COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

ANALISIS KEAMANAN JARINGAN WIFI DI PTPN III KEBUN BANDAR SELAMAT TERHADAP ANCAMAN *PACKET SNIFFING*

Raviridho[1*], Abdul Jabbar Lubis [2], Calvin Chiuloto [3]

1,2,3) Prodi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan, Indonesia

*Coresponding Email: raviridho339@gmail.com

Abstrak

Banyaknya tindakan yang terjadi dalam pencurian informasi atau data karyawan seperti usemame serta password asal suatu akun atau data-data penting disebabkan sang hacker karena tidak adanya perlindungan terhadap aspek *confidentialit* pada suatu jaringan komputer. Tujuan dalam penelitian ini adalah untuk menganalisa keamanan jaringan wireless di Kantor PTPN III Kebun Bandar Selamat terhadap *packet sniffing* dan untuk mengevaluasi keamanan jaringan wireless di Kantor PTPN III Kebun Bandar Selamat terhadap *packet sniffing*. Tingkat keamanan yang diterapkan pada *website* PTPN III Kebun Bandar. Selamat. Seperti yang diketahui tingkat kearnanan bukan hanya berasal dari aplikasi *website* PTPN III yang sudah ada namun keamanan *website* PTPN III Kebun Bandar Selamat juga dapat dilihat pada saat proses komunikasi data antara *client* dengan *web server* pada jaringan. Keamanan *website* PTPN III Kebun Bandar Selamat masih perlu peningkatan yang terbukti pada hasil percobaan *sniffing* pada aplikasi Wireshark masih ditemukannya paket data berisi informasi penting seperti *username* dan *password* pada saat melakukan *login*, akses *domain name server* (DNS) yang dituju serta informasi lainnya.

Kata Kunci: Keamanan, Wireless, *Packet Sniffing*, Data.

Abstract

Many actions that occur in theft of employee information or data such as usernames and passwords from an account or important data are caused by hackers because there is no protection for the confidential aspect of a computer network. The aim of this research is to analyze the security of the wireless network at the PTPN III Kebun Bandar Selamat Office against packet sniffing and to evaluate the security of the wireless network at the PTPN III Kebun Bandar Selamat Office against packet sniffing. The level of security implemented on the PTPN III Kebun Bandar Selamat website. As is known, the level of security does not only come from the existing PTPN III website application, but the security of the PTPN III Kebun Bandar Selamat website can also be seen during the data communication process between the client and the web server on the network. The security of the PTPN III Kebun Bandar Selamat website still needs improvement as proven by the rsults of sniffing experiments on the Wireshark application where data packets containing important information such as username and password when logging in, accessing the target domain name server (DNS) and other information were still found.

Keywords: Security, Wireless, Packet Sniffing, Data.

PENDAHULUAN

Masalah keamanan jaringan menjadi perhatian penting di era digital saat ini(Aulia et al., 2023). Jaringan yang terkoneksi ke internet pada dasarnya tidak aman dan selalu berpotensi diakses oleh pihak-pihak yang tidak bertanggung jawab, baik itu melalui jaringan

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

kabel (*wired* LAN) maupun *nirkabel* (*wireless* LAN)(Sembiring, 2020). Ketika file atau data dikirim melalui beberapa terminal di jaringan, peluang bagi hacker untuk menyadap atau mengubah data tersebut meningkat(Indah et al., 2023).

Dalam konteks ini, pentingnya perencanaan dan pemahaman sistem keamanan jaringan yang akan dihubungkan ke internet menjadi sangat vital. Tujuannya adalah untuk melindungi sumber daya, seperti file dan data, secara aman dan efektif, serta meminimalisir serangan dari *hacker*. Salah satu alat yang sering digunakan dalam analisis keamanan jaringan adalah *Wireshark*, sebuah *tool packet sniffing* yang dapat digunakan untuk menganalisis protokol jaringan dan mengaudit keamanan jaringan(Hanipah & Dhika, 2020). *Wireshark* memiliki kemampuan untuk memblokir lalu lintas jaringan, mencuri *password*, dan menyadap protokol umum yang aktif(Farhan & Kusuma, 2023).

