JOURNAL OF INFORMATICS AND COMPUTING (RANDOM)
Vol. 2, No. 1 (Tahun 2023), Hal. 48 - 54

PENGGUNAAN METODE DHCP SNOOPING DALAM MELAKUKAN PENCEGAHAHAN TERHADAP DHCP ROGUE PADA LABORATORIUM TEKNIK INFORMATIKA

Willy Permana Putra[1*], Muhamad Zulfikar Azis[2]

[1,2]Program Studi Rekayasa Perangkat Lunak, Jurusan Teknik Informatika, Politeknik Negeri Indramayu
*Email: willy@polindra.ac.id

INFORMASI ARTIKEL

Diajukan:
24 Agustus 2022
Direvisi:
5 April 2023
Diterima:
31 Mei 2023

Kata kunci:

DHCP Snooping
DHCP Rogue
Keamanan Jaringan
Laboratorium
Wireshark

Abstrak

Koneksi jaringan memiliki peran penting bagi masyarakat khususnya bagi mahasiswa Politeknik Negeri Indramayu Jurusan Teknik Informatika. yang berfungsi untuk membantu kegiatan pratikum, yang dilakukan pada Laboratorium Jurusan Teknik Informatika. DHCP Rogue merupakan ancaman yang bisa terjadi pada suatu jaringan, yang dimana dapat membelokan paket data yang melintas. Tindakan ini bisa dilakukan oleh orang yang tidak bertanggung jawab. Oleh karena itu perlu adanya keamanan jaringan untuk mencegah ancaman dari DHCP Rogue, untuk mengatasi masalah tersebut diperlukanya metode DHCP Snooping yang digunakan untuk mencegah adanya DHCP Rogue pada jaringan. Mengingat ancaman tersebut, dilakukanya beberapa tahapan dengan mengkonfigurasi DHCP Snooping, konfigurasi DHCP server, dan Monitoring jaringan menggunakan aplikasi Wireshark. Yang di implementasikan pada Laboratorium Teknik Informatika, untuk menjaga paket data yang melintas, dan bisa mengetahui jika ada DHCP Rogue dalam jaringan. Pada artikel ini, hasil dari pencegahan DCHP Rogue bisa ditangani dengan menggunakan metode DHCP Snooping melalui hasil testing, dan monitoring pada jaringan.

USE OF THE DHCP SNOOPING METHOD IN DOING PREVENTION OF DHCP ROGUE IN LABORATORIES INFORMATICS ENGINEERING

ARTICLE INFORMATION

Submitted:
24 August 2022
Received:
5 April 2023
Accepted:
31 May 2023

Keywords:

DHCP Snooping
DHCP Rogues
Network Security
Laboratory
Wireshark

Abtract

Network connection has an important role for the community, especially for students of the Indramayu State Polytechnic Department of Informatics. which serves to assist practical activities, which are carried out at the Informatics Engineering Department Laboratory. DHCP Rogue is a threat that can occur on a network, which can deflect data packets that pass. This action can be done by an irresponsible person. Therefore, there is a need for network security to prevent threats from DHCP Rogue, to overcome this problem, a DHCP Snooping method is needed to prevent DHCP Rogue on the network. Given the threat, he carried out several stages by configuring DHCP Snooping, configuring the DHCP server, and monitoring the network using the Wireshark application. Which is implemented at the Informatics Engineering Laboratory, to maintain data packets that pass, and can find out if there is a DHCP Rogue in the network. In this article, the results of preventing DCHP Rogue can be handled using the DHCP

