Jurnal Ilmiah Informatika (JIF)
| ISSN (Print) 2337-8379 | ISSN (Online) 2615-1049 |
Jurnal online di akses di http://ejournal.upbatam.ac.id/index.php/jif

Analisis Keamanan Jaringan Wifi Mahasiswa UBD Dari Serangan Packet Sniffing

Tamsir Ariyadi[1] , Irwansyah[2] , M.Syaiful Huda[3]
[1,2,3]*Universitas Bina Darma, Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, 30264, Indonesia*

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 19 Februari 2024
Revisi Akhir: 05 Maret 2024
Diterbitkan *Online*: 12 Maret 2024

KATA KUNCI

Keamanan Jaringan Wifi, Packet Sniffing, Ettercap Dan Wireshark

KORESPONDENSI

E-mail: tamsirariyadi@binadarma.ac.id

A B S T R A C T

The wifi network of Bina Darma University is open to potential attacks by hackers, as they are unavoidably carried out. Network security is the act of recognizing and blocking unwanted users, or intruders, from computer networks. It serves as a safeguard for a network system against unauthorized and careless network users. In this study, the "Experiment Method" is employed. One approach that seeks to both test and explain an event is the experiment technique. Using the tools ettercap and wireshark, tests on network security were run and the findings analyzed for this study. The study's findings show that the network security encryption utilized at Bina and the security mechanism on the ubd student wifi network are both in good working order.

1. PENDAHULUAN

Kemajuan dan perkembangan teknologi saat ini sangat pesat.Salah satu teknologi yang paling populer pada saat ini adalah Wi-Fi (wireless fedeliti) teknologi ini memungkinkan banyak komputer terhubung ke jaringan tanpa kabel lokal area (WLAN)[1][2]. Jaringan Wi-Fi menggunakan standar IEEE 802.11 untuk berkomunikasi dan dapat beroperasi dalam jarak sekitar ratusan meter, atau standar IEEE 802.11 untuk W-LAN di dalam ruangan[3]. [4]Di era saat ini, keamanan jaringan Wi-Fi atau jaringan tanpa kabel menjadi lebih penting karena jaringan yang terhubung dengan internet pastinya tidak selalu aman dan bisa di eksploitasi oleh hacker baik pada jaringan kabel dan nirkabel [5]oleh sebab itu analisis keamanan jaringan wifi sangat penting untuk melindungi data dan informasi yang tertransmisikan melalui sinyal nirkabel[6][7].

Universitas Bina Darma menggunakan akses jaringan internet dalam menjalankan aktivitas, namun walaupun sering digunakan tanpa disadari bahwa jaringan internet memiliki beberapa kelemahan terutama dibidang keamanan. contohnya serangan hacker, pencurian data informasi dan Serangan packet sniffing[8]. Keamanan Jaringan Merupakan Suatu pelindung dalam sebuah system jaringan untuk memproses mencegah para pengguna jaringan yang tidak berhak dan yang tidak bertanggung jawab serta proses mencegah dan mengidentifikasi pengguna yang tidak sah (penyusup) dari jaringan komputer[9].

Penelitian ini menggunakan aplikasi ettercap dan wireshark. Ettercap adalah alat packet sniffer yang digunakan untuk memverifikasi keamanan jaringan dan menganalisis protokol jaringan[10]. Selain itu, ia dapat mencuri kata sandi, memblokir lalu lintas di jaringan lokal, dan mendengarkan protokol jaringan secara aktif Selain dikenal sebagai network packet analyzer, wireshark adalah alat yang dirancang untuk menganalisis paket data jaringan. Fungsinya adalah untuk mengumpulkan semua data saat komunikasi data di jaringan internet dan menampilkan data tersebut sedetail mungkin[11].

