STORAGE – Jurnal Ilmiah Teknik dan Ilmu Komputer, Vol. 2 No. 2, Mei 2023, 55-60
e-ISSN: 2828-5344 | DOI: 10.55123

ANALISIS PAKET ICMP WEBSITE UNIVERSITAS BINADARMA MENGGUNAKAN WIRESHARK

Tamsir Ariyadi[1)], Eggy Saputra[2)], Kundari[3)], Muhammad Tio Farizky[4)]

[1,2,3,4)]Program Studi Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma, Palembang

Email : tamsirariyadi.binadarma.ac.id[1)], eggys7522@gmail.com[2)], kundarikun01@gmail.com[3)], tiofarizky@gmail.com[4)].

INFO ARTIKEL

Riwayat Artikel :
Diterima : 27 Mei 2023
Disetujui : 31 Mei 2023

Kata Kunci:
ICMP, capture, wireshark.

ABSTRAK

ICMP atau Internet Control Message Protocol merupakan protokol yang berperan penting dalam fungsi jaringan internet, ICMP sendiri biasanya digunakan oleh berbagai perangkat seperti router, server dan lain-lain. Protokol ICMP berguna untuk mengirim pesan antar perangkat di jaringan komputer. Untuk menguji apakah protokol dapat berfungsi dengan baik, akan dilakukan proses Capture. Capture adalah proses menangkap dan menampilkan informasi tentang situs web, baik itu alamat IP, paket seperti HTTP, ICMP, SSDP, TCP. Capture ini sendiri biasanya digunakan untuk memantau dan menguji kelayakan jaringan di internet. Capture biasanya bisa dilakukan dengan berbagai alat, salah satunya Wireshark. Dengan alat Wireshark ini, peneliti dapat memantau lalu lintas pada jaringan komputer berdasarkan capture, yang dapat menampilkan alamat IP sumber ke alamat IP tujuan.

ARTICLE INFO

Article History :
Received : May 27, 2023
Accepted : May 31, 2023

Keywords*:*
ICMP, capture, wireshark.

ABSTRACT

ICMP or Internet Control Message Protocol is a protocol that plays an important role in internet network functions, ICMP itself is usually used by various devices such as routers, servers and others. The ICMP protocol is useful for sending messages between devices on a computer network. To test whether the protocol can function properly, a Capture process will be carried out. Capturing is the process of capturing and displaying information about websites, be it IP addresses, packets such as HTTP, ICMP, SSDP, TCP. This capture itself is usually used to monitor and test network feasibility on the internet. Capture can usually be done with a variety of tools, one of which is Wireshark. With this Wireshark tool, researchers can monitor traffic on a computer network based on capture, which can display the source IP address to the destination IP address.

1. PENDAHULUAN

Seiring dengan semakin berkembangnya teknologi internet, maka kejahatan yang memanfaatkan teknologi ini juga semakin meningkat. Di era globalisasi, perkembangan teknologi informasi terus berkembang dengan sangat cepat, menuntut kecepatan arus informasi karena menjadi kebutuhan utama. Kebutuhan akan informasi telah menjadi kebutuhan penting bagi manusia, dan keamanan informasi jaringan informasi yang berperan penting untuk penerapan teknologi serta informasi pada dunia saat ini.[1] Kebutuhan jaringan internet juga semakin meningkat untuk melakukan transaksi dan aktivitas dengan maksud jahat, seperti contohnya pencurian data oleh oknum yang tidak bertanggung jawab. Analisis jaringan merupakan suatu perpaduan pemikiran yang logis. Analisis jaringan memungkinkan perencanaan jaringan interaktif yang efektif.[2]

Website Universitas Bina Darma merupakan website yang menyimpan segala informasi tentang Universitas Bina Darma Palembang, biasanya terdiri dari informasi tentang jenis fakultas, program studi, tata cara pendaftaran dan perkuliahan lainnya. niversitas Bina Darma merupakan salah satu kampus swasta terbaik yang menyediakan sistem pembelajaran dalam jaringan (daring) berbasis website.[3] Website Universitas Bina Darma biasanya mengunggah berbagai pengumuman penting bagi mahasiswa dan fakultas. Oleh karena itu, peneliti perlu menganalisis keamanan situs sehingga peneliti dapat memprediksi bagaimana situs akan meningkat jika terjadi serangan atau gangguan internal atau eksternal.

