Modem: Jurnal Informatika dan Sains Teknologi
Volume. 4, Nomor. 1 Januari 2026
E-ISSN .: 3046-7209; P-ISSN .: 3046-7217, Hal. 10-22
DOI: https://doi.org/10.62951/modem.v4i1.694
Tersedia : https://journal.aptii.or.id/index.php/Modem

Analisis Keamanan Jaringan Komputer Menggunakan Metode *Penetration Testing*

Alfian Hongu Moly[1*], Stefanus D.I. Mau[2], Dian Fransiska Ledi[3]
[1-3]Program Studi Teknik Informatika, Universitas Stella Maris Sumba, Indonesia
**Penulis Korespondensi: ivanmau1108@gmail.com*

Abstract. *Data security in web services is a critical aspect that must be considered to prevent information leakage and unauthorized access. This study aims to analyze the security level of the Universitas Andalas Repository site, specifically regarding its vulnerability to sniffing attacks due to the use of the unencrypted HTTP protocol. The research employs a penetration testing method with an experimental approach. The testing process is carried out in three main stages: reconnaissance using Nmap to identify the services and protocols in use, sniffing using Wireshark to capture and analyze data packets, and evaluation of results based on modern web security standards to assess the level of risks found. The results of the study indicate that the Universitas Andalas Repository site still uses the HTTP protocol in its communication process, meaning that all data transmitted between the client and server can be read in plaintext. The Nmap scan results confirm that the web service operates on port 80 without SSL/TLS encryption support. Meanwhile, the packet analysis results using Wireshark show that both HTTP requests and responses can be captured and directly observed, including request parameters, cookies, and other potentially sensitive information. These findings suggest that the site has significant vulnerabilities to sniffing attacks and man-in-the-middle attacks, posing a potential risk to user data security.*

Keywords*: Data Security; Encryption; HTTP Protocol; Penetration Testing; Sniffing*

Abstrak. Keamanan data pada layanan web merupakan aspek penting yang harus diperhatikan untuk mencegah terjadinya kebocoran informasi dan penyalahgunaan akses. Penelitian ini bertujuan untuk menganalisis tingkat keamanan situs Repository Universitas Andalas, khususnya terkait kerentanan terhadap serangan *sniffing* akibat penggunaan protokol HTTP yang tidak dienkripsi. Penelitian menggunakan metode *penetration testing* dengan pendekatan eksperimen. Proses pengujian dilakukan melalui tiga tahap utama, yaitu *reconnaissance* menggunakan Nmap untuk mengidentifikasi layanan dan protokol yang digunakan, *sniffing* menggunakan Wireshark untuk menangkap dan menganalisis paket data, serta evaluasi hasil berdasarkan standar keamanan web modern untuk menilai tingkat risiko yang ditemukan. Hasil penelitian menunjukkan bahwa situs Repository Universitas Andalas masih menggunakan protokol HTTP pada proses komunikasinya, sehingga seluruh data yang ditransmisikan antara *client* dan server dapat terbaca dalam bentuk *plaintext*. Hasil pemindaian Nmap mengonfirmasi bahwa layanan web berjalan pada port 80 tanpa dukungan enkripsi SSL/TLS. Sementara itu, hasil analisis paket menggunakan Wireshark menunjukkan bahwa *request* dan *response* HTTP dapat ditangkap serta diamati secara langsung, termasuk parameter permintaan, *cookie*, dan informasi lain yang berpotensi sensitif. Temuan ini menunjukkan bahwa situs tersebut memiliki kerentanan signifikan terhadap serangan *sniffing* dan *man-in-the-middle attack*, sehingga berpotensi membahayakan keamanan data pengguna.

Kata kunci: Enkripsi; Keamanan Data; *Penetration Testing*; Protokol HTTP; *Sniffing*

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi yang sangat pesat telah membawa dampak besar dalam berbagai bidang kehidupan (Rahma et al., 2021). Salah satu aspek penting dari perkembangan ini adalah pemanfaatan jaringan komputer sebagai tulang punggung dalam pengelolaan data dan komunikasi digital. Di era digital saat ini, hampir seluruh aktivitas organisasi, baik dalam bidang pendidikan, pemerintahan, bisnis, maupun layanan publik, sangat bergantung pada jaringan komputer untuk menjalankan operasional sehari-hari (Khasanah & Putri, 2021). Jaringan komputer tidak hanya menjadi alat bantu, melainkan juga menjadi komponen vital yang menjamin efisiensi, produktivitas, dan kontinuitas layanan.

Naskah Masuk: 09 Oktober 2025; Revisi: 06 November 2025; Diterima: 04 Desember 2025; Tersedia: 09 Desember 2025

Seiring dengan meningkatnya ketergantungan terhadap jaringan komputer (Syahputra et al., 2024), ancaman terhadap keamanan sistem informasi pun ikut meningkat secara signifikan. Serangan *sniffing* menjadi salah satu tantangan utama yang dihadapi oleh organisasi modern (Hae & Sulistyo, 2021). Keamanan jaringan komputer (*network security*) merupakan aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Oleh karena itu, dibutuhkan upaya yang sistematis dan menyeluruh dalam menilai dan memperkuat sistem pertahanan jaringan dari berbagai potensi serangan. Salah satu pendekatan yang banyak diterapkan oleh para profesional keamanan siber adalah *penetration testing*, atau sering disebut sebagai *pentest*. *Penetration testing* adalah metode yang digunakan untuk menguji keamanan sistem dengan cara mensimulasikan serangan yang dilakukan oleh pihak luar seperti peretas (Fachri et al., 2021). Tujuannya adalah untuk mengidentifikasi dan mengevaluasi titik-titik lemah (*vulnerabilities*) dalam sistem sebelum ditemukan dan dieksploitasi oleh pihak yang tidak bertanggung jawab.

