SIMULASI KEAMANAN JARINGAN WIFI PUBLIK DI PERUMAHAN CV. DEWI MAKASSAR

TUGAS AKHIR

Karya tulis sebagai salah satu syarat
Untuk memperoleh gelar Sarjana dari
Universitas Fajar

Oleh:

MUH SURYADI ADAM

NIM. 1920221034

PROGRAM STUDI TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS FAJAR

2023

HALAMAN PENGESAHAN

SIMULASI KEAMANAN JARINGAN WIFI PUBLIK DI PERUMAHAN CV. DEWI MAKASSAR

Disusun Oleh :

MUH SURYADI ADAM
1920221034

Telah diperiksa dan disetujui oleh Dosen Pembimbing

Makassar, 29 April 2024

Pembimbing I	Pembimbing II
Ika Puspita, S.T., M.T	**Safaruddin, S.Si., M.T**
NIDN. 0927098801	**NIDN. 0909106901**

Mengetahui,

Dekan Fakultas Teknik	Ketua Program Studi
Prof. Dr. Ir. Erniati, S.T., M.T	**Safaruddin, S.Si., M.T**
NIDN : 0906107701	**NIDN. 0909106901**

PERNYATAAN ORISINALITAS

Penulis dengan ini menyatakan bahwa Tugas Akhir :

"**Simulasi Keamanan Jaringan Wifi Publik Di Perumahan Cv. Dewi Makassar**" adalah karya tulis orisinal saya dan setiap serta seluruh lembar acuan telah ditulis sesuai dengan Panduan Penulisan Ilmiah yang berlaku di Fakultas Teknik Universitas Fajar.

Makassar, 10 April 2024

Yang menyatakan

MUH SURYADI ADAM

KATA PENGANTAR

Puji dan syukur kehadirat Tuhan Yang Maha Esa atas Rahmat dan Hidayahnya penulis dapat menyelesaikan Proposal Penelitian ini.

Adapun Proposal Penelitian ini disusun untuk memenuhi persyaratan dalam menyelesaikan kurikulum di Jurusan Teknik Elektro Fakultas Teknik Universitas Fajar. Proposal Penelitian ini disusun berdasarkan studi literatur, diskusi dengan pembimbing yang berjudul **"Simulasi Keamanan Jaringan Wifi Publik Di Perumahan Cv. Dewi Makassar".**

Dalam melaksanakan penyusunan Proposal Penelitian hingga selesainya laporan, penulis tidak terlepas dari bantuan dan dorongan berbagai pihak secara moril maupun material. Untuk itu, saya pribadi ingin mengucapkan banyak terima kasih terutama kepada :

1. Allah SWT atas segala nikmat berupa kesempatan dan kesehatan yang diberikan dalam penyusunan Proposal Penelitian ini.
2. Orang tua dan seluruh keluarga yang selalu menasehati dan memberikan banyak motivasi semangat.
3. Ibu Prof. Dr. Ir Erniati, ST.,MT, Selaku Dekan Fakultas Teknik Universitas Fajar.
4. Bapak Safaruddin, S.Si., M.T selaku Ketua Prodi Teknik Elektro, Fakultas Teknik, Universitas Fajar.
5. Ibu Ika Puspita, ST., MT. selaku Dosen Pembimbing I.
6. Bapak Safaruddin, S.Si., M.T. selaku Dosen Pembimbing II.
7. Seluruh dosen dan staf Jurusan Teknik Elektro, Fakultas Teknik, UniversitasFajar.
8. Kepada tuan pemilik NIM 1920421003 yang telah berkontribusi banyak dalam membersamai penulis selama penyusunan dan pengerjaan skripsi dalam kondisi apapun. Terimakasih atas waktu, tenaga, pikiran, emosi, dan suport terbaik dalam mengantarkan ke gerbang menuju gelar yang sama-sama didambakan. Terimakasih telah menjadi rumah yang tidak hanya berupa tanah

atau bangunan.

9. Teman-teman Teknik Elektro angkatan 2019 serta seluruh pihak yang telah banyak membantu dalam menyelesaikan Proposal Penelitian ini.

Penulis menyadari bahwa dalam laporan ini masih banyak terdapat kekurangan, untuk itu saran dari semua pihak sangat diharapkan demi kesempurnaan laporan Proposal Penelitian ini. Akhirnya, penulis berharap semoga laporan ini dapat bermanfaat bagi semua pihak, Amin.

Makassar, April 2024

Penulis

ABSTRAK

Perkembangan digital yang semakin modern menjadikan masyarakat ketergantungan terhadap internet. Hal menjadikan WiFi publik sebagai sarana popular tanpa mengetahui bahaya ancaman terhadap kelemahan keamanan yang dapat merugikan pengguna. Penelitian ini bertujuan untuk melakukan simulasi keamanan jaringan WiFi publik di perumahan CV Dewi Makassar serta menganalisa keamanan jaringannya menggunakan *Wireshark* dengan metode penyerangan *DNS Spoofing*. Penelitian dilakukan dengan membentuk topologi terkendali lalu melakukan pemantauan *trafik ARP (Addrress Resolution Protocol)* jaringan menggunakan *wireshark,* dengan membandingkan jumlah *ARP (Adrress Resolution Protocol)* sebelum dan sesudah dilakukan penyerangan *DNS Spoofing*. Hasil dari penelitian ini yaitu dipercobaan 1 sebelum terjadi penyerangan koneksi komunikasi stabil. Sedangkan sesudah penyerangan koneksi komunikasi menjadi tidak stabil dan berhasil mengirim 9 ARP palsu. Pada Percobaan 2 sebelum terjadi penyerangan koneksi komunikasi stabil. Sedangkan sesudah penyerangan koneksi komunikasi menjadi tidak stabil dan berhasil mengirim 10 ARP palsu. Dan dipercobaan 3 sebelum terjadi penyerangan koneksi komunikasi stabil. Sedangkan sesudah penyerangan koneksi komunikasi menjadi tidak stabil dan berhasil mengirim 11 ARP palsu. kondisi koneksi target dimana saat sebelum penyerangan koneksi komunikasi terlihat masih stabil. Sedangkan pada saat sesudah penyerangan, koneksi target tersendat. Ini disebabkan oleh perubahan data DNS yang mengarahkan target ke server yang salah atau sumber daya yang tidak valid. Dari hasil penelitian didapatkan bahwa terdapat perbedaan jumlah *displayed ARP* sebelum dan sesudah penyerangan. Peningkatan jumlah ini dapat menjadi tanda bahwa ada aktifitas yang mencurigakan dalam jaringan, terutama pada perubahan yang signifikan dalam *request ARP*.Dari data diketahui %keberhasilan penyerangan 83,3% dan %kegagalan 16,7%, sehingga dapat disimpulkan bahwa sistem keamanan jaringan WiFi publik di perumahan CV Dewi sangat rentan terhadap bahaya ancaman termasuk serangan *DNS Spoofing* bagi keamanan informasi dan data yang dikirim melalui jaringan tersebut. Hal ini disebabkan karena jaringan yang terbuka dan dapat mengekspos semua lalu lintas jaringan.

Kata kunci : Keamanan, Jaringan, Wifi Publik, Wireshark, DNS Spoofing.

ABSTRACK

Increasingly modern digital developments make people dependent on the internet. This makes public WiFi a popular tool without knowing the dangers of security weaknesses that could harm users. This research aims to simulate the security of the public WiFi network at the CV Dewi Makassar housing complex and analyze the network security using Wireshark with the DNS Spoofing attack method. The research was carried out by forming a controlled topology and then monitoring network ARP (Address Resolution Protocol) traffic using Wireshark, by measuring the number of ARP (Address Resolution Protocol) before and after the DNS Spoofing attack. The results of this research are experiment 1 before a stable communication connection attack occurs. Meanwhile, after the attack the communication connection became unstable and managed to send 9 fake ARPs. In Experiment 2, before the attack, the communication connection was stable. Meanwhile, after the attack the communication connection became unstable and managed to send 10 fake ARPs. And tried 3 before the attack occurred, the communication connection was stable. Meanwhile, after the attack the communication connection became unstable and managed to send 11 fake ARPs. the condition of the target connection where before the attack the communication connection appeared to be still stable. Meanwhile, during the next attack, the target connection was interrupted. This is caused by a change in DNS records that directs the target to the wrong server or invalid resource. From the research results, it was found that there was a difference in the number of ARPs displayed before and after the attack. An increase in this number can be a sign that there is suspicious activity in the network, especially significant changes in ARP requests. From the data it is known that the attack success rate is 83.3% and the failure rate is 16.7%, so it can be concluded that the public WiFi network security system The CV Dewi housing complex is very vulnerable to threats including DNS spoofing attacks for the security of information and data sent over the network. This is because the network is open and can expose all network traffic.

Keywords: *Security, Network, Public Wifi, Wireshark, DNS Spoofing.*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

I.1. Latar Belakang

Pada zaman era digital yang semakin tumbuh pesat, menjadikan internet sebagai kebutuhan utama dikalangan masyarakat. Internet merupakan akses yang dapat menghubungkan kita dengan mudah dan cepat dengan siapapun secara jarak jauh hingga belahan dunia(Liantoni, 2022). Internet tidak hanya sebatas media komunikasi, namun digunakan sebagai tempat mengekspresikan diri, berkreasi, media informasi, bahkan tidak jarang digunakan sebagai media untuk menghasilkan uang serta kecanggihannya yang dapat digunakan sebagai tempat untuk menyimpan data-data penting.

Seiring dengan perkembangan tersebut menjadikan WiFi publik sebagai sarana yang popular agar dapat terhubung ke internet. Hal itu dikarenakan, WiFi publik mudah ditemukan seperti pada kafe, restoran, bandara, hotel, lapangan dan tempat umum lainnya. Namun, dibalik peningkatan penggunaan WiFi publik, memberikan tantangan tersendiri terkhusus pada keamanan yang semakin besar (Nugroho et al., 2021).

WiFi publik memberikan kenyamanan dan kemudahan bagi pengguna untuk mengakses internet, tetapi perlu diberikan perhatian utama pada keamanannya. Pada umumnya WiFi publik memiliki beberapa kelemahan keamanan yang perlu dianalisa agar pengguna terhindar dari ancaman yang mungkin ada didalamnya(Supriyanto, 2022)

Salah satu satu ancaman dalam WiFi publik yaitu serangan *Man-In-The-Middle* (MITM). Dimana serangan ini dapat digunakan oleh penyerang untuk memantau dan mengintervensi komunikasi antara pengguna dan titik akses WiFi publik (Mcshane et al., 2019). Pada kasus ini, penyerang dapat dengan mudah mencuri informasi sensitif seperti kata sandi, data pribadi dan informasi keuangan.

Selain itu, ancaman besar yang perlu kita waspadai yaitu peretas pada WiFi Publik. Serangan ini berpusat pada pencobaan untuk mengakses WiFi Publik dan

mengambil alih kontrol pada perangkat yang terhubung. Dengan memanfaatkan celah keamanan pada sistem, peretas dapat mencuri data pengguna atau meluncurkan serangan lebih lanjut pada perangkat lain yang terhubung pada WiFi Publik(Rachman, 2021).

Salah satu alat yang dapat digunakan untuk menganalisis keamanan jaringan yaitu *Wireshark. Wireshark* merupakan perangkat lunak yang dapat digunakan untuk melihat lalu lintas jaringan. Dengan menggunakan *Wireshark*, peneliti dapat memantau dan menganalisis paket data yang dikirim dan diterima oleh perangkat terhubung ke jaringan Wifi publik (Liantoni, 2022).

Pada kasus ini, peneliti memilih suatu lokasi yang berada di Kota Makassar yaitu CV. Dewi. Lokasi tersebut merupakan tempat dimana terdapat sebuah kompleks yang menyediakan sarana WiFi Publik. Sekitar lapangan merupakan wilayah kos-kosan yang mengakses WiFi Publik tersebut. Kondisi tersebut memberikan lingkungan yang cocok untuk melakukan penelitian karena jumlah pengguna WiFi potensial dalam area yang relatif kecil agar analisis lebih terfokus.

I.2. Rumusan Masalah

Berdasarkan latar belakang yang termuat, maka penelitian ini dapat dirumuskan yaitu:

1. Bagaimana melakukan simulasi keamanan jaringan Wifi Publik di perumahan CV. Dewi Makassar?
2. Bagaimana menganalisa keamanan jaringan wifi publik tersebut?

I.3. Tujuan Penelitian

Adapun tujuan penelitian ini yaitu:

1. Untuk melakukan simulasi keamanan jaringan Wifi Publik di perumahan CV. Dewi Makassar
2. Untuk menganalisa keamanan jaringan wifi publik tersebut?

I.4. Batasan Masalah

Pada penelitian ini, dibatasi dengan:

1. Penelitian ini hanya berfokus pada Simulasi analisa keamanan jaringan
2. Penelitian ini menggunakan *software Wireshark*

BAB II

TINJAUAN PUSTAKA

II.1. Tinjauan Teori

II.1.1 Analisis Jaringan

Analisis merupakan ilmu pengetahuan yang penting di berbagai bidang dalam kehidupan sehari-hari. Dalam matematika, analisis berkaitan dengan studi fungsi dan konsep matematis lainnya. Dalam ekonomi, analisis berkaitan dengan penguraian data dan mendukung dalam pengambilan keputusan. Dalam sains, analisis digunakan untuk memahami fenomena alamiah.

Dalam konteks umum, analisis dapat merujuk pada interpretasi data, pemecahan masalah dan penguraian informasi untuk menyatakan makna dan keterkaitan yang tersembunyi. Hal ini merupakan kondisi dimana dilakukan pemahaman yang mendalam tentang suatu hal. Analisis merupakan sebuah kunci atau jawaban atas pertanyaan-pertanyaan rumit untuk memberikan wawasan yang lebih luas tentang dunia.

Dalam dunia informasi, analisis jaringan juga diperlukan untuk memahami struktur suatu sistem beroperasi dan berinteraksi, mengidentifikasi poin lemah dan pusat pengaruh. Analisis jaringan adalah suatu metode yang digunakan untuk memahami dan menganalisis hubungan atau interaksi antara elemen-elemen dalam suatu jaringan (Stiawan & Rini, 2019). Elemen-elemen ini berupa jaringan sosial, jaringan komunikasi, jaringan transportasi dan jaringan lainnya.

II.1.2 Jaringan

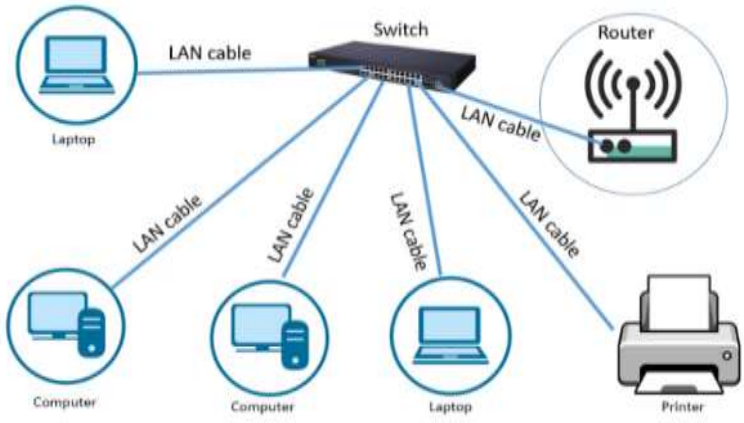
Jaringan merupakan kumpulan perangkat komputer yang saling terhubung satu sama lain untuk berbagi data, sumber daya, dan layanan. Jaringan memungkinkan pengiriman informasi antar perangkat dengan menggunakan protokol komunikasi.

