ANALISIS KEAMANAN JARINGAN LOKAL PADA MEDIA ACCESS CONTROL ADDRESS SPOOFING DENGAN METODE ADDRESS RESOLUTION PROTOCOL (Studi Kasus : SMK Prisma Depok)

[*]Jiyan Suhada[1], Tukiyat[2], Makhsun[3]

[1]Mahasiswa Prodi Teknik Informatika Program Pascasarjana, Universitas Pamulang, Kota Tangerang Selatan, Banten
[2,3]Dosen Prodi Teknik Informatika, Program Pascasarjana, Universitas Pamulang/BRIN

e-mail: [1] jiyanjunior7@gmail.com
[2] dosen02711@unpam.ac.id
[3] dosen00345@unpam.ac.id

Abstract

The development of the internet network is now increasingly accessible and continues to widen its reach as is the case in education which in the current era cannot be separated from internet access to find references for learners or school data management, besides that there are also things that must be known that each device, be it a cellphone, laptop, router, switch, has a different MAC address and will not change, but it can change if there is spoofing activity in a network so that the MAC address will change. The devices or software used include proxy, Windows 10 OS, and also Kali Linux OS. Previously there was research that discussed MAC address spoofing which used wireshark tools to view network traffic, especially in the protocol address resolution protocol which resulted in a simulation of an attack that obtained information in the form of the media access control (MAC) address of the attacker and victim along with the time of the attack. Testing on this MAC address spoofing uses tools in the Linux OS called Macchanger with a note that it is connected to one network first so that the results in the analysis can be detected on the router, 2C: 60: 0C: 79: 4A: 0B The MAC address is the original identity of the device used but changes to A8: 1B:18:BC:4A:03 of the two can still access the internet, therefore by recording the MAC address Address Resolution Protocol on the router server makes the path can be held if spoofing occurs, so the existence of this Address Resolution Protocol successfully entered the spoofing prevention category.

Keywords** : **Windows 10; MAC Address; Spoofing; Address Resolution Protocol; Kali Linux

Abstrak

Perkembangan jaringan internet saat ini semakin mudah diakses dan terus luas untuk jangkauannya seperti halnya di pendidikan yang di era sekarang tidak lepas dari akses internet untuk mencari referensi pembelajar ataupun pengelohan data sekolah, disamping itu juga ada hal yang musti diketahui bahwasanya setiap perangkat baik itu handphone, laptop, router, switch memiliki MAC address yang berbeda dan tidak akan berubah-ubah, tetapi bisa terjadi berubah apabila ada kegiatan spoofing didalam suatu jaringan sehingga MAC address tersebut akan berubah. Perangkat atau software yang digunakan diantara lain seperti mikrotik, OS windows 10, dan juga OS Kali Linux. Sebelumnya ada penelitian yang membahas tentang spoofing MAC address yang mempergunakan tools wireshark untuk melihat lalu lintas jaringan, terutama pada protocol address resolution protocol yang menghasilkan simulasi serangan yang memperoleh informasi berupa Alamat media access control (MAC) address penyerang dan korban beserta waktu terjadinya serangan. Pengujian pada spoofing MAC address ini mengunakan tools yang ada di OS kali linux yang Bernama Macchanger dengan catatan sudah tersambung dengan satu jaringan terlebih dahulu sehingga hasil pada analisis dapat terdeteksi di router ,

2C:60:0C:79:4A:0B MAC address tersebut merupakan identitas asli dari perangkat yang digunakan namun berubah menjadi A8:1B:18:BC:4A:03 dari kedua tersebut dapat masih mengakses internet , maka dari itu dengan adanya pencatatan MAC address *Address Resolution Protocol* di router server membuat jalur tersebut dapat ditahan apabila terjadinya spoofing, dengan begitu adanya *Address Resolution Protocol* ini berhasil masuk katagori pencegahan spoofing.

Kata kunci: **Windows 10; *MAC Address*; *Spoofing*; *Address Resolution Protocol; Kali Linux***

1. PENDAHULUAN

Pertumbuhan dan pengembangan internet pada saat ini semakin luas dan terus di jadikan bahan penelitian karna penguna terus meningkat untuk meningkatkan optimalisasi layanan internet di setiap wilayah. Dengan kemudahan layanan internet yang bisa di akses maka di lain sisi pun penyedia atau pengembang layanan internet juga harus memperhatikan dari segi keamanan lalu lintas data internet yang di transfer ataupun di receive, seperti halnya di ruang lingkup Pendidikan di era sekarang sudah hal yang wajib di berikan layanan atau fasilitas sekolah yaitu akses internet yang dapat di akses oleh siswa dan guru untuk mencari wawasan dan reverensi tugas-tugas yang sesuai mata pelajaranya.