Repository Universitas Andalas adalah sebuah sistem penyimpanan digital yang dikelola oleh Universitas Andalas untuk mengumpulkan, mengelola, mendokumentasikan, dan menyediakan akses terbuka terhadap berbagai karya ilmiah sivitas akademika. Repository ini berfungsi sebagai pusat arsip digital yang menyimpan beragam bentuk publikasi akademik, seperti skripsi, tesis, disertasi, jurnal, prosiding, laporan penelitian, buku, serta karya ilmiah lainnya.

Permasalahan utama pada situs Repository Universitas Andalas adalah masih digunakannya protokol HTTP dalam proses transmisi data, sehingga informasi yang dikirimkan termasuk kredensial pengguna tidak dienkripsi dan berpotensi mudah disadap melalui serangan *sniffing* (Haq, 2025). Kondisi ini menimbulkan risiko kebocoran data serta membuka peluang bagi pihak tidak bertanggung jawab untuk melakukan penyadapan dan penyalahgunaan informasi yang ditransmisikan melalui jaringan

Berdasarkan uraian tersebut, dapat diketahui bahwa penelitian terdahulu lebih banyak berfokus pada analisis keamanan jaringan secara umum maupun pada aplikasi web dengan kerentanan berbeda, sedangkan hingga saat ini belum ditemukan penelitian yang secara khusus menganalisis kerentanan terhadap serangan *sniffing* pada situs Repository Universitas Andalas. Oleh karena itu, penelitian ini diperlukan untuk mengidentifikasi potensi kelemahan, mengevaluasi tingkat keamanan transmisi data, serta memberikan rekomendasi perbaikan terhadap kerentanan yang terindikasi pada situs tersebut.

2. KAJIAN TEORITIS

Dalam menemukan gap penelitian ini maka peneliti membahas penelitian terdahulu yang pernah dilakukan dengan topik yang mirip dengan judul pembahasan saat ini, berikut penelitian terdahulu:

Penelitian yang dilakukan Silmina et al. (2022) dengan judul Analisis Keamanan Jaringan 9Sistem Informasi Sekolah Menggunakan *Penetration Test* dan *Issaf*, penelitian ini bertujuan untuk mencari celah keamanan dan mengetahui tingkat keamanan jaringan untuk menghindari adanya tindakan yang tidak diinginkan seperti pencurian data atau penyalahgunaan hak akses. Metode yang digunakan pada penelitian ini adalah *Information System Security Assessment Framework* (ISSAF). Hasil akurasi ini menunjukkan bahwa Sistem Informasi Sekolah MTsN 8 Bantul aman dari celah keamanan.

Adapun penelitian yang dibahas oleh Munawar et al. (2023) dengan judul Analisis Keamanan Pada Teknologi *Blockchain*, pada penelitian ini bertujuan untuk menganalisis keamanan pada teknologi *blockchain*, metode yang digunakan kerangka PDI . Hasil dari penelitian ini adalah arsitektur, kerangka, dan standar keamanan teknologi *blockchain* dan kerangka kerja untuk mengurangi risiko keamanan dunia maya saat menggunakan teknologi *blockchain*. Dengan penelitian ini semoga dapat meningkatkan literatur mutakhir tentang keamanan *blockchain* dan mengusulkan penelitian di masa depan.

Penelitian yang diberikan oleh Irfan et al. (2024) dengan judul Analisis Keamanan Jaringan Nirkabel Menggunakan *Wireless Intrusion Detection System* (WIDS), bertujuan untuk mengimplementasikan *tools Wireless Intrusion Detection System* (WIDS) pada kantor DPRD Kabupaten Soppeng. Metode yang digunakan dalam penelitian ini adalah *System Development Life Cycle* (SDLC). Hasil dari penelitian ini adalah dapat mendeteksi serangan yang terjadi di dalam sistem jaringan pada kantor DPRD Kabupaten Soppeng.

Penelitian yang dilakukan oleh Pratikno (2025) adalah bagaimana menganalisis metode yang telah digunakan dalam mengamankan *Wireless Access Point* (WAP) melalui pendekatan *Systematic Literature Review* (SLR) Proses tinjauan dilakukan dengan metode PRISMA, yang melibatkan pemilihan literatur berdasarkan kriteria inklusi tertentu dari berbagai sumber akademik seperti Google Scholar. Hasil dari penelitian ini adalah keamanan WAP memerlukan pengujian yang komprehensif dan berkelanjutan untuk mengantisipasi ancaman siber yang terus berkembang.