Sejarah singkat jaringan dimulai dari pengembangannya sejak tahun 1960-an dengan proyek ARPANET oleh Departemen Pertahanan Amerika Serikat yang merupakan jaringan pertama yang menggunakan protokol sehingga dapat

mengirim data antar perangkat. Sejak saat itu, jaringan terus mengalami perkembangan pesat hingga zaman modern yang mencakup berbagai protokol dan jenis jaringan(Ruslianto et al., 2021).

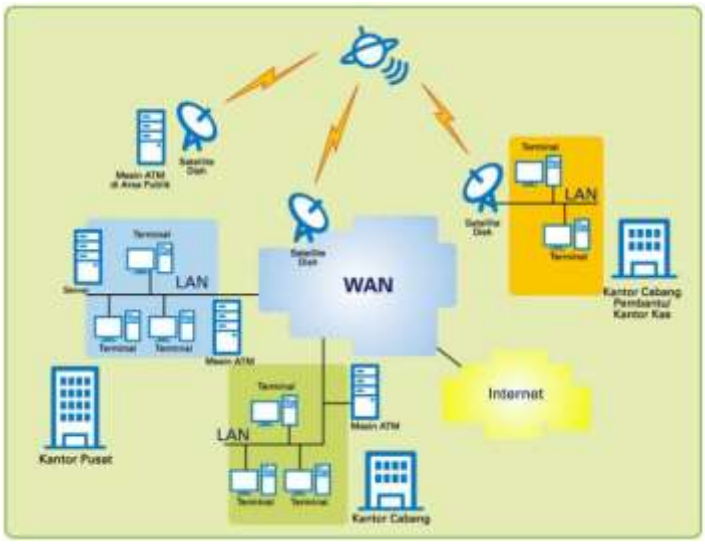
Jenis jaringan utama dapat dibagi dua yaitu jaringan berdasarkan skala dan jaringan berdasarkan topologi.

a. Jaringan Berdasarkan Skala
   - Jaringan Lokal (*Local Area Network* – LAN) yang merupakan jenis jaringan yang cakupannya di area terbatas seperti kantor, gedung, atau lingkungan geografis yang relatif kecil seperti pada gambar 2.1. Pada umumnya, jaringan ini menghubungkan perangkat-perangkat dalam jarak yang terbatas menggunakan nirkabel (WiFi).
   - Jaringan Luas (*Wide Area Network* – WAN), yang merupakan jenis jaringan yang cakupannya sangat luas seperti mencakup wilayah besar missal kota, negara atau bahkan benua seperti pada gambar 2.2. Jaringan ini memungkinkan untuk koneksi jarak jauh menggunakan jaringan telpon, satelit atau internet.



Sumber:[*https://www.nesabamedia.com/wpcontent/uploads/2017/09/pengertian-LAN.jpg*](https://www.nesabamedia.com/wpcontent/uploads/2017/09/pengertian-LAN.jpg)

Gambar 2. 1 Gambar Jaringan Lokal

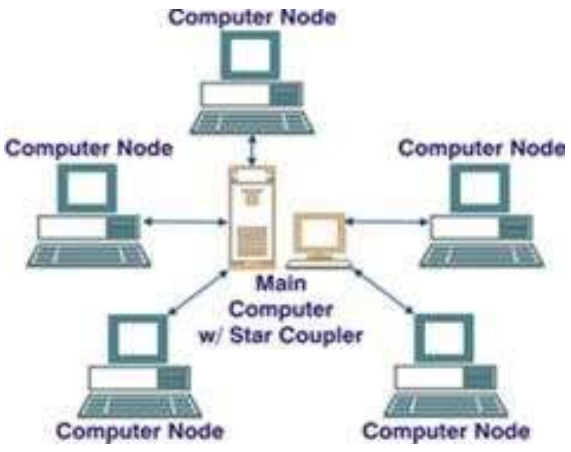


Sumber:[*http://smktwismawisnu.sch.id/media_library/posts/large/27876af214e663f4cba08b9ab792fb6c.jpg*](http://smktwismawisnu.sch.id/media_library/posts/large/27876af214e663f4cba08b9ab792fb6c.jpg)

Gambar 2. 2 Gambar Jaringan Luas

b. Jaringan Berdasarkan Topologi (secara umum)

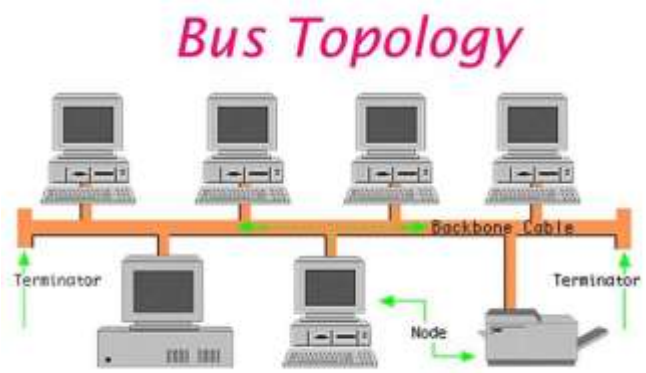
- Topologi Bintang, dimana setiap perangkat terhubung dengan pusat dan ketika salah satu mengalami masalah, perangkat lain tidak berpengaruh atau masih berjalan dengan baik. Ilustrasi jaringan ini dapat kita lihat pada gambar 2.3



Sumber : [*https://1.bp.blogspot.com/-QSASqo5aVCs/WpwDtirQtZI/AAAAAAAAAhA/GV8ITGDQKb4PlA5O1X_8R7wfZL0UacFLACLcBGAs/s1600/topologi%2Bstar.jpg*](https://1.bp.blogspot.com/-QSASqo5aVCs/WpwDtirQtZI/AAAAAAAAAhA/GV8ITGDQKb4PlA5O1X_8R7wfZL0UacFLACLcBGAs/s1600/topologi%2Bstar.jpg)

Gambar 2. 3 Topologi Bintang

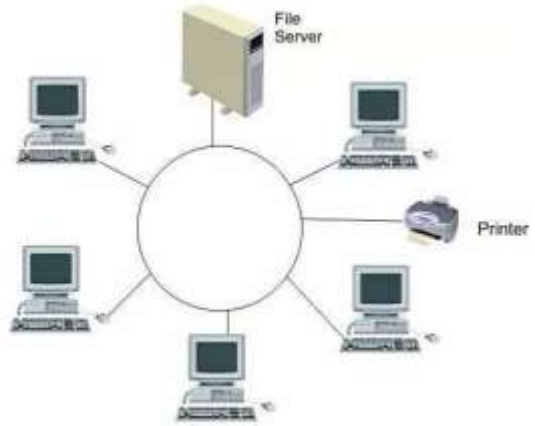
- Topologi Bus, dimana semua perangkat terhubung dengan kabel induk utama sebagai jalur komunikasi sehingga ketika kabel induk bermasalah, semua jaringan terpengaruh. Ilustrasi jaringan dapat kita lihat pada gambar 2.4.



Sumber: http://www.geocities.ws/nisaazmi/10.jpg

Gambar 2. 4 Topologi Bus

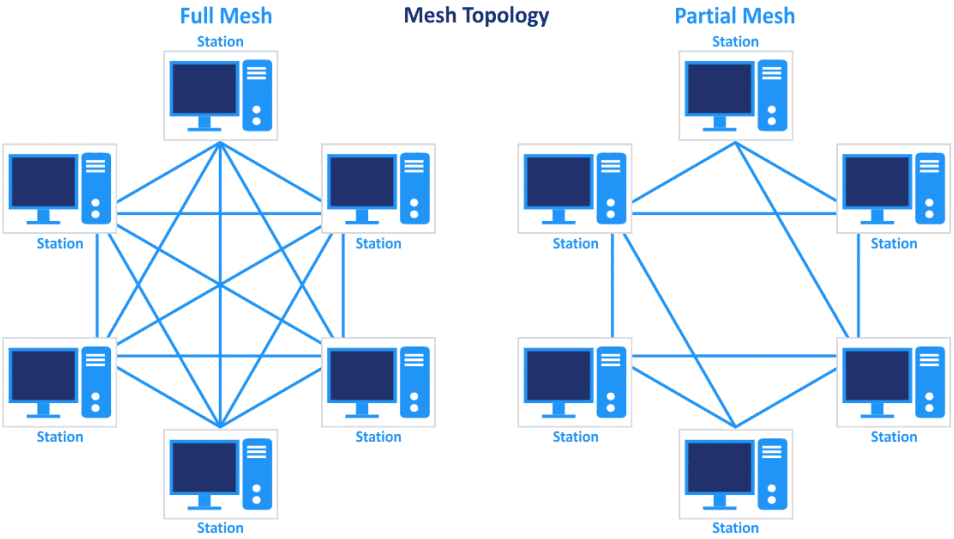
- Topologi Cincin, dimana setiap perangkat terhubung dengan membentuk lingkaran dan data bergerak satu arah melalui perangkat sampai ujung. Topologi ini mengalirkan data sepanjang satu arah lingkaran cincin tertutup tanpa melewati garis simpul tengah. Ilustrasi jaringan dapat dilihat pada gambar 2.5.



Sumber : http://www.seputarit.com/wp-content/uploads/2015/12/topologi-cincin-488x420.jpg

Gambar 2. 5 Topologi Cincin

- Topologi Mesh, dimana setiap perangkat terhubung dengan setiap perangkat lain dalam jaringan. Namun perangkat ini memerlukan kabel yang banyak dan bentuk yang kompleks. Ilustrasi jaringan dapat dilihat pada gambar 2.6.



Sumber:https://tse3.mm.bing.net/th?id=OIP.IsX4jNq0-v2KMvU8aV2iZgHaEF&pid=Api&P=0&h=180

Gambar 2. 6 Topologi Mesh

II.1.2.1 Komponen Jaringan

Jaringan terdiri dari beberapa komponen yang saling bekerja sama dalam menyediakan konektivitas dan berbagi sumber daya seperti sebagai berikut:

a. Perangkat Klien : komputer, laptop, smartphone dan tablet yang mengakses dan menggunakan sumber daya jaringan.
b. Perangkat Server: perangkat yang menyimpan dan menyediakan sumber daya, seperti data, aplikasi dan layanan kepada klien jaringan.
c. Perangkat Jaringan : *Router, Switch* yang membantu mengarahkan lalu lintas data di jaringan dan sebagai penghubung perangkat klien dan server.
d. Media Transmisi : Kabel tembaga, serat optik, dan teknologi nirkabel yang digunakan untuk mentransmisikan data antar perangkat jaringan.

e. Protokol Komunikasi : aturan dan pedoman yang digunakan perangkat untuk berkomunikasi satu sama lain seperti HTTP dan FTP.

II.1.2.2 Protokol Jaringan

Adapun protokol jaringan yang digunakan untuk dapat berkomunikasi antar perangkat secara terstruktur. Seperti namanya, protokol atau aturan memastikan data uang dikirim, diterima dan diinterpretasikan dengan benar oleh jaringan. Contoh protokol jaringan sebagai berikut:

a. TCP/IP : Protokol utama yang digunakan untuk mentransmisikan data antar perangkat.
b. HTTP/HTTPS : Protokol yang digunakan untuk mengakses dan mengirimkan data melalui *World Wide Web*
c. SMTP/POP3/IMAP : Protokol yang digunakan mengirim dan menerima email.
d. FTP/SFTP : Protokol yang digunakan untuk mengirim dan menerima file melalui jaringan.
e. ICMP : Protokol yang digunakan untuk mengirim pesan kontrol dan kesalahan dalam jaringan.

II.1.3 Keamanan

Keamanan merupakan aspek utama yang perlu diperhatikan dalam kehidupan. Keamanan berperan melindungi, mencegah, dan merespon berbagai ancaman atau resiko yang mungkin terjadi. Dalam konteks ini dikatakan bebas dari ancaman atau bahaya yang berpotensi merugikan dan dapat mencakup berbagai aspek kehidupan seperti kesehatan fisik, keamanan finansial, keamanan teknologi, keamanan nasional dan lain sebagainya(Siregar, 2019).

Secara umum, keamanan adalah suatu konsep meminimalkan risiko dan kerentanan aset, nilai dan sumber daya yang berharga yang dapat merusak atau mengancam stabilitas, keselamatan dan kesejahteraan. Pengertian keamanan terus mengalami perkembangan seiring dengan perubahan zaman dan tantangan global yang dihadapi.

II.1.4 Keamanan Jaringan

Keamanan jaringan adalah langkah dari sebuah tindakan yang memiliki tujuan dalam melindungi sistem jaringan dari ancaman, serangan, atau akses yang illegal. Secara singkat, memiliki tujuan utama yaitu menjaga kerahasiaan, integritas dan ketersediaan data serta layanan yang terdapat dalam jaringan(Pratama & Syamsuar, 2022)

Kerahasiaan dalam kasus ini menyatakan adanya jaminan terhadap informasi yang hanya dapat diakses oleh pihak yang berwenang karena bersifat sensitive(Patil et al., 2021). Integritas yang menyatakan adanya jaminan keutuhan atau dengan kata lain tidak adanya perubahan data/informasi selama penyimpanan, transmisi atau pemrosesan. Ketersediaan yang mengacu pada ketersediaan data dan sumber daya jaringan dengan waktu respon yang cepat agar dapat melindungi jaringan dari serangan dan menjaga performa sistem berjalan dengan baik.

Keamanan jaringan merupakan salah satu poin penting dalam teknologi informasi. Hal ini menjadi landasan dalam kepekaan akan potensi ancaman yang mungkin terjadi dan mengaplikasikan strategi perlindungan yang tepat untuk melindungi sistem dan data dari serangan(Susanto & Raharja, 2021).