Namun, banyak masyarakat yang masih belum paham cara menggunakan *Wireshark*. Kantor PTPN III Bandar Selamat telah menerapkan jaringan LAN dan WLAN untuk berbagai keperluan, termasuk pelayanan umum, kepegawaian, dan informasi penting lainnya. Wi-Fi di setiap ruangan rentan terhadap serangan oleh pihak yang tidak bertanggung jawab. Banyak pengguna yang tidak menyadari bahaya saat terhubung ke *wireless access point* (WPA).

Penggunaan jaringan komputer semakin penting dalam berbagai bidang seperti pekerjaan, pendidikan, dan hiburan(Wijaya & others, 2022). Oleh karena itu, menjaga keamanan jaringan menjadi sangat penting untuk melindungi data dari peretas(Santoso et al., 2022). Serangan *packet sniffing* adalah salah satu teknik yang digunakan untuk memonitor dan mencuri data yang melintas di jaringan(Nurbahri et al., 2023).

Penelitian sebelumnya, seperti yang dilakukan oleh (Nuroji, 2023) dan (R. Kurniawan & Prakoso, 2020), menunjukkan bahwa ada berbagai metode untuk meningkatkan keamanan jaringan, seperti menggunakan sistem pencegahan intrusi (IPS) dan *packet filtering* berbasis Mikrotik. Namun, perlindungan aspek kerahasiaan pada jaringan komputer masih sering diabaikan.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis keamanan jaringan pada fasilitas Wi-Fi di PTPN III Kebun Bandar Selamat terhadap

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

serangan *packet sniffing*. Dengan demikian, diharapkan dapat memberikan solusi untuk meningkatkan keamanan jaringan dan melindungi data penting dari ancaman peretasan.

KAJIAN TEORI

Jaringan Komputer

Jaringan komputer adalah sistem yang terdiri dari dua atau lebih komputer yang terhubung satu sama lain untuk tujuan berbagi data dan sumber daya. Dalam jaringan komputer, perangkat seperti komputer, printer, dan perangkat lainnya dapat berkomunikasi satu sama lain melalui media transmisi seperti kabel, gelombang radio, atau teknologi inframerah(Mulyanto & Prakoso, 2020). Jaringan ini memungkinkan penggunanya untuk saling bertukar informasi, berbagi file, dan menggunakan perangkat keras bersama, seperti printer dan penyimpanan data. Jenis-jenis jaringan komputer meliputi jaringan lokal (LAN), jaringan area luas (WAN), dan jaringan pribadi virtual (VPN)(Pelealu et al., 2020). Prinsip dasar dari jaringan komputer meliputi protokol komunikasi, arsitektur jaringan, dan model referensi seperti OSI dan TCP/IP, yang semuanya bekerja bersama untuk memastikan data dapat dikirim dan diterima dengan benar dan aman(Bahtiar et al., 2021). Jaringan komputer menjadi landasan penting dalam era digital saat ini, mendukung segala macam aktivitas dari perkantoran hingga komunikasi global(An'ars et al., 2022).

Keamanan Jaringan

Keamanan jaringan adalah upaya untuk melindungi integritas, kerahasiaan, dan ketersediaan data yang dikirim melalui jaringan komputer dari berbagai ancaman dan serangan. Ini melibatkan penggunaan perangkat keras dan perangkat lunak untuk mendeteksi, mencegah, dan merespons akses yang tidak sah serta ancaman seperti virus, worm, dan peretas(Rivaldi & Marpaung, 2023). Keamanan jaringan mencakup berbagai teknik dan langkah-langkah seperti enkripsi, firewall, antivirus, dan sistem deteksi serta pencegahan intrusi (IDS/IPS)(Munawar et al., 2020). Tujuan utamanya adalah untuk memastikan bahwa data tetap aman selama transmisi dan hanya dapat diakses oleh pihak yang berwenang. Dengan meningkatnya ancaman siber, pentingnya keamanan jaringan menjadi semakin kritis untuk melindungi informasi sensitif dan menjaga operasi bisnis serta layanan online tetap berjalan lancar(Simanjuntak et al., 2024).