Penelitian yang dilakukan Santoso et al. (2022) adalah pada penelitian ini *port knocking* digunakan untuk melakukan penelitian untuk pembuatan jaringan komputer yang aman Berdasarkan hasil analisis dan pengujian implementasi sistem, dapat disimpulkan bahwa

sistem dapat berfungsi secara efektif dan keamanan jaringan bawaannya dapat ditingkatkan dibandingkan dengan keamanan non-jaringan. Pasang keamanan *port knock* pada tempatnya. Kehadiran otentikasi yang sesuai saat mengakses adalah buktinya.

Dari kelima penelitian tersebut, terlihat bahwa belum ada penelitian yang secara khusus menganalisis kerentanan keamanan pada layanan web perguruan tinggi, khususnya situs Repository Universitas Andalas, dengan pendekatan *penetration testing* berbasis serangan *sniffing*. Selain itu, penelitian sebelumnya tidak memfokuskan pengujian pada protokol komunikasi HTTP yang masih digunakan pada situs tertentu dan berpotensi menimbulkan kebocoran data melalui penyadapan paket.

Oleh karena itu, penelitian ini memiliki perbedaan yang signifikan, yaitu melakukan analisis keamanan terhadap situs Repository Universitas Andalas dengan menargetkan kerentanan transmisi data yang tidak terenkripsi, menggunakan *penetration testing* berbasis metode *sniffing*, serta memanfaatkan *tools* Wireshark dan Nmap untuk mengidentifikasi potensi penyadapan, celah keamanan, serta risiko yang mungkin timbul akibat penggunaan protokol HTTP (Rahman et al., 2025). Gap inilah yang melandasi pentingnya penelitian ini sebagai upaya memberikan gambaran aktual mengenai tingkat keamanan layanan web tersebut dan rekomendasi mitigasi untuk mencegah ancaman serupa.

3. METODE PENELITIAN

Algoritma Penelitian

Penelitian ini menggunakan jenis penelitian *penetration testing* dengan pendekatan eksperimental, yaitu melakukan pengujian langsung terhadap keamanan jaringan dan protokol komunikasi yang digunakan pada situs Repository Universitas Andalas. Pendekatan ini dipilih untuk mengidentifikasi celah keamanan, khususnya kerentanan penyadapan (*sniffing*) akibat penggunaan protokol HTTP yang tidak terenkripsi. Penelitian ini menekankan pada analisis teknis dengan merekam lalu lintas jaringan, mengamati pola transmisi data, serta menguji potensi kebocoran informasi menggunakan *tools* Wireshark dan Nmap.

Alur Penelitian

Prosedur penelitian dilakukan melalui beberapa tahap berikut:

Perencanaan

a. Menentukan objek yang akan dianalisis, yaitu situs Repository Universitas Andalas.
b. Menentukan metode pengujian keamanan berbasis *sniffing*.
c. Menyiapkan perangkat dan *tools* yang diperlukan.

Pengumpulan Informasi Awal (Reconnaissance)

a. Melakukan identifikasi alamat IP, *port*, dan layanan menggunakan Nmap.
b. Mengamati struktur komunikasi website melalui browser dan *tools* developer.

Pengujian Keamanan (Penetration testing)

Pengujian dilakukan menggunakan dua teknik utama:

a. *Scanning* dan *Service Enumeration* (Nmap)
    1) Melakukan *port scanning* pada target.
    2) Mengidentifikasi protokol dan layanan yang terbuka.
    3) Menentukan apakah server menggunakan HTTP tanpa enkripsi.
b. *Sniffing* dan Analisis Paket (Wireshark)
    1) Menangkap paket jaringan selama proses akses ke situs repository.
    2) Menganalisis apakah terdapat data sensitif yang dikirim dalam bentuk *plaintext*.
    3) Mengamati *request-response* HTTP, termasuk parameter autentikasi.
    4) Mengidentifikasi potensi serangan seperti *session hijacking*, *credential leakage*, atau informasi lain yang dapat disadap.

Analisis Hasil

a. Mengevaluasi hasil tangkapan paket untuk menemukan indikasi kelemahan.
b. Menginterpretasikan data apakah benar terdapat risiko *sniffing*.
c. Membandingkan hasil pengujian dengan standar keamanan web modern.

Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan dengan cara:

Observasi Teknis

Mengamati langsung struktur komunikasi antara *client* dan server website melalui Wireshark (Nurcahyani et al., 2023).

Eksperimen / Uji Coba (Testing)

Melakukan percobaan *sniffing* dan scanning untuk melihat potensi kebocoran data (Arib et al., 2024).

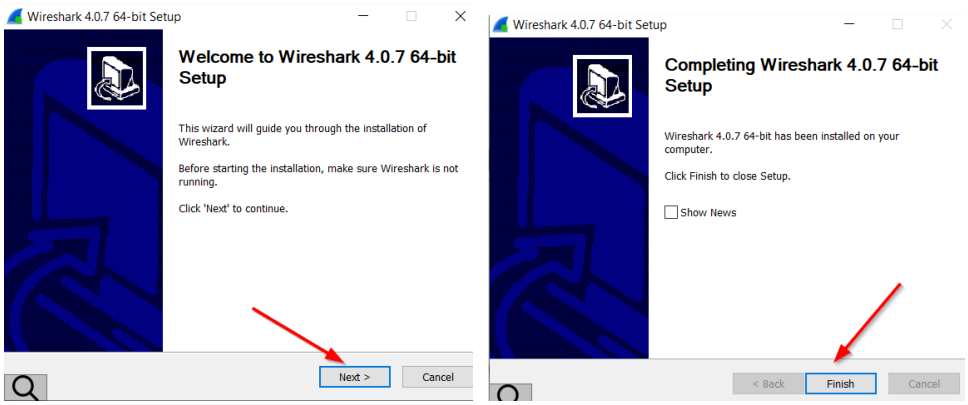
Dokumentasi

Merekam hasil uji berupa *screenshoot*, tangkapan paket, log Nmap, dan catatan konfigurasi (Hasan et al., 2022).