II.1.4.1 Ancaman Keamanan Jaringan

Adapun beberapa ancaman terhadap keamanan jaringan sebagai berikut:

a. *Malware*

   Malware merupakan ancaman ini merupakan serangan dari jenis perangkat lunak yang berbahaya. Program ini merupakan program komputer yang diciptakan untuk merusak, mengakses, mengganggu, atau mengambil alih sistem komputer tanpa pengetahuan pengguna. *Malware* berpotensi bersifat bahaya terhadap keamanan jaringan dan informasi sensitif. Tujuan utama dari *Malware* mencakup berbagai jenis program seperti virus, worm, trojan, ransomware, spyware, adware dll.

b. Serangan DDoS (*Distributed Denial of Service)*

DDoS (*Distributed Denial of Service)* merupakan serangan sistem yang membanjiri jaringan atau server dengan lalu lintas internet palsu agar situs web tidak dapat diakses. Bentuk serangan siber ini bersifat merugikan yang mengganggu ketersediaan dan kinerja sistem, layanan, atau jaringan dengan cara membanjiri lalu lintas data. Tujuan utama dari serangan DDoS yaitu mengakibatkan penolakan akses terhadap layanan yang digunakan pengguna yang sah, dengan cara membebani sumber daya infrastruktur komputasi dan jaringan secara ekstrem, yang menyebabkan layanan tidak responsif atau bahkan tidak dapat diakses oleh pengguna yang sah.

c. *Phishing*

Phishing merupakan serangan penyamaran sebagai entitas terpercaya agar mendapatkan/mencuri informasi pribadi. Jenis ancangan ini menggunakan metode paling umum dan menjadi perusak dalam dunia siber karena menggunakan teknik sosial rekayasa untuk memancing korban agar memberikan informasi yang diinginkan yang akan di terima melalui email, situs web atau pesan lainnya,

d. *Man-in-the-Middle*

Man-in-the-Middle merupakan serangan yang melakukan penyerangan dengan memantau dan memanipulasi komunikasi antara dua pihak yang berinteraksi. Serangan ini menciptakan skenario penyerangan dengan membuat posisi palsu diantara dua pihak yang berkomunikasi, sehingga penyerang dapat memantau bahkan memanipulasi aliran informasi yang berjalan tanpa sepengetahuan pihak yang berkomunikasi.

e. *Brute Force*

Brute Force merupakan teknik serangan dimana penyerang akan mencoba semua kombinasi kata sandi dengan tujuan mendapatkan akses ke akun atau sistem. Serangan ini didasarkan pada pendekatan metode kasar dengan menggunakan kecepatan komputasi modern untuk mengatasi kata sandi yang kuat.

f. *Social Engineering*

serangan ini merupakan penipuan yang melibatkan psikologis untuk memanipulasi orang agar mendapatkan informasi akses ke sistem tanpa user sadari. Jenis ancaman ini mengekploitasi kerentanan manusia seperti kecenderungan percaya, rasa ingin tahu, atau emosi dinadingkan eksploitasi kerentanan teknis dalam perangkat lunak atau sistem.

II.I.4.2 Teknik Keamanan Jaringan

a. Penggunaan *Firewalls* : tujuan digunakannya *firewall* agar lalu lintas jaringan dapat terkontrol berdasarkan aturan dan kebijakan keamanan, membatasi akses tidak sah ke jaringan.
b. Enkripsi data : mengenkripsi data saat transit dan saat disimpan pada perangkat agar informasi dapat terlindungi dari akses ilegal.
c. *Virtual Private Network* : VPN menyediakan layanan aman dan ter-enkripsi untuk menghubungkan perangkat secara jarak jauh ke jaringan internal, sehingga data tidak dapat diakses oleh pihak yang tidak berwenang.
d. Sistem Deteksi Intrusi (SDI) dan Sistem Pencegahan Intrusi (SPI) : sistem ini sangat bekerjasama dalam menjalankan tugas masing-masing. Dimana SDI bertugas memantau lalu lintas yang mencurigakan sedangkan SPI bertugas mengambil tindakan untuk mencegah serangan yang terdeteksi.
e. *Patching* dan Pembaruan Perangkat Lunak : untuk mengatasi kerentanan keamanan yang terjadi, sistem ini memastikan perangkat lunak dan sistem selalu diperbarui dengan *patch* terkini.
f. Pengelolaan akses pengguna. Sebuah sistem yang memberlakukan otorisasi dan otentikasi yang kuat untuk mengontrol akses pengguna ke sumber daya jaringan.

Keamanan jaringan menjadi tantangan yang terus mengalami perkembangan seiring dengan kemajuan teknologi(Pangestu & Liza, 2022). Keprofesionalan keamanan jaringan diperlukan inovasi serta pengadopsian strategi dan teknologi yang sesuai agar dapat melindungi jaringan dari ancaman yang ikut terus berkembang.

II.1.5 Wireless Fidelity (WiFi)

WiFi merupakan revolusi digital modern dimana memungkinkan untuk menghubungkan perangkat elektronik seperti komputer, smartphone, tablet dan lain sebagainya ke internet dan jaringan lokal tanpa menggunakan(Kohlios & Hayajneh, 2018) kabel fisik. Berdampingan dengan era globalisasi yang semakin modern, termasuk dalam dunia teknologi dan informasi yang semakin canggih menjadikan WiFi sebagai sarana yang paling digemari karena konektivitas yang disediakan lebih cepat, handal dan fleksibel.

II.1.5.1 Komponen Utama Wifi

a. Router yang merupakan perangkat yang bertujuan untuk mengirimkan sinyal WiFi sebagai pusat yang berperan menghubungkan perangkat-perangkat nirkabel ke jaringan internet melalui modem.
b. Perangkat Klien merupakan perangkat yang terhubung dengan WiFi dan mengakses internet atau melakukan interaksi dengan perangkat lain di jaringan lokal.
c. *Acsess Point* (AP) merupakan perangkat tambahan yang memperluas jangkauan jaringan WiFi dan meningkatkan kapasitas pengguna yang dapat mengakses jaringan WiFi.
d. Frekuensi dimana Wifi memiliki dua frekuensi utama yaitu 2,4 GHz dan 5 GHz, pada frekuensi yang lebih tinggi menawarkan transfer data yang semakin cepat namun jangkauan semakin pendek dibandingkan frekuensi yang rendah,
e. Protokol dan standar dimana teknologi WiFi berdasarkan serangkaian standar IEEE, dan setiap standar memilki kecepatan, jangkauan dan fitus yang berbeda.

Teknologi nirkabel yang memungkinkan konektivitas lebih cepat dan memudahkan pengguna mengakibatkan WiFi sebagai daya tarik pengunjung diberbagai sarana umum tidak hanya di Indonesia, namun fakta ini berlaku di beberapa negara lainnya yang hampir sepanjang lokasi menyediakan layanan WiFi Publik (Sombatruang et al., 2020).

II.1.6 Simulasi Penyerangan Jaringan WiFi

Simulasi penyerangan jaringan WiFi adalah suatu proses skenario yang disusun untuk melakukan penyerangan pada jaringan nirkabel yang telah ditentukan untuk mengidentifikasi, mengevaluasi dan memahami potensi kelemahan suatu jaringan dari ancaman serangan.

Tujuan dari simulasi ini adalah untuk dilakukan pengujian agar dapat mengetahui keamanan jaringan WiFi dengan cara terkendali dan realistis., tanpa harus mengganggu operasi jaringan sebenarnya.

II.1.6.1 Manfaat Simulasi Penyerangan Jaringan WiFi

a. Identifikasi Kerentanan : Simulasi penyerangan dapat membantu untuk mengetahui kerentanan potensial pada konfigurasi jaringan WiFi, Perangkat, atau protokol keamanan yang dilakukan.
b. Evaluasi Keamanan : Dari simulasi penyerangan dapat digunakan sebagai bahan evaluasi mengenai keefektifikan mekanisme keamanan jaringan yang diterapkan dan Tindakan apa yang perlu dilakukan.
c. Pengujian Respons : Simulasi penyerangan berkaitan dengan pengujian tanggapan jaringan terhadap serangan, dan memastikan jika sistem keamanan dapat mendeteksi dan merespons serangan dengan tepat.
d. Pelatihan Personal : Simulasi penyerangan memberikan pelatihan kepada tim keamanan dalam menghadapi serangan dan mengembangkan keterampilan respons yang diperlukan.
e. Pemantauan Jaringan : Simulasi penyerangan dapat memberikan wawasan tentang area yang potensial yang perlu di kembangkan pemantauan jaringan.

II.1.6.2 Metode Simulasi Penyerangan Jaringan WiFi

Metode simulasi penyerangan ini dapat dibedakan menjadi 2 jenis yaitu sebagai berikut:

a. Simulasi di Lingkungan Terkendali, dimana simulasi ini dilakukan di lingkungan terkendali seperti laboratorium dengan bantuan alat keras dan

perangkat lunak yang didesain khusus untuk melakukan simulasi penyerangan.

b. Simulasi di Lingkungan Nyata, dimana simulasi ini dilakukan di lingkungan nyata namun dilakukan dengan seizin dan pengawasan yang dibutuhkan untuk mencegah gangguan nyata pada jaringan.

II.1.7 Wireshark

Wireshark merupakan perangkat lunak bebas dan sumber terbuka yang digunakan untuk memantau lalu lintas jaringan. Wireshark merupakan software yang popular dan efektif digunakan untuk menangkap, menganalisis dan memantau paket data yang berjalan dalam jaringan komputer(Liantoni, 2022). Logo *Wireshark* dapat kita lihat pada gambar 2.7.

Sumber:https://tse2.mm.bing.net/th?id=OIP.yrmVI9SjXtm_oUm4dMlc0gHaBC&pid=Api&P=0&h=180

Gambar 2. 7 Logo Wireshark

Sejarah *Wireshark* dimulai pada saat Gerald Combs memperkenalkan pada tahun 1998 sebagai *Ethereal*. Namun, karena masalah merek dagang sehingga diubah menjadi *Wireshark* pada tahun 2006. Kemudian dengan bantuan dan dukungan luas dari komunitas pengembang dan pengguna, sehingga *Wireshark* terus mengalami pengembangan dan menjadi software yang popular.

II.1.7.1 Fungsi Utama *Wireshark*

a. Penangkapan paket : *Wireshark* dapat berfungsi sebagai penangkapan paket paket antarmuka dengan jaringan yang dipilih sehingga dapat dianalisis lebih mendalam pada lalu lintas jaringan.

b. Analisis Protokol : *Wireshark* juga dapat difungsikan untuk mengetahui protokol yang terjadi pada interaksi lali lintas jaringan karena didukung oleh banyak protokol jaringan.

c. Penyaringan : sebagai pengguna *Wireshark* dapat menggunakan fitur untuk mengisolasi dan menganalisis paket yang mengandung informasi yang relevan.
d. Visualisasi : *Wireshark* memberikan fitur penyediaan data dalam bentuk grafik dan tabel yang mudah dipahami, sehingga dapat dengan mudah untuk melihat, menganalisis dan membandingkan data.

II.1.8 *Domain Name System* (DNS) *Spoofing*

DNS *Spoofing* merupakan serangan yang dapat mengancam keamanan dan privasi online dari pengguna. Serangan ini memanfaatkan pengguna yang menggunakan jaringan yang sama untuk mengalihkan lalu lintas jaringan dengan mengirimkan paket palsu. Paket palsu yang dikirim mengandung pemetaan palsu antara domain dan alamat IP. Sehingga ketika pengguna mengakses data palsu tersebut dan membuka situs web yang bersangkutan akan diarahkan ke alamat IP yang salah dimana dapat dikendalikan oleh penyerang.

Dampak dari penyerangan DNS *Spoofing* yaitu:

a. Pencurian data : penyerang dapat menggunakan teknik serangan *Spoofing* untuk mencuri data pribadi, seperti kata sandi. Informasi kartu kredit atau informasi sensitif lainnya yang melewati jaringan yang terinfeksi.
b. *Phising* : penyerang dapat mengarahkan pengguna ke situs web palsu yang dirancang untuk mencuri informasi pribadi.
c. Injeksi Malware : penyerang dapat menggunakan teknik serangan *Spofing* untuk mengarahkan pengguna ke situs web yang mengandung malware atau untuk menginjeksi malware ke dalam perangkat pengguna.
d. Penghentian Layanan : DNS *Spoofing* juga dapat digunkan untuk menghentikan akses layanan tertentu dengan mengarahkan lalu lintas server yang tidak responsif.

II.2 State of The Art

Tabel 2. 1 *State Of The Art*

No	Nama Peneliti	Judul Peneliti	Tahun	Metode yang Digunakan	Hasil Penelitian
1	Abraham Yano Suharmanto, Arie S.M Lumenta, Xaverius B.N. Najoan	Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi	2018	Metode yang digunakan penelitian adalah *observasi, testing* dan *literatur*. Pada awalnya peneliti mencari informasi alamat ip lalu mencari celah menggunakan tools. kemudian melakukan percobaan penyadapan dan mencari literatur yang relevan dengan penelitian yang dilakukan.	Hasil dari penelitian yaitu Universitas Sam Ratulangi belum sepenuhnya dikatakan aman. Walaupun tingkat ancaman yang didapatkan berada di level rendah namun, tidak menutup kemungkinan untuk terkena *Flooding* dan juga penyerangan DDoS masih bisa dilakukan.

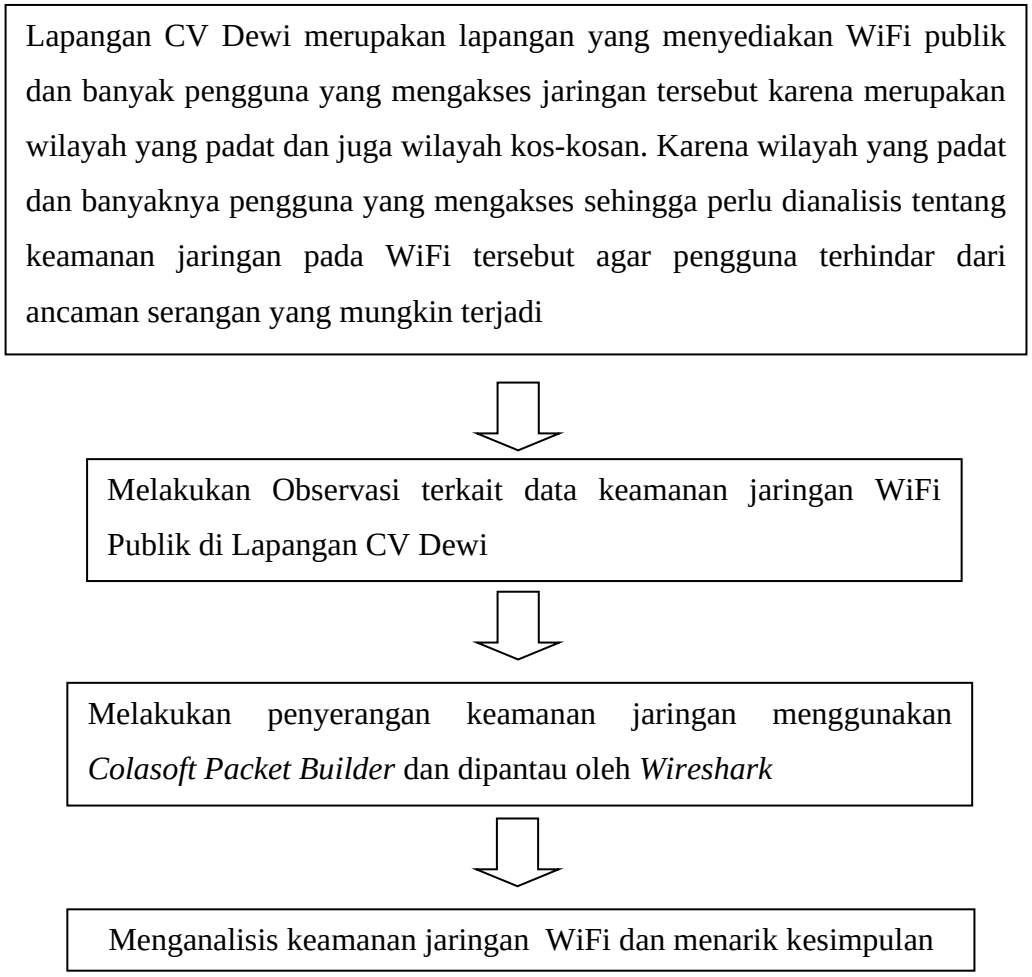
				Tools yang digunakan yaitu *Whois, Acunetix, Loic, Wireshark.*	
2	Taufiq Ismail Siregar	Analisis Keamanan Jaringan Pada Fasilitas Internet (WIFI) Terhadap Serangan Packet Siffing.	2019	Metode yang digunakan pada penelitian ini yaitu Penyerangan *Packet Sniffing* dengan menggunakan *Ettercap*	Hasil dari penelitian yaitu keamanan jaringan LAN yang mencakup jaringan kabel dan nirkabel pada PT. (PERSERO) Angkasa Pura II bandar Udara Internasional Kualanamu Medan masih sangat rentan akan ancaman serangan oleh karena itu perlu dilakukan peningkatan agar memperkuat