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

Wireless Fidelity (Wi-Fi)

Wi-Fi (*Wireless Fidelity*) adalah teknologi jaringan nirkabel yang memungkinkan perangkat seperti komputer, smartphone, dan tablet terhubung ke internet atau berkomunikasi satu sama lain tanpa memerlukan kabel fisik. Wi-Fi menggunakan gelombang radio frekuensi tinggi untuk mengirim dan menerima data melalui udara, biasanya dalam pita frekuensi 2.4 GHz atau 5 GHz. Teknologi ini memanfaatkan standar IEEE 802.11 yang mengatur komunikasi jaringan nirkabel dan memastikan kompatibilitas antar perangkat yang berbeda(Sinaga et al., 2024). Keuntungan utama dari Wi-Fi adalah kemudahan akses dan mobilitas, memungkinkan pengguna untuk terhubung ke jaringan dari berbagai lokasi dalam jangkauan sinyal(Mustamu et al., 2022). Namun, karena bersifat nirkabel, keamanan Wi-Fi menjadi penting untuk mencegah akses yang tidak sah dan melindungi data yang dikirimkan melalui jaringan. Teknik keamanan seperti WPA2 (*Wi-Fi Protected Access* 2) digunakan untuk mengenkripsi data dan memastikan hanya pengguna yang berwenang yang dapat mengakses jaringan Wi-Fi(Adiguna & Widagdo, 2022).

Serangan *Nirkabel*

Serangan nirkabel adalah upaya oleh pihak yang tidak berwenang untuk mengakses, mengganggu, atau memanipulasi jaringan nirkabel (*Wi-Fi*) dan data yang dikirim melalui jaringan tersebut. Serangan ini dapat mencakup berbagai metode seperti penyadapan (*eavesdropping*), serangan *man-in-the-middle* (MITM), dan serangan *denial-of-service* (DoS)(Arief et al., 2022). Penyadapan melibatkan pemantauan lalu lintas jaringan untuk mencuri informasi sensitif, sementara serangan MITM memungkinkan penyerang untuk menyusup di antara dua pihak yang berkomunikasi dan mengubah atau mencuri data(Khasanah & Sutabri, 2023). Serangan DoS bertujuan untuk membuat jaringan tidak dapat diakses oleh pengguna yang sah dengan membanjiri jaringan dengan lalu lintas yang berlebihan(Haris et al., 2022). Keamanan jaringan nirkabel sangat penting untuk mencegah serangan ini, termasuk penggunaan enkripsi yang kuat seperti WPA2, pemantauan jaringan secara terus-menerus, dan pembaruan perangkat lunak secara berkala untuk menutup celah keamanan(Pangestu & Liza, 2022).

Paket Sniffing

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

Packet sniffing adalah teknik untuk menangkap dan menganalisis data yang ditransmisikan melalui jaringan komputer. Proses ini dilakukan oleh perangkat keras atau perangkat lunak yang dikenal sebagai sniffer, yang memantau dan mencatat setiap paket data yang melewati jaringan(Zulfa et al., 2023). *Packet sniffing* dapat digunakan untuk tujuan yang sah, seperti pemantauan jaringan untuk menjaga kinerja dan keamanan, serta mendeteksi masalah teknis atau pelanggaran kebijakan. Namun, packet sniffing juga dapat disalahgunakan oleh penyerang untuk menyadap informasi sensitif, seperti kata sandi, email, dan data pribadi lainnya, yang dikirimkan melalui jaringan tanpa enkripsi yang memadai. Oleh karena itu, penting untuk menerapkan langkah-langkah keamanan yang tepat, seperti enkripsi data dan penggunaan protokol yang aman, untuk melindungi data dari penyadapan oleh pihak yang tidak berwenang.

