

Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing di Universitas PGRI Sumatera Barat

Wi-Fi Network Security Analysis Against Packet Sniffing Attacks at Universitas PGRI Sumatera Barat

Fatimah[*)], Thomson Mary, Anggri Yulio Pernanda

[*)]Universitas PGRI Sumatera Barat

[1)]*mmahfati @gmail.com,* [2)]*thomsonmary1980@gmail.com,* [3)]*anggriyulio@gmail.com*

Abstrak - Universitas PGRI Sumatera Barat memiliki wi-fi yang tidak menutup kemungkinan terjadi serangan pada jaringan wi-fi yang dilakukan oleh hacker. Keamanan Jaringan merupakan suatu pelindung dalam sebuah system jaringan dalam proses untuk mencegah para pengguna jaringan yang tidak berhak dan tidak bertanggung jawab. Penelitian ini termasuk penelitian deskriptif, Metode penelitian deskriptif adalah salah satu metode penelitian yang bertujuan untuk menjelaskan suatu kejadian. Penelitian ini dilakukan dengan cara menguji dan menganalisis hasil pengujian pada keamanan jaringan menggunakan aplikasi Wireshark dan Ettercap (OS Kali Linux). Hasil dari penelitian ini berupa sistem keamanan jaringan wi-fi pada gedung A1, gedung B1, gedung D1 di Universitas PGRI Sumatera Barat sudah baik. Pada saat dilakukan scan for hosts tidak ditemukan IP dari laptop korban penyerangan packet snffing..

Kata kunci - Analisis Keamanan Jaringan, Wi-Fi, Packet Sniffing

Abstract – Universitas PGRI Sumatera Barat has wi-fi which does not rule out attacks on wi-fi networks carried out by hackers. Network Security is a protector in a network system in the process of preventing unauthorized and irresponsible network users. This research includes descriptive research. Descriptive research method is a research method that aims to explain an event. This research was conducted by testing and analyzing the test results on network security using Wireshark and Ettercap applications (Kali Linux OS). The results of this study in the form of a wi-fi network security system in building A1, building B1, building D1 at Universitas PGRI Sumatera Barat is good. During the scan for hosts, the IP of the laptop victim of the packet snffing attack was not found.

Keywords - Network Security Analysis, Wi-Fi, Packet Sniffing

I. PENDAHULUAN

Keamanan jaringan menjadi sangat penting untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para *hacker,* baik pada jaringan kabel maupun jaringan nirkabel. Menurut (Hidayat et al., 2018) (Hidayat et al., 2018)*Packet Sniffing*/*Sniffer* adalah sebuah metode serangan dengan cara memonitor seluruh paket yang lewat pada sebuah media komunukasi, baik itu media kabel maupun nirkabel.

Universitas PGRI Sumatera Barat memiliki wi-fi yang tidak menutup kemungkinan terjadinya serangan pada jaringan tersebut. Berdasarkan wawancara yang dilakukan di Universitas PGRI Sumatera Barat dengan salah satu staf di ruangan ICT diperoleh informasi bahwasanya Universitas PGRI Sumatera Barat mendestribusikan layanan jaringan kabel maupun nirkabel. Pembagian jaringan wi-fi pada gedung A, gedung B, gedung C, dan gedung D, dan diperoleh juga informasi untuk keamanan jaringan wi-fi di Universitas PGRI Sumatera Barat belum mengetahui keamanan jaringannya.

Menurut (Suyuti Ma'sum et al., 2017) Keamanan Jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Menurut (Dharma & Thamrin, 2020) *Wireless Fidelity* (Wi-fi) adalah suatu teknologi yang memungkinkan sejumlah komputer terhubung dalam sebuah jaringan tanpa kabel alias *wireless local area network* (WLAN). Menurut (iwan sofana, 2014) Router adalah sebuah alat yang digunakan untuk menghubungkan beberapa *network.* Menurut (Fauzi & Suartana, 2018) *Packet sniffing* merupakan teknik pemantauan setiap paket yang melintasi jaringan, dan bagian dari perangkat lunak atau perangkat keras yang memonitor seluruh lalu lintas yang melintasi suatu jaringan. Menurut

ISSN: 2829-4343 DOI: 10.22202/jurteii.2022.5707

(Sabdho & Ulfa, 2018) Kali Linux adalah sistem distribusi linux yang dikembangan dengan fokus pada tugas penetration testing. Menurut (Putra et al., 2018) *Wireshark* merupakan *tools* yang ditujukan untuk penganalisisan paket data jaringan. Menurut (Turkhamun Adi Kurniawan, 2020) (Turkhamun Adi Kurniawan, 2020) *Ettercap* merupakan alat untuk analisis protokol jaringan dan audit keamanan.