					keamanan jaringan yang digunakan
3	Teguh Pangestu dan Risko Liza	Analisis Keamanan Jaringan pada jaringan *Wireless* dari Serangan *Man In The Middle Attack DNS Spoofing*	2022	Metode yang dilakukan oleh peneliti yaitu metode kualitatif, dimana peneliti mencoba meningkatkan keamanan menggunakan sistem keamanan *Firewall* di saat terjadi serangan *Man In The Middle attack DNS.* Aplikasi yang digunakan yaitu *Oracle vm VirtualBox, Wireshark, Ettercap-G, Iptables, TCPflow.*	Hasil dari penelitian ini yaitu dengan menggunakan sistem keamanan *firewall iptables* dapat mencegah serta memblokir penyerang ketika terkena dampak serangan *man in the middle attack DNS spoofing,* dengan melakukan pengujian juga didapatkan bahwa dengan menggunakan *wireshark* dapat mengetahui alamat *MAC address*

					penyerang
4	Angga Pratama, Dedy Syamsur	Analisis Keamanan Jaringan Pada Layanan Internet Publik Menggunakan Metode Penetration Testing Execution Standard (Ptes) Dprd Provinsi Sumatra Selatan	2021	Metode yang dilakukan dalam penelitian ini yaitu dengan melakukan penyerangan jaringan dengan metode *Penetration Execution Standart (PTES)* melalui pengujian *cracking the encryption, Bypassing MAC Address, ARP Spoofing, dan Man in the Middle Attck*	Hasil dari penelitian ini yaitu keamanan jaringan WLAN pada DPRD Sekretariat Provinsi Sumatera Selatan bisa dikatakan aman karena sudah menerapkan keamanan WPA/WPA2-PSK namun memungkinkan bisa terdapat celah jika pass terdapat di dalam *data base word list* yang telah dibuat dan dijalankan dengan teknik *Bruto force.*

5	Liantoni	Analisis Keamanan Jaringan Publik Pada Fasilitas Sosial di Kota Palangka Raya menggunakan Wireshark	2022	Metode yang digunakan dalam penelitian ini yaitu metode deskripsi kualitatif, dimana peneliti akan menjelaskan situasi atau keadaan yang sebenarnya atau terjadi. Metode tersebut diperkuat dengan diperkuat dengan melakukan observasi, kuesioner, dan dokumentasi. Software yang digunakan yaitu wir*eshark.*	Hasil dari penelitian ini yaitu keamanan jaringan pada Taman Pasuk Kameloh palangkaraya masih sangat rentan dari ancaman serangan dikarenakan sistem keamanan yang digunakan jaringan WEP dimana bersifat statis sehingga sangat tidak cocok untuk keamanan jaringan umum atau khusus.

II.3 Kerangka Berpikir



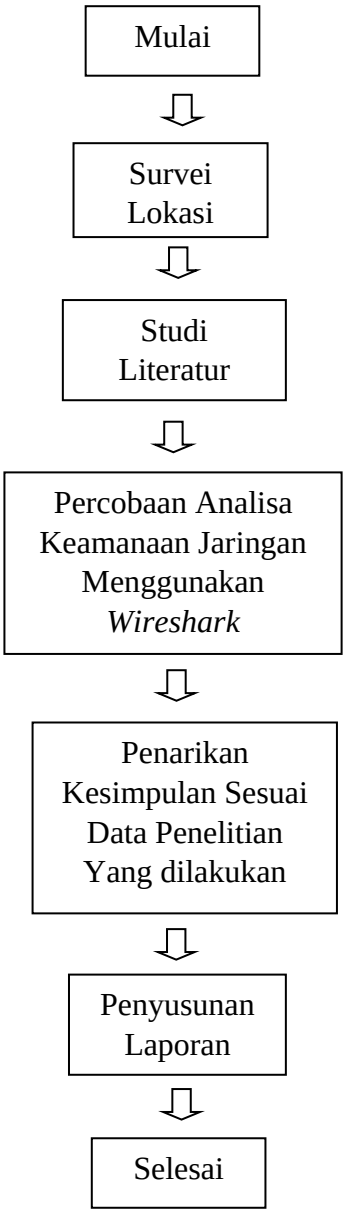
Gambar 2. 8 Kerangka Berpikir

BAB III

METODOLOGI PENELITIAN

III.1 Bagan Alur Penelitian

Bagan alur penelitian merupakan proses yang akan dilakukan dari awal penelitian hingga akhir. Tujuan dari bagan alur penelitian agar pada saat melakukan penelitian lebih terarah dan sistematis. Bagan alur penelitian dapat kita lihat pada gambar 3.1.



Gambar 3. 1 Bagan Alur Penelitian

Berdasarkan bagan alur penelitian diatas dijelaskan bahwa:

1. Mulai

   Penelitian ini dimulai untuk membantu masyarakat terkhusus masyarakat sekitar CV Dewi atau pengakses jaringan WiFi Publik di lapangan CV Dewi, dalam pengecekan keamanan jaringan untuk menghindari serangan ancaman yang akan terjadi.
2. Survei Lokasi

   Survei lokasi merupakan tahapan awal untuk melihat atau melakukan observasi kondisi lokasi penelitian untuk mengumpulkan data yang akan menunjang dalam penelitian penulis. Tahapan ini juga merupakan tempat untuk melengkapi dan mengumpulkan surat perizinan penelitian kepada pihak yang bersangkutan.
3. Studi Literatur

   Tahapan ini dimana peneliti mencari sumber informasi dari penelitian terdahulu, buku atau sumber lainnya yang relevan dengan penelitian agar mempermudah dalam pengumpulan data.
4. Percobaan Analisa Keamanan Jaringan Menggunakan *Wireshark*

   Tahapan ini merupakan puncak penelitian, dimana peneliti akan mengecek atau menganalisa masalah atau titik pusat dari penelitian yang dilakukan dan analisa keamanan tersebut menggunakan *Wireshark.*
5. Penarikan Kesimpulan

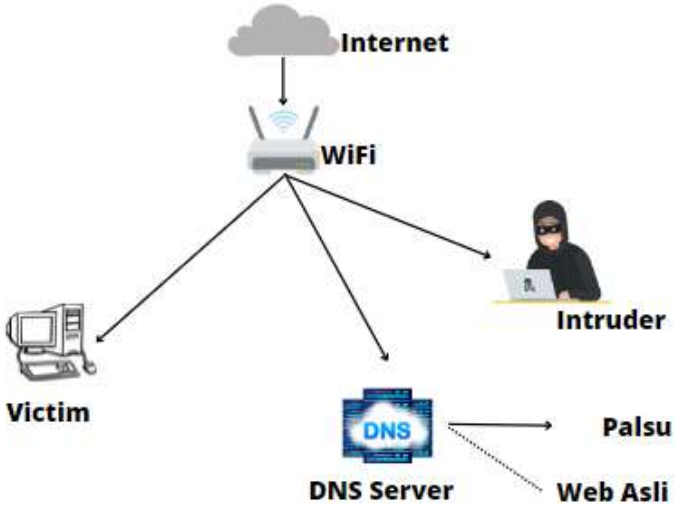
   Tahap ini merupakan langkah menarik kesimpulan sesuai dengan hasil penelitian yang telah dilakukan.
6. Penyusunan Laporan

   Tahapan ini merupakan penyusunan data atau olah data untuk menjadi sebuah laporan yang akan dibutuhkan.
7. Selesai

   Tahapan ini merupakan tahapan akhir dari penelitian dimana peneliti akan mengumpulkan hasil laporan yang telah dikerjakan.

III.2 Rancangan Penelitian

Perancangan penelitian merupakan penjelasan sebuah permasalahan yang diangkat dalam sebuah penelitian dan disajikan dalam bentuk diagram yang bertujuan untuk mempermudah pemahaman dalam penelitian tersebut. Perancangan umum sistem dapat kita lihat pada Gambar 3.2

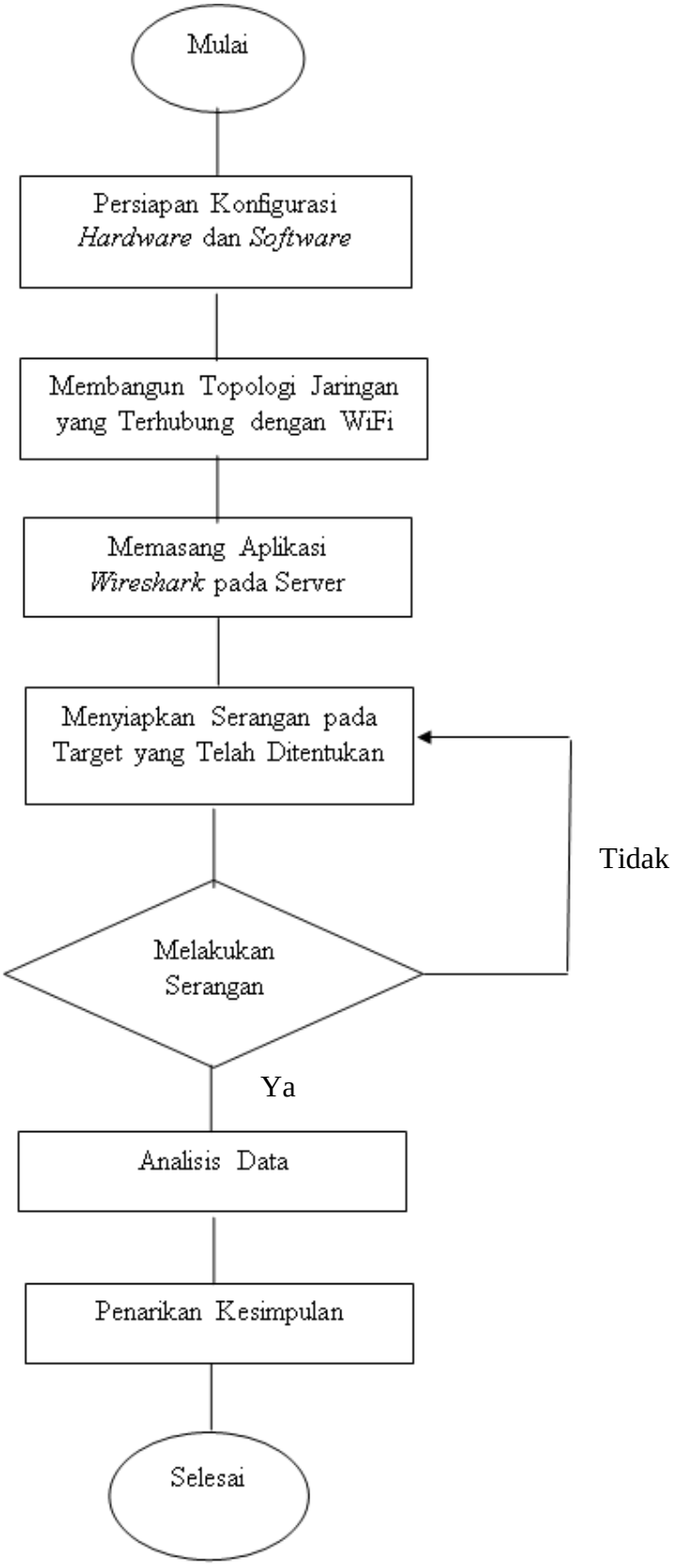


Gambar 3. 2 Topologi Serangan DNS *Spoofing*

Berdasarkan Gambar 3.2 dapat dideskripsikan :

User yang mengakses internet menggunakan WiFi akan di pantau *Intruder* atau penyerang dan akan menjadi *Victim* atau target. *Intruder* akan langsung memulai aksinya dengan mengirimkan paket (web palsu) untuk mengalihkan lalu lintas jaringan

Adapun *Flowchart* pada penelitian ini dapat kita lihat pada gambar 3.3.



Gambar 3. 3 Flowchart Penelitian

Langkah pada penelitian Tugas Akhir ini sebagai berikut:

1. Menyiapkan segala kebutuhan untuk menunjang penelitian ini termasuk mencari literatur serta persiapan *Hardware* dan *Software* yang akan digunakan dan pemasangan aplikasi *Wireshark* pada server.
2. Melakukan persiapan penyerangan untuk mengambil data yang dibutuhkan dan masuk ke dalam penyerangan dimana jika berhasil (Ya) akan lanjut ke analisa data dan penarikan kesimpulan untuk menyusun sebuah laporan. Dan jika penyerangan tidak berhasil (Tidak) maka akan kembali ke persiapan penyerangan.
3. Jika semua telah dilakukan maka penelitian telah dilakukan dan peneliti mengumpulkan hasil laporan sesuai data yang telah berhasil didapatkan.

III.3 Waktu dan Lokasi Penelitian

III.3.1 Waktu Penelitian

Penelitian ini akan dilakukan terhitung mulai pada bulan September 2023 sampai November 2023.

III.3.2 Lokasi Penelitian

Penelitian akan dilakukan di kompleks CV Dewi , Kec. Panakkukang, Kota Makassar, Sulawesi Selatan.

III.4 Alat dan Bahan Penelitian

a. Hardware

Laptop merek hp dengan spesifikasi

- *Processor Intel Core* i3-1005G1
- *Memory RAM* 4GB DDR4
- *Harddisk* 256 GB SSD
- Layar 14 Inch (1366 x 768)

b. *Software*

- *Microsoft Windows* 11 sebagai Sistem Operasi.
- *Wireshark* sebagai aplikasi penerangan dan analisa keamanan jaringan.
- *Colasoft Packet Builder* sebagai aplikasi membuat dan mengirim paket *Mac Address* Palsu

III.5 Metode Pengumpulan Data

Metode pengumpulan data adalah cara yang dilakukan untuk mengumpulkan data dan informasi yang dibutuhkan. Adapun metode pengumpulan data pada penelitian ini yaitu sebagai berikut:

1. Eksperimen

   Eksperimen merupakan metode yang akan dilakukan oleh peneliti untuk mencoba atau menguji sistem keamanan jaringan pada WiFi publik yang akan diteliti.
2. Studi Literatur

   Studi literatur merupakan metode untuk mencari informasi dari penelitian terdahulu, buku atau sumber lainnya yang relevan dengan penelitian yang dilakukan.