p-ISSN 2986-1942
e-ISSN 2986-1187

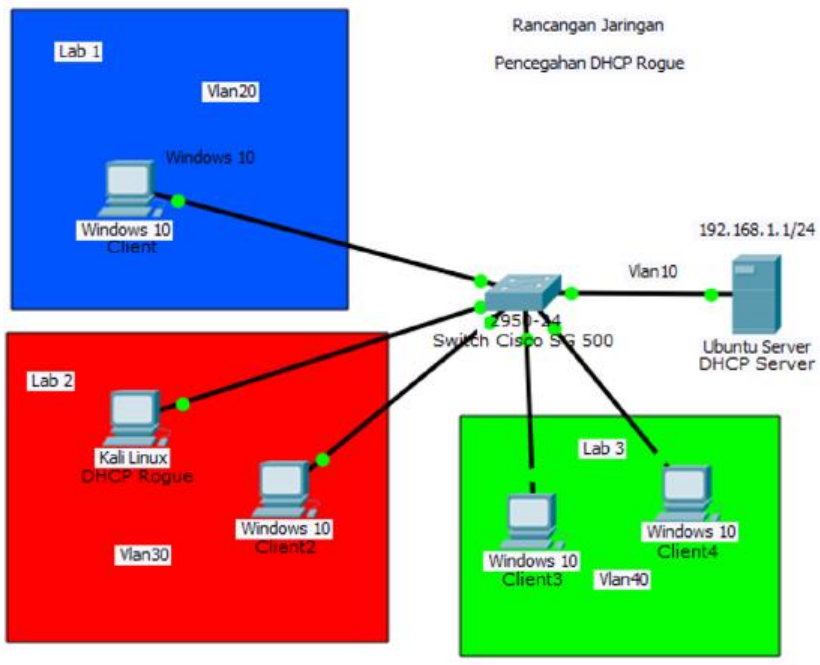
Snooping method through testing results, and monitoring on the network.

PENDAHULUAN

Pada saat ini, perkembangan teknologi begitu pesat. Hal tersebut dibuktikan dengan semakin maraknya penggunaan internet di dunia digital. Perkembangan teknologi ini sangat menguntungkan bagi manusia, karena tujuan utama dari perkembangan teknologi yaitu untuk memudahkan manusia dalam menyelesaikan pekerjaannya. Penggunaan teknologi di dunia digital harus terhubung dengan jaringan internet. Internet (*interconnected networking*) merupakan sebuah hubungan antara berbagai jenis komputer dan jaringan di dunia yang berbeda sistem operasi maupun aplikasinya, di mana hubungan tersebut memanfaatkan kemajuan media komunikasi (telepon dan satelit) yang menggunakan protokol standar dalam berkomunikasi (Gani, 2017). Internet sering digunakan dalam kegiatan-kegiatan antara lain media pembelajaran, media sosial maupun media berita dan masih banyak lagi. Kegiatan ini dapat dilakukan di mana saja bahkan di beberapa tempat kafe atau restoran atau tempat-tempat publik yang menyediakan *WiFi* gratis. Semakin banyak pengguna internet semakin mudah kita mendapatkan informasi semakin banyak pula peluang-peluang tindakan pencurian data dalam dunia digital. Internet juga merupakan salah satu akses terjadinya sebuah kebocoran informasi yang dilakukan oleh orang-orang yang tidak bertanggung jawab, seperti *hacker*. Hal ini juga ditambah pengguna internet yang tidak memahami seluk-beluk jaringan internet, Ketika perangkat terhubung dengan internet tidak memikirkan jaringan ini aman atau tidak, momen inilah yang sering terjadi yaitu kita tidak tahu bahwa koneksi kita aman atau tidak ini bisa saja terjadi serangan *DHCP Rogue*, *DHCP Rogue* yaitu *DHCP Server* palsu yang memberikan alamat *gateway* palsu pada klien yang akan meminta alamat IP supaya bisa terkoneksi dengan internet. Serangan inilah yang sering disalah gunakan oleh orang yang tidak bertanggung jawab, oleh karena itu keamanan dalam jaringan harus ada salah satunya adalah peningkatan keamanan *DHCP Snooping* yang akan membatu dalam mengatasi proses *DHCP* palsu ini.

METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini pada tahap awal menggunakan software simulasi *Cisco Packet Tracer 8.2.* Adapun topologi yang digunakan dalam penelitian ini sebagai berikut:



Gambar 1. Desain Jaringan

Pada gambar 1 merupakan sebuah tahap awal perancangan dan pembuatan desain jaringan yang akan dibangun. Tahap ini bertujuan untuk memberikan gambaran yang seharusnya dikerjakan, serta membantu dalam menspesifikasikan kebutuhan *hardware* dan *software* dan mendefinisikan arsitektur sistem secara keseluruhan, Simulasi Prototyping Pada Gambar 1 merupakan sebuah tahap pembuatan prototype sistem sesuai dengan desain yang telah dibuat, sebagai simulasi rancangan sistem pencegahan DHCP Rogue pada jaringan yang akan dibangun, Tahapan - tahapannya yaitu:

1. Konfigurasi interfaces
2. Konfigurasi DHCP sever
3. Pengecekan IP pada komputer client
4. Konfigurasi switch SG500
5. Testing
6. Monitoring