II. METODE

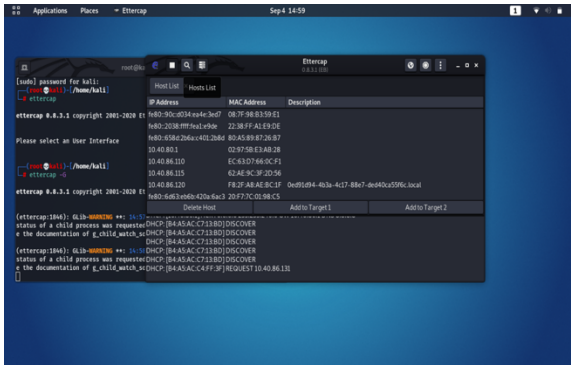
Jenis penelitian ini ialah menggunakan metode deskriptif. Menurut (Putra et al., 2018) Penelitian deskriptif merupakan suatu metode dalam meneliti status sekelompok manusia, suatu objek,suatu set kondisi, suatu sistem pemikiran ataupun suatu kelas peristiwa atau kejadian pada masa sekarang. Metode penelitian deskriptif adalah salah satu metode penelitian yang bertujuan untuk menjelaskan suatu kejadian

III. HASIL DAN PEMBAHASAN

Berikut adalah hasil dari penelitian pada jaringan wi-fi di Universitas PGRI Sumatera Barat yang dilakukan pada: Gedung A1, Gedung B1, dan Gedung D1.

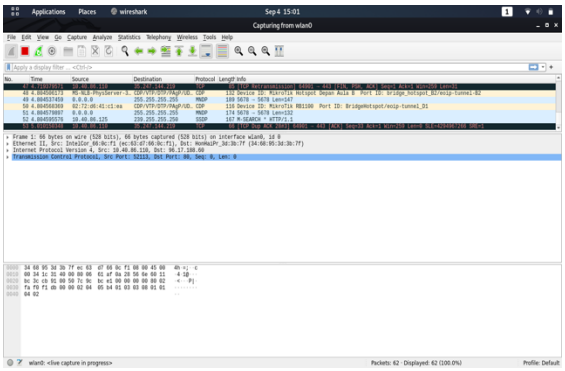
1. *Hotspot* Pada Gedung A1

Pada gambar dibawah ini pada saat melakukan pengujian terhadap serangan *packet sniffing*, gambar tersebut menunjukkan ketika IP dari laptop korban penyerangan bisa terdeteksi, maka *IP address* dari jaringan kita letakan pada target 1, dan *IP address* korban penyerangan pada target 2 pada *tools Ettercap*.



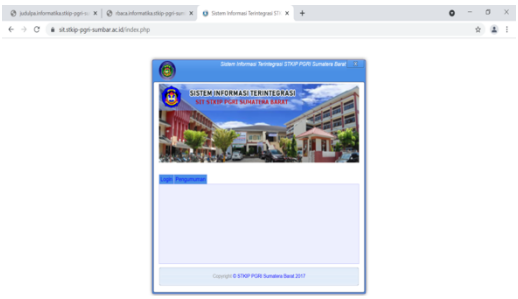
Gambar 1. Tampilan *Ettercap* menampilkan *IP address*

Pada gambar 2 dibawah ini selanjutnya buka *wireshark*, pada gambar ini menunjukkan hasil dari melakukan *Capture*, ketika memulai menekan " *Start capturing packets*" pada *wireshark* akan melakukan *sniffing* sesuai dengan konfigurasi yang sudah dilakukan, dan proses pengambilan dari paket data yang melintasi suatu jaringan ini yaitu akan berlangsung secara *real time*. Semakin lama melakukan *sniffing,* semakin besar juga *file* yang akan dihasilkan. Laptop 1 sebagai *sniffing* atau penyerang.



Gambar 2. Tampilan Saat Memulai *Capture*

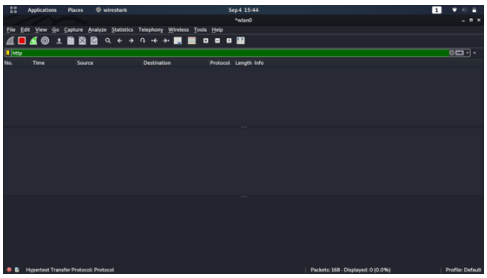
Pada gambar 3 dibawah ini menunjukkan bahwa, ketika kita sudah memulai untuk melakukan *sniffing* menggunakan *wireshark* maka pada laptop 2 sebagai korban penyerangan dari serangan *sniffing*, disini akan mencoba untuk mengakses situs-situs yang akan diuji coba. Ketika mencoba mengakses beberapa situs disini terlihat bahwa situs-situs ini tidak bisa di akses atau dijangkau karena secara otomatis pada laptop korban penyerangan akses jaringannya terputus dan tersambung ketika melakukan *sniffing*. Karena jaringan *hotspot* pada A1 ini, jaringannya sangat lemah, dan jaringan sering terputus dan terhubung, dan untuk melanjutkan sniffing tidak bisa dilakukan atau terhenti.



