Jurnal FUSE – Teknik Elektro
|Vol. 4 | No. 1 | Halaman 61 – 66 | [Juni][2024]

Analisis Kerentanan Jaringan pada Fasilitas Internet Nirkabel pada Serangan *Packet Sniffing*

Iik Muhamad Malik Matin[1], Fahri Ramadhan[2], Glorya S Hutasoit[3], Alifia Aurellia Hapsari[4]

[1,2,3,4]Departemen Teknik Informatika dan Komputer Politeknik Negeri Jakarta
Jl. Prof. DR. G.A. Siwabessy, Kukusan, Kecamatan Beji, Kota Depok, Jawa Barat, Indonesia

Korespondensi: iik.muhamad.malik.matin@tik.pnj.ac.id

ARTICLE HISTORY

Received:19-03-2024	***Revised:24-6-2024***	***Accepointed:28-6-2024***

Abstrak

Keamanan jaringan telah menjadi isu krusial dalam era konektivitas digital saat ini, di mana jaringan yang terhubung dengan internet rentan terhadap berbagai serangan oleh peretas. Gedung PT. XYZ telah mengadopsi jaringan komputer berbasis kabel dan nirkabel untuk pertukaran data dan informasi yang bersifat penting. Namun, jaringan *WiFi* sering menjadi sasaran serangan oleh peretas karena potensi kelemahan dalam pengamanan, seperti serangan *sniffing* yang dapat mengakibatkan pencurian data sensitif. Oleh karena itu, penelitian ini bertujuan untuk merancang sistem keamanan jaringan *WiFi* di Gedung PT. XYZ dengan menggunakan alat *packet* sniffer *Ettercap* untuk mengidentifikasi dan mengurangi celah keamanan yang mungkin dimanfaatkan oleh peretas.

Kata kunci: *sniffing, Ettercap, WiFi.*

Network Vulnerability Analysis in Wireless Internet Facilities in Packet Sniffing Attacks

Abstract

Network security has become an important issue in the current era of digital connectivity, where networks connected to the internet are vulnerable to various attacks by hackers. PT. XYZ building has adopted wired and wireless computer networks to exchange important data and information. However, WiFi networks are often the target of attacks by hackers due to potential weaknesses in security, such as sniffing attacks that can lead to theft of sensitive data. Therefore, this research aims to design a WiFi network security system in the PT. XYZ building used Ettercap's packet sniffer tool to identify and mitigate security gaps that hackers might exploit.

Key words: *sniffing, Ettercap, wifi*

1. Pendahuluan

Saat ini, keamanan jaringan menjadi isu krusial yang harus diberi perhatian serius. Dalam era globalisasi dan digitalisasi saat ini, konektivitas jaringan telah menjadi tulang punggung bagi berbagai aktivitas, baik dalam skala personal maupun institusional. Jaringan nirkabel (*WiFi*) merupakan salah satu teknologi yang paling umum digunakan untuk memfasilitasi akses internet tanpa kabel, memberikan fleksibilitas dan mobilitas dalam berbagai konteks penggunaan. Namun, seiring dengan meningkatnya adopsi teknologi ini, tantangan dalam mengamankan jaringan *WiFi* juga semakin kompleks. Meningkatnya adopsi teknologi *WiFi* juga memperkenalkan tantangan baru dalam hal keamanan, dengan serangan *packet sniffing* menjadi salah satu ancaman yang perlu ditangani secara serius [1].

Gedung di PT. XYZ merupakan salah satu entitas pendidikan dan administratif yang memiliki peran penting dalam menyediakan layanan akademik, administratif, dan komersial. Dalam lingkungan yang demikian, keamanan jaringan menjadi hal yang sangat krusial, terutama dalam menghadapi potensi ancaman serangan oleh peretas yang bertujuan untuk mencuri data sensitif, mengganggu layanan, atau bahkan merusak reputasi institusi.

Jaringan *WiFi* yang ada di Gedung PT. XYZ tidak luput dari risiko serangan, terutama karena sifatnya yang terbuka dan rentan terhadap berbagai jenis serangan seperti serangan *sniffing*. Serangan *sniffing* memungkinkan peretas untuk mencuri informasi sensitif yang dikirim melalui jaringan *WiFi*, seperti kredensial *login*, data pribadi, atau bahkan informasi keuangan. Oleh karena itu, perlindungan terhadap jaringan *WiFi* Gedung PT. XYZ menjadi prioritas yang tidak dapat diabaikan.