III.6 Analisis Data

Metode analisis yang digunakan pada penelitian ini yaitu sebagai berikut:

1. Melakukan observasi lokasi lapangan yang akan diteliti
2. Melengkapi berkas perizinan penelitian.
3. Menganalisis keamanan jaringan pada WiFi publik menggunakan *Wireshark*

BAB IV

HASIL DAN PEMBAHASAN

IV.1 Persiapan Penyerangan

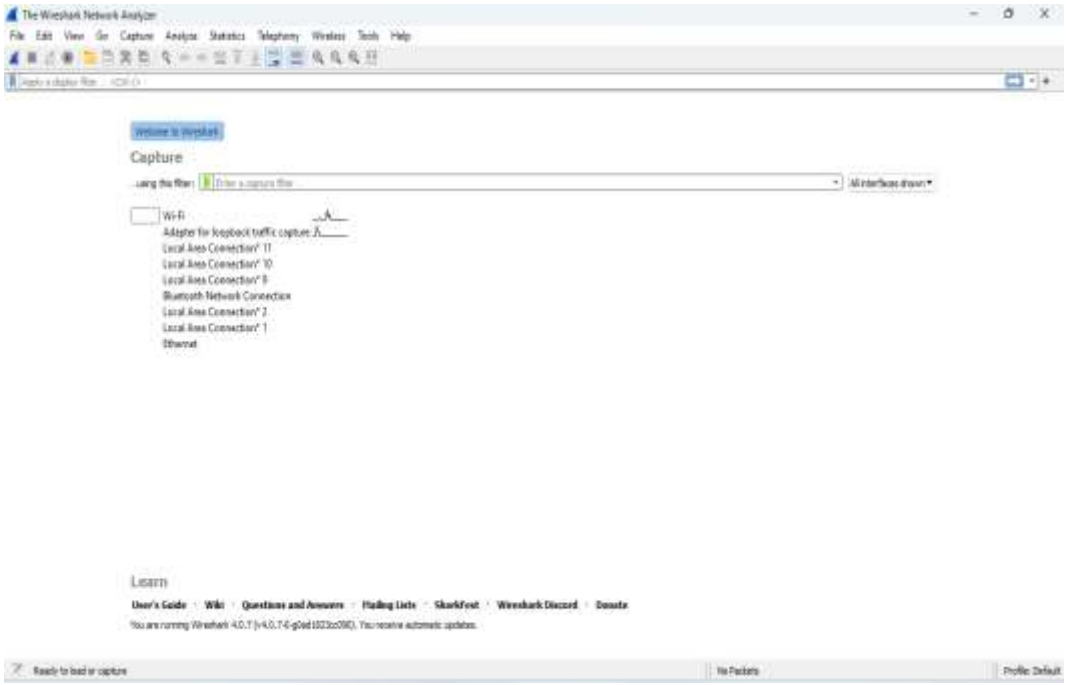
Sistem keamanan jaringan akan di uji dengan melakukan pemantauan *trafik ARP (Addrress Resolution Protocol)* jaringan menggunakan *wireshark.* Ukuran keberhasilan menggunakan metode ini dengan membandingkan jumlah *ARP (Adrress Resolution Protocol)* sebelum dan sesudah dilakukan penyerangan.

1) Monitoring paket *ARP (Addrress Resolution Protocol)*

   Langkah pertama yang akan dilakukan yaitu dengan membuka aplikasi *wireshark.* Setelah terbuka, tampilan laman *wireshark* akan menyajikan *interface* yang terhubung dengan jaringan seperti pada Tabel 4.1 dan Gambar 4.1. Lalu kemudian pilih WiFi

Tabel 4. 1 Tampilan Interface yang Terhubung pada Jaringan

No	Interface
1	WiFi
2	Adaptor for Loopback Trafic Capture
3	Local Area Connection* 11
4	Local Area Connection* 10
5	Local Area Connection* 9
6	Bluetooth Network Connection
7	Local Area Connection* 2
8	Local Area Connection* 1
9	Ethernet



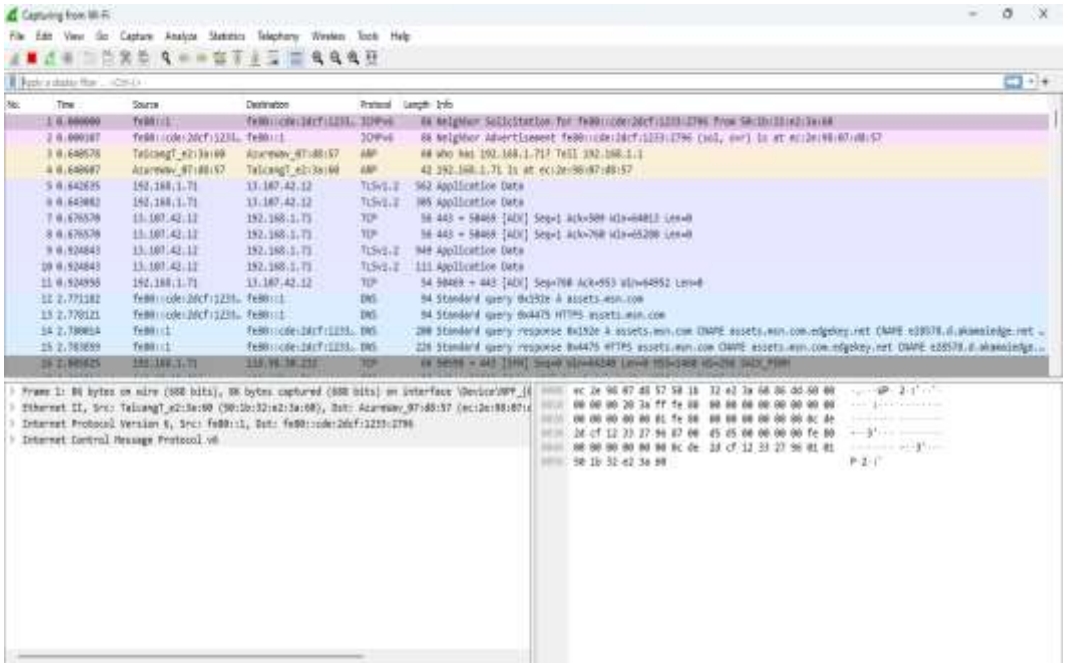
Gambar 4. 1 Tampilan awal Wireshark

Selanjutnya akan muncul seluruh protokol yang yang terdapat pada WiFi seperti ARP, TCP,DNS, dan lain sebagainya yang dapat dilihat pada Tabel 4.2 dan Gambar 4.2. Untuk melihat *Trafik ARP* secara spesifik maka dapat mengetik pada arp pada *filter* kemudian tekan *enter*

Tabel 4. 2 Tampilan Seluruh Protocol pada Wireshark

No	Time	Source	Destination	Protocol	Length	Info
1	0.00000	fe80: :1	fe80: :cde:2dcf:1233_	ICMPv6	86	Neighbor solicitation for fe80: :cde:2dcf:1233:2796 from 50:1b:32:e2:3a:60
2	0.000107	fe80: :cde:2dcf:1233_	Fe80: :1	ICMPv6	86	Neighbor Advertisment fe80: :cde:2dcf:1233:2796 (sol, ovr) is at ec:2e:98:07:d8:57
3	0.640578	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	60	Who has 192.168.1.71? Tell 192.168.1.1
4	0.640607	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57
5	0.642835	192.168.1.71	13.107.42.12	TLSv1.2	562	Application Data
6	0.643082	192.168.1.71	13.107.42.12	TLSv1.2	305	Application Data
7	0.676570	13.107.42.12	192.168.1.71	TCP	56	443 50469 [ACK] Seq=1 Ack=509 Win=64013 Len=0
8	0.676570	13.107.42.12	192.168.1.71	TCP	56	443 50469 [ACK] Seq=1 Ack=760 Win=65280 Len=0
9	0.924863	13.107.42.12	192.168.1.71	TLSv1.2	949	Application Data
10	0.924843	13.107.42.12	192.168.1.71	TLSv1.2	111	Application Data
11	0.924958	192.168.1.71	13.107.42.12	TCP	54	50469 443 [ACK] Seq=760 Ack=953 Win=64952 Len=0
12	2.771182	fe80: :cde:2dcf:1233_	fe80: :1	DNS	94	Standard query 0x192e A assets.msn.com
13	2.778121	fe80: :cde:2dcf:1233_	fe80: :1	DNS	94	Standard query 0x4475 HTTPS assets.msn.com
14	2.780014	fe80: :1	fe80: :cde:2dcf:1233_	DNS	200	Standard query response 0x192e A assets.msn.com CNAME assets.msn.com CNAME e28578.d.akamaiedge.net _
15	2.783859	fe80: :1	fe80: :cde:2dcf:1233_	DNS	226	Standard query response 0x4475 HTTPS assets.msn.com CNAME assets.msn.com CNAME e28578.d.akamaiedge.net._
16	2.805825	192.168.1.71	118.98.30.232	TCP	66	50469 443 [SYN] Seq=0 Win=64240 Len=0 MSS=256 SACK_PERM

Sumber : Data Olahan 2023



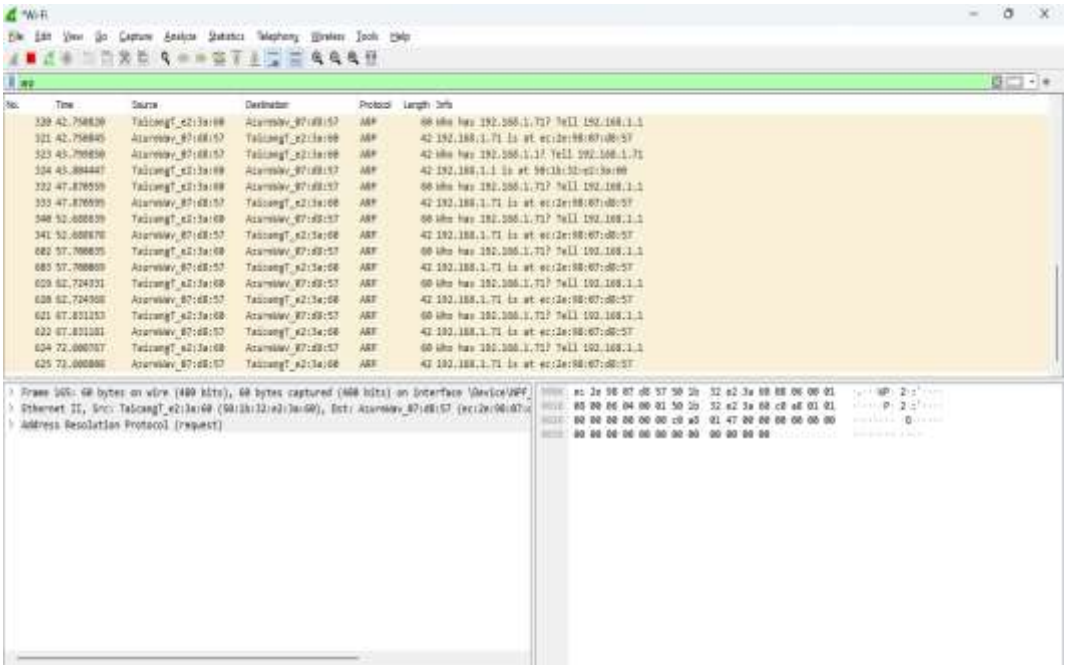
Gambar 4. 2 Tampilan Seluruh Protocol pada Wireshark

Sehingga tampilan protokol akan muncul seluruh ARP secara spesifik yang dapat kita lihat pada Tabel 4.3 dan Gambar 4.3. Dan gambar berikut merupakan tampilan komunikasi yang stabil antara *Client dan Router* sebelum terjadi penyerangan.

Tabel 4. 3 Tampilan Kondisi Koneksi Stabil

No	Time	Source	Destination	Protocol	Length	Info
1	42.750820	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	60	Who has 192.168.1.71? Tell 192.168.1.1
2	42.750845	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57
3	43.799850	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	Who has 192.168.1.1? Tell 192.168.1.71
4	43.804447	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	42	192.168.1.1 is at 50:1b:32:e2:3a:60
5	47.870559	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	60	Who has 192.168.1.71? Tell 192.168.1.1
6	47.870595	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57
7	52.688639	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	60	Who has 192.168.1.71? Tell 192.168.1.1
8	52.688678	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57
9	57.700035	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	60	Who has 192.168.1.71? Tell 192.168.1.1
10	57.700069	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57
11	62.724331	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	60	Who has 192.168.1.71? Tell 192.168.1.1
12	62.724638	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57
13	67.831153	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	60	Who has 192.168.1.71? Tell 192.168.1.1
14	67.831181	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57
15	72.608767	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	60	Who has 192.168.1.71? Tell 192.168.1.1
16	72.608808	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57