Gambar 3. Tampilan Login situs SIT

Pada gambar 4 dibawah menunjukkan tidak ada aktifitas yang melintasi lalu lintas jaringan dari hasil

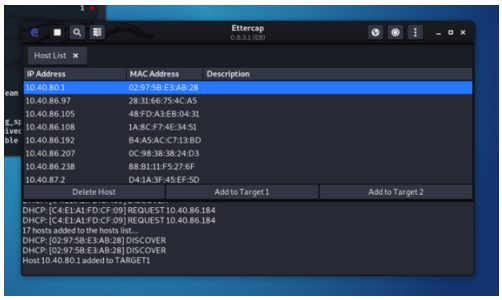
ter-*capture* yang dilakukan oleh penyerang, disini tidak bisa mendapatkan informasi datanya atau akses yang dilakukan oleh korban penyerangan dan aktifitas yang dilakukan korban penyerangan tidak bisa ditangkap oleh penyerang. Karena saat melakukan *sniffing* jaringan wi-fi-nya terputus. Pada penelitian ini membuktikan bahwa data informasi yang diperoleh dalam melakukan serangan *packet sniffing* pada jaringan wi-fi gedung A1 di Universitas PGRI Sumatera Barat, khususnya *hotspot* yang disediakan untuk mahasiswa pada Gedung A1, dinyatakan bahwa keamanan jaringan sudah aman.



Gambar 4. Tampilan *Capture*

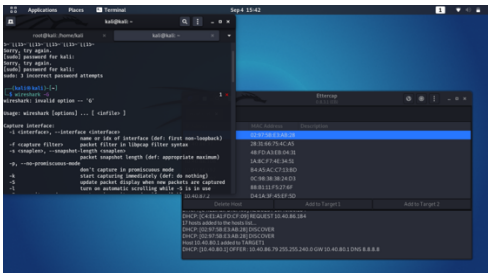
2. *Hotspot* Pada Gedung B1

Pada gambar 5 dibawah ini menunjukkan bahwa pada saat melakukan pengujian terhadap serangan *packet sniffing*, gambar tersebut menunjukkan ketika IP dari laptop korban penyerangan tidak terdeteksi pada *tools Ettercap*.



Gambar 5. Tampilan *Ettercap* menampilkan *IP address*

Pada gambar 6 dibawah ini menunjukkan, ketika melakukan untuk menampilkan *Wireshark* disini aplikasi *wireshark invalid* dan tidak bisa ditampilan. Otomatis untuk melakukan *sniffing* pada jaringan *hotspot* pada gedung B1 tidak bisa di lakukan serangan *packet sniffing* di Universitas PGRI Sumatera Barat, dinyatakan bahwa keamanan jaringan sudah aman.



Gambar 6. Tampilan saat memunculkan *wireshark*

3. *Hotspot* Pada Gedung D1

Pada *hotspot* gedung D1, sama dengan pada gedung B1 jaringan wi-fi tidak bisa dilakukan serangan *packet sniffing*, dinyatakan bahwa keamanan jaringan sudah aman.

Tabel 1. Hasil dari pengujian serangan *packet sniffing*

No	Serangan	Titik Pengujian	Situs yang Diuji	Hasil	Keterangan
1	*Packet Sniffing*	*Hotspot* jaringan wi-fi Gedung A1	• Portal • E-learning • Sistem TA Pendidikan • Sistem Informatika • Ruang Baca Pendidikan Informatika • Sistem PLK Pendidikan Informatika	Aman	Tidak berhasil menangkap paket data informasi dari jaringan wi-fi untuk mahasiswa

2	*Packet Sniffing*	*Hotspot* jaringan wi-fi Gedung B1	• Portal • E-learning • Sistem TA Pendidikan • Sistem Informatika Ruang Baca Pendidikan Informatika • Sistem PLK Pendidikan Informatika	Aman	Tidak berhasil mendeteksi IP address pada laptop korban terhadap serangan *sniffing* pada jaringan wi-fi untuk mahasiswa
3	*Packet Sniffing*	H*otspot* jaringan wi-fi Gedung D1	• Portal • E-learning • Sistem TA Pendidikan • Sistem Informatika Ruang Baca Pendidikan Informatika • Sistem PLK Pendidikan Informatika	Aman	Tidak berhasil mendeteksi IP address pada laptop korban terhadap serangan *sniffing* pada jaringan wi-fi untuk mahasiswa