Wireshark

Wireshark adalah perangkat lunak *open-source* yang digunakan untuk menganalisis lalu lintas jaringan secara *real-time*. Alat ini berfungsi sebagai *network protocol analyzer*, memungkinkan pengguna untuk menangkap dan memeriksa data yang melewati jaringan komputer dalam bentuk paket. *Wireshark* mendukung berbagai protokol jaringan dan mampu menampilkan data yang sangat rinci untuk setiap paket yang ditangkap, sehingga berguna untuk *troubleshooting* jaringan, pemantauan keamanan, dan pengembangan protokol. Dengan *Wireshark*, administrator jaringan dapat mengidentifikasi masalah kinerja, mendeteksi intrusi, dan menganalisis komunikasi jaringan untuk memastikan integritas dan keamanan data. Meskipun sangat berguna, penggunaan *Wireshark* memerlukan keahlian dan tanggung jawab, karena penyalahgunaannya untuk mengintip lalu lintas jaringan yang tidak sah dapat menimbulkan pelanggaran privasi dan keamanan.

Penelitian Terdahulu

Berikut ini terdapat beberapa penelitian terdahulu terkait dengan kemanan jaringan terhadap ancaman *paket sniffing* disajikan pada tabel 1 berikut:

Tabel 1. Penelitian Terdahulu

No	Peneliti	Penelitian Yang Dibahas
1.	(T. A. Kurniawan, 2020)	Penelitian ini bertujuan untuk menganalisis keamanan jaringan WiFi terhadap serangan *packet sniffing*, yang merupakan teknik penyadapan data yang dikirim melalui jaringan nirkabel oleh pihak

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

		yang tidak berwenang. Dalam penelitian ini, berbagai langkah keamanan dieksplorasi untuk melindungi data dari ancaman penyadapan, termasuk penggunaan enkripsi WPA2-PSK pada hotspot WiFi, memperbarui perangkat lunak dan *firmware* secara berkala, serta menerapkan *Virtual Private Network* (VPN) untuk mengenkripsi lalu lintas jaringan. Penelitian juga menekankan pentingnya segmentasi jaringan untuk memisahkan jaringan publik dan pribadi, serta pemantauan jaringan secara *real-time* menggunakan alat seperti *Wireshark* untuk mendeteksi aktivitas mencurigakan. Selain itu, edukasi pengguna tentang praktik keamanan yang baik juga diidentifikasi sebagai langkah penting untuk mengurangi risiko serangan *packet sniffing*. Hasil penelitian ini diharapkan dapat memberikan solusi praktis untuk meningkatkan keamanan jaringan WiFi dan melindungi data dari ancaman serangan *cyber*.
2.	(Sahara et al., 2022)	Penelitian ini bertujuan untuk menganalisis ancaman *sniffing* pada jaringan WiFi di PT. Stepa Wirausaha Adiguna. Sniffing adalah teknik yang digunakan oleh penyerang untuk menangkap dan menganalisis data yang berlalu lintas di jaringan WiFi, yang dapat berisi informasi sensitif seperti kata sandi dan data pribadi. Dalam penelitian ini, dilakukan serangan *sniffing* pada jaringan WiFi untuk mengevaluasi tingkat keamanannya dan mengidentifikasi celah keamanan yang dapat dimanfaatkan oleh penyerang. Hasil penelitian menunjukkan bahwa kesadaran akan keamanan jaringan internet sangat penting bagi siapa saja dan di mana saja. Oleh karena itu, penelitian ini menekankan pentingnya menerapkan langkah-langkah keamanan yang tepat, seperti penggunaan enkripsi yang kuat, pembaruan perangkat lunak secara berkala, dan edukasi pengguna tentang praktik keamanan yang baik.
3.	(Arini et al., 2024)	Penelitian ini bertujuan untuk meningkatkan keamanan jaringan Wi-Fi di PT. Akurat. Co terhadap serangan *packet sniffing* dengan menggunakan *firewall rule*. *Packet sniffing* adalah teknik di mana penyerang dapat menangkap dan menganalisis data yang melewati jaringan untuk mencuri informasi sensitif seperti kata sandi dan data pribadi. Penelitian ini mengimplementasikan aturan *firewall* sebagai langkah perlindungan utama.