Pada penelitian ini akan dilakukan percobaan sniffing pada jaringan wifi mahasiswa UBD menggunakan metode eksperimen. Hasil percobaan tersebut kemudian akan dilakukan analisis untuk mengetahui tingkat kesulitan dan keamanan dari kegiatan sniffing pada jaringan wifi mahasiswa Universitas Bina Darma. Kontribusi dari penelitian ini diharapkan mampu membantu mengidentifikasi atau mendeteksi pola serangan yang ada di jaringan wi-fi Mahasiswa di Universitas Bina Darma

2. TINJAUAN PUSTAKA

2.1 Definisi Jaringan Nirkabel

Jaringan nirkabel adalah sebuah infrastruktur komunikasi yang memungkinkan perangkat bisa terhubung dan berkomunikasi tanpa kabel fisik dalam definisi secara luas dapat diartikan sebagai jaringan nirkabel mencakup berbagai teknologi dengan

memanfaatkan sumber gelombang elektromagetik gelombang radio atau gelombang mikro sebagai penghubung antar perangkat definisi ini mencakup berbagai jenis jaringan termasuk jaringan lokal nirkabel (wlan) jaringan seluler dan teknologi nirkabel lainnya.

Berikut manfaat adanya teknologi jaringan nirkabel atau jaringan wifi[12][13].

1. keleluasaan mobilitas

jaringan nirkabel memungkinkan perangkat untuk terhubung tanpa memerlukan kabel fisik. Ini memberikan kebebasan mobilitas yang tinggi, memungkinkan pengguna untuk bergerak bebas dan tetap terhubung ke jaringan di berbagai lokasi.

2. Akses internet tanpa batas

jaringan nirkabel memungkinkan akses internet tanpa batas, baik di dalam rumah, di tempat kerja, di tempat umum, atau bahkan saat bepergian. Ini memfasilitasi pertukaran informasi dengan cepat dan efisien.

3. Konektivitas perangkat

Jaringan nirkabel mendukung konektivitas antar berbagai perangkat, termasuk smartphone, tablet, laptop, dan perangkat IoT. Ini menciptakan ekosistem terhubung yang memungkinkan berbagi data dan kolaborasi antar perangkat dengan mudah.

4. Skalabilitas yang mudah

Jaringan nirkabel memungkinkan menambah atau mengurangi perangkat yang terhubung tanpa perlu mengganti atau menambahkan kabel. Ini memberikan skalabilitas yang tinggi dan memudahkan penyesuaian dengan pertumbuhan atau perubahan kebutuhan.

5. Peningkatan produktivitas

Karena pengguna dapat terhubung ke jaringan di mana saja dan kapan saja, produktivitas meningkat. Karyawan dapat bekerja dari tempat yang nyaman, mengakses data, dan berkomunikasi tanpa terbatas oleh lokasi fisik

2.2 Metode Eksperimen

Menurut djamarah dan zain metode eksperimen adalah cara penyajian dimana kita melakukan sebuah percobaan atau testing untuk mengetahui dan membuktikkan sendiri sesuatu yang telah dipelajari.

2.3 Jaringan komputer

Jaringan komputer adalah kumpulan komputer yang terhubung satu sama lain sehingga perangkat dapat berkomunikasi dan berbagi data. Beberapa keuntungan menggunakan jaringan komputer untuk aktivitas apapun termasuk pesan langsung, video, email, dan komunikasi melalui email, serta fitur berbagi perangkat seperti printer, mesin foto kopi, pemindai, berbagi file dan perangkat lunak berbasis sistem jarak jauh. Keamanan jaringan komputer melibatkan perlindungan terhadap integritas, kerahasiaan, dan ketersediaan data. Serta aspek keamanan mencakup enkripsi data, pengaturan akses, dan pemantauan aktivitas untuk mencegah serangan siber.

2.4 Hacker

Peretas, juga dikenal sebagai hacker, adalah orang yang mahir dalam komputer, pemrograman, dan jaringan yang dapat merusak sistem dan jaringan yang aman dengan menggunakan kerentanan Sistem yang sudah ada. Setiap tindakannya selalu merugikan pihak tertentu Jika saat beraksi dan kegiatannya sudah pasti terlibat dalam kegiatan kriminal.