Jika dilihat pada tabel hasil penelitian di atas yang sudah dilakukan dengan serangan *packet sniffing* yang telah dilakukan pada jaringan wi-fi atau *Hotspot* pada gedung A1, gedung B1, dan gedung D1 yang dikhususkan untuk mahasiswa di kampus Universitas PGRI Sumatera Barat. Pada saat dilakukan pengujian peneliti tidak bisa melakukan serangan *Packet Sniffing* pada sebuah jaringan wi-fi dikarenakan jaringan wi-fi di Universitas PGRI Sumatera Barat tersebut sudah menggunakan *enskripsi* keamanan jaringannya menggunakan WPA2 dan jaringan wi-fi di Universitas PGRI Sumatera Barat dinyatakan sudah aman dari serangan yang telah diuji cobakan menggunakan serangan *packet sniffing* oleh peneliti. Sedangkan untuk situs-situs yang diuji cobakan, situs yang bisa ditangkap datanya yaitu situs atau sebuah sistem ataupun aplikasi adalah yang menggunakan protokol HTTP, sedangkan untuk situs-situs yang menggunakan protokol HTTPS data tidak bisa didapatkan, karena data tersebut ter-*enskripsi* atau tidak bisa dibaca.

IV. KESIMPULAN

Dengan analisis keamanan jaringan wi-fi terhadap serangan *packet sniffing* di Universitas PGRI Sumatera Barat. Tidak dapat mendeteksi masalah keamanan jaringan karena saat pengujian tidak bisa memperoleh *IP Address* dari laptop pengujian. Berdasarkan hasil dari analisis data dan percobaan terhadap serangan *packet sniffing* yang sudah dilakukan, maka dapat disimpulkan bahwa sistem keamanan jaringan wi-fi pada gedung A1, gedung B1, gedung D1 di Universitas PGRI Sumatera Barat sudah baik. *Enskripsi* keamanan yang digunakan di Universitas PGRI Sumatera Barat yaitu *security* keamanan WPA2.

Hal ini dibuktikan dari hasil penelitian yang telah dilakukan yaitu:

1. Setelah dilakukan pengujian serangan *packet sniffing* menggunakan aplikasi *wireshark* dan *ettercap* pada (OS) kali linux pada jaringan wi-fi yang di khususkan jaringanya untuk mahasiswa di Universitas PGRI Sumatera Barat sama sekali tidak didapatkan adanya aktifitas seperti mengakses akun situs.
2. Pada saat dilakukan serangan *packet sniffing* diketahui bahwa jaringan wi-fi di Universitas PGRI Sumatera Barat sudah dilindungi keamanannya dengan *security* atau *enskripsi* keamanan WPA2.

V. UCAPAN TERIMAKASIH

Terimakasih kepada dosen pembimbing yang telah membimbing penulis dalam menyelesaikan skripsi ini. Dan teristimewa ucapan terima kasih penulis persembahkan kepada kedua orang tua tercinta dan seluruh keluarga yang telah berusaha sekuat tenaga memberi dukungan moril dan materil kepada penulis dalam menyelesaikan skripsi ini.

VI. DAFTAR PUSTAKA

Dharma, S., & Thamrin, T. (2020). Analisis Kinerja Jaringan WIFI. *Voteteknika (Vocational Teknik Elektronika Dan Informatika)*, *8*(2), 35. https://doi.org/10.24036/voteteknika.v8i2.109129

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

Hidayat, M. T., Sn, F. M., & Kurniati, N. I. (2018). *Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Gratis Terhadap Serangan Packet Sniffing*. *1*(2), 112–119.

iwan sofana. (2014). *cisco ccna & jaringan komputer*. Informatika Bandung.

Putra, E. M., Tujni, B., & Negara, E. S. (2018). Analisis Kemanan Jaringan Internet (Wifi) Dari Serangan Packet Data Sniffing Di Universitas Muhammadiyah Palembang. *Jurnal Ilmiah Teknologi Informasi*.

Sabdho, H. D., & Ulfa, M. (2018). Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang. *Semhavok*, *1*(1), 15–24.

Suyuti Ma'sum, M., Azhar Irwansyah, M., & Priyanto, H. (2017). Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *5*(1), 56–60.

Turkhamun Adi Kurniawan. (2020). ANALISA KEAMANAN JARINGAN WIFI TERHADAP SERANGAN PACKET SNIFFING.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International License.