ANALISIS KEAMANAN SISTEM INFORMASI ABSENSI BKAD KANTOR WALIKOTA MEDAN

M. Arfan Drizal, Faizin Ridho
Informatika, Politeknik Ganesha Medan
arfandrizal2003@gmail.com

Abstrak

Perkembangan teknologi informasi mendorong digitalisasi sistem absensi di instansi pemerintah, termasuk BKAD Kota Medan. Meskipun sistem berbasis web menawarkan efisiensi, ia juga menghadapi ancaman keamanan yang dapat merusak integritas data pegawai. Sistem absensi online sering mengalami masalah seperti lemahnya mekanisme otentikasi, kurangnya enkripsi data, dan kerentanan terhadap serangan seperti man-in-the-middle. Celah ini dapat dimanfaatkan untuk manipulasi data dan pencurian informasi pribadi. Penelitian ini bertujuan untuk menganalisis tingkat keamanan sistem informasi absensi BKAD Kota Medan, mengevaluasi risiko yang ada, dan memberikan rekomendasi perbaikan untuk meningkatkan keamanan sistem. Metode yang digunakan adalah penetration testing dengan teknik sniffing menggunakan aplikasi Wireshark untuk menganalisis kerentanan dalam sistem. Hasil analisis menunjukkan bahwa sistem memiliki kerentanan signifikan, terutama pada protokol HTTP. Informasi sensitif seperti username dan password dapat diakses dengan mudah. Penggunaan HTTPS meningkatkan keamanan tetapi masih ada risiko kebocoran informasi.

Kata kunci: *Keamanan, Sistem Informasi, Absensi, Penetration Testing, Sniffing, Wireshark*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong digitalisasi sistem absensi di berbagai instansi pemerintah, termasuk Badan Keuangan dan Aset Daerah (BKAD) Kota Medan. Sistem informasi absensi berbasis web memungkinkan pencatatan kehadiran pegawai secara lebih efisien dan akurat. Namun, sistem online juga membuka peluang terjadinya berbagai ancaman keamanan yang dapat membahayakan integritas dan kerahasiaan data pegawai [1].

Beberapa permasalahan keamanan yang umum ditemui pada sistem absensi online antara lain lemahnya mekanisme otentikasi, kurangnya enkripsi data, serta kerentanan terhadap serangan man-in-the-middle [2]. Celah keamanan tersebut dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk memanipulasi data absensi, mencuri informasi pribadi pegawai, atau bahkan melumpuhkan sistem.

Oleh karena itu, analisis keamanan terhadap sistem informasi absensi perlu dilakukan secara berkala untuk mengidentifikasi potensi kerentanan dan melakukan langkah-langkah mitigasi yang diperlukan [3]. Penelitian ini bertujuan untuk menganalisis tingkat keamanan sistem informasi absensi BKAD Kota Medan saat ini, mengevaluasi risiko keamanan yang dihadapi, serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan sistem.

2. TINJAUAN PUSTAKA

Penelitian ini menggunakan metode penetration testing dengan teknik sniffing untuk menganalisis keamanan sistem informasi absensi BKAD Kota Medan. Penetration testing merupakan metode pengujian keamanan sistem dengan cara mensimulasikan serangan yang mungkin dilakukan oleh pihak yang tidak berwenang [4].

2.1. Sistem Informasi

Sistem yang menggabungkan pengolahan transaksi harian dengan operasi manajerial dan strategis untuk memberikan laporan yang diperlukan kepada pihak eksternal dikenal sebagai sistem informasi organisasi [5]. Dalam konteks bisnis, sistem informasi adalah solusi organisasi dan manajemen berbasis teknologi informasi untuk tantangan yang ditimbulkan oleh lingkungan bisnis.
Sistem informasi terdiri dari lima komponen utama:

a. Hardware: Perangkat fisik seperti komputer, server, dan perangkat jaringan.
b. Software: Program dan aplikasi yang menjalankan sistem.
c. Data: Informasi yang dikumpulkan, diproses, dan disimpan oleh sistem.
d. Prosedur: Instruksi dan proses yang menentukan bagaimana data diproses dan digunakan.
e. People: Pengguna dan administrator yang berinteraksi dengan sistem.