2.5 Sniffing

Sniffing adalah teknik serangan yang memantau atau Mengontrol setiap paket yang dikirim melalui media komunikasi kabel atau nirkabel. Ini dilakukan melalui perangkat lunak atau perangkat keras yang memantau lalu lintas yang masuk ke jaringan. Berikut Adalah Beberapa Jenis Ancaman Serangan Yang Dapat Muncul Dari Teknik Sniffing:

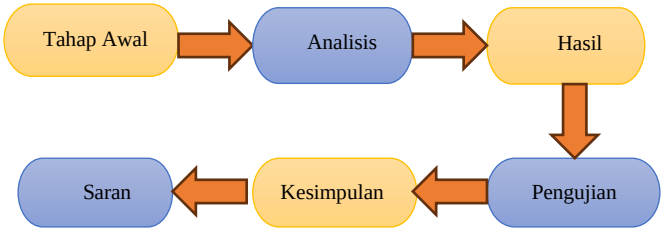
1. Pencurian Data Pengguna, Sniffing Dapat Digunakan Untuk Mencuri Informasi Pengguna Seperti Nama Pengguna, Kata Sandi, Atau Data Pribadi Yang Dikirimkan Melalui Lalu Lintas Jaringan. Dampaknya Penyerang Dapat Mendapatkan Akses Ke Akun Pengguna Dan Melakukan Penyalahgunaan Informasi Pribadi.
2. Pengintaian Aktivitas Pengguna, Sniffing Dapat Digunakan Untuk Mengintai Aktivitas Pengguna, Termasuk Riwayat Browsing, Email, Atau Obrolan Online.Dampaknya Dapat Mengancam Privasi Pengguna.
3. Serangan Man In The Middle (Mitm), Sniffing Dapat Menjadi Komponen Dari Serangan Mitm, Di Mana Penyerang Menempatkan Diri Di Antara Dua Entitas Yang Sedang Berkomunikasi. Dampaknya Memungkinkan Penyerang Untuk Memodifikasi Atau Mencuri Data Yang Melewati Mereka Tanpa Diketahui Oleh Pihak Yang Berkomunikasi.
4. Pencurian Informasi Bisnis, Sniffing Dapat Digunakan Dalam Mencuri Informasi Bisnis Rahasia,Rencana Strategis Atau Data Terkait Bisnis, Dampaknya Dapat Mengancam Kerahasiaan Perusahaan Dan Dapat Merugikan Persaingan Bisnis.
5. Pencurian Informasi Indentitas, Sniffing Dapat Digunakan Untuk Merekam Dan Mencuri Informasi Identitas Pribadi Seseorang, Seperti Nama Lengkap, Alamat, Tanggal Lahir, Nomor KTP, Atau Informasi Keuangan Yang Terkait. Dampak Nya Ialah Informasi Identitas Yang Dicuri Dapat Digunakan Untuk Membuat Akun Online Atau Melakukan Kegiatan Kriminal Di Dunia Maya Atas Nama Korban.

3. METODOLOGI

Metode Yang Digunakan Dalam Penelitian Ini Menggunakan Metode eksperimen dengan melakukan percobaan serangan sniffing pada jaringan wifi Mahasiswa UBD. Tahapan Penelitian bisa dilihat pada gambar 1.

3.1. Tahapan Penelitian

Tahapan dalam metode eksperimen bisa dilihat Pada gambar 1 dibawah Ini



Gambar 1. Topologi Tahapan Penelitian.