Sumber : Data Olahan 2023

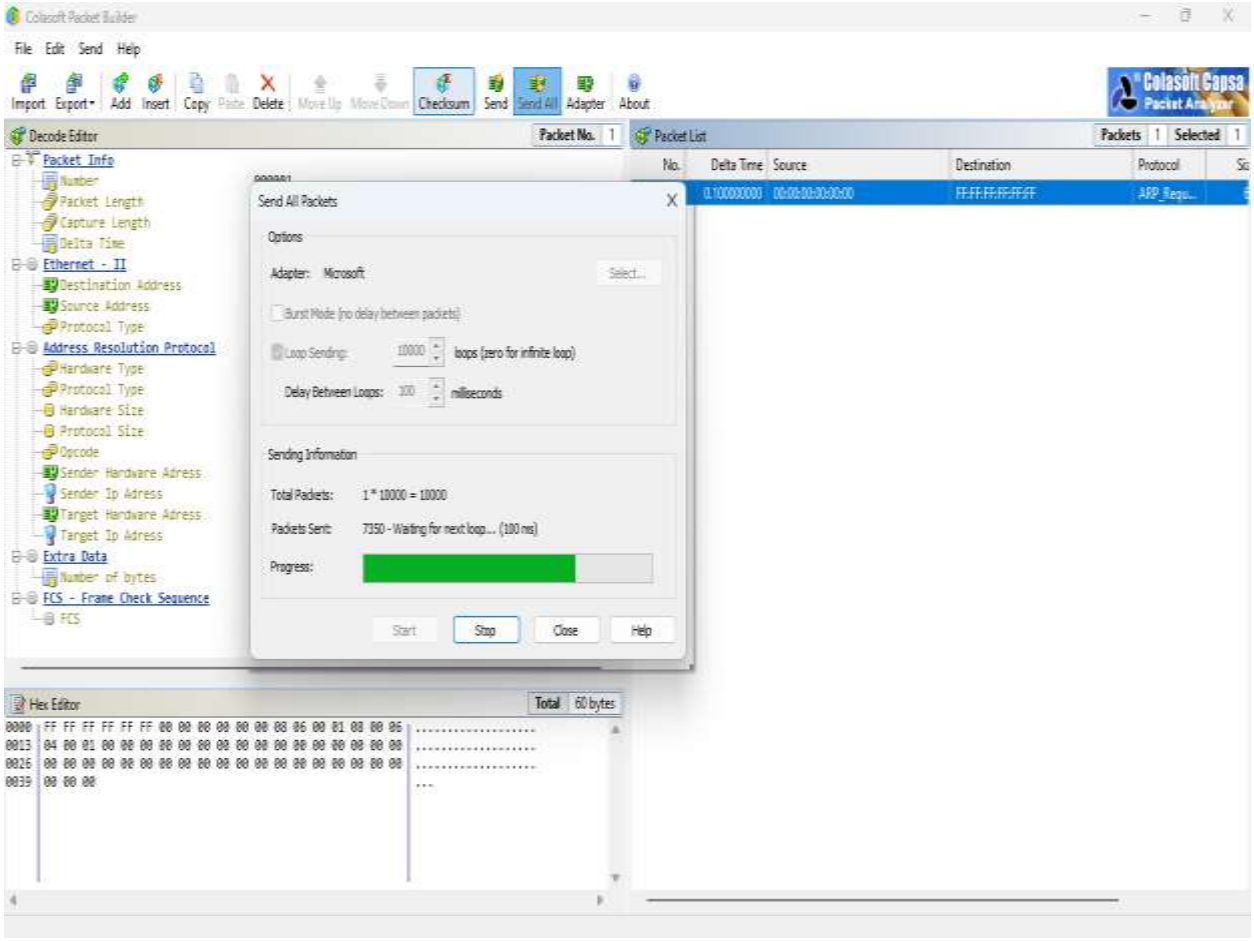


Gambar 4. 3 Kondisi Koneksi Stabil

2) Proses Spoofing

Pengiriman paket ARP palsu yang dilakukan oleh spoofer sebanyak 1000 paket dalam 100 *milisecond* untuk merusak komunikasi antara pengguna jaringan lainnya menggunakan mikrotik. Pada saat *Client* mencari *macc address* mikrotik sehingga penggambaran komunikasi dalam jaringan misalnya IP 192.168.1.71 meminta *macc address* ke mikrotik dengan IP 192.168.1.1. proses komunikasi yang dimaksud yaitu "*who has 192.168.1.71? tell 192.168.1.1"* (siapa yang saat ini memakai IP 192.168.1.71? hubungi saya di IP 192.168.1.1) kurang lebih seperti itulah proses komunikasi yang terjadi. Disaat itulah mikrotik mencatat secara otomatis IP dan *macc address* 192.168.1.71 di *table ARP (Address Resolution Protocol)* dan mikrotik yang saat ini menggunakan IP tersebut akan membalas pesan dengan mengirim ke *client* 192.168.1.71 dan 192.168.1.71 menerima *macc address* 192.168.1.1 lalu menyimpannya di *table ARP (Address Resolution Protocol). Table ARP (Address Resolution Protocol)* setiap perangkat melakukan pembaruan ketika masih menggunakan layanan dhcp dan hal itulah menjadi celah *spoofer* untuk merusak komunikasi dengan

mengirim paket palsa *macc address* yang telah di modifikasi menggunakan aplikasi *Colasoft Packet Builder 2.0.* Pada saat *client* belum lengkap melakukan pembaruan pada *table ARP (Address Resolution Protocol), spoofer* akan masuk merusak proses komunikasi yang terjadi.



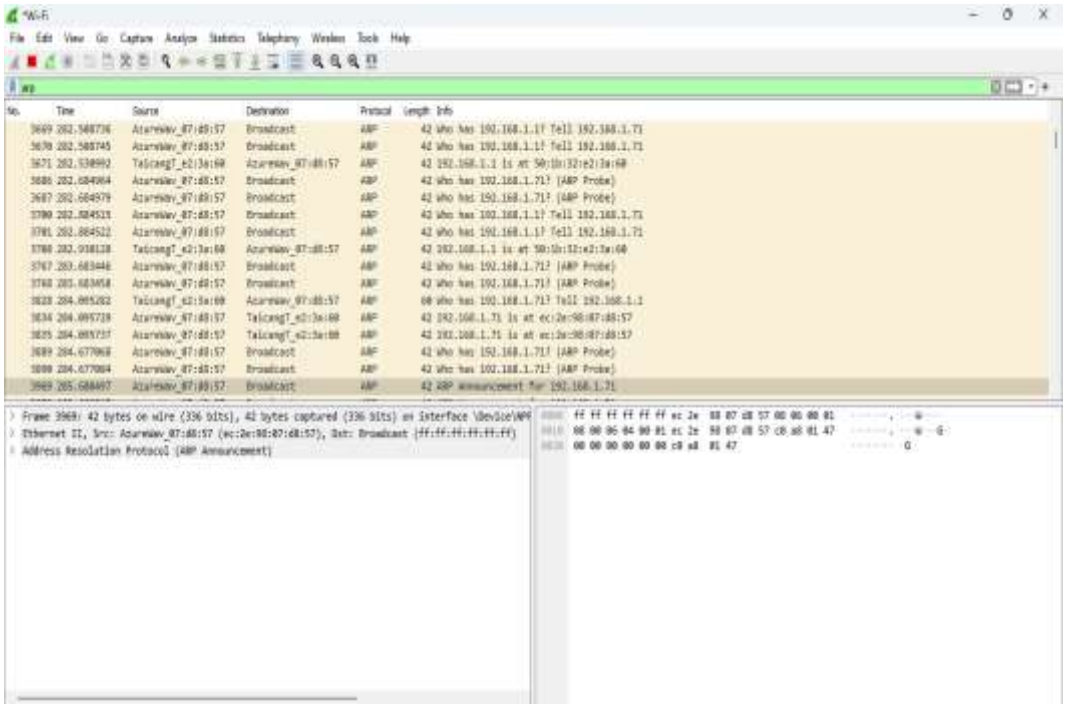
Gambar 4. 4 Proses Pemalsuan Macc Address

Setelah proses pemalsuan *macc address* dan pengiriman paket dilakukan maka pada *table ARP (Address Resolution Protocol)* akan membaca *broadcast* paket palsu yang dikirimkan menggunakan *Colasoft Packet Builder 2.0* yang dapat dilihat pada Tabel 4.4 dan Gambar 4.5.

Tabel 4. 4 Kondisi Koneksi Pemalsuan Macc Address

No	Time	Source	Destination	Protocol	Length	Info
1	282.508736	AzureWav_07:d8:57	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.1
2	282.508745	AzureWav_07:d8:57	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.1
3	282.530992	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	42	192.168.1.1 is at 50:1b:32:e2:3a:60
4	282.684964	AzureWav_07:d8:57	Broadcast	ARP	42	Who has 192.168.1.71? (ARP Probe)
5	282.684979	AzureWav_07:d8:57	Broadcast	ARP	42	Who has 192.168.1.71? (ARP Probe)
6	282.884515	AzureWav_07:d8:57	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.1
7	282.884522	AzureWav_07:d8:57	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.1
8	282.930128	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57
9	282.683446	AzureWav_07:d8:57	Broadcast	ARP	42	Who has 192.168.1.71? (ARP Probe)
10	282.683458	AzureWav_07:d8:57	Broadcast	ARP	42	Who has 192.168.1.71? (ARP Probe)
11	282.095282	TaicangT_e2:3a:60	AzureWav_07:d8:57	ARP	60	Who has 192.168.1.71? Tell 192.168.1.1
12	282.095729	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57
13	282.095737	AzureWav_07:d8:57	TaicangT_e2:3a:60	ARP	42	192.168.1.71 is at ec:2e:98:07:d8:57
14	282.677068	AzureWav_07:d8:57	Broadcast	ARP	42	Who has 192.168.1.71? (ARP Probe)
15	282.677084	AzureWav_07:d8:57	Broadcast	ARP	42	Who has 192.168.1.71? (ARP Probe)
16	282.680497	AzureWav_07:d8:57	Broadcast	ARP	42	ARP Announcement for 192.168.1.71

Sumber : Data Olahan 2023



Gambar 4. 5 Kondisi Koneksi Pemalsuan Macc Address

VI.2 Pengujian Koneksi Victim

Penelitian ini dilakukan dengan menentukan target client yang sedang terkoneksi ke internet dan satu laptop spoofing yang sedang melakukan serangan pemalsuan *macc address*. Berikut merupakan hasil uji koneksi dari proses serangan ARP spoofing atau pemalsuan *macc address* yang dilakukan laptop *spoofer.*

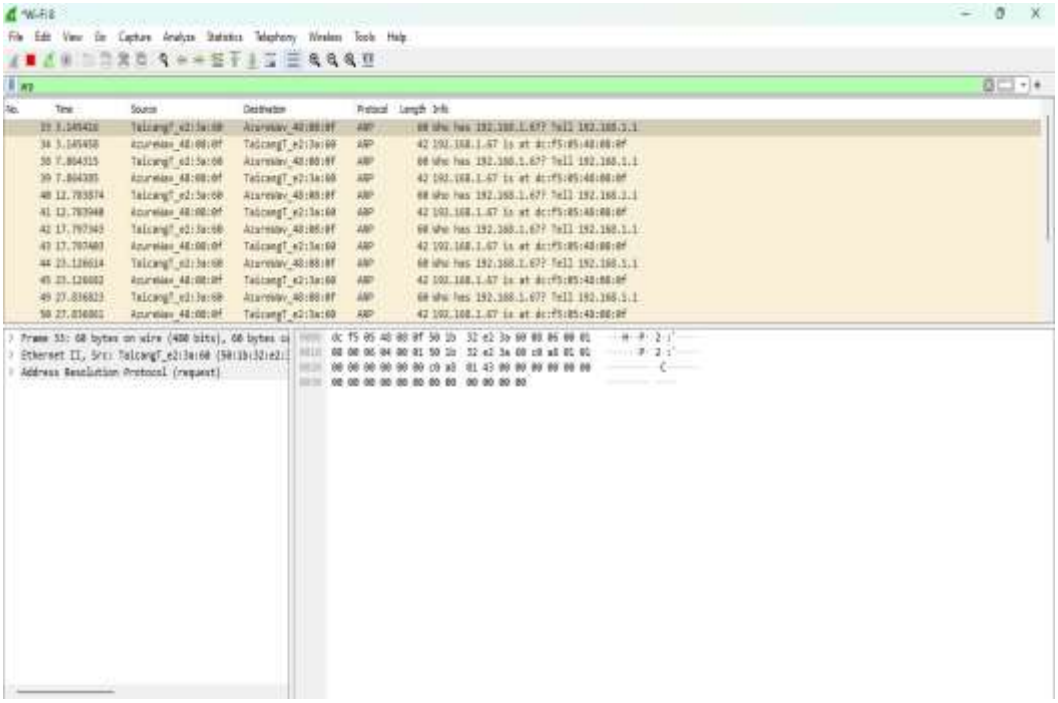
a) Percobaan 1

Laptop target sebelum penyerangan dapat dilihat koneksi komunikasi stabil yang dapat dilihat pada Tabel 4.5 dan Gambar 4.6.

Tabel 4. 5 Sebelum Penyerangan Paket Palsu

No	Time	Source	Destination	Protocol	Length	Info
1	3.145416	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
2	3.145458	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
3	7.864315	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
4	7.864385	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
5	12.783874	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
6	12.783940	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
7	17.797343	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
8	17.797403	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
9	23.126614	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
10	23.126682	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
11	27.836823	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
12	27.836861	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f

Sumber : Data Olahan 2023



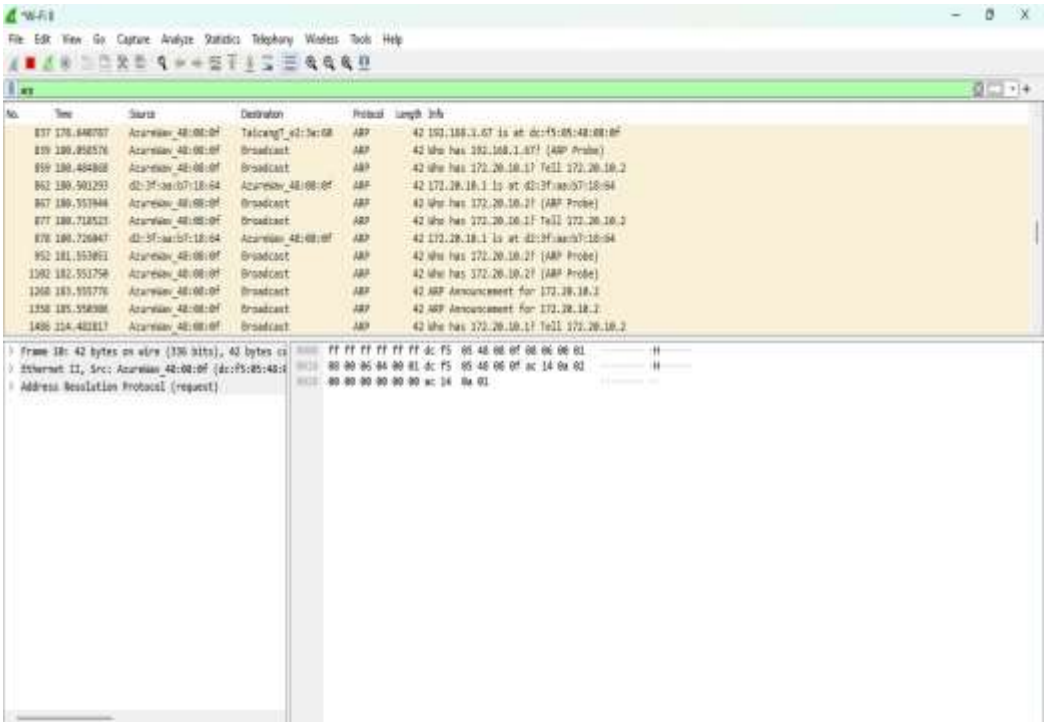
Gambar 4. 6 Sebelum penyerangan paket palsu

Setelah penyerangan paket palsu koneksi komunikasi menjadi teracak atau tidak stabil yang dapat dilihat pada Tabel 4.8 dan Gambar 4.7. Ini menandakan penyerang mulai mengirimkan banyak permintaan ARP palsu pada target. Tujuan dilakukan hal tersebut untuk memperoleh alamat MAC perangkat yang menjadi target sehingga penyerang dapat mengalihkan lalu lintas DNS ke server yang di kendalikan nya.