Pada tahap implementasi ini penulis membagi tahap menjadi dua bagian, yaitu konfigurasi dan pengujian jaringan yang meliputi proses instalasi dan konfigurasi terhadap rancangan topologi jaringan yang akan dibangun, untuk yang akan dikonfigurasi ada IP static pada ethernet server, *DHCP server*, *DHCP Snooping* pada switch Cisco SG 500, konfigurasi VLAN dengan membuat VLAN10 akan digunakan pada server, VLAN20 digunakan pada Lab Sistem Operasi, VLAN30 digunakan pada Lab Rekayasa perangkat lunak, VLAN40 digunakan pada Lab Jarkom, dan VLAN 50 digunakan pada Lab Pemrograman, yang dikonfigurasi pada port yang ada pada *switch*, dan Testing jaringan menggunakan *tools Ettercap* yang dimiliki Kali Linux untuk melakukan *DHCP Rogue*.
Proses implementasi yang dilakukan dengan tahapan sebagai berikut:

1. Pengecekan IP pada komputer client
2. Konfigurasi Switch SG500
3. Testing
4. Monitoring

Tahap Monitoring ini merupakan sebuah tahapan untuk memastikan bahwa jaringan yang telah dibangun sudah sesuai dengan kebutuhan dan dapat mencegah terjadinya peretasan yang dilakukan menggunakan *DHCP Rogue.*

Tahap Management ini merupakan sebuah tahap final. Pemeliharaan dalam tahap ini mencakup proses untuk memperbaiki kesalahan yang tidak ditemukan pada Langkah sebelumnya. Perbaikan implementasi unit jaringan dan monitoring jaringan yang sudah diamankan agar bisa lebih maksimal lagi terhadap pengamanan jaringan yang sudah di implementasikan pada Lab Informatika Politeknik Negeri Indramayu.

HASIL DAN PEMBAHASAN

1. Hasil

Pada tahap ini adalah tahap pembahasan dari hasil implementasi yang penulis kerjakan, dari analisa dan rancangan sampai tercipta pencegahan serangan *DHCP Rogue* dengan menggunakan *DHCP Snooping*.

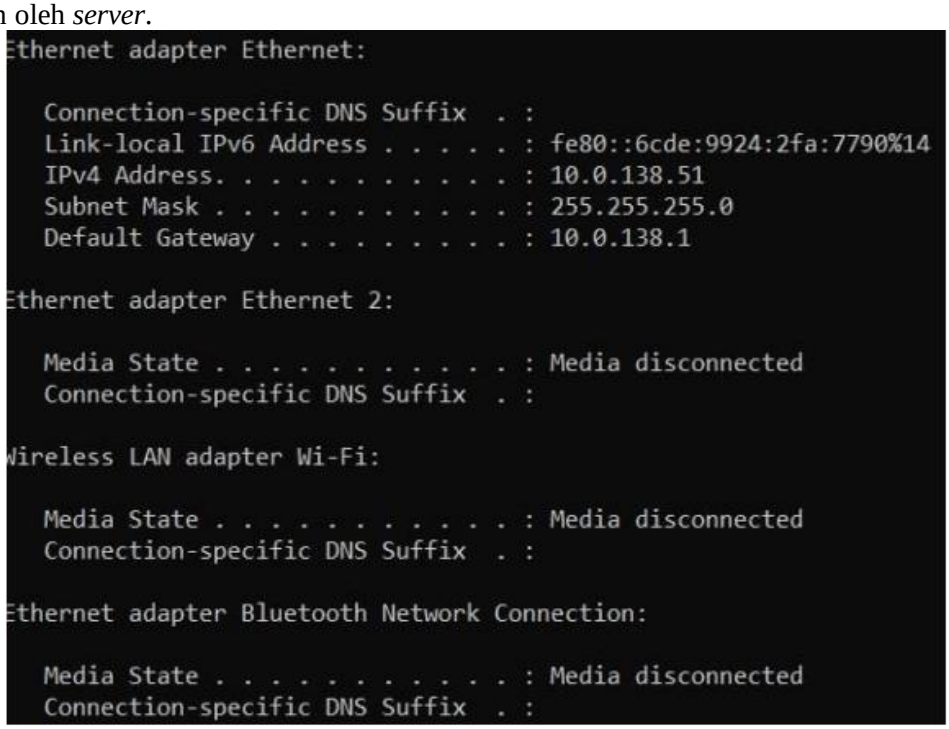
2. Pembahasan

Dalam pembahasan ini penulis akan membahas tahapan dalam pencegahan *DHCP Rogue* pada suatu jaringan.