Sistem informasi memainkan peran krusial dalam operasi organisasi modern, memungkinkan pengambilan keputusan yang lebih baik, meningkatkan efisiensi, dan memberikan keunggulan kompetitif.

2.2. Keamanan Sistem

Keamanan Sistem adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik [6]. Beberapa aspek penting dari keamanan sistem meliputi:

a. Autentikasi: Memverifikasi identitas pengguna atau sistem.
b. Otorisasi: Menentukan hak akses pengguna yang terautentikasi.
c. Enkripsi: Mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi.
d. Firewall: Memantau dan mengontrol lalu lintas jaringan berdasarkan aturan keamanan.
e. Deteksi dan Pencegahan Intrusi: Mengidentifikasi dan merespons aktivitas mencurigous dalam jaringan.
f. Patch Management: Memperbarui sistem dan aplikasi untuk mengatasi kerentanan yang baru ditemukan.

Keamanan sistem bukan hanya tentang mencegah penipuan, tetapi juga melibatkan deteksi cepat, respons terhadap insiden, dan pemulihan dari serangan. Ini adalah proses berkelanjutan yang memerlukan pemantauan konstan dan penyesuaian terhadap ancaman yang berkembang.

2.3. Absensi

Absensi dapat dikatakan suatu pendataan kehadiran yang merupakan bagian dari aktifitas pelaporan yang ada dalam sebuah institusi [7]. Ini bukan hanya sekadar pendataan, tetapi juga merupakan komponen penting dari manajemen sumber daya manusia dan operasional organisasi.
Sistem absensi modern sering menggunakan teknologi seperti:

a. Biometrik (sidik jari, pengenalan wajah, pemindaian retina)
b. Aplikasi mobile dengan geo-tagging
c. Sistem berbasis web

Manfaat sistem absensi yang efektif meliputi:

a. Peningkatan akurasi pencatatan kehadiran
b. Efisiensi dalam pengelolaan sumber daya manusia
c. Dasar untuk perhitungan gaji dan tunjangan
d. Analisis pola kehadiran untuk meningkatkan produktivitas
e. Kepatuhan terhadap regulasi ketenagakerjaan

Dalam konteks digital, sistem absensi sering terintegrasi dengan sistem informasi manajemen yang lebih luas, memungkinkan analisis real-time dan pengambilan keputusan berbasis data.

2.4. *Confidentiality, Integrity, Availability* (CIA) *Triad*

Confidentiality, Integrity, Availability (CIA) *Triad* Kerahasiaan, Integritas, dan Ketersediaan (CIA) adalah tiga sifat penting dari data, yang sering disebut sebagai triad CIA. Triad CIA dapat sangat berpengaruh pada bisnis komputerisasi. Ini karena data dapat dianggap sebagai bagian penting dari berbagai jenis bisnis. Data harus aman karena data digital tidak dapat rusak dan hanya dapat diakses oleh orang yang berwenang atasnya. Oleh karena itu, integritas data dapat didefinisikan sebagai keharusan untuk menjaga keakuratan, konsistensi, dan kepercayaan sistem informasi [8].

2.5. *Wireshark*

Menurut Huzaenia, *Wireshark* adalah aplikasi yang dirancang untuk menganalisis paket data jaringan yang sedang berlangsung. Dia juga disebut sebagai *network packet analyzer*, dan dapat menangkap dan menampilkan semua detail paket [9]. Fitur utamanya meliputi:

a. *Packet Capture*: Merekam lalu lintas jaringan secara real-time.
b. *Deep Packet Inspection*: Menganalisis isi paket data secara detail.
c. *Protocol Analysis*: Mendukung berbagai protokol jaringan.
d. *Filtering*: Memungkinkan pencarian dan penyaringan paket spesifik.
e. *Visualisasi*: Menyajikan data dalam format yang mudah dibaca.