Pada setiap jaringan baik itu local maupun interlocal pasti ada kegiatan yang mengancam keamanan jaringan yang tersedia di tempat-tempat yang ada layanan jaringan publik khsusnya di sekolah yang memberikan fasilitas *wi-fi*. Untuk hal pengguna layanan jaringan tanpa melakukan pembatasan akses ke dalam jaringan dapat mengunakan sistem keamanan Media Access Control Address filtering yang dalam implementasinya ini dapat bekerja untuk memfilter untuk perangkat yang akan melakukan akses kedalam jaringan komputer.

MAC Address Snooping merupakan Teknik atau cara untuk mengubah control access layanan atau media yang sudah di tetapkan dari suatu layanan jaringan. Spoofing sendiri berasal dari kata spoof yang berarti meniru atau mengandakan fungsi dari program yang asli, hal ini biasanya dilakukan oleh seorang hacker/cracker.

Menemukan informasi bukti serangan Address Resolution Protocol (ARP) Spoofing beberapa alamat Media Access Control (MAC) Address penyerang dan korban beserta waktu terjadinya serangan.Penelitian ini menggunakan tools wireshark untuk melihat lalu lintas jaringan, terutama pada protokol Address Resolution Protocol (ARP) dan menggunakan metode National Insitute of Standard Technology (NIST) sebagai kerangka kerja selama proses simulasi sampai dengan pembuatan laporan barang bukti (Imam Riadi ,2020).

Di sekolah SMK Prisma Depok memiliki layanan jaringan internet untuk di pergunakan bagi siswa maupun tenaga pendidik agar mempermudah mengupgrade materi ataupun literasi yang ingin di pelajari selama kegiatan belajar mengajar berlangsung, untuk mendistribusikan layanan tersebut harus lah optimal dalam pengunaanya selain melihat dari pada itupun juga dilihat dari segi sistemnya yang selalu berjalan secara realtime dan harus di control agar tidak terjadi kepadatan data yang di kirim maupun yang menerima, secara teknis dalam pemberian layanan internet di sekolah masih hanya terpaku pada daya tampung atau kecepatan internetnya saja, sehingga tidak menutup kemungkinan dari sisi perangkat yang digunakan oleh user tidak diperhatikan atau tidak dianggap seperti celah kelemahan jaringan lokal yang di terapkan di sekolah, namun dengan adanya perhatian khusus itu dapat ditangulangi dengan cara menganalisis Mac Address yang di gunakan oleh user yang kemudian di jadikan acuan agar tidak banyak device yang terhubung secara tidak wajar, hal ini yang bisa di katakan menjadi pemicu terjadinya down pada akses internet, karna pada dasarnya setiap jaringan internet baik itu local ataupun interlocal pasti sudah membuat infrastruktur jaringan terlebih dahulu untuk kebutuhan tertentu.

2. METODE

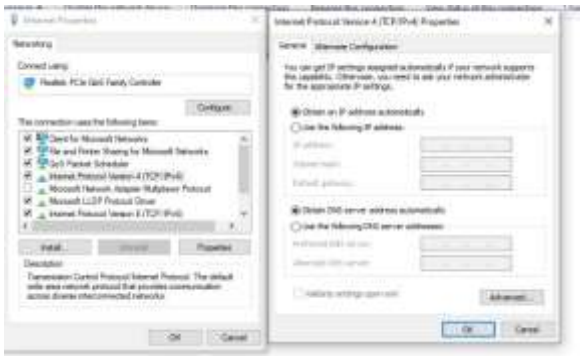
Metode penelusuran yang digunakan dalam penelitian ini menggunakan metode penelitian deskriptif kualitatif, dengan pengumpulan data menggunakan teknik studi literatur dan observasi. Secara Teknis studi literatur dilakukan dengan mempelajari literatur yang ada hubungannya dengan objek penelitian ini. Dalam penelitian ini, teknik pengumpulan data berhubungan dengan topik yang diangkat dalam penelitian ini. data didapatkan dari berbagai sumber jurnal, tesis, dan

internet. Selama teknik observasi peneliti pengumpulan data melalui pengamatan langsung dan/atau peninjauan secara cermat dan langsung di lapangan atau lokasi penelitian di laboratorium SMK Prisma Depok.