4. HASIL DAN PEMBAHASAN

Pembahasan pada bab ini akan memberikan hasil dari analisis penetrasi jaringan yang berhasil di *capture* dengan tujuan protokol http :

Tampilan Instalasi Wireshark



Gambar 1. Tahap Instalasi Wireshark

Pada tahap awal proses instalasi Wireshark, pengguna akan disambut dengan jendela bertajuk "Welcome to Wireshark 4.0.7 64-bit Setup". Pada layar ini terdapat informasi bahwa wizard akan memandu pengguna melalui seluruh proses instalasi Wireshark. Pengguna juga diingatkan untuk memastikan bahwa aplikasi Wireshark tidak sedang berjalan sebelum memulai instalasi.

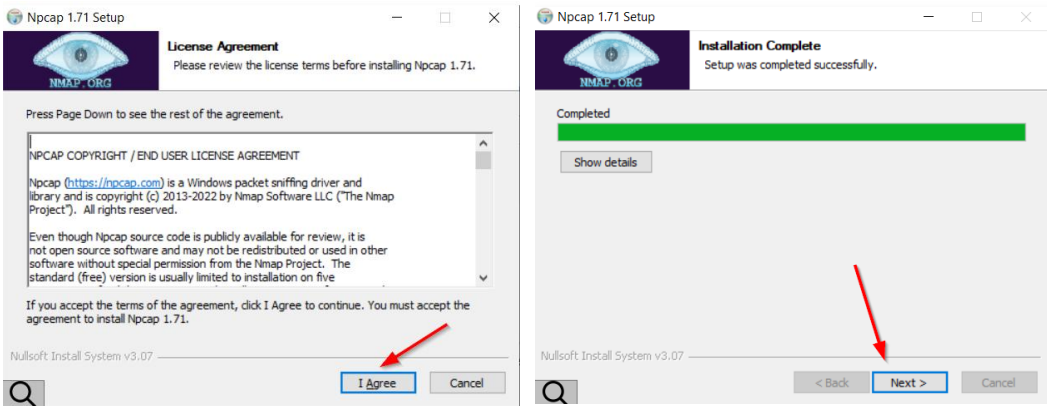
Di bagian bawah jendela, terdapat tiga tombol utama:

a. *Next* > – untuk melanjutkan proses instalasi (ditandai dengan panah pada gambar).

b. *Cancel* – untuk membatalkan proses instalasi.

Tahap ini berfungsi sebagai pengantar sebelum pengguna memasuki pengaturan instalasi berikutnya hingga *finish* instalasi.