Tabel 4. 6 Setelah Penyerangan Paket Palsu

No	Time	Source	Destination	Protocol	Length	Info
1	178.640787	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.67 is at dc:f5:05:48:08:0f
2	180.058576	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 192.168.1.67? (ARP Probe)
3	180.484868	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 172.20.10.1? Tell 172.20.10.2
4	180.501293	d2:3f:aa:b7:18:64	AzureWav_48:08:0f	ARP	42	172.20.10.1 is at d2:3f:aa:b7:18:64
5	180.553944	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 172.20.10.2? (ARP Probe)
6	180.718523	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 172.20.10.1? Tell 172.20.10.2
7	180.726047	d2:3f:aa:b7:18:64	AzureWav_48:08:0f	ARP	42	172.20.10.1 is at d2:3f:aa:b7:18:64
8	181.553051	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 172.20.10.2? (ARP Probe)
9	182.551750	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 172.20.10.2? (ARP Probe)
10	183.555776	AzureWav_48:08:0f	Broadcast	ARP	42	ARP announcemen for 172.20.10.2
11	185.550306	AzureWav_48:08:0f	Broadcast	ARP	42	ARP announcemen for 172.20.10.2
12	214.482817	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 172.20.10.1? Tell 172.20.10.2

Sumber : Data Olahan 2023



Gambar 4. 7 Setelah penyerangan paket palsu

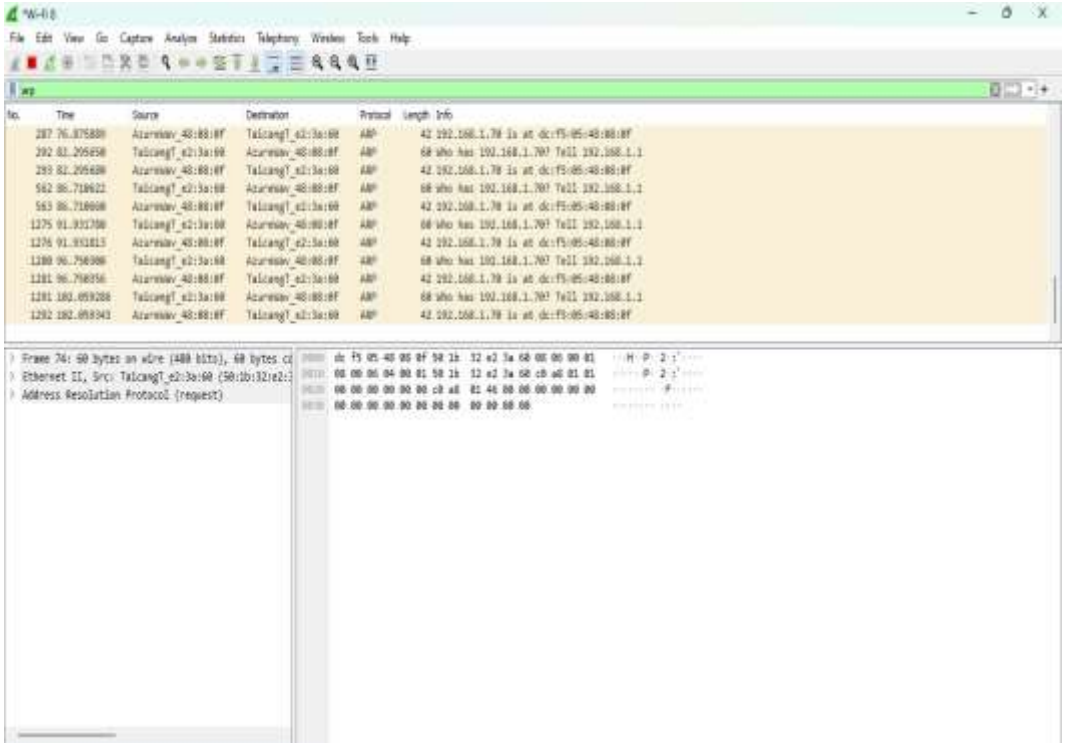
b). Percobaan 2

Laptop target sebelum penyerangan dapat dilihat koneksi komunikasi stabil yang dapat dilihat pada Tabel 4.7 dan Gambar 4.8.

Tabel 4. 7 Sebelum Penyerangan Paket Palsu

No	Time	Source	Destination	Protocol	Length	Info
1	76.875889	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
2	82.295650	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.70? Tell 192.168.1.1
3	82.295650	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
4	86.710622	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.70? Tell 192.168.1.1
5	86.710660	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
6	91.931780	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.70? Tell 192.168.1.1
7	91.931813	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
8	96.750300	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.70? Tell 192.168.1.1
9	96.750356	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
10	96.750356	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.70? Tell 192.168.1.1
11	102.059343	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
12	102.059343	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.70? Tell 192.168.1.1

Sumber : Data Olahan 2023



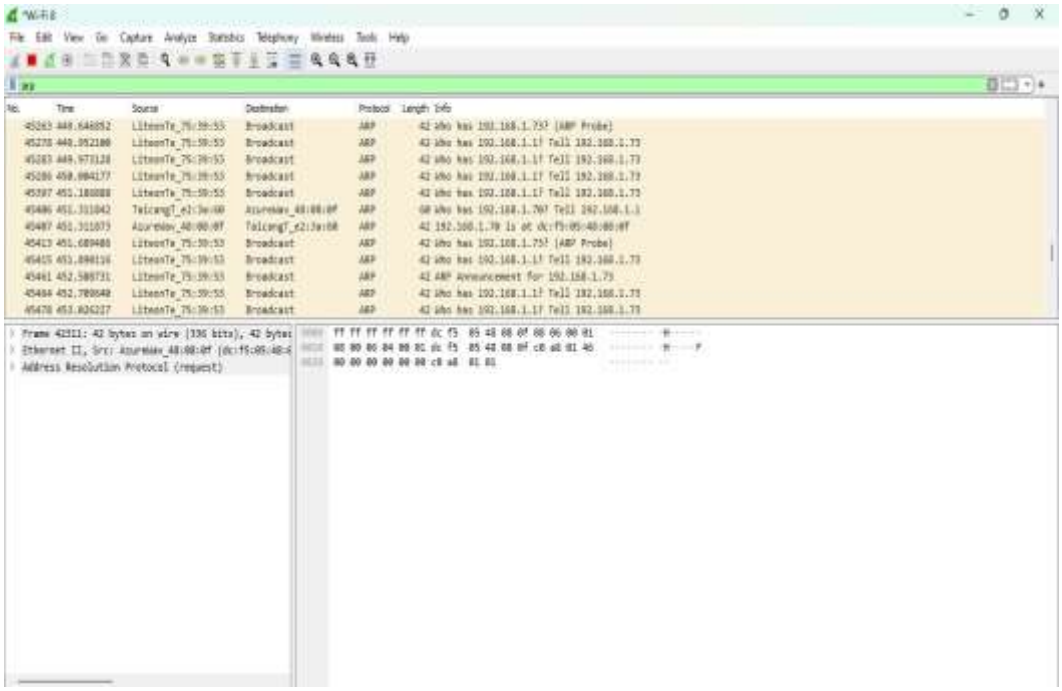
Gambar 4. 8 Sebelum Penyerangan Paket Palsu

Setelah penyerangan paket palsu Setelah penyerangan paket palsu koneksi komunikasi menjadi teracak atau tidak stabil yang dapat dilihat pada Tabel 4.8 dan Gambar 4.9 , bisa kita lihat adanya perbedaan dengan percobaan 1. Dimana pada percobaan 2 hanya menembus 10 ARP palsu sedangkan percobaan 1 menembus 9 ARP. Ini dapat disebabkan karena adanya deteksi dan respon jaringan yang menyadari serangan ARP awal yang menyebabkan adanya perlawanan sehingga terjadi penyesuaian jaringan dengan penambahan jumlah ARP yang dikirimkan.

Tabel 4. 8 Setelah Penyerangan Paket Palsu

No	Time	Source	Destination	Protocol	Length	Info
1	449.646852	LiteonTe_75:39:53	Broadcast	ARP	42	Who has 192.168.1.70? (ARP Probe)
2	449.952100	LiteonTe_75:39:53	Broadcast	ARP	42	Who has 192.168.1.70? Tell 192.168.1.1
3	449.973128	LiteonTe_75:39:53	Broadcast	ARP	42	Who has 192.168.1.70? Tell 192.168.1.1
4	450.004177	LiteonTe_75:39:53	Broadcast	ARP	42	Who has 192.168.1.70? Tell 192.168.1.1
5	451.186888	LiteonTe_75:39:53	Broadcast	ARP	42	Who has 192.168.1.70? Tell 192.168.1.1
6	451.311842	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.70? Tell 192.168.1.1
7	451.311873	LiteonTe_75:39:53	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
8	451.689485	LiteonTe_75:39:53	Broadcast	ARP	42	Who has 192.168.1.70? (ARP Probe)
9	451.890116	LiteonTe_75:39:53	Broadcast	ARP	42	Who has 192.168.1.70? Tell 192.168.1.1
10	452.508731	LiteonTe_75:39:53	Broadcast	ARP	42	ARP Announcement for 192.168.1.73
11	452.709640	LiteonTe_75:39:53	Broadcast	ARP	42	Who has 192.168.1.70? Tell 192.168.1.1
12	453.026227	LiteonTe_75:39:53	Broadcast	ARP	42	Who has 192.168.1.70? Tell 192.168.1.1

Sumber : Data Olahan 2023



Gambar 4. 9 Setelah Penyerangan Paket

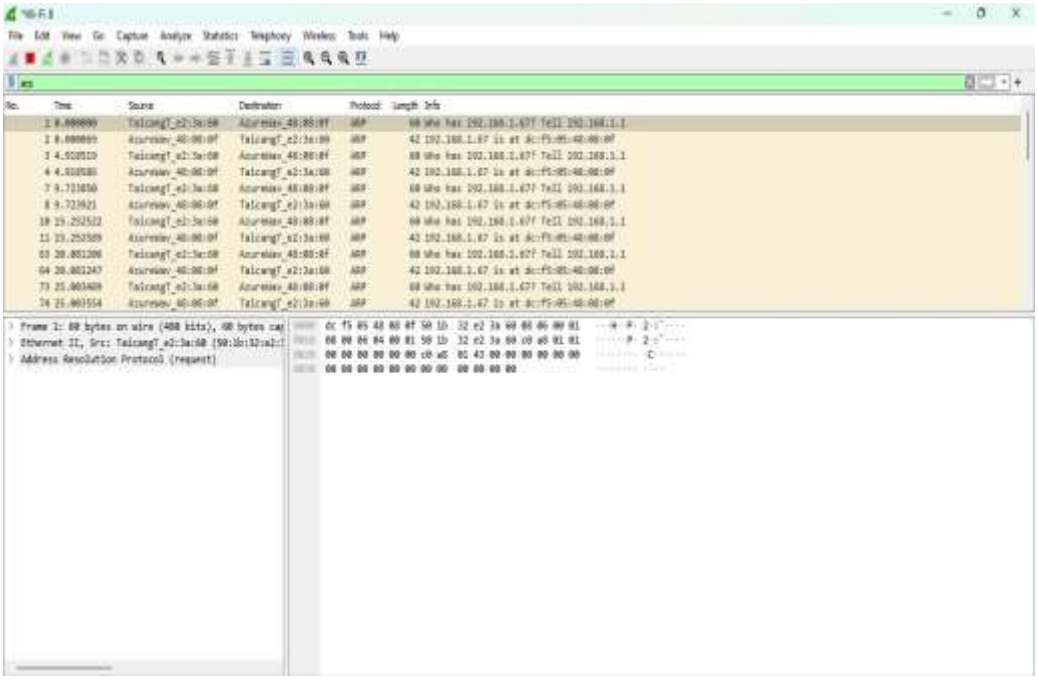
c). Percobaan 3

Laptop target sebelum penyerangan dapat dilihat koneksi komunikasi stabil yang dapat dilihat pada Tabel 4.9 dan Gambar 4.1

Tabel 4. 9 Sebelum Penyerangan Paket Palsu

No	Time	Source	Destination	Protocol	Length	Info
1	0.000000	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
2	0.000069	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
3	4.918518	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
4	4.918586	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
5	9.723850	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
6	9.723921	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
7	15.252522	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
8	15.252589	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
9	20.081206	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
10	20.081247	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f
11	25.003489	TaicangT_e2:3a:60	AzureWav_48:08:0f	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
12	25.003554	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.78 is at dc:fs:05:48:08:0f

Sumber : Data Olahan 2023



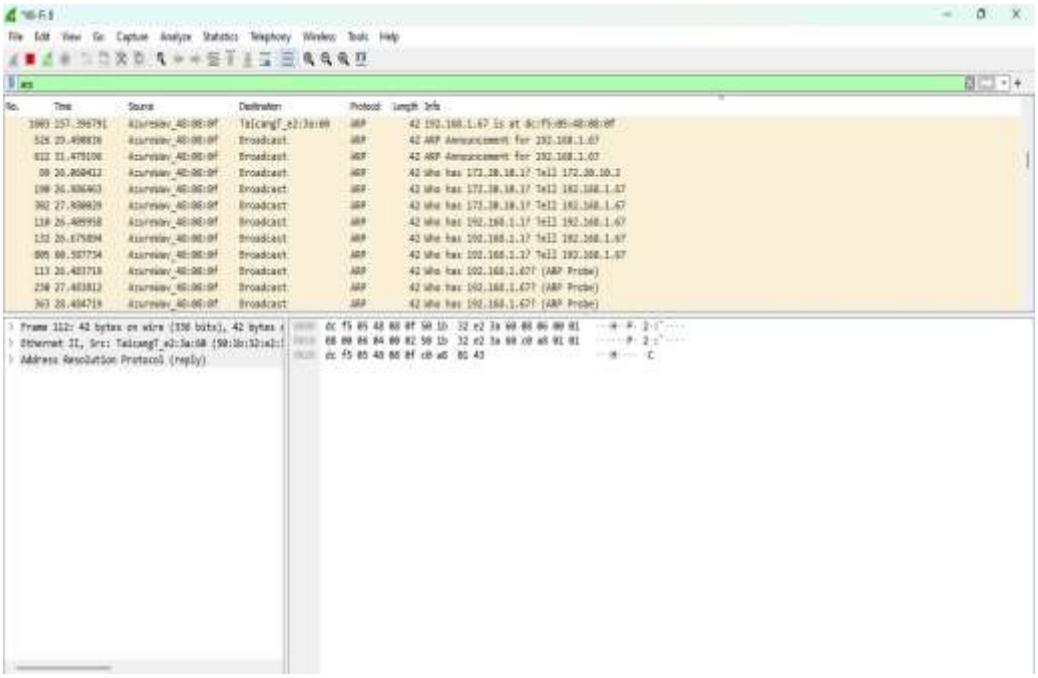
Gambar 4. 10 Sebelum Penyerangan Paket Palsu

Setelah penyerangan paket palsu Setelah penyerangan paket palsu koneksi komunikasi menjadi teracak atau tidak stabil yang dapat dilihat pada Tabel 4.10 dan Gambar 4.11 . pada percobaan 3 ini, bisa kita lihat bahwa jumlah ARP palsu semakin banyak dibandingkan dengan percobaan 1 dan 2 . ini juga disebabkan dari deteksi dan respon jaringan yang menyadari penyerangan ARP awal. Sehingga semakin dilakukan penyerangan semakin terjadi penyesuaian taktik penyerangan jaringan.