Dari gambar diatas metode yang dilakukan melalui beberapa tahapan dapat diuraikan sebagai berikut :

1. Tahap awal

Pada tahap awal, penulis menyiapkan peralatan penelitian. Untuk melakukan sniffing, aplikasi ettercap diinstal dan dipasang pada perangkat keras yang terkoneksi ke jaringan WiFi mahasiswa universitas bina darma

2. Analisis

Di tahap ini penulis melakukan serta menganalisa permasalah yang terjadi pada objek dan fenomena yang sedang terjadi.dan juga menganalisa keamanan dengan menerapkan sistem keamanan agar dapat mencegah dari kejahatan serangan

3. Pengujian/testing

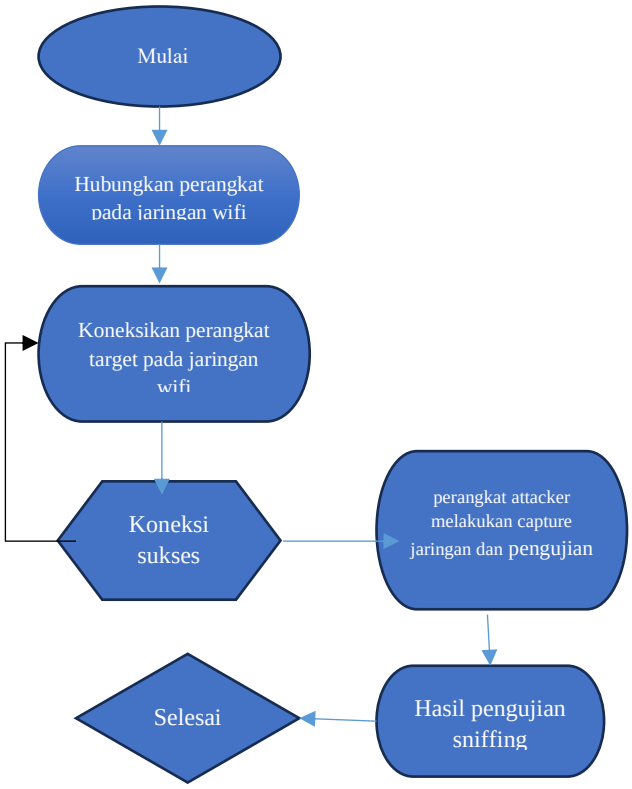
Peneliti akan melakukan pengujian serangan pada jaringan wifi mhs yang sudah terkoneksi ke internet dan mendapatkan hasil berdasarkan permasalahan yang ada pada dan nantinya akan mendapatkan hasil dari analisis berdasarkan permasalahan yang ada pada permasalahan penelitian ini.

4. Hasil

Hasil dari pengujian sistem serangan dan keamanan tersebut bermanfaat untuk menangani kasus yang berdasarkan fenomena munculnya permasalahan yang ada pada penelitian ini,serta menghasilkan solusi dalam mengatasi permasalahan tersebut

3.2. Alur kerja

Alur kerja penelitian dapat dilihat pada gambar 2 *flowchart*



Gambar 2 *Flowchart* Penelitian

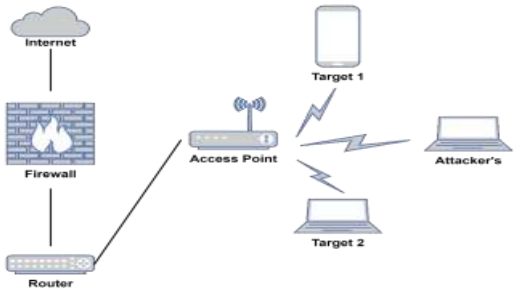
3.3. Perangkat hardware dan software

A. Perangkat hardware

B. Laptop/PC

C. Router wireless /wifi yang terkoneksi di jaringan wifi mahasiswa UBD

- Aplikasi ettercap dan wireshark dengan topologi jaringan



seperti gambar 3 berikut ini

Gambar 3. Topologi jaringan sumber 2.