Implementasi Testing memakai *tools Ettercap* untuk switch sudah dikonfigurasi Pada tahap ini merupakan tahap untuk melakukan testing terhadap jaringan yang dimana *switch* dalam konfigurasi DHCP Snooping, sehingga untuk mengetahui apakah komputer *client* yang berada pada Lab. Jarkom dan Lab. Sistem operasi mendapatkan IP dari *DHCP Rogue* atau tidak.
Melakukan serangan *DHCP Rogue* pada switch yang sudah dikonfigurasi

Gambar 2. Serangan *DHCP Rogue* pada port yang telah dikonfigurasi

Pada gambar diatas dimana kondisi *DHCP Rogue* melakukan serangan namun tidak bisa memberikan IP pada *client* karena posisi *client* terhubung pada port yang sudah dikonfigurasi, dengan tidak adanya keterangan ACK:10.0.1.138 255.255.255.0 GW 10.0.138.42 DNS 10.0.138.1 yang menuju pada, dimana *client* mendapat IP 10.0.138.51 dari hasil permintaan pada *switch* yang dimana IP tersebut yang diberikan oleh *server*.



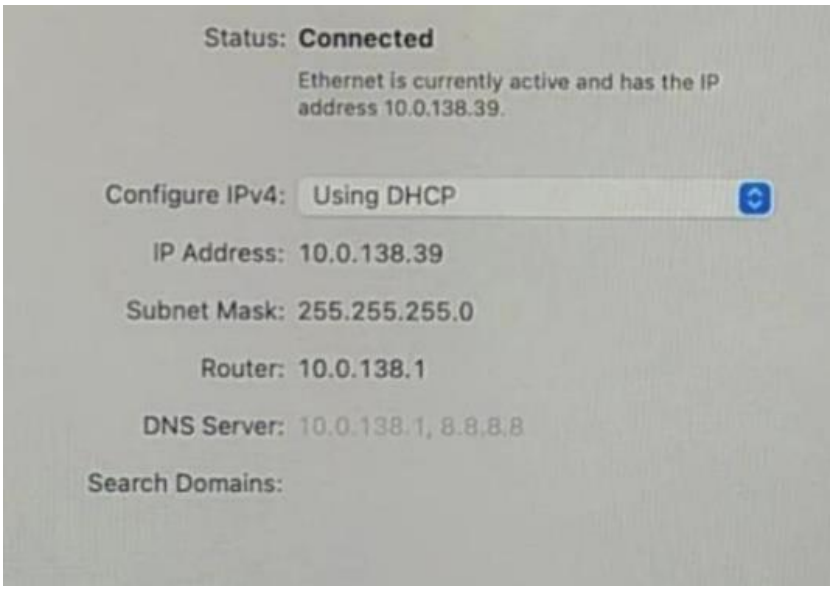
Gambar 3. Pengecekan IP pada komputer Lab.Jarkom

Pada gambar diatas dimana kondisi *DHCP Rogue* melakukan serangan Lab. Sistem operasi namun tidak bisa memberikan IP pada *client* karena posisi *client* terhubung pada port yang sudah dikonfigurasi, dengan tidak adanya keterangan *Request* yang menuju pada IP *DHCP Rogue*, yang dimana *client* mendapat IP 10.0.138.39 dari hasil permintaan pada *switch* yang dimana IP tersebut yang diberikan oleh server.