Teknik *sampling* yang digunakan adalah metode *Network Development Life Cycle* (NDLC). Pada metode NDLC terdiri dari 6 tahapan, yaitu *Analisis, Desain, Simulasi Prototype, Fabrikasi, Monitoring*, dan *Manajemen*. *Metode Network Development Life Cycle* (NDLC) merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data.

3. HASIL

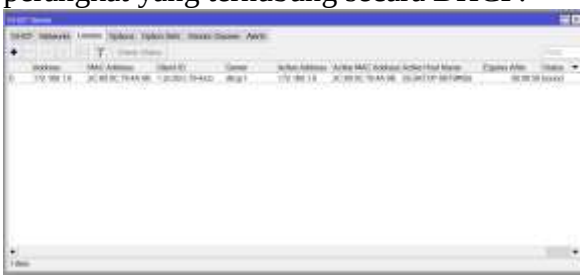
Untuk menjalankan hasil konfigurasi sebelumnya dari komputer client di cek terlebih dahulu IP address yang di dapat melalui kabel LAN yang sudah terpasang di komputer, yang mana artinya ip address dan juga MAC Address akan terdeteksi secara rinci dari jaringan yang di dapatkan. Awal mulanya komputer client meminta ip address secara dynamic, lalu akan terjadi proses pemberian ip address untuk client.



Gambar.1. Tampilan internet protocol TCP/Ipv4 windows

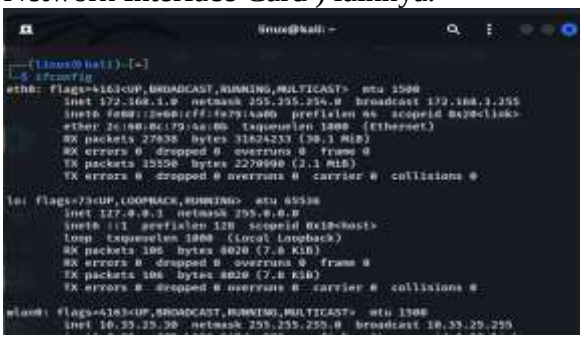
Gambar.2. Tampilan IP address client

Setelah mendapatkan ip address maka dari hasilnya pun menunjukan bahwa client yang pertama ini mendapatkan Ipv4 address nya adalah 172.168.1.0 dengan subnet mask nya 255.255.254.0 dengan ip gateway yang di dapat yaitu 172.168.1.1 dan dengan MAC Address yang di dapat adalah 2C-60-0C-79-4A-08 dan MAC Address ini lah akan di mulainya simulasi spoofing MAC Address sehingga mengantisipasinya dengan cara meng ARP kan MAC address ini di router, namun sebelum itu dari sisi winbox nya akan memeriksa leases yang sudah digunakan atau perangkat yang terhubung secara DHCP.

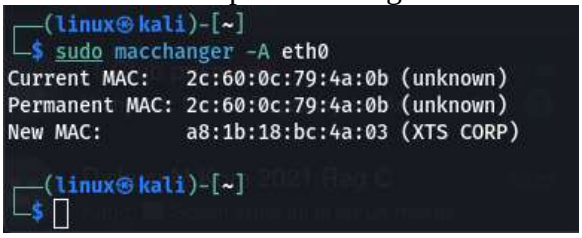


Gambar.3. Tampilan DHCP Server leases

Untuk sisi di OS kali linux, Pada tahap ini dengan tool macchanger yang bisa di artikan sebagai max spoofing yang memberikan cara seperti meniru dengan mengubah identitas pada mac address, hal ini di manfaat kan untuk berbagai keperluan autentifikasi pada server untuk bertukar informasi, dan tentu hasil nanti dari pengujian spoofing ini agar mencoba melakukan max spoofing untuk mendapatkan akses kejaringan atau bisa juga melakukan bypass access control di server atau bisa juga berguna untuk menyembuyikan identitas dengan meniru MAC address pabrikan NIC (Network Interface Card) lainnya.