Beberapa penelitian telah dilakukan diantaranya oleh Aykarahmi Umasugi dkk [1] melakukan analisisi keamanan pada jaringan *WiFi* di kampus A Univeristas Muhammadiyah Maluku Utara menggunakan *wireshark*. Zaky Maula dkk [2] juga memanfaatkan *wireshark* untuk *sniffing* komunikasi data pada protokol http pada jaringan internet. Riad Sahara [3] melakukan analisis *sniffing* pada jaringan PT. Stepa Adiguna menggunakan cain and Abel. Fatimah dkk [4] melakukan analisis keamanan jaringan *WiFi* di universitas PGRI Sumatera Barat. Yacob Hae [5] menganalisis keamanan jaringan pada web di kampsu UKSW menggunakan b*ettercap*.

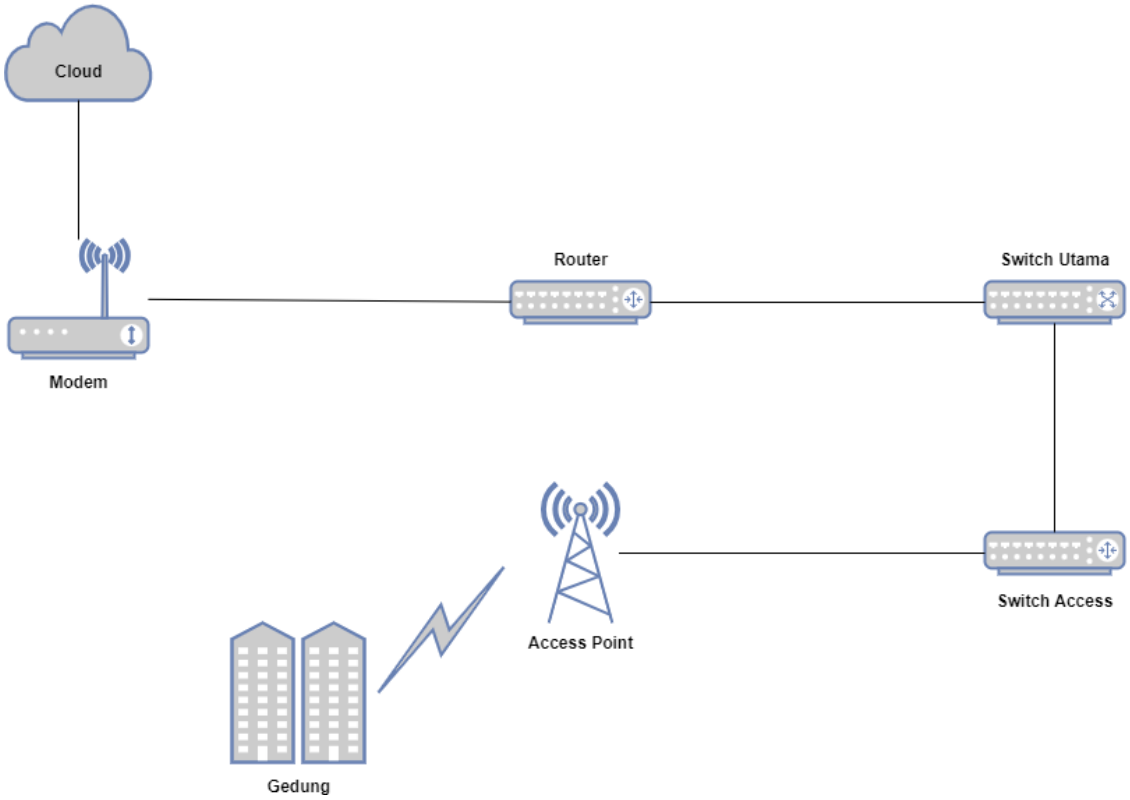
Penelitian ini bertujuan untuk menganalisis sistem keamanan jaringan *WiFi* di Gedung PT. XYZ. Dengan menggunakan alat *packet* sniffer *Ettercap*, penelitian ini mengidentifikasi celah keamanan yang ada dalam jaringan *WiFi*, menganalisis protokol jaringan, dan mengidentifikasi potensi serangan yang dapat terjadi. Diharapkan penelitian ini dapat memberikan kontribusi yang signifikan dalam memperkuat infrastruktur keamanan jaringan *WiFi* dan melindungi aset digital institusi.