D. Perangkat Software

1. Sistem Operasi :
2. Windows 10 – 11 (64-Bit)
3. Virtual Box (64-Bit)
4. Kali Linux (64-Bit)
5. Cmd Windows

4. HASIL DAN PEMBAHASAN

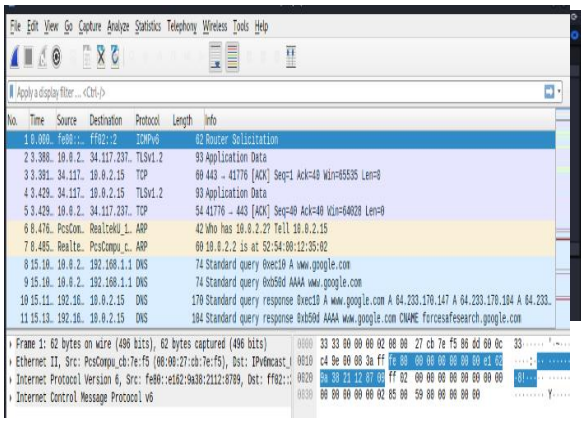
4.1. Tampilan Ip Address Pada Jaringan Wifi Mahasiswa UBD

Gambar 4. Tampilan pada aplikasi ettercap

Pada gambar 4 merupakan tampilan ettercap menampilkan ip address pada tahap awal terlihat saat melakukan pengujian serangan sniffing gambar di atas ini menunjukkan bagaimana IP laptop korban serangan dapat dideteksi, IP address jaringan pelaku diletakkan pada target 1, dan IP address laptop korban serangan diletakkan pada target 2 pada tools Ettercap.

4.2. Tampilan *capture* paket jaringan

1. Pada gambar 5 menunjukkan bahwa penulissedang melakukan analysis dan pencapturean pada jaringan wifi. ketika memulai menekan " *Start capturing packets* Sniffing pada Wireshark akan dilakukan penangkapan pada jaringan sesuai dengan konfigurasi yang sudah dilakukan serta proses pengambilan paket data yang melintasi jaringan akan berlangsung real tiime. file yang akan dihasilkan.

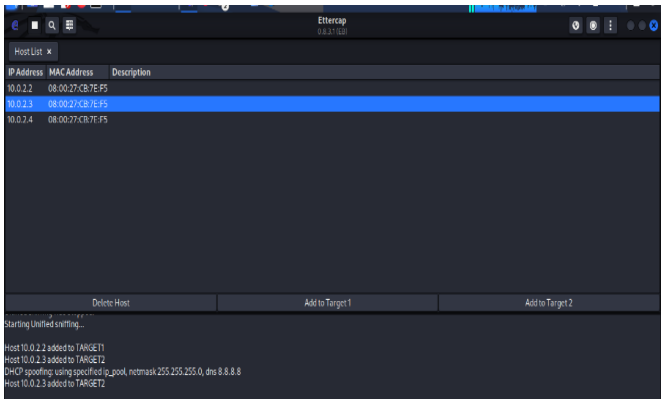


Gambar 5. Capture jaringan di wireshark

1. Pada gambar 6 dibawah ini menunjukkan bahwa ketika ketika kita sudah memulai untuk melakukan *sniffing* menggunakan *wireshark*, disini akan mencoba untuk mengakses situs-situs yang akan diuji coba salah satunya web portal login universitas Bina darma

Gambar 6. Login Web Elearning Universitas Bina Darma

2. Pengujian Penangkapan Jaringan Wifi Menggunakan Tools Ettercap Kali Linux.

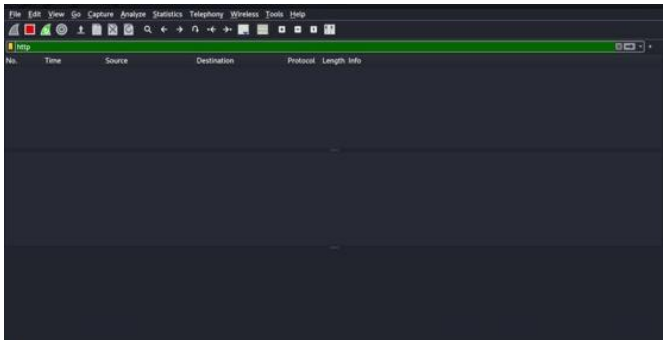


Gambar 7. proses penangkapan jaringan wifi pada ettercap

Gambar diatas menunjukkan bahwa pada saat melakukan pengujian pada serangan sniffing menunjukkan bahwa ip dari laptop korban penyerangan tidak terdeteksi oleh Ettercap. ini menunjukkan bahwa tidak ada aktivitas *sniffing* pada lalu lintas jaringan menandakan bahwa jaringan wi-fi Mhs Ubd tergolong aman dari serangan sniffing.