Gambar.4. tampilan ifconfig kali linux



Gambar.5. tampilan set random vendor

Gambar.6. tampilan perintah macchanger –s

4. PEMBAHASAN

Hasil pengujian jaringan local yang di peruntunkan untuk MAC Address client dapat di spoofingkan, dan tentu dalam hal ini harus ada pencegahan agar mencoba meminimalisir terjadi nya spoofing di sekolah khususnya di SMK Prisma depok, walaupun jarang terjadi di jaringan local yang di sediakan oleh sekolah namun antisipasi wajib di waspadai dan perlu di tingkatkan Kembali kepemahaman spoofing ini dengan adanya ARP yang di terapkan pada jaringan server, ada kemungkinan juga akan meminimalisir terjadinya spoofing, seperti halnya gambar.7 dan juga gambar.8 yang di mana dari hasil sebelum dan sesudah akan terlihat menimbulkan perbedaan identitas.

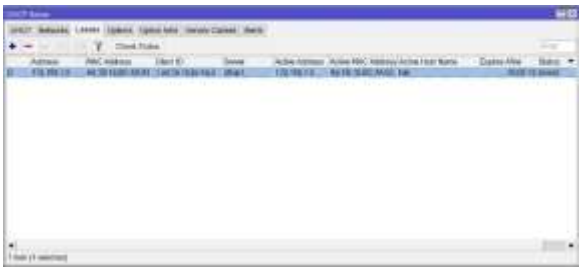
Komputer	Physical Address		Keterangan
	Kali linux	Windows	
Server	-	-	
client	2C:60:0C:79:4A:0B	2C:60:0C:79:4A:0B	Bisa akses Internet

Gambar.7. hasil sebelum pengujian spoofing

Komputer	Physical Address		Keterangan
	Kali linux	Windows	
Server	-	-	
client	A8:1B:18:BC:4A:03	A8:1B:18:BC:4A:03	Bisa akses internet

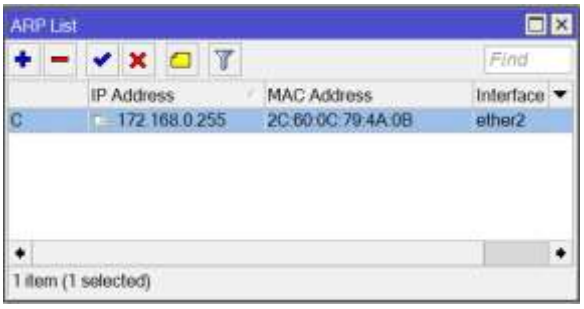
Gambar.8. hasil setelah pengujian spoofing

Dari gambar tersebut di atas dijelaskan bahwa untuk spoofing ini bisa mengubah physical address namun tidak mengubah ip address pada komputer client yang awalnya 172.168.1.0, akan tetapi berubah pada mac addressnya, walaupun begitu masih bisa mengakses internet dengan baik yang harusnya dengan perubahan mac address itu dapat memberhentikan jalur internet yang di berikan oleh server client.



Gambar.9. tampilan DHCP server setelah spoofing

Kalau dilihat dari sisi dashboard dhcp server untuk client ikut berubah karna dari server akan mendeteksi perangkat yang terhubung dengannya sehingga router akan menampilkan informasi secara realtime. Selanjutnya akan secara singkat di berikan identitas aslinya di ARP sehingga apabila ada perubahan mac address akan diketahui secara realtime.



Gambar.10. Tampilan ARP pada router server

5. KESIMPULAN DAN SARAN

KESIMPULAN:

Dari hasil pengujian analisis pada penelitian ini dapat diambil beberapa kesimpulan sebagai berikut :

a. Hasil pendeteksian spoofing pada mac address masih dapat di laluin oleh macchanger yang dapat mengubah identitas asli dari suatu perangkat yang digunakan, namun tidak dapat mengubah ip address disebabkan untuk ip address sendiri di berikan secara DHCP yang sudah di atur dari server.
b. Dengan adanya monitoring Address Resolution Protocol pada jaringan server tentu dapat melihat akses yang didapatkan oleh setiap client, khususnya di ranah MAC address yang sudah menjadi dasar identitas perangkat yang di gunakan seperti halnya router,

komputer, switch dan perangkat lainnya.

Hasil dari tampilan dashboard winbox bahwasanya dapat menjadi acuan atau bahan memonitoring perangkat yang terhubung dan bisa mencegah terjadinya spoofing MAC address.