Keamanan jaringan menjadi penting dan harus selalu jadi perhatian, baik itu jaringan nirkabel maupun *wireless*. Salah satu komponen jaringan paling penting adalah keamanan jaringan. Namun, masalah keamanan jaringan sering kali kurang diperhatikan. Untuk meningkatkan keamanan jaringan, Ada banyak jenis paket data di internet dan masing-masing memiliki fungsi yang berbeda dan berkaitan. Ini termasuk informasi seperti kata sandi, alamat situs web, nama pengguna, protokol IP, dan informasi lainnya. Dibalik kemudahan penggunaan internet terdapat ancaman yang dapat mengganggu lalu lintas jaringan, yang memungkinkan menyebabkan hilangnya data maupun informasi. Menganalisis situs web Universitas Bina Darma memerlukan prosedur, prosedur pemantauan yaitu dengan cara memonitoring. Pemantauan atau monitoring jaringan dapat dipahami sebagai kegiatan yang ditujukan untuk mengatur sistem jaringan di area tertentu atau dengan topologi jaringan tertentu.[4] adalah bagian dari manajemen jaringan. Pemantauan dilakukan pada website Universitas Bina Darma untuk menganalisis kerentanan website tersebut, yang selanjutnya dilakukan melalui proses penangkapan jaringan atau Capture. Proses capture diperlukan untuk memantau situs web, kegiatan capture ini digunakan oleh peneliti untuk memantau paket ICMP pada website Universitas Bina Darma Palembang agar dapat memperoleh informasi mengenai jenis jenis jaringan yang digunakan pada website Universitas Bina Darma.[5] Dalam penelitian ini, proses sniffing akan dilakukan dengan software Wireshark. Dengan bantuan software Wireshark ini, lalu lintas data di Internet dapat dipantau dan informasi penting dapat dipanggil dengan menghubungkan alamat Ip website ke adapter perangkat.[6] Wireshark juga dikenal sebagai penganalisa paket jaringan yang fungsinya untuk menampilkan semua informasi paket secara keseluruhan dan menangkap paket yang dikirim atau diterima.[7] Wireshark adalah alat pemantauan yang dapat merekam aktivitas jaringan yang sudah di capture pada website Universitas Bina Darma Palembang.

Dalam survei jurnal ini, peneliti memantau website Universitas Binadarma Palembang. Tujuan dari penelitian ini adalah untuk melakukan ping ke jaringan website Universitas Binadarma Palembang melalui PING pada computer prompt (CMD). Menghasilkan output, ICMP atau Internet Control Message Protocol. ICMP (Internet Control Message Protocol) adalah protokol yang melakukan pelaporan kesalahan untuk perangkat jaringan, seperti yang digunakan oleh router untuk menghasilkan pesan kesalahan ke alamat IP sumber. ICMP membuat dan mengirim pesan ke alamat IP sumber yang menyatakan bahwa router Internet gateway, layanan atau server untuk paket tidak dapat dihubungi. ICMP sebuah protocol yang memiliki fungsi yang sedikit berbeda dari protocol TCP atau UDP dari segi

penggunaannya. Dikarenakan protokol ICMP tidak dapat digunakan secara langsung oleh aplikasi jaringan milik pengguna.[8] Serangan sniffing dapat terjadi pada website yang menggunakan Paket ICMP. Akan tetapi itu tergantung keamanan dari website itu sendiri. Penerapan serangan sniffing pada website di Universitas Bina Darma ini yaitu ingin mengetahui penangkapan data apa yang terjadi ketika terjadi serangan sniffing. Jika terjadi penangkapan data ICMP website tersebut tahap selanjutnya bagaimana penulis memberikan solusi untuk mengatasi masalah yang terjadi dan memberikan saran untuk pengelola website Universitas Bina Darma Palembang terhadap kerentanan serangan pada website.

