancangan Inter Vlan Routing Pada Juniper Switch: Perancangan Inter Vlan Routing Pada Juniper Switch." *Journal of Network and Computer Applications (ISSN: 2964-6669)* 1.2 (2022): 1-12.