METODE PENELITIAN

Dalam menjelaskan sebuah alur penelitian disajikan untuk mempermudah pemahaman dalam penelitian tersebut. Metode tersaji dalam diagram alir penelitian seperti pada gambar 1 berikut.

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

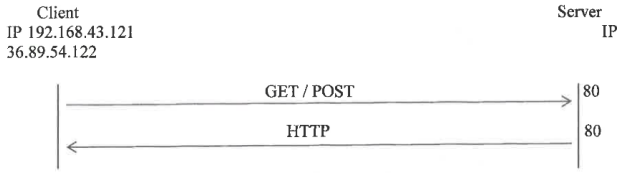
Gambar 1. Alur Penelitian

Untuk ditahap awal dilakukan analisis, hal ini perlu dilakukan untuk mengetahui seberapa aman tingkat keamanan yang diterapkan pada website PTPN Ill Kebun Bandar Selamat. Seperti yang diketahui tingkat keamanan bukan hanya berasal dari aplikasi *website* PTPN III yang sudah ada namun keamanan website PTPN III Kebun Bandar Selamat juga dapat dilihat pada saat proses komunikasi data antara *client* dengan *web server* pada jaringan. Keamanan *website* PTPN III Kebun Bandar Selamat masih perlu peningkatan yang terbukti pada hasil percobaan *sniffing* pada aplikasi *Wireshark* masih ditemukannya paket data berisi informasi penting seperti *username* dan *password* pada saat melakukan *login*, akses *domain name server* (DNS) yang dituju serta informasi lainnya.

Selanjutnya dilakukan analisis terhadap serangan *pakect sniffing*, hsil dengan dilakukannya analisis uji coba dalam penelitian ini menunjukkan bahwa *website* www.ptpn.co.id rentan terhadap pencurian data dengan menggunakan metode serangan sniffing pada jaringan nirkabel. Hal ini terjadi karena pada website www.ptpn.co.id masih menggunakan protokol HTTP sedangkan *website Google Accounts* menggunakan protokol TLS. Perbedaanya yaitu terletak pada cara kerjanya. Pada saat target mengakses website www.ptpn.co.id menggunakan browser, kemudian browser meminta data pada server, server langsung mengirim data yang di minta dalam bentuk teks biasa melalui TCP tanpa adanya perlindungan lebih. Sehingga pada saat melakukan proses *sniffing*, seluruh data yang

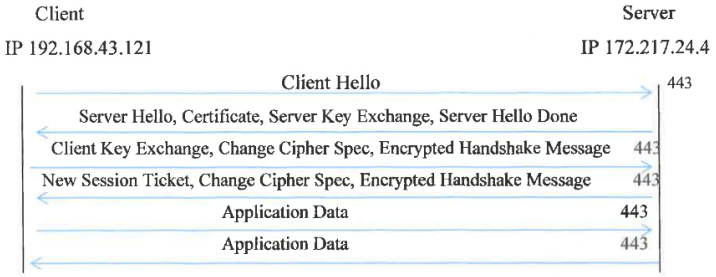
COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

melewati komputer penyerang akan tercaprute pada aplikasi *wireshark* dan data tersebut dapat dibaca langsung oleh penyerang. Untuk proses komunikasi data website ptpn3.co.id digambarkan sebagai berikut.



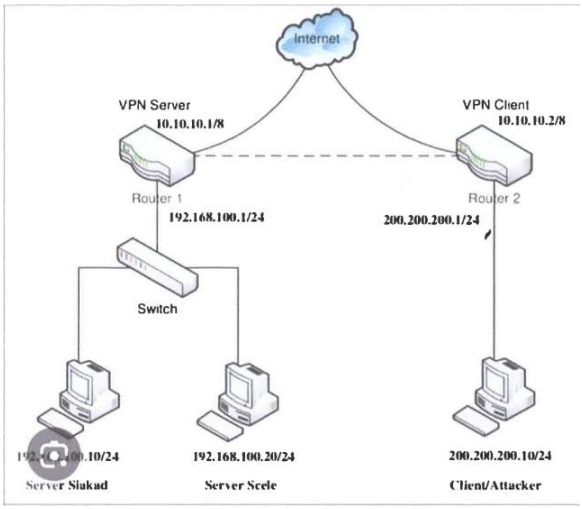
Gambar 2. Proses Komunikasi Data Website **www.ptpn3.co.id**

Diamana secara sederhana proses komunikasi data *website google accounts* dapat dilihat pada gambar 3 berikut.