Wireshark digunakan untuk berbagai tujuan, termasuk:

a. Troubleshooting masalah jaringan
b. Analisis keamanan dan deteksi intrusi
c. Pengembangan aplikasi jaringan
d. Pembelajaran dan penelitian protokol jaringan

Meskipun powerful, penggunaan Wireshark harus dilakukan dengan tanggung jawab dan etis, karena dapat mengakses informasi sensitif dalam jaringan.

2.6. Encryption

Enkripsi (*encryption*) yaitu proses merubah data asli (*plaintext*) menjadi data samaran (*chipertext*) dan dekripsi (*decryption*) yaitu proses pengembalian chipertext menjadi *plaintext* kembali [10]. Komponen utama enkripsi meliputi:

a. *Plaintext*: Data asli sebelum dienkripsi.
b. *Ciphertext*: Data yang telah dienkripsi.
c. *Encryption Algorithm*: Metode untuk mengubah plaintext menjadi ciphertext.
d. *Decryption Algorithm*: Metode untuk mengembalikan ciphertext menjadi plaintext.
e. *Key*: Informasi rahasia yang digunakan dalam proses enkripsi dan dekripsi.

Jenis-jenis enkripsi utama:

a. *Symmetric Encryption*: Menggunakan kunci yang sama untuk enkripsi dan dekripsi.
   Contoh: AES, DES
b. *Asymmetric Encryption*: Menggunakan pasangan kunci publik dan privat.
   Contoh: RSA, ECC
c. *Hashing*: Mengubah data menjadi nilai tetap yang tidak dapat dibalik.
   Contoh: SHA-256, MD5 (tidak direkomendasikan untuk keamanan)

Enkripsi sangat penting dalam menjaga kerahasiaan data, terutama dalam komunikasi online, penyimpanan data sensitif, dan transaksi keuangan.

2.7. Audit

Pengumpulan dan evaluasi buku informasi dikenal sebagai audit. Tujuan audit adalah untuk menentukan dan melaporkan tingkat kesesuaian antara informasi dan standar yang telah ditetapkan. Audit adalah serangkaian pemeriksaan yang menyeluruh terhadap laporan keuangan, pengawasan intern, dan catatan akuntansi perusahaan [11]. Audit dalam konteks sistem informasi adalah proses sistematis untuk mengevaluasi dan memverifikasi kepatuhan sistem terhadap kebijakan, prosedur, dan regulasi yang berlaku. Komponen utama audit meliputi:

a. Audit Keamanan: Menilai efektivitas kontrol keamanan sistem.
b. Audit Kinerja: Mengevaluasi efisiensi dan efektivitas sistem.
c. Audit Kepatuhan: Memastikan sistem memenuhi standar industri dan regulasi.
d. Audit Keuangan : Menilai aspek keuangan dari investasi dan operasi .

Proses audit biasanya melibatkan:

a. Perencanaan audit
b. Pengumpulan bukti
c. Analisis data
d. Pelaporan temuan
e. Rekomendasi perbaikan
f. Follow-up dan implementasi

Audit penting untuk memastikan integritas, keandalan, dan keamanan sistem informasi organisasi, serta untuk mengidentifikasi area yang memerlukan perbaikan.

2.8. Pentest

Penetration testing adalah metode untuk menguji kerentanan dalam sistem, identifikasi konfigurasi sistem yang buruk, kecacatan perangkat keras dan perangkat lunak serta kelemahan teknis pada sistem informasi yang diujikan [12]. Tahapan umum dalam pentest meliputi:

a. Perencanaan dan Persiapan: Menentukan ruang lingkup dan tujuan pengujian.
b. Pengumpulan Informasi: Mengumpulkan data tentang target (reconnaissance).
c. Identifikasi Kerentanan: Menganalisis sistem untuk menemukan potensi kelemahan.
d. Eksploitasi: Mencoba memanfaatkan kerentanan yang ditemukan.
e. Post-Exploitation: Menilai potensi dampak jika serangan berhasil.
f. Analisis dan Pelaporan: Mendokumentasikan temuan dan rekomendasi.