ISSN **2797-815X**
P-ISSN **2797-8745**

2. Metode

2.1 Rancangan

Pada penelitian ini, dilakukan evaluasi keamanan pada *wireless* pada jaringan berbasis *WiFi*. Pengujian dilakukan dengan fokus penetrasi pada jaringan menggunakan aplikasi *ettercap* sebagai alat analisis protokol serta pengguna aktif yang terutama berada dalam jangkauan penggunaan jaringan nirkabel. Gambar 1 menunjukan topologi yang digunakan di gedung PT. XYZ.



Gambar 1. Topologi Jaringan

Pada gambar 1. menunjukan topologi jaringan yang terdapat pada PT. XYZ. Pada gambar ini terdiri dari modem yang merupakan akses dari internet menuju jaringan lokal. Kemudian terdapat *router* dan dua *switch* akses. Akses ini didstribusikan menggunakan kabel. Sedangkan pada gedung PT. XYZ, distribusi akses internet dilakukan dengan perangkat *access point*.

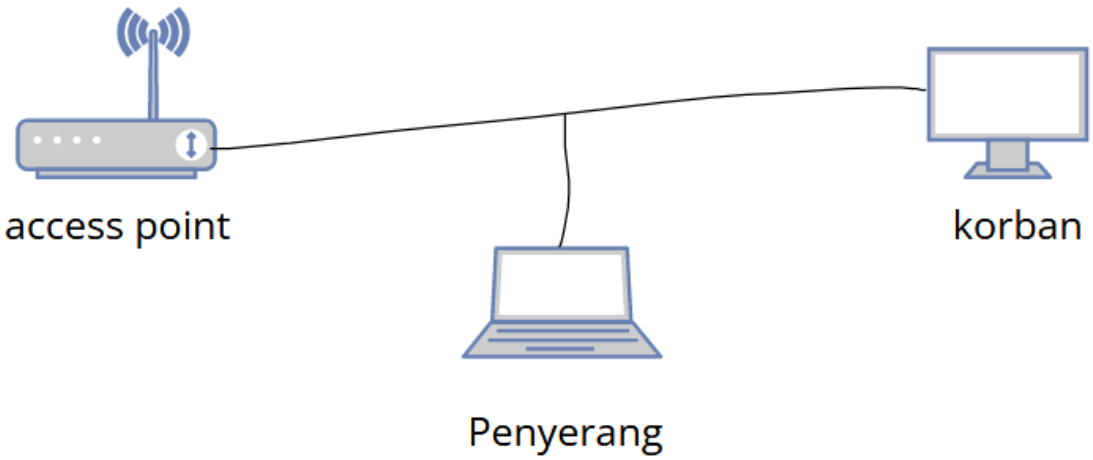
ISSN **2797-815X**
P-ISSN **2797-8745**

2.2 Tahapan Penelitian

Tahapan penelitian ini terdiri dari:

1. Persiapan
   Persiapan dilakukan untuk mengidentifikasi tujuan penelitian dan sasaran yang akan dievaluasi, menyiapkan lingkungan perangkat keras dan perangkat lunak yang dibutuhkan.dan metode pengumpulan data dan alat yang akan digunakan untuk analisis.
2. Menentukan topologi
   Menentukan topologi terdiri dari observasi dan membuat desain topologi jaringan yang akan digunakan dalam penelitian, menentukan masing-masing perangkat dalam jaringan, seperti *router*, dan perangkat lainnya. dan menentukan lokasi dan konfigurasi titik akses *WiFi* serta penempatan alat *sniffing*.
3. Instalasi dan konfigurasi alat
   Instalasi dan konfigurasi alat meliputi instalasi perangkat lunak yang diperlukan seperti *packet* sniffers *Ettercap*, mengkonfigurasi alat-alat dan memastikan konektivitas dan fungsi alat-alat yang digunakan.
4. analisis
   Analisis dimulai dari proses pengumpulan data dengan menjalankan alat *sniffing* untuk merekam lalu lintas jaringan, menganalisis hasil *sniffing* untuk mengidentifikasi paket data yang sensitif atau rentan terhadap serangan
5. Kesimpulan.
   Pada kesimpulan dilakukan penyusunan hasil analisis dan mengevaluasi keamanan jaringan *WiFi* terhadap serangan *packet sniffing.*

3. Hasil dan Pembahasan



Gambar 2. Skenario Serangan

Serangan yang ditargetkan yaitu pada protokol yang tidak aman yaitu pada FTP dan HTTP. Pada penelitian ini, skenario yang dilakukan berupa pengiriman request protokol

ISSN **2797-815X**
P-ISSN **2797-8745**

pada HTTP dan FTP yang dilakukan PC korban. Paket yang ditransmisikan melalui *access point* kemudian ditangkap oleh penyerang menggunakan *Ettercap*. Skenario dapat digambarkan pada Gambar 2.