Gambar 3. Proses Komunikasi Data *Website Google Accounts*

Selanjutnya dapat digambarkan topologi jaringan yang ada seperti gambar 4 berikut.

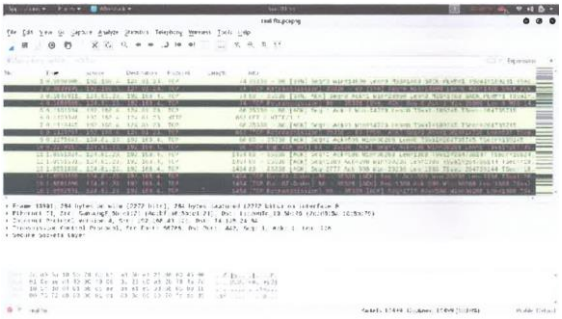


Gambar 4. Topologi Jaringan PTPN III

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

HASIL DAN PEMBAHASAN

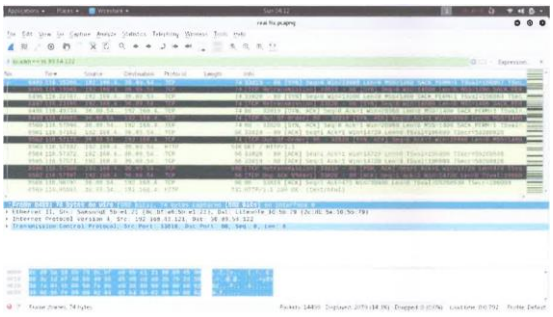
Untuk langkah diawal dilakukan perekaman paket data pada website PTPN III. Adapun hasil data perekaman disajikan pada gambar 5 berikut.



Gambar 5. Data Hasil Rekaman Paket Data

Pada gambar 5 merupakan tampilan hasil rekaman serangan *packet sniffing* pada software Wireshark yang telah merekam seluruh aktivitas yang terjadi pada jaringan. Untuk melihat paket yang berasal dari website ptpn3.co.id, maka diharuskan melakukan penyaringan dahulu dari paket yang telah direkam. Sebelum melakukan penyaringan terlebih dahulu, penulis harus mengetahui *IP address* dari website ptpn3.co.id, yaitu www.ptpn3.co.id dengan cara membuka terminal kemudian mengetikkan perintah yang sesuai dan menekan *Enter* pada keyboard. Maka, akan muncul *IP address* dari www.ptpn3.co.id.

Hal ini dapat diterangkan bahwa angka yang diberi tanda persegi panjang merah merupakan *IP address* dari website ptpn3.co.id. Setelah mengetahui *IP address* dari **www.ptpn3.co.id**, maka selanjutnya dilakukan penyaringan paket pada *address bar filter* yang ada di bawah kumpulan *icon* aplikasi Wireshark dengan memasukkan perintah “ip.addr==36.89.54.122” maka akan tampil paket-paket yang memiliki *IP address* tersebut.



Gambar 6. Hasil Penyaringan Paket Data Website PTPN III

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

Gambar 6 menunjukkan semua paket data yang memiliki Alamat IP yang ditemukan baik di *Source* maupun di *Destination*. Tampak jelas bahwa *Source* dan *Destination* selalu bertukar tempat. Dari 2070 paket data yang ditampilkan, terdapat dua jenis protokol yang digunakan: *protokol transmission control protocol* (TCP) dan protokol lain yang relevan dengan proses analisis.