SARAN :

Peneliti ini sudah dilakukan dengan semaksimal mungkin, namun peneliti menyadari masih banyak adanya keterbatasan dan kekurangan. Berdasarkan penelitian yang telah dilakukan maka saran yang di dapat diberikan adalah bagi peneliti selanjutnya diantara sebagai berikut.

a. Perlu kajian lebih mendalam pada pemahaman spoofing yang dapat di jalan kan di kali linux dengan tools macchanger
b. Masih perlu membandingkan secara teliti apabila ada perangkat yang memiliki mac address sebagai identitasnya didalam suatu NIC yang berbeda-beda di setiap perangkat.

Masih perlu juga cara alternatif ataupun konsep yang dapat mempermudah memonitoring secara berkala agar perangkat terhubung terus berjalan dengan ketentuan dasar dari identitas perangkat seperti MAC Address

6. UCAPAN TERIMAKASIH

1. Direktur Pascasarjana Universitas Pamulang.
2. Para Dosen Universitas Pamulang untuk bimbingannya.
3. Teman-teman mahasiswa sekalian.
4. Istri tecinta yang senantiasa menemani penulis untuk berkarya.
5. Orang Tua yang sudah mendo'akan penulis hingga selesai dengan baik.

7. DAFTAR PUSTAKA

[1] Afrizal, F., Muzawi, R., & Efendi, Y. (2018).Analisis Keamanan Lalu Lintas Paket Data Pada Ubuntu Menggunakan Metode Attack Centric. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *1*(3), 277–282. https://doi.org/10.29207/resti.v1i3.74

[2] Al Fikri, K., & Djuniadi. (2021). Keamanan Jaringan Menggunakan Switch Port Security. *InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan*, *5*(2), 302–307.

[3] Almaarif, A., & Yazid, S. (2018). ARP CachePoisoning sebagai Teknik Alternatif untuk Membatasi Penggunaan Bandwidth berbasis Waktu ARP Cache Poisoning as an Alternative Technique to Limit Bandwidth Usage based on Time. *Jurnal Rekayasa Sistem Dan Industri*, *05*, 2–7.

[4] Choiruman, M. R., Ginting, J. G. A., & Iryani, N. (2022). InfoTekJar : Jurnal Nasional InformatikadanTeknologiJaringan Analisis Pendeteksian Serangan ARP Poisoning Dengan Menggunakan Metode Live Forensic. *InfoTekJar :Jurnal Nasional InformatikadanTeknologiJaringan*, *2*, 0–4.

[5] Elektro, J. T., Teknik, F., Kuala, U. S., Tgk, J., Abdurrauf, S., & Aceh, B. (2016). *Pengujian keamanan jaringan terhadap serangan arp poisoning*. 28–29.

[6] Fakhmi, M., & Gultom, L. M. (2021). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw (Studi kasus : Sekolah Menengah Kejuruan Negeri 3 Bengkalis). *Seminar Nasional Industri Dan Teknologi (SNIT)*, 260–277.

[7] Ginanti, D. E., Christian, A., & Hidayat, T. (2022). Analisa Dan Implementasi Jaringan Wireless Mac Address Menggunakan Filtering Pada Pt. Faya Kuntura Agung Konsultindo. *INTI Nusa Mandiri*, *16*(2), 79–84. https://doi.org/10.33480/inti.v16i2.2781

[8] Hafizh, M. N., Riadi, I., & Fadlil, A. (2020). Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic. *Jurnal Telekomunikasi Dan Komputer*, *10*(2), 111. https://doi.org/10.22441/incomtech.v10i2.8757

[9] Hamid, H. (2017). Analisis Keamanan Aplikasi Email Bawaan Android Dan Gmail Pada Jaringan Nirkabel. *Teknoin*, *23*(2), 125–136. https://doi.org/10.20885/teknoin.vol23.iss2.art5

[10] Hidayat, A. S., Nuha, U., Nuryamin, Y., & Suleman, S. (2021). Quality Of Service Filtering Dengan Metode Filtering Mac Address Jaringan Wireless. *Jurnal Teknologi Informatika Dan Komputer*, *7*(1), 52–59. https://doi.org/10.37012/jtik.v7i1.502

[11] Ilham Firdaus, Januar Al Amien, & Soni, S. (2020). String Matching untuk Mendeteksi Serangan Sniffing (ARP Spoofing) pada IDS Snort. *Jurnal CoSciTech (Computer Science and Information Technology)*, *1*(2), 44–49. https://doi.org/10.37859/coscitech.v1i2.2180

[12] Ismail, R. W. (2020). Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi. *Jurnal Mahasiswa Bina Insani*, *5*(1), 53–62.