Tampilan Instalasi NMAP.ORG

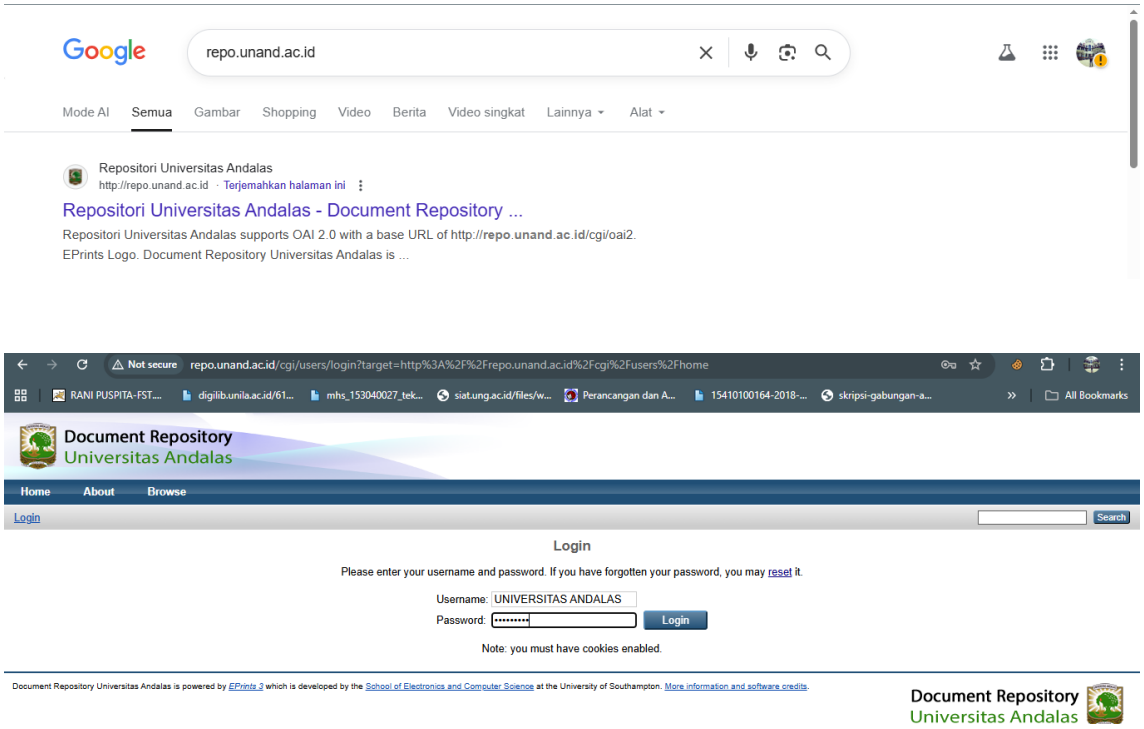


Gambar 2. Tahap instalasi NMAP

Pada tahap awal instalasi Npcap versi 1.71, pengguna ditampilkan jendela *License Agreement*. Jendela ini berisi informasi mengenai hak cipta serta ketentuan penggunaan perangkat lunak Npcap. Untuk melanjutkan proses instalasi, pengguna harus membaca dan menyetujui persyaratan lisensi yang ditampilkan. Setelah memahami isi lisensi, pengguna memilih tombol "*I Agree*" sebagai bentuk persetujuan terhadap ketentuan tersebut. Tanpa menyetujui lisensi, proses instalasi tidak dapat dilanjutkan.

Setelah proses instalasi selesai dijalankan oleh sistem, ditampilkan jendela dengan indikator *progress bar* berwarna hijau yang menunjukkan bahwa instalasi telah berhasil 100%. Pada jendela ini terdapat pesan *"Setup was completed successfully"* sebagai konfirmasi keberhasilan instalasi. Untuk melanjutkan ke tahap berikutnya, pengguna menekan tombol "*Next*".

Target Alamat Web untuk Penetrasi



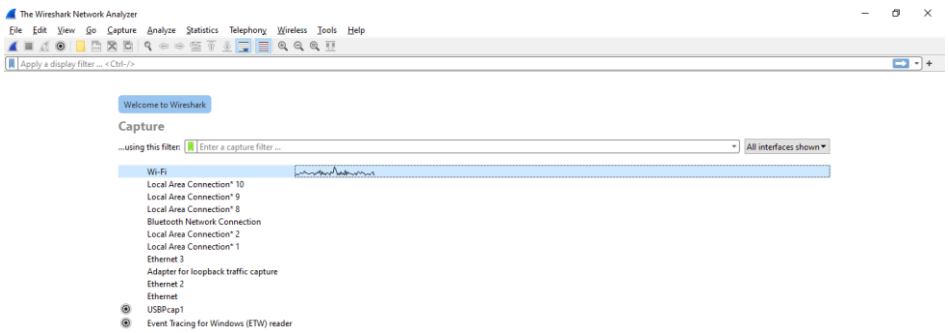
Gambar 3. Alamat Web untuk Uji Coba

Gambar tersebut menampilkan halaman *login Document* Repository Universitas Andalas yang diakses melalui antarmuka web. Pada halaman ini, pengguna diminta memasukkan *username* dan *password* untuk dapat mengakses sistem. Elemen-elemen yang tampak meliputi kolom *input* kredensial, tombol *Login*, serta tautan pemulihan kata sandi (*reset it*).

Dalam konteks pengujian keamanan protokol HTTP, halaman *login* seperti pada gambar ini menjadi salah satu titik krusial untuk dianalisis. Apabila halaman *login* diakses

menggunakan protokol HTTP tanpa enkripsi, maka data sensitif seperti *username* dan *password* yang dikirimkan melalui jaringan berpotensi disadap (*sniffing*) oleh pihak yang tidak berwenang.

Tampilan Awal Aplikasi Wireshark

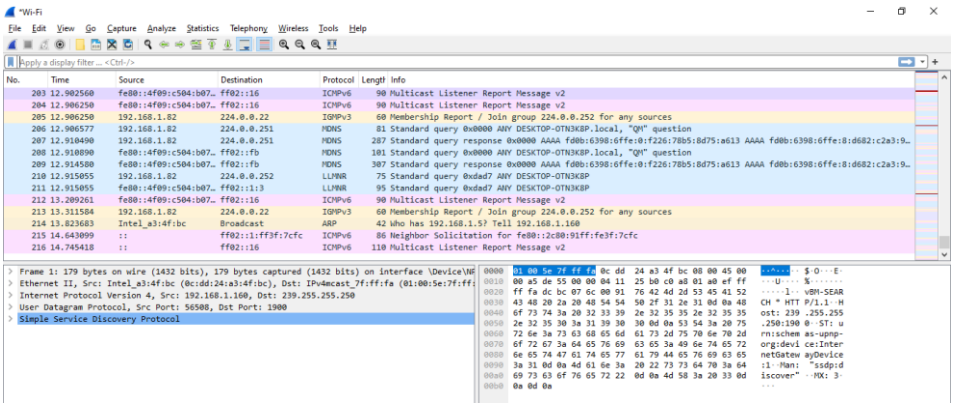


Gambar 4. Tampilan Awal Wireshark

Gambar tersebut menampilkan tampilan awal aplikasi Wireshark pada sistem operasi Windows. Pada bagian antarmuka terlihat menu utama di bagian atas yang terdiri dari *File*, *Edit*, *View*, *Capture*, *Analyze*, *Statistics*, *Telephony*, *Wireless*, *Tools*, dan *Help*. Di bawahnya terdapat panel *Capture* yang menyediakan daftar antarmuka jaringan (*network interfaces*) yang dapat digunakan untuk melakukan proses penangkapan paket.