Berikut salah satu tampilan detail *packet data protocol* TLS yang memiliki info *Application Data*.

Untuk melihat proses komunikasi pada saat korban mengkases *website Google Accounts* dapat dilakukan dengan cara mengklik *"Statistik"* pada menu bar kemudian pilih *"Flow Graph"* berikut ini adalah tampilannya.

Gambar 8. Proses Komunikasi Data *accounts.google.com*

Gambar 8. Menunjukan proses komunikasi data antara *client* yang memeiliki *IP address* 192.168.43.121 sedangkan *server* yaitu *accounts.google.com* memiliki *IP address* 74.125.24.84.

SIMPULAN

Setelah melakukan penelitian, beberapa langkah penting dapat diambil untuk meningkatkan keamanan jaringan terhadap serangan. Pertama, menggunakan enkripsi WPA2-PSK pada hotspot Wi-Fi sangat krusial, karena hanya orang-orang tertentu yang dapat terhubung ke jaringan tersebut, sehingga serangan sniffing oleh pihak yang tidak terhubung ke jaringan dapat dicegah. Kedua, memperbarui *browser* ke versi terbaru sangatlah penting, karena versi lama berisiko terhadap berbagai serangan akibat celah keamanan yang sudah diketahui dan dapat digunakan untuk mencuri informasi sensitif. Penggunaan *browser* versi

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

terbaru menjamin keamanan saat terhubung ke internet, karena menyimpan daftar informasi sertifikat *Secure Socket Layer* (SSL) dari berbagai situs web, yang membantu mencegah serangan *man-in-the-middle* (MITM).

DAFTAR PUSTAKA

Adiguna, M. A., & Widagdo, B. W. (2022). Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus: Router Tp-Link Mercusys Mw302r). *Jurnal SISKOM-KB (Sistem Komputer Dan Kecerdasan Buatan)*, *5*(2), 1–8.

An'ars, M. G., Wahyudi, A. D., Hendrastuty, N., Damayanti, D., Hutagalung, S., & Mahendra, A. (2022). Pelatihan Jaringan Microtik Untuk Meningkatkan Keterampilan Siswa Di Smk Negeri 2 Bandarlampung. *Journal of Social Sciences and Technology for Community Service (JSSTCS)*, *3*(2), 218–223.

Arief, M. F., Santoso, N. A., & Kurniawan, R. D. (2022). Systematic Literatur Review: Keamanan Komputer Pada Jaringan Nirkabel. *Indonesian Journal of Informatics and Research*, *3*(2), 1–8.

Arini, A., Arsalan, M. L., & Sukmana, H. T. (2024). Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus: Pt. Akurat. Co). *Cyber Security Dan Forensik Digital*, *6*(2), 30–38.

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital. *JUSTINFO| Jurnal Sistem Informasi Dan Teknologi Informasi*, *1*(1), 9–20.

Bahtiar, D., Febrianto, W. J., Maulana, A., Saputra, S., Darmawan, W., Tafonao, R. P., Julianto, R., Zai, R., & Djutalov, R. (2021). Pengenalan dasar instalasi jaringan komputer menggunakan mikrotik. *J. Kreat. Mhs. Inform*, *2*(3), 507–518.

Farhan, R. M., & Kusuma, G. H. A. (2023). Teknik Sniffing Jaringan Menggunakan Wireshark. *Journal of Informatics and Advanced Computing (JIAC)*, *4*(1), 87–93.

Hanipah, R., & Dhika, H. (2020). Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark. *DoubleClick: Journal of Computer and Information Technology*, *4*(1), 11–23.

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Komputika: Jurnal Sistem Komputer*, *11*(1), 67–76.

Indah, F., Sidabutar, A. Q., & Nasution, N. A. (2023). Peran cyber security terhadap keamanan data penduduk negara Indonesia (Studi kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1), 57–64.

Khasanah, N., & Sutabri, T. (2023). Analisis Kejahatan Cybercrime Pada Peretasan Dan Penyadapan Aplikasi Whatsapp. *Blantika: Multidisciplinary Journal*, *1*(2), 44–55.