Jenis-jenis pentest:

a. *Black Box Testing*: Tester tidak memiliki pengetahuan internal tentang sistem.
b. *White Box Testing*: Tester memiliki akses penuh ke informasi sistem.
c. *Gray Box Testing*: Kombinasi dari black box dan white box.

Pentest membantu organisasi mengidentifikasi dan memperbaiki kelemahan keamanan sebelum dapat dieksploitasi oleh penyerang yang sebenarnya.

2.9. HTTP dan HTTPS

Protokol jaringan aplikasi *Hypertext Transfer Protocol* (HTTP) digunakan untuk mengirimkan informasi antara komputer server dan komputer client. Server yang dimaksud di sini adalah jenis web server yang terletak di jaringan komputer yang besar. Sementara client adalah web browser yang memiliki kemampuan untuk mengakses, menerima, dan menampilkan konten melalui browser, *Hypertext Transfer Protocol Secure* (*HTTPS*) adalah pengembangan dari versi sebelumnya dari *HTTP*. *HTTPS* memiliki tingkat keamanan yang lebih tinggi daripada *HTTP*, sehingga membuat klien merasa lebih aman saat mengakses konten web [13].

3. METODE PENELITIAN

3.1. Pengumpulan *Data*

Penelitian ini digunakan dengan Simulasi menggunakan metode Snifing dengan aplikasi Wireshark.Teknik pengumpulan data pada penelitian ini adalah sebagai berikut :

3.2. Observasi

Metode pengumpulan data dalam penelitian ini adalah dengan melihat melalui media internet untuk mencari informasi yang cukup untuk bahan penelitian..

3.3. Studi Pustaka

Teknik pengumpulan data studi literatur berupa jurnal, karya ilmiah, dan studi pustaka lainnya digunakan sebagai penunjang keilmuan untuk penelitian ini. Dengan mencari studi kasus yang serupa yang bisa dijadikan sebagai acuan pada penelitian ini.

3.4. Penyerangan

Pada titik ini, penulis akan mencoba melakukan penyerangan Sniffing Attack. Mereka menggunakan metode Pentest, yang merupakan kegiatan pengujian keamanan software. Ada tahapan uji kerentanan perangkat lunak yang harus dilakukan saat melakukan pengujian keamanan software. Oleh karena itu, uji dapat diorganisir dengan baik.

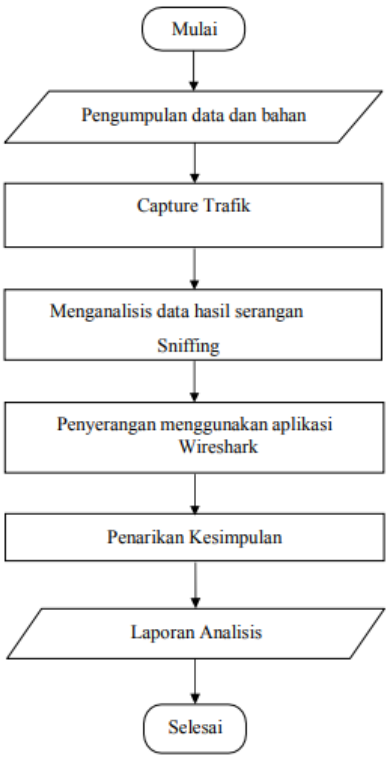
3.5. Penarikan Kesimpulan

Dalam tahap ini penulis akan melakukan analisis hasil dan mengambil kesimpulan dari hasil penyerangan tersebut.

3.6. *Sniffing*

Sniffing sering digunakan oleh hacker untuk mendapatkan informasi sensitive seperti username dan password yang dikirimkan melalui jaringan. Sniffing pada sistem absensi adalah aktivitas menyadap lalu lintas data absensi karyawan tanpa izin dan sepengetahuan korban. Umumnya dilakukan

dengan tujuan mencuri data absensi untuk kepentingan tertentu. Metode tersebut terdapat pada Gambar 1. Teknik *Sniffing*