Tabel 4. 10 Setelah Penyerangan Paket Palsu

No	Time	Source	Destination	Protocol	Length	Info
1	157.396791	AzureWav_48:08:0f	TaicangT_e2:3a:60	ARP	42	192.168.1.67 is at dc:f5:05:48:08:0f
2	29.490836	AzureWav_48:08:0f	Broadcast	ARP	42	ARP Announcement for 192.168.1.67
3	31.479196	AzureWav_48:08:0f	Broadcast	ARP	42	ARP Announcement for 192.168.1.67
4	26.060412	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 172.20.10.1? Tell 172.20.10.2
5	26.986423	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 172.20.10.1? Tell 192.168.1.67
6	27.980029	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 172.20.10.1? Tell 192.168.1.67
7	26.409958	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.67
8	26.675894	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.67
9	60.387734	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.67
10	26.483719	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 192.168.1.67? (ARP Probe)
11	27.483812	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 192.168.1.67? (ARP Probe)
12	28.484719	AzureWav_48:08:0f	Broadcast	ARP	42	Who has 192.168.1.67? (ARP Probe)

Sumber : Data Olahan 2023



Gambar 4. 11 Setelah Penyerangan Paket Palsu

Dari hasil penelitian didapatkan bahwa terdapat perbedaan *ARP (Address Resolution Packets)* sebelum dan sesudah penyerangan. Perubahan dapat menjadi tanda bahwa ada aktifitas yang mencurigakan dalam jaringan, terutama pada perubahan yang signifikan dalam *request* atau *reply ARP*.

Kondisi koneksi target dimana saat sebelum penyerangan koneksi komunikasi terlihat masih stabil. Ini dikarenakan, target dengan lancar mengakses situs web yang diinginkan dan berkomunikasi dengan server dengan benar melalui DNS yang asli. Sedangkan pada saat sesudah penyerangan, koneksi target tersendat. Ini disebabkan oleh perubahan data DNS yang mengarahkan target ke server yang salah atau sumber daya yang tidak valid. Artinya DNS telah dipalsukan dan mengarahkan ke situs web palsu. Pada saat koneksi komunikasi tersendat biasanya karena adanya upaya pengguna untuk mengakses sumber daya yang sebenarnya melibatkan perubahan arah dan pemrosesan data tambahan untuk mencari alamat IP yang benar.

Pada saat target telah berhasil diarahkan pada server yang diinginkan. Penyerang dapat mengendalikan server tersebut sehingga dapat mencuri data-data

pribadi target. Hal ini tentu sangat merugikan target sehingga diperlukan langkah-langkah perlindungan agar terhindar dari serangan *DNS Spoofing*.

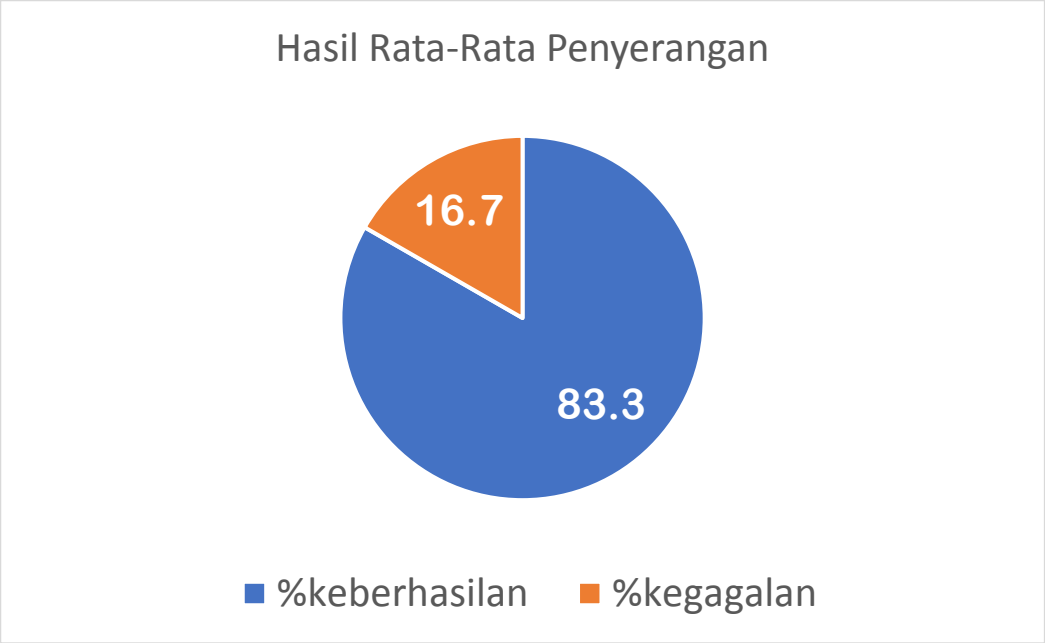
Berdasarkan data yang telah dikumpulkan sehingga hasil uji penyerangan dapat disusun berdasarkan tabel 4.11.

Tabel 4. 11 Hasil Uji Penyerangan

Percobaan	Berhasil	%	Gagal	%
1	9	75	3	25
2	10	83,3	2	16,7
3	11	91,7	1	8,3
Rata-rata	**10**	**83,3**	**2**	**16,7**

Sumber : Data Olahan 2023

Dari data tersebut sehingga dapat disusun dalam sebuah grafik yang dapat dilihat pada Gambar 4.12



Sumber : Data Olahan 2023

Gambar 4. 12 %Hasil Rata-rata Penyerangan.

Terkait hasil data yang telah dikumpulkan, %keberhasilan pada penyerangan 83,3% yang dapat dipengaruhi oleh konfigurasi keamanan yang lemah, kuramgng kesadaran pengguna dan perangkat lunak yang rentan sedangkan %kegagalan 16,7% dipengaruhi oleh deteksi dan respon jaringan.

Ini menyatakan bahwa sistem keamanan jaringan WiFi publik di perumahan CV Dewi sangat rentan terhadap bahaya ancaman termasuk serangan *DNS Spoofing* bagi keamanan informasi dan data yang dikirim melalui jaringan tersebut. Hal ini disebabkan karena jaringan yang terbuka dan dapat mengekspos semua lalu lintas jaringan. Sehingga aktivitas komunikasi atau data yang melintas di jaringan ini akan sangat mudah terbaca menggunakan *Wireshark*.

Pencegahan serangan DNS *spoofing* pada umumnya dengan mengaktifkan AP *Isolation* dan ARP *Static* pada *wireshark*. AP *Isolation* merupakan pengaturan pada umumnya yang ditemukan di *router* atau *access point(AP).* Fungsinya yaitu untuk membatasi komunikasi langsung antara perangkat yang terhubung ke jaringan nirkabel yang sama. Ini dapat membantu melindungi perangkat dalam jaringan dari serangan lokal seperti ARP spoofing, tetapi tidak secara khusus mencegah serangan DNS spoofing.

Sedangkan ARP *Static* merupakan protokol yang berfungsi sebagai pengait alamat IP dengan alamat fisik (MAC *Address}* dalam jaringan. Konfigurasi ARP statis memungkinkan menghubungkan alamat IP dengan alamat MAC tertentu. Ini dapat membantu mencegah serangan ARP spoofing. Namun, pengaturan ARP statis juga merupakan bukan solusi yang tepat digunakan dan dapat membutuhkan administrasi yang rumit. Jadi, mengaktifkan kedua pengaturan hanya melakukan pencegahan sementara namun, tidak memberikan perlindungan yang tepat.

Untuk melindungi jaringan dari serangan DNS spoofing, dapat melakukan beberapa cara sebagai berikut:

1. Menggunakan DNSSEC (DNS Security Extensions): DNSSEC adalah standar keamanan DNS yang membantu memastikan bahwa tanggapan DNS yang diterima benar-benar berasal dari sumber yang sah.

2. Memantau dan mengelola lalu lintas DNS dengan hati-hati menggunakan alat keamanan jaringan seperti firewall dan sistem deteksi intrusi (IDS).
3. Memastikan bahwa perangkat dan perangkat lunak dalam jaringan diperbarui secara teratur untuk mengatasi kerentanannya terhadap serangan DNS spoofing.

BAB V

PENUTUP

V.1 Kesimpulan

Berdasarkan data penelitian yang telah tersusun, maka dapat disimpulkan bahwa:

1. Simulasi keamanan jaringan dilakukan dengan membentuk topologi terkendali untuk melakukan penyerangan DNS spoofing. Serangan ini dilakukan dengan mengirimkan Mac Address palsu kepada target menggunakan C*olasoft Packet Builder 2.0* lalu membandingkan ARP sebelum dan sesudah penyerangan menggunakan *Wireshark* .
2. Penelitian dilakukan dengan membandingkan koneksi komunikasi serta *Displayed ARP request* sebelum dan sesudah penyerangan, sehingga didapati koneksi komunikasi menjadi tidak stabil atau teracak. Peningkatan *request* tersebut menjadikan tanda adanya aktifitas mencurigakan. Cara pencegahan sementara dapat dilakukan dengan pengaktifan AP *Isolation* dan ARP *Static* dan beberapa langkah yang tepat yaitu menggunakan DNSSEC (*DNS Security Extensions*), memantau dan mengelola lalu lintas DNS menggunkan *firewall* dan IDS.

V.2 Saran

Berdasarkan hasil dan pembahasan sehingga dapat diuraikan saran pada penelitian selanjutnya yaitu:

1. Penelitian selanjutnya sebaiknya menggunakan Aplikasi yang lebih banyak dan menggunakan metode pengumpulan data yang bervariasi.
2. Penelitian selanjutnya sebaiknya mencoba serangan jaringan lainnya sehingga menjadi penunjang untuk menambah perlindungan yang lebih baik.

DAFTAR PUSTAKA

Kohlios, C. P., & Hayajneh, T. (2018). A comprehensive attack flow model and security analysis for Wi-Fi and WPA3. *Electronics (Switzerland)*, *7*(11). https://doi.org/10.3390/electronics7110284

Liantoni. (2022). *Analisa Keamanan Jaringan Publik pada fasilitas sosial di kota palangkaraya menggunakan wireshark*.

Mcshane, I., Gregory, M. A., & Wilson, C. K. (2019). *Practicing safe public wi-fi Assessing and managing data-security risks*. https://ssrn.com/abstract=2895216Electroniccopyavailableat:https://ssrn.com/abstract=2895216

Nugroho, B. A., Supriyono, H., & Wantoro, J. (2021). *ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) TERHADAP SERANGAN PACKET SNIFFING*.

Pangestu, T., & Liza, R. (2022). Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing. *JITEKH*, *10*(2), 60–67.

Patil, P., Meshram, B. B., & Ambavkar, P. (2021). *Analysis of Security in Wireless Network*. *2*, 315–319. https://www.researchgate.net/publication/231178407

Pratama, A., & Syamsuar, D. (2022). ANALISIS KEAMANAN JARINGAN PADA LAYANAN INTERNET PUBLIK MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES) DPRD PROVINSI SUMATRA SELATAN. *Bina Darma Conference on Computer Science*.

Rachman, R. (2021). *analisis kemanan jaringan wireles (WLAN) dengan metode penetration testing pada PT PLN (PERSERO) sektor pengendalian pembangkitan pekanbaru*.

Ruslianto, I., Hidayati, R., Rekayasa Sistem Komputer, J., & Hadari Nawawi, J. H. (2021). ANALISIS PERBANDINGAN SISTEM KEAMANAN JARINGAN WI-FI PROTECTED ACCESS 2-PRE SHARED KEY (WPA2-PSK) DAN CAPTIVE PORTAL PADA JARINGAN PUBLIK WIRELESS. In *Coding : Jurnal Komputer dan Aplikasi* (Vol. 09, Issue 01).

Siregar, T. (2019). *Analisis Keamanan Jaringan Pada Fasilitas Internet (WIFI) Terhadap Serangan Paket Siffing*.

Sombatruang, N., Kadobayashi, Y., Sasse, M. A., Baddeley, M., & Miyamoto, D. (2020). *The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan*. www.group.macromill.com

Stiawan, D., & Rini, D. P. (2019). *ANALISIS PERBANDINGAN SISTEM KEAMANAN WEP/WPA/RADIUS PADA JARINGAN PUBLIK WIRELESS HOTSPOT*.

Suharmanto, A., Lumentas, A., & Najoan, X. (2020). Analisa Keamanan Jaringan Wireless Di Universitas SAM Ratulangi. *Jurnal Teknik Informatika*.

Supriyanto, A. (2022). Analisis Kelemahan Keamanan pada Jaringan Wireless. *Jurnal Teknologi Informasi DINAMIK*, *XI*(1), 38–46.

Susanto, A., & Raharja, W. K. (2021). Simulation and Analysis of Network Security Performance Using Attack Vector Method for Public Wifi Communication. *The IJICS (International Journal of Informatics and Computer Science)*, *5*(1), 7. https://doi.org/10.30865/ijics.v5i1.2764

LAMPIRAN

1. Surat Izin Penelitian

Nomor : 1676/B/DFT/TE-UNIFA/XI/2023
Lamp : -
Hal : **Permohonan Izin Penelitian**

Kepada Yth.
Kepala Dinas Komunikasi dan informatika Kota Makassar
Di-
Jl. A.P. Pettarani No. 62

Dengan Hormat,

Sehubungan dengan studi mahasiswa kami yang sedang berlangsung di Program Studi Teknik Elektro Fakultas Teknik Universitas Fajar, maka bersama dengan surat ini kami memohon agar kiranya Bapak/Ibu berkenan memberikan izin kepada mahasiswa/i kami untuk melaksanakan Penelitian dan Pengambilan Data dalam rangka penyusunan Tugas Akhir (TA) di Perusahaan yang Bapak/Ibu pimpin dalam kurun waktu **7 Hari**. Program ini salah satu mata kuliah dalam kurikulum Program Studi Teknik Elektro Fakultas Teknik Universitas Fajar.

Adapun nama mahasiswa/I yang kami usulkan dalam menjalankan penelitian yakni sebagai berikut:

No	Nama	Stambuk	Program Studi/Konsentrasi	Judul Tugas Akhir
1	Muh. Suryadi Adam	1920221034	Teknik Elektro / Telekomunikasi	Simulasi Analisis Keamanan Jaringan Pada Wifi Publik di CV. Dewi Menggunakan Wireshark

CP: 0895334133984

Demikian Permohonan ini, atas kesediaan dan perhatiannya kami ucapkan terima kasih.

Makassar, 7 November 2023
Dekan Fakultas Teknik,

UNIFA
UNIVERSITAS FAJAR
DEKAN FAKULTAS TEKNIK

Prof. Dr. Ir. Erniati, ST., MT.
NIDN: 0904107701

website: ft.unifa.ac.id email: ft@unifa.ac.id
Jl. Prof. Abdurrahman Basalamah No. 101 Telp. (0411) 447508 – 459938 Makassar 90231

2. Lokasi Penelitian

3. Proses Penelitian


MAYA