Antarmuka-antarmuka tersebut ditampilkan lengkap dengan nama koneksi, seperti *Wi-Fi*, *Ethernet*, *Local Area Connection*, serta *USBPcap*. Wireshark juga menyediakan kolom untuk memasukkan *capture filter* sebelum proses penangkapan paket dimulai. Tampilan ini merupakan halaman awal yang ditampilkan aplikasi sebelum pengguna memilih antarmuka jaringan untuk memulai proses *packet capturing*, pada penelitian ini penulis memilih jaringan *wifi* untuk melakukan proses *capturing*.

Tampilan Proses Capturing



Gambar 5. Proses *Capturing*

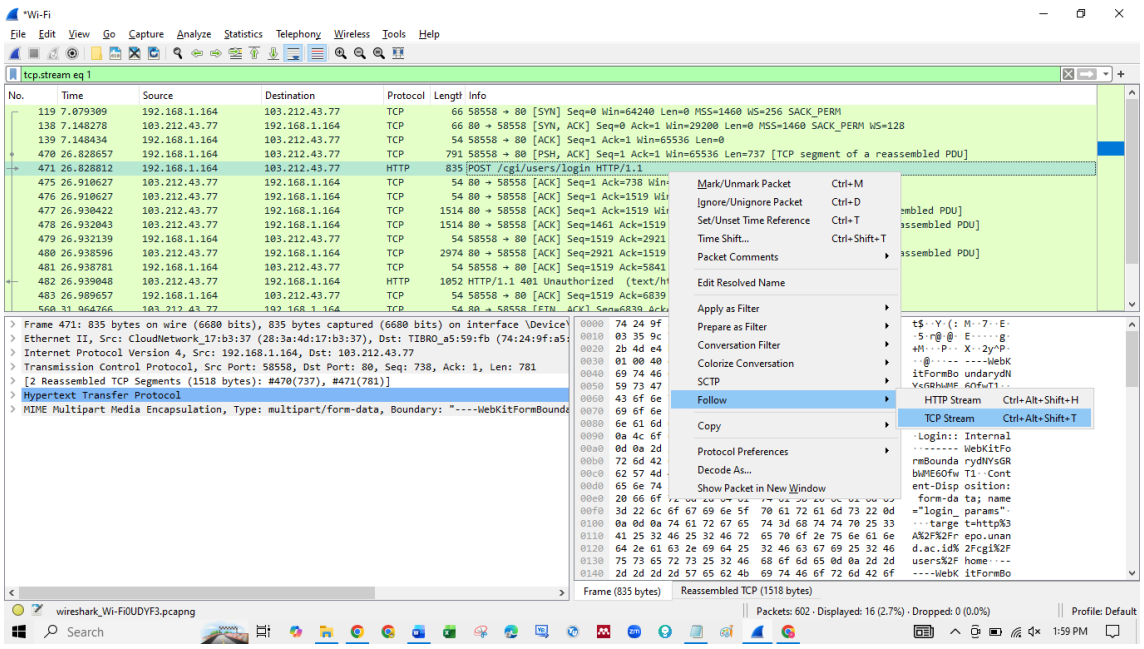
Gambar tersebut menunjukkan tampilan proses penangkapan paket (*packet capturing*) pada aplikasi Wireshark. Pada bagian utama jendela terlihat daftar paket yang sedang ditangkap

secara *real time*, ditampilkan dalam bentuk tabel dengan beberapa kolom seperti *No.*, *Time*, *Source*, *Destination*, *Protocol*, *Length*, dan *Info*. Setiap baris merepresentasikan satu paket data yang melewati antarmuka jaringan yang sedang dipantau.

Pada gambar tersebut dapat terlihat berbagai protokol jaringan yang terdeteksi, antara lain ICMPv6, IGMPv3, MDNS, LLMNR, ARP, dan Http. Informasi pada kolom *Source* dan *Destination* menampilkan alamat IP atau alamat perangkat yang melakukan komunikasi. Kolom *Info* memberikan ringkasan isi paket, seperti pesan *query*, *response*, atau *report* dari protokol terkait.

Di bagian bawah jendela, Wireshark menampilkan detail paket yang dipilih dalam bentuk struktur protokol berlapis, mencakup informasi *frame*, *Ethernet II*, *Internet Protocol*, serta *User Datagram Protocol*. Panel paling bawah menampilkan representasi data paket dalam format hexadecimal beserta translasi ke karakter ASCII, sehingga memudahkan analisis lebih mendalam terhadap isi paket. Tampilan ini memperlihatkan bagaimana Wireshark menguraikan paket jaringan secara rinci untuk kepentingan analisis lalu lintas data.