Melakukan serangan DHCP Rogue pada port yang sudah dikonfigurasi

Gambar 4. Serangan *DHCP Rogue* pada port yang telah dikonfigurasi

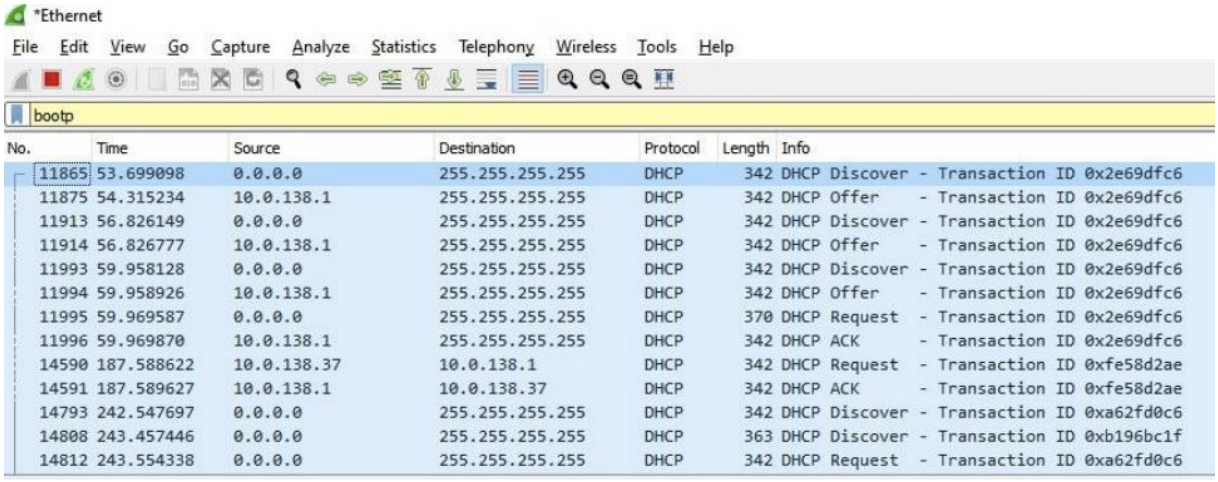
Pada gambar diatas dimana kondisi *DHCP Rogue* melakukan serangan Lab. Sistem operasi namun tidak bisa memberikan IP pada *client* karena posisi *client* terhubung pada port yang sudah dikonfigurasi, dengan tidak adanya keterangan Request yang menuju pada IP *DHCP Rogue*, yang dimana client mendapat IP 10.0.138.39 dari hasil permintaan pada *switch* yang dimana IP tersebut yang diberikan oleh server.



Gambar 5. Pengecekan IP pada komputer Lab. Sistem operasi

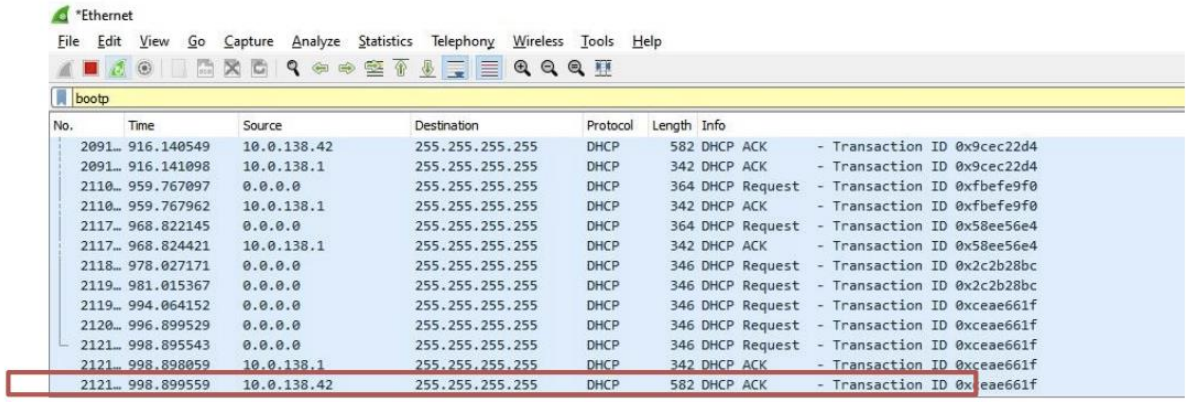
Pada gambar diatas merupakan kondisi komputer client di Lab. Sistem operasi terhubung pada port yang dikonfigurasi *DHCP Snooping* sehingga mendapatkan IP 10.0.138.49 yang diberikan oleh server, dari hasil Testing dapat diketahui bahwa perbedaan antara komputer yang terkena serangan *DHCP Rogue* dengan yang tidak terkena *DHCP Rogue* yaitu dapat dilihat dari *gateway* yang ada pada list "*ipconfig*".

Implementasi Monitoring *DHCP Rogue* pada jaringan



Gambar 6. Melihat protokol *dhcp* pada *wireshark*

Pada gambar diatas merupakan kondisi saat *DHCP Rogue* tidak melakukan serangan pada jaringan untuk melihat aktivitas jaringan dengan protokol *DHCP* yang terdapat pada suatu jaringan dengan menggunakan aplikasi *Wireshark*, lalu mengetikan "*bootp*." Pada kolom *search* dan akan tampil list kegiatan dari protokol *DHCP* yang ada pada jaringan.