2. METODE

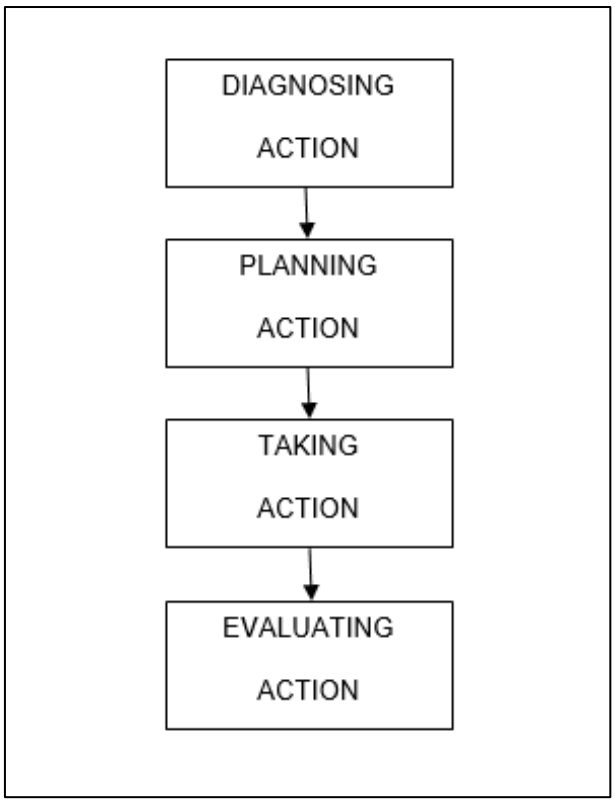
Penelitian ini menggunakan metode Action Research yang digunakan untuk menjelaskan dan mem-pertimbangkan pemantauan situs website Universitas Bina Darma. Metode ini juga cocok untuk pengujian situs web, membuat penelitian menjadi mudah, cepat dan bermakna.[9] Tujuan utama dari penelitian Action Research adalah untuk mengetahui situasi, membuat perubahan, dan memantau hasil dengan tujuan untuk menemukan cara yang efektif untuk menghasilkan perubahan yang disengaja dalam lingkungan yang sebagian terkontrol.[10]

Metode penelitian Action Research ini terdiri dari rangkaian tahapan seperti diagnosis, perencanaan tindakan atau action planning, pelaksanaan tindakan atau action taking, dan evaluasi. Diagnosis adalah proses pemetaan objek yang akan dirancang. Pada tahap ini, peneliti mewawancarai pengelola website Universitas Bina Darma Palembang. Tujuannya untuk mendapatkan informasi mengenai IP address website dan juga untuk mencari informasi mengenai kerentanan yang terdapat pada website Universitas Bina Darma Palembang.

Action Planning merupakan tahap persiapan dari apa yang diperlukan untuk memantau situs Universitas Bina Darma palembang. Pada tahap ini, para peneliti menyiapkan alat Wireshark berdasarkan sistem operasi Windows 64-bit. Untuk menggunakan alat Wireshark ini, Anda membutuhkan jaringan yang terhubung dengan internet yang stabil agar tidak terjadi masalah pemantauan.

Action Taking adalah langkah yang digunakan untuk melakukan operasi dan menjalankannya pada suatu objek. Pada tahap ini, peneliti melakukan ping IP address website Universitas Bina Darma Palembang menggunakan command prompt (CMD). Pada titik ini, peneliti dapat melihat berapa banyak sumber dan jawaban online yang dapat ditemukan di website Universitas Bina Darma Palembang.

Evaluasi adalah langkah terakhir yang diambil untuk mendapatkan hasil akhir atau kesimpulan tentang materi pelajaran yang akan dianalisis. Pada tahap ini, peneliti melakukan proses akuisisi menggunakan alat Wireshark. Koleksi ini bertujuan untuk menampilkan informasi paket ICMP pada website Universitas Bina Darma Palembang.



Gambar1. Alur Proses Metode Action Research

3. HASIL DAN PEMBAHASAN

3.1 Tahapan Pengumpulan Data (Diagnosis)

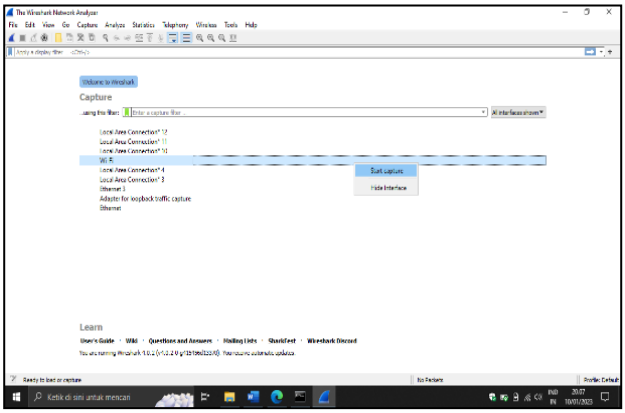
Penelitian diawali dengan proses pengumpulan data, untuk tahapan pertama peneliti harus mencari informasi tentang website Universitas Bina Darma ini. Dengan mengetahui

Domain name dari website Universitas Bina Darma, peneliti dapat mengakses dan mengumpulkan informasi tentang alamat IP yang digunakan website Universitas Bina Darma ini.