Berdasarkan hasil skenario yang telah dijalankan, *ettercap* memungkinkan untuk dengan mudah mengakses informasi *login*, seperti *username* dan *password*, saat melakukan aktivitas *login* menggunakan perangkat yang terhubung ke jaringan *WiFi* PT. XYZ. Protokol yang ditransmisikan dapat ditangkap oleh *Ettercap* baik pada protokol HTTP maupun FTP. Selain itu paket yang diterima dapat dibaca secara utuh sehingga informasi *password*, *username* maupun data lainnya dapat diketahui. Hail dan kesimpulan dapat ditunjukan pada tabel 1.

Tabel 1. Hasil Serangan.

Protokol	Informasi	Kesimpulan
HTTP	User, dan Password	Tidak Aman
FTP	User dan Password	Tidak Aman

Penelitian ini menunjukan bahwa jaringan WiFi di Gedung PT. XYZ memiliki celah keamanan terutama pada protokol yang tidak aman seperti HTTP dan FTP. Penyerang dapat memanfaatkan alat seperti Ettercap untuk mencuri informasi login dan data sensitif lainnya. Berdasarkan pada temuan ini, maka PT. XYZ perlu mengambil langkah-langkah serius untuk meningkatkan keamanan jaringan WiFi. Ini dapat mencakup penerapan enkripsi yang lebih kuat, penggunaan protokol yang aman seperti HTTPS dan SFTP, serta pelatihan pengguna mengenai praktik keamanan yang baik.

Penelitian ini juga menunjukkan bahwa jaringan WiFi di Gedung PT. XYZ rentan terhadap serangan sniffing, terutama pada protokol yang tidak aman seperti HTTP dan FTP. Dengan menggunakan Ettercap, penyerang dapat dengan mudah mengakses informasi sensitif yang dikirim melalui jaringan. Oleh karena itu, penting bagi PT. XYZ untuk meningkatkan langkah-langkah keamanan jaringan untuk melindungi data dan memastikan kelancaran operasional institusi.

4. Kesimpulan

Berdasarkan hasil analisis data dan percobaan penyerangan yang dilakukan, dapat disimpulkan bahwa sistem keamanan jaringan nirkabel di Gedung PT. XYZ belum cukup aman. Hal ini dapat dibuktikan adanya informasi yang dapat diakses oleh penyerang (penyerang) saat dilakukan percobaan *sniffing* pada *WiFi*. Untuk itu perlu pencegahan seperti penggunaan protokol yang aman, penggantian *password* secara berkala dan menghindari protokol yang tidak aman.

ISSN **2797-815X**
P-ISSN **2797-8745**

Daftar Pustaka

[1] A. Umasugi, M. D. Suratin, and S. Hamza, "Analisis Keamanan Jaringan Wifi Terhadap Packet Sniffing DiKampus a Universitas Muhammadiyah Maluku Utara," *Produktif J. Ilm. Pendidik. Teknol. Inf.* , vol. 6, no. 2, pp. 597–602, 2022.

[2] 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.

[3] R. Sahara, S. Abdullah, and R. Saputra, "Analisis Ancaman Sniffing pada Jaringan WiFi di PT. Stepa Wirausaha Adiguna," *Pros. Semin. Nas. Ris. Dan Inf. Sci.*, vol. 4, pp. 224–230, 2022.

[4] Fatimah, T. Mary, and A. Y. Pernanda, "Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing di Universitas PGRI Sumatera Barat," *JURTEII J. Teknol. Inf.*, vol. 1, no. 2, pp. 7–11, 2022, doi: 10.22202/jurteii.2022.5707.

[5] Y. Hae, "Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 4, pp. 2095–2105, 2021, doi: 10.35957/jatisi.v8i4.1196.

ISSN **2797-815X**
P-ISSN **2797-8745**