Gambar 7. Mengetahui IP *DHCP Rogue* pada jaringan

Pada gambar diatas merupakan kondisi saat *DHCP Rogue* melakukan serangan pada jaringanm, terdapat keterangan *DHCP ACK* pada kolom info yang dimana keterangan tersebut seharusnya dimiliki oleh IP milik server dengan IP 10.0.138.1, namum ada keterangan DHCP ACK dimiliki oleh IP 10.0.138.42 yang dimana IP tersebut milik *DHCP Rogue*.

KESIMPULAN

Dari hasil penelitian ini yang berjudul Penggunaan metode DHCP Snooping dalam melakukan pencegahan terhadap DHCP Rogue pada laboratorium Teknik Informatika dapat disimpulkan sebagai berikut:

1. Sistem pencegahan DHCP Rogue dengan melakukan konfigurasi Switch yang memiliki fitur DHCP Snooping.
2. Menginstall DHCP server dan melakukan konfigurasi sehingga sistem pada server bisa memberikan IP DHCP pada client.
3. Melakukan monitoring pada jaringan menggunakan Wireshark dengan adanya keterangan offer atau DHCP ACK pada kolom info.

UCAPAN TERIMA KASIH

Terimakasih kepada Pusat Penelitian dan Pengabdian Masyarakat (P3M) Politeknik Negeri Indramayu (POLINDRA) yang telah memberikan kesempatan dan dukungan kepada kami untuk melakukan penelitian serta pengabdian DHCP ini semoga bisa bermanfaat juga tentunnya bagi jurusan Teknik Informatika.

DAFTAR PUSTAKA

[1] Prayitno, M. Hadi, Hendarman Lubis. (2020). Penerapan Logical Unit Number (LUN) pada Drobo Virtual Storage dengan Metode Network Development Life Cycle (NDLC). Jurnal Sistem Informasi dan Telematika.

[2] Gani, Alcianno G. (2017). Pengenalan Teknologi Internet serta Dampaknya. Jurnal Sistem Informasi. 2(2), 71-86

[3] Putra. Willy Permana, A Sumarudin. (2019). Rancang Bangun Internet Sehat Di SMP Negeri Unggulan Indramayu Menggunakan Proxy Server. Jurnal Ilmiah Ilmu Komputer Fakultas Ilmu Komputer Universitas Al Asyariah Mandar

[4] Putra. Willy Permana, A Sumarudin, Suheryadi. Adi, Hidayat. Risanuri, (2022). Vessel Monitoring Application Using Automatic Identification System Data 2022 International Conference on Electrical Engineering, Computer and Information Technology (ICEECIT)

[5] Pradana. Dio Aditya , Budiman. Ade Surya (2021). The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack. International Journal on Informatics for Development

[6] W. Odom, Cisco CCNA: Routing and Switching 200-120 Official Cert Guide Library, April 2013. Indianapolis, USA: Cisco Press, 2013.

[7] M. Yaibuates and R. Chaisricharoen, "Implementing of IP address Recovery for DHCP Service," Int. J. Appl. Eng. Res., vol. 13, no. 5, pp. 2659–2662, 2018, [Online]. Available: http://www.ripublication.com.

[8] D. Kurnia, "Analisis Serangan DHCP Starvation Attack Pada Router OS Mikrotik," J. Ilm. Core IT, vol. 8, no. 5, pp. 12–17, 2020.

[9] MikroTik, "DHCP Snooping and DHCP Option 82," Manual:Interface/Bridge. https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge#DHCP_Snooping_and_DHCP_Option_82 (accessed Jan. 19, 2021).

[10] D. Diwan, V. K. Narang, and A. K. Singh, "Security Mechanism in RIPv2 , EIGRP and OSPF for Campus Network - A Review," Int. J. Comput. Sci. Trends Technol., vol. 5, no. 2, pp. 399–404, 2017.

[11] T. Ariyadi, "Mitigasi Keamanan Dynamic Host Control Protocl (DHCP) Untuk Mengurangi Serangan Pada Local Area Network (LAN)," Inovtek Polbeng - Seri Inform., vol. 3, no. 2, pp. 147–154, 2018, doi: 10.35314/isi.v3i2.455.

[12] R. Natarajan, "Different Possibilities of DHCP Attacks and Their Security Features," Glob. Res. Dev. J. Eng., vol. 1, no. 1, pp. 20–23, 2015.