3. Capture Jaringan Di Wireshark

Pada tahap selanjutnya penulis akan mencoba melakukan penangkapan jaringan wi-fi menggunakan tools wireshark untuk memastikan bahwa jaringan Wi-Fi Mhs Ubd benar-benar aman dari serangan sniffing.



Gambar 8. Tampilan hasil capture di wireshark

Terlihat pada Gambar 8 menunjukkan bahwa penyerang tidak dapat menangkap apa pun yang dilakukan korban penyerangan; oleh karena itu, penyerang tidak dapat mendapatkan informasi data atau akses korban, dan penyerang tidak dapat menangkap apa pun yang dilakukan korban penyerangan. karena saat melakukan sniffing, jaringan Wi-Fi-nya telah terputus. Menurut penelitian ini, data yang dikumpulkan dari serangan packet sniffing pada jaringan WiFi Mahasiswa di Universitas Bina Darma Sumatera Selatan, menunjukkan bahwa keamanana jaringan sudah aman

4.3. Hasil dari pengujian serangan packet sniffing

Tabel 1 Hasil dari pengujian serangan *packet sniffing*

Titik pengujian	Situs yang di uji coba	Hasil	Keterangan
Jaringan wifi Mahasiswa UBD	Portal Halaman WEB	Aman	Tidak Berhasil Menangkap Paket Data Informasi Jaringan Mhs Ubd
Jaringan wifi Mahasiswa UBD	*E-LEARNING BINA DARMA*	*AMAN*	*Tidak Berhasil Menangkap Paket Data Informasi Jaringan Mhs Ubd*

Tabel 2 analisis ancaman serangan

Ancaman Serangan	Status	Keterangan
Pencurian informasi	AMAN	Tidak ditemukan
Serangan man in the middle attack	AMAN	Tidak ditemukan
Pencurian credensial wifi	AMAN	Tidak ditemukan
Pengawasan aktivitas pengguna	AMAN	Tidak ditemukan
Pencurian data user dan pass	AMAN	Tidak ditemukan
Pemantauan lalu lintas jaringan	AMAN	Tidak ditemukan

Tabel hasil penelitian di atas menunjukkan bahwa serangan sniffing paket telah dilakukan pada jaringan Wifi Mahasiswa universitas Bina Darma. Pada saat pengujian serangan sniffing, peneliti tidak bisa melakukan serangan packet sniffing pada jaringan Wifi wifi Mahasiswa UBD karena jaringan tersebut telah dienskripsikan untuk keamanan menggunakan WPA2. Selain itu, jaringan WiFi Mahasiswa Universitas Bina Darma Sumatera Selatan dinyatakan aman dari serangan packet sniffing yang telah diujicobakan oleh peneliti

5. KESIMPULAN DAN SARAN

Pada Analisis Keamanan Jaringan Wifi Mhs UBD dari serangan packet sniffing, penguji tidak dapat mendeteksi masalah keamanan jaringan karena saat pengujian serangan tidak ditemukannya identitas ip address dari target serangan. Dari hasil analisis data dan percobaan serangan packet sniffing yang telah dilakukan maka Dapat Disimpulkan bahwa sistem keamanan pada jaringan wifi Mahasiswa UBD tidak mengalami masalah dan enskripsi keamanan jaringan yang digunakan di universitas bina darma sangat baik. Saran untuk penelitian berikutnya adalah dengan membuat penelitian ini lebih spesifik lagi serta dapat menambahkan point point yang relevan pada penelitian tersebut. tentunya penelitian yang kami buat masih banyak kekurangan. Saran dari penulis, gunakan lah tools ettercap dan wireshark dengan bijak dan sebaik mungkin tanpa merugikan pihak manapun.