Tampilan Hasil Data Username dan Akun Pada protokol HTTP



Gambar 6. Hasil *Capture Packet* HTTP Akun Target Repository

Gambar tersebut menampilkan hasil tangkapan (*capture*) protokol HTTP pada aplikasi Wireshark. Pada bagian utama terlihat deretan paket yang ditampilkan dalam bentuk tabel dengan kolom *No.*, *Time*, *Source*, *Destination*, *Protocol*, *Length*, dan *Info*. Seluruh paket yang tampil merupakan komunikasi berbasis protokol TCP dan HTTP, yang menunjukkan terjadinya pertukaran data antara klien dan server.

Pada kolom *Info* terlihat salah satu paket penting yang menampilkan perintah "POST /*cgi*/*users*/*login* HTTP/1.1", yang mengindikasikan bahwa klien sedang melakukan permintaan *login* ke server melalui metode HTTP POST. Permintaan POST ini biasanya digunakan untuk mengirim data formulir, termasuk kredensial pengguna, sehingga proses ini penting dalam analisis keamanan jaringan.

Selain itu, tampak menu konteks (*right-click*) yang terbuka pada paket tersebut, dengan opsi *Follow* → TCP *Stream* yang digunakan untuk menelusuri alur komunikasi HTTP secara berurutan. Fitur ini memudahkan peneliti dalam melihat keseluruhan isi permintaan dan respons HTTP dari satu sesi komunikasi.

Gambar 7. *Username* dan *Password* Akun

Gambar tersebut menampilkan hasil tampilan fitur "*Follow* TCP *Stream*" pada aplikasi Wireshark, yang digunakan untuk menelusuri isi komunikasi HTTP secara utuh dalam satu alur percakapan (*stream*). Pada jendela ini terlihat dengan jelas permintaan HTTP (HTTP *Request*) dan respons dari server (HTTP *Response*) yang merupakan bagian dari proses autentikasi pada sebuah aplikasi web.

Pada bagian awal tampak header HTTP POST, seperti *User-Agent*, *Referer*, *Accept-Encoding*, serta *Content-Type* yang menunjukkan bahwa data yang dikirimkan merupakan formulir (*multipart/form-data*) dengan beberapa parameter. Selanjutnya ditampilkan isi *payload* yang berisi sejumlah field formulir, termasuk parameter yang merepresentasikan data kredensial *login*, seperti *username*, *password*, serta *action* yang menunjukkan bahwa pengguna sedang melakukan proses masuk (*login*) ke dalam sistem.

Isi kredensial yang tampil dalam data ini adalah contoh data autentikasi yang dikirimkan melalui metode POST, dan menunjukkan bahwa proses *login* tidak dilakukan melalui enkripsi *end-to-end*, sehingga dapat terlihat dalam bentuk teks biasa (*plaintext*) ketika

jaringan dipantau menggunakan Wireshark di mana *username* : UNIVERSITAS ANDALAS dan *password* : Admin repository.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian mengenai analisis keamanan pada situs Repository Universitas Andalas menggunakan *penetration testing* dengan metode *sniffing*, dapat disimpulkan beberapa hal. Pertama, situs Repository Universitas Andalas masih menggunakan protokol HTTP, yang menyebabkan proses transmisi data antara *client* dan server tidak dilindungi oleh mekanisme enkripsi. Hal ini menjadikan data yang dikirimkan rentan untuk disadap oleh pihak ketiga melalui serangan *sniffing*. Kedua, hasil pemindaian menggunakan Nmap menunjukkan bahwa layanan web yang digunakan berjalan pada *port* standar HTTP tanpa dukungan HTTPS. Kondisi ini semakin memperkuat indikasi bahwa komunikasi yang terjadi pada situs tersebut sangat rentan terhadap penyadapan, pengintaian, dan potensi *man-in-the-middle attack*. Ketiga, melalui proses *sniffing* menggunakan Wireshark, ditemukan bukti bahwa paket-paket data HTTP dapat ditangkap dan dibaca dalam bentuk *plaintext*. Informasi seperti *request*, *parameter form*, *cookie*, dan *metadata* komunikasi dapat diamati secara langsung, yang menunjukkan bahwa situs ini berpotensi membocorkan informasi penting apabila pengguna melakukan autentikasi atau pertukaran data sensitif. Keempat, hasil analisis keseluruhan menunjukkan bahwa tingkat keamanan situs Repository Universitas Andalas belum memenuhi standar keamanan web modern, karena tidak menerapkan enkripsi SSL/TLS sebagai langkah dasar perlindungan data. Kondisi ini menambah potensi risiko kebocoran informasi, penyalahgunaan akses, dan ancaman keamanan lainnya. Kelima, penelitian ini mengonfirmasi adanya gap antara kebutuhan keamanan dan implementasi yang diterapkan pada situs tersebut. Oleh karena itu, penerapan teknologi keamanan seperti HTTPS, konfigurasi *hardening server*, serta pemantauan aktivitas jaringan sangat diperlukan untuk mengurangi risiko serangan *sniffing* dan serangan siber lainnya.