Gambar2. Tampilan Awal Website Universitas Bina Darma Palembang

3.2 Tahapan Perancangan (Action Planning)

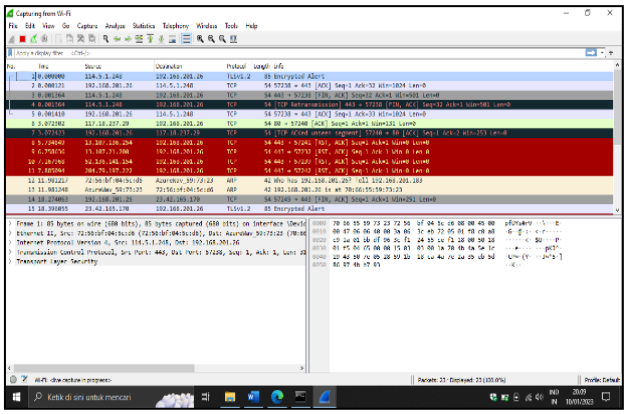
Selanjutnya, peneliti melakukan konfigurasi alat Wireshark. Konfigurasi dilakukan dengan memilih antarmuka jaringan yang akan digunakan, dalam hal ini antarmuka nirkabel (WIFI), dan kemudian perekaman aktivitas jaringan WLAN dimulai.



Gambar3. Pemilihan Jenis Interface pada Wireshark

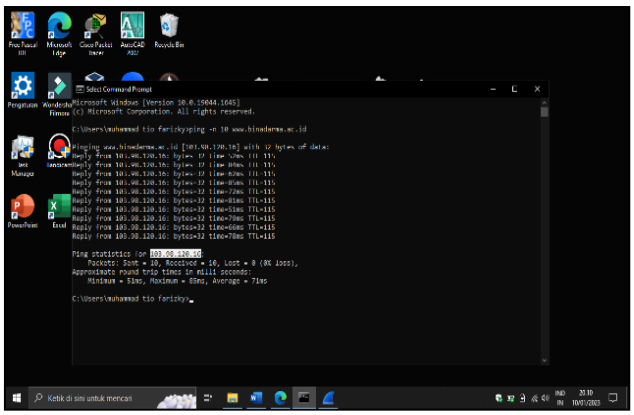
3.3 Tahapan Eksekusi (Action Taking)

Langkah selanjutnya setelah menjalankan tahapan perancangan adalah tahapan eksekusi, yaitu melakukan percobaan Capture awal pada software Wireshark. Proses dilakukan seperti yang ditunjukkan di bawah ini. Pada awal pengumpulan, beberapa alamat IP dan protokol yang terkait dengan jaringan WiFi ditampilkan. Biasanya ini adalah data dari hasil pencarian web pada alamat IP koneksi Wi-Fi. Dari proses awal Capture jaringan ini akan memudahkan software Wireshark untuk menangkap jaringan dengan frekuensi yang lebih luas dan cepat sehingga paket – paket jaringan seperti HTTP, ICMP, dan sebagainya akan mudah untuk di Capture.



Gambar4. Proses Awal Capture Wireshark

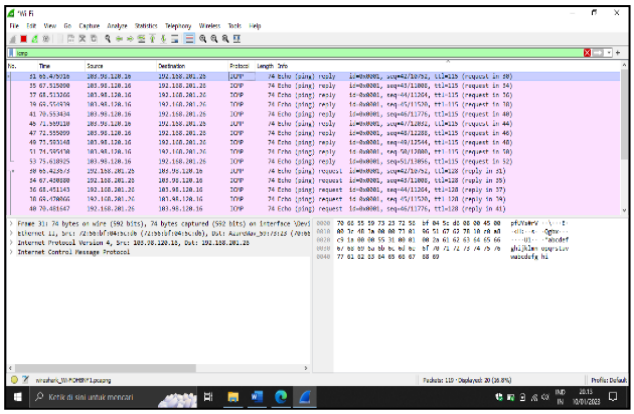
Dengan proses capture yang berlangsung, saatnya PING website Bina Darma Universitas Palembang. Tujuan dari PING ini adalah untuk menguji apakah sebuah situs web dapat menerima transmisi dari Internet melalui alamat IP antarmuka WIFI.