DAFTAR PUSTAKA

[1] M. Hasbi, A. Reza Aristiadi Nurwa, D. Febriyan Priambodo, W. Riski Aulia Putra, S. Sinar Nusantara, and P. Siber dan Sandi Negara, "Infrastructure as Code for Security Automation and Network Infrastructure Monitoring," *Tek. Inform. dan Rekayasa Komput.*, vol. 22, no. 1, pp. 203–217, 2022, doi: 10.30812/matrik.v22i1.2471.

[2] A. Zappone, M. Di Renzo, and M. Debbah, "Wireless Networks Design in the Era of Deep Learning: Model-Based, AI-Based, or Both?," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 7331–7376, 2019, doi: 10.1109/TCOMM.2019.2924010.

[3] T. Ariyadi and A. T. Maulana, "Penerapan Web Proxy Dan Management Bandwidth Menggunakan Mikrotik Routerboard Pada Kantor Pos Palembang 30000," *J. Ilm. Inform.*, vol. 9, no. 02, pp. 116–122, 2021, doi: 10.33884/jif.v9i02.4444.

[4] T. Ariyadi and M. A. Prabowo, "Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security," *INOVTEK Polbeng - Seri Inform.*, vol. 6, no. 1, p. 80, 2021, doi: 10.35314/isi.v6i1.1698.

[5] T. Ariyadi *et al.*, "Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Dengan Metode NDLC (Network Development Life Cycle) Pada PT Kirana Permata," no. 3, 2023.

[6] N. Fahmi, E. Prayitno, and S. Fitriani, "Web of Thing Application for Monitoring Precision Agriculture Using Wireless Sensor Network," *J. INFOTEL (Informatika - Telekomun. - Elektron.*, vol. 11, no. 1, pp. 22–28, 2019.

[7] T. Ariyadi, "Mitigasi Distributed Denial of Service (DDoS) Attack Pada Arsitektur Software Defined Network (SDN)," *Techno.Com*, vol. 21, no. 4, pp. 878–886, 2022, doi: 10.33633/tc.v21i4.6879.

[8] T. Ariyadi, "ANALISIS PAKET ICMP WEBSITE UNIVERSITAS BINADARMA," vol. 2, no. 2, pp. 55–60, 2023.

[9] M. Bogdanoski, A. Risteski, and T. Shuminovski, "TCP SYN Flooding Attack in Wireless Networks," *Innov. Commun. Theory*, no. May 2014, pp. 2010–2013, 2012, doi: 10.13140/2.1.3487.3282.

[10] P. A. Dharmesta, "Efektivitas Sniffer Menggunakan Natural Language dalam Pembelajaran," vol. 1, no. 10, pp. 392–403, 2021.

[11] I. P. Agus, E. Pratama, P. A. Dharmesta, and T. Informasi, "IMPLEMENTASI WIRESHARK DALAM MELAKUKAN PEMANTAUAN PROTOCOL JARINGAN (Studi Kasus : Intranet Jurusan Teknologi Informasi Universitas Udayana)," vol. 3, no. 1, pp. 94–99, 2019.

[12] W. N. A. Dwi Bayu Rendro; Ngatono, "ANALISIS MONITORING SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SOFTWARE NMAP," *PROSISKO*, vol. 7, no. 2, 2020.

[13] F. Arif, A. Tama, M. Kom, F. Panjaitan, and M. Kom, "Analisis Keamanan Jaringan Pada FasilitasInternet (wifi) Terhadap Serangan PacketSniffing".

BIODATA PENULIS

Tamsir Ariyadi, M.Kom.
Penulis merupakan dosen pada Program Studi Teknik Komputer Universitas Bina Darma, beberapa publikasi berkaitan tentang Network Security & Computer Network.

Irwansyah, M.M., M.Kom.
Penulis merupakan dosen pada Program Studi Teknik Komputer Universitas Bina Darma, beberapa publikasi berkaitan tentang Computer Network.

M. Syaiful Huda Mubarok

Mahasiswa pada Program Studi Teknik Komputer Universitas Bina Darma.