Berdasarkan hasil penelitian yang telah dilakukan, beberapa saran yang dapat diberikan adalah sebagai berikut. Pertama, pihak pengelola disarankan untuk segera mengaktifkan sertifikat SSL/TLS agar seluruh komunikasi data terenkripsi dan tidak dapat dibaca melalui *sniffing*. Kedua, melakukan *hardening* pada server web dengan pembaruan layanan, pengaturan *header* keamanan seperti HSTS, *X-Frame-Options*, dan *X-Content-Type-Options*, serta konfigurasi *firewall* untuk mencegah potensi eksploitasi. Ketiga, pengujian penetrasi (*penetration testing*) sebaiknya dilakukan secara rutin untuk memastikan bahwa website tetap aman dari ancaman serangan baru yang terus berkembang. Keempat, penerapan sistem deteksi

intrusi (IDS) dan pencegahan intrusi (IPS) dapat membantu mendeteksi aktivitas mencurigakan pada jaringan. Terakhir, pengelola sistem perlu memberikan pelatihan kepada administrator dan pengguna mengenai pentingnya keamanan data, pola ancaman, dan praktik penggunaan sistem yang aman.

DAFTAR REFERENSI

Arib, M. F., Rahayu, M. S., Sidorj, R. A., & Afgani, M. W. (2024). Experimental research dalam penelitian pendidikan. *Journal Of Social Science Research*, *4*, 5497–5511.

Fachri, F., Fadlil, A., Riadi, I., Studi, P., Elektro, T., & Dahlan, U. A. (2021). Analisis keamanan webserver menggunakan penetration test. *JURNAL INFORMATIKA*, *8*(2), 183–190.

Hae, Y., & Sulistyo, W. (2021). Analisis keamanan jaringan pada web dari serangan *sniffing* dengan metode eksperimen. *Jurnal Teknik Informatika Dan Sistem Informasi*, *8*(4), 2095–2105.

Haq, M. S. (2025). Analisis keamanan jaringan nirkabel dari packet *sniffing* pada kantor dinas penanaman modal dan pelayanan terpadu satu pintu Kota Palopo. *Jurnal Ilmu Komputer*, *1*(2).

Hasan, H., Informasi, S., Vidio, D., & Pendahuluan, I. (2022). Pengembangan sistem informasi dokumentasi terpusat pada stmik tidore mandiri. *Jurnal Sistem Informasi Dan Komputer*, *2*(1), 23–29.

Irfan, A., Nusri, A. Z., Rachmat, Z., & Wulandari, S. (2024). Analisis keamanan jaringan nirkabel menggunakan Wireless Intrusion Detection System (WIDS). *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika*, *7*(April), 110–119.

Khasanah, M., & Putri, A. M. (2021). Penguatan literasi, numerasi, dan adaptasi teknologi pada pembelajaran di sekolah. *Jurnal Eksponen*, *11*(2), 1–11.

Munawar, Z., Putri, N. I., Widhiantoro, D., Informatika, M., Informasi, S., Kebangsaan, U., Indonesia, R., Informatika, T., Bandung, U. N., Informatika, T. E., & Jakarta, P. N. (2023). Analisis keamanan pada teknologi blockchain. *Jurnal Infotronik Volume*, *8*(2), 67–79. https://doi.org/10.32897/infotronik.2023.8.2.2062

Nurcahyani, D., Sari, S. N., & Hermawan, A. (2023). Analisis perbandingan biaya pembangunan rumah konvensional 1 lantai tipe 40 menggunakan ahsp 2016 dan AHSP 2022 (Studi Kasus : Rumah di Triharjo, Kabupaten Sleman). *Jurnal Ilmiah Teknik Unida*, *4*(1), 191–202. https://doi.org/10.55616/jitu.v4i1.577

Pratikno, R. S. (2025). Kajian literatur analisis keamanan jaringan. *Jurnal Ilmiah Pendidikan Dasar*, *20*(2), 250–258.

Rahma, M., Yulis, E., Pratiwi, N., Susanto, R., & Syofyan, H. (2021). Pemanfaatan teknologi informasi dan komunikasi untuk mengembangkan kompetensi pedagogik guru. *Eduscience: Jurnal Ilmu Pendidikan*, *6*(2), 97–105. https://digilib.esaunggul.ac.id/public/UEU-Journal-19913-11_1192.pdf

Rahman, R., Hartono, A. K., & Tanduklangi, E. (2025). Serangan dan deteksi port scanning menggunakan wireshark dan snort. *JURNAL ILMIAH MULTI DISIPLIN*, *1*(4), 2138–2144.

Santoso, N. A., Affandi, K. B., & Kurniawan, R. D. (2022). Implementasi keamanan jaringan menggunakan port knocking network security implementation using port knocking. *Jurnal Janitra Informatika Dan Sistem Informasi*, *2*(2), 90–95. https://doi.org/10.25008/janitra.v2i2.156

Silmina, E. P., Firdonsyah, A., Adhella, R., & Amanda, A. (2022). Menggunakan penetration test dan issaf. *Jurnal ilmiah teknik elektro*, *2*(3), 83–91.

Syahputra, G., Erdiansyah, U., & Hidayat, H. T. (2024). Rancang bangun nas server di lingkungan jurusan tik pnl dalam upaya mengurangi ketergantungan terhadap jaringan internet. *Nasional Politeknik Negeri Lhokseumawe*, *7*(1), 49–52.