Kurniawan, R., & Prakoso, F. (2020). Implementasi Metode IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System) untuk Meningkatkan Keamanan Jaringan. *SENTINEL*, *3*(1), 231–242.

Kurniawan, T. A. (2020). Analisa Keamanan Jaringan Wifi Terhadap Serangan Packet Sniffing. *Jurnal Ilmiah Fakultas Teknik LIMIT'S Vol*, *16*(2), 11.

Mulyanto, Y., & Prakoso, S. B. (2020). Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawadengan Metode Network Development Life Cycle (NDLC): Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspe. *Jurnal Informatika Teknologi Dan Sains (Jinteks)*, *2*(4), 223–233.

Munawar, Z., Putri, N. I., & others. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa*, *2*(01), 14–20.

Mustamu, L. P., Ayub, M., & Liliawati, S. L. (2022). Manajemen Risiko Pemasangan Wifi pada Perusahaan Telekomunikasi dengan Framework Risk Information Technology. *Jurnal Teknik Informatika Dan Sistem Informasi*, *8*(1), 246–260.

Nurbahri, R., Nurcahyo, G. W., & others. (2023). Analisis Penggunaan Metode Port Knocking pada Sistem Keamanan Jaringan Komputer (Studi Kasus di Universitas Baiturrahmah). *Jurnal Sistim Informasi Dan Teknologi*, 102–108.

Nuroji, N. (2023). Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan komputer sebagai pencegahan serangan Port-Scanning. *Journal of Data Science and Information Systems*, *1*(2), 41–49.

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 165-177
https://jurnal.compartdigital.com/index.php/comptech

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.

Pelealu, R. R. A. A., Wonggo, D., & Kembuan, O. (2020). Perancangan dan Implementasi Jaringan Komputer Smk Negeri 1 Tahuna. *JOINTER: Journal of Informatics Engineering*, *1*(01), 5–11.

Rivaldi, O., & Marpaung, N. L. (2023). Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata. *Jurnal Inovtek Polbeng Seri Informatika*, *8*(1), 141–153.

Sahara, R., Abdullah, S., & Saputra, R. (2022). Analisis Ancaman Sniffing pada Jaringan WiFi di PT. Stepa Wirausaha Adiguna. *Prosiding Seminar Nasional Riset Information Science (SENARIS)*, *4*(2), 224–230.

Santoso, N. A., Affandi, K. B., & Kurniawan, R. D. (2022). Implementasi keamanan jaringan menggunakan port knocking. *Jurnal Janitra Informatika Dan Sistem Informasi*, *2*(2), 90–95.

Sembiring, A. S. (2020). Penerapan Model Protokol Aaa (Authentication, Authorization, Accounting) Pada Keamanan Jaringan Komunikasi Wan (Wide Area Network). *Jurnal Multimedia Dan Teknologi Informasi (Jatilima)*, *2*(1), 19–29.

Simanjuntak, E. N., Irmayani, D., & Nasution, F. A. (2024). Tinjauan penerapan kecerdasan buatan dalam keamanan jaringan tantangan dan prospek masa depan. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, *7*(2), 370–375.

Sinaga, A. P., Syahputra, I., & others. (2024). Optimalisasi Jaringan Wifi (Wireless Fidelity) sebagai Fasilitas Pendukung Akademik Mahasiswa (Studi Kasus di UINSU). *Cognoscere: Jurnal Komunikasi Dan Media Pendidikan*, *2*(4).

Wijaya, A., & others. (2022). Implementasi Metode Rekayasa Sistem Jaringan Komputer untuk Pengembangan Jaringan Komputer. *Implementasi Metode Rekayasa Sistem Jaringan Komputer Untuk Pengembangan Jaringan Komputer*.

Zulfa, M. I., Tena, S., & Rizkiono, S. D. (2023). Aktivitas Sniffing Pada Malware Pencuri Uang Di Smartphone Android. *RENATA: Jurnal Pengabdian Masyarakat Kita Semua*, *1*(1), 7–10.