[13] Journal, I. (2022). *Instalasi Konfigurasi Sniff / Sadap Hasil*. *11*(1), 24–28.

[14] Jude Saskara, G. A., Oktap Indrawan, I. P., & Maha Putra, P. (2019). Keamanan Jaringan Komputer Nirkabel Dengan Captive Portal Dan Wpa/Wpa2 Di Politeknik Ganesha Guru. *Jurnal Pendidikan Teknologi Dan Kejuruan*, *16*(2), 236. https://doi.org/10.23887/jptk-undiksha.v16i2.18559

[15] Laksono, A. T., & Nasution, M. A. H. (2020). Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *1*(2), 83. https://doi.org/10.30865/json.v1i2.1920

[16] Marcus, R. D., Rosyadi, H. E., & ... (2021). Prototype Sistem Administrasi Dan Keamanan Jaringan Komputer Berbasis DHCP Server Mikrotik. In *Briliant: Jurnal Riset dan …* (Vol. 6, Issue 62, pp. 685–695).

[17] Martias, & Djuanda, R. F. (2018). Pembatasan Jumlah Client Menggunakan Security MAC-Address with Cisco. *Transistor EI (Jurnal Elektro Dan Informatika) UNISSULA*, *3*(3).

[18] Prayoga Hutabarat, A., & Haeruddin. (2020). Analisa Dan Perancangan Keamanan Jaringan End User Dari Serangan Exploit Menggunakan Metode Penetration. *Journal of Information System and Technology*, *01*(02), 31–36.

[19] Prisscilya, V., & Santoso, T. (2021). Implementasi Keamanan Jaringan Menggunakan Intrusion. *Journal of Information Technology*, 1–8.

[20] Purnama. (2019). Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering MAC Address. *Indonesian Journal On Networking and Security*, *8*(4), 43–47.

[21] Ramadhan, I., Seta, H. B., & Astriratma, R. (2020). Pengamanan Wireless Local Area Network Dari Serangan Arp Spoofing Menggunakan Pendekatan Deteksi Pasif Dan Deauthentication Attack Berbasis Rasp. *Senamika*, 761–770.

[22] Riadi, I., Fadlil, A., & Hafizh, M. N. (2020). Analisis Bukti Serangan Address Resolution Protocol Spoofing menggunakan Metode National Institute of Standard Technology. *Edumatic : Jurnal Pendidikan Informatika*, *4*(1), 21–29. https://doi.org/10.29408/edumatic.v4i1.2046

[23] Rizal Fauzi, A., & Made Suartana, I. (2018). Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids. *Jurnal Manajemen Informatika*, *8*(2), 7.

[24] Terdistribusi, L. S., Informatika, J. T., Teknik, F., & Madura, U. T. (2010). *Pada Jaringan Ipv4 Dan Ipv6*. *1*(3), 171–183.

[25] Veny Charnita Br Ginting, Mahendra Data, & Dany Primanita Kartikasari. (2019). Deteksi Serangan ARP Spoofing berdasarkan Analisis Lalu Lintas Paket Protokol AR. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(5), 5049–5057.

[26] Wahyudi, W. (2022). Proteksi Akses Jaringan WIFI berbasis MAC Address. *Techno Xplore : Jurnal Ilmu Komputer Dan Teknologi Informasi*, *7*(1), 27–34. https://doi.org/10.36805/technoxplore.v7i1.2036

[27] Widodo, S., Sutrisman, A., Amin, M. M., Fernaldo Harefa, M., Farhan, M. A., Reinaldo, M., Jurusan,), Komputer, T., & Sriwijaya, P. N. (2022). Keamanan Data User Pada Jaringan Wirelles. *Jurnal JUPITER*, *14*(1), 37–44.

[28] Yudha, G. S., & Laluma, R. H. (2019). Sistem Keamanan Jaringan Dalam Ujian Online Sma/Smk Menggunakan Metode Algoritma Advanced Encryption Standard (Aes). *Infotronik : Jurnal Teknologi Informasi Dan Elektronika*, *4*(2), 71. https://doi.org/10.32897/infotronik.2019.4.2.261

[29] Zonggonau, K., & Sajati, H. (2015). Membangun Sistem Keamanan Arp Spoofing Memanfaatkan Arpwatch Dan Addons Firefox. *Compiler*, *4*(1), 49–58. https://doi.org/10.28989/compiler.v4i1.87