Gambar5. Proses PING pada Website Universitas Bina Darma Menggunakan CommandPrompt

3.4 Tahapan Evaluasi (Evaluation)

Untuk tahapan terakhir ini. Dilihat pada selama proses aplikasi ping yang mengirimkan pesan ICMP Echo Request (dan menerima Echo Reply) untuk menentukan apakah tujuan dapat dijangkau dan berapa lama waktu yang dibutuhkan tujuan untuk merespon paket yang dikirimkan, dapat berhasil dilakukan seperti yang ditunjukkan pada tampilan di bawah ini.



Gambar6. Hasil Akhir Capture Website Universitas Bina Darma Dengan Wireshark

4. PENUTUP

4.1. Kesimpulan

Dari penelitian ini dapat disimpulkan bahwa analisis jaringan ICMP *website* Universitas Bina Darma Palembang menunjukkan kecepatan waktu yang tinggi dalam menerima transmisi dalam format PING. Dengan pemantauan dalam penelitian ini adalah untuk memberikan pengetahuan tentang cara mengendus dalam suatu jaringan, dan dari penelitian ini diharapkan akan meningkatkan keamanan suatu jaringan dengan menggunakan aplikasi wireshark monitoring.

4.2. Saran

Dalam analisis ini, para peneliti juga memberikan saran terhadap situs web Universitas Bina Darma karena memiliki sedikit kerentanan terhadap ancaman. Saran untuk pengelola website agar untuk lebih diantisipasi dengan memperkuat pertahanan terhadap keamanan situs web Universitas Bina Darma.

5. DAFTAR PUSTAKA

[1] T. Ariyadi and A. Kasim, "Analisis Paket DHCP Rogue Pada Jaringan Local Area Network (LAN) Menggunakan Wireshark," *Pros. Semin. Nas. ...*, pp. 97–101, 2018, [Online]. Available: http://eprints.binadarma.ac.id/4358/.

[2] Tamsir, "ANALISIS KUALITAS JARINGAN LAN DENGAN METODE QOS DI PT. SEMEN BATURAJA (PERSERO) Tbk," *Pros. Semin. Has. Penelit. Vokasi*, vol. 1, no. 1, pp. 150–157, 2019.

[3] R. N. Dasmen, T. L. Widodo, and M. Tio, "PENGUJIAN PENETRASI PADA WEBSITE ELEARNING2 . BINADARMA . AC . ID DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD)," vol. 11, no. 1, pp. 91–95, 2023, doi: 10.35508/jicon.v11i1.9809.

[4] A. F. Ramdhany, "Perancangan desain monitoring jaringan komputer untuk easy maintenance di telkom university landmark tower," vol. 07, pp. 1176–1188, 2022.

[5] M. F. Qomarudin, A. Amrullah, U. A. Yogyakarta, and U. A. Yogyakarta, "SISTEM MONITORING JARINGAN REALTIME BERBASIS INTERNET CONTROL MESSAGE PROTOCOL," vol. 3, no. 2, pp. 67–80, 2022.

[6] Z. M. Luthfansa and U. D. Rosiani, "Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet," *J. Inf. Eng. Educ. Technol.*, vol. 5, no. 1, pp. 34–39, 2021, doi: 10.26740/jieet.v5n1.p34-39.

[7] F. Huzaeni, I. Gunawan, D. Cahya, M. Yanti, and N. Krisdayanti, "Analisis Keamanan Data Pada Website Dengan Wireshark," *JES (Jurnal Elektro Smart)*, vol. 1, no. 1, pp. 13–17, 2021, [Online]. Available: https://www.sttrcepu.ac.id/jurnal/index.php/jes/article/view/161.

[8] I. P. A. E. Pratama and P. A. Dharmesta, "Implementasi Wireshark Dalam Melakukan Pemantauan Protocol Jaringan (Studi Kasus : Intranet Jurusan Teknologi Informasi Universitas Udayana)," *Mantik Penusa*, vol. 3, no. 1, pp. 94–99, 2019.

[9] D. Hermanto and M. S. Anam, "Implementasi Sistem Keamanan Hotspot

Jaringan Menggunakan Metode OpenSSL (Secure Socket Layer)," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 6, no. 1, p. 57, 2020, doi: 10.24014/coreit.v6i1.8394.

[10] R. Hidayat, "ANALISIS DAN MONITORING TRAFFIC JARINGAN DI MSAN-D PT. TELKOM BERBASIS CACTI," pp. 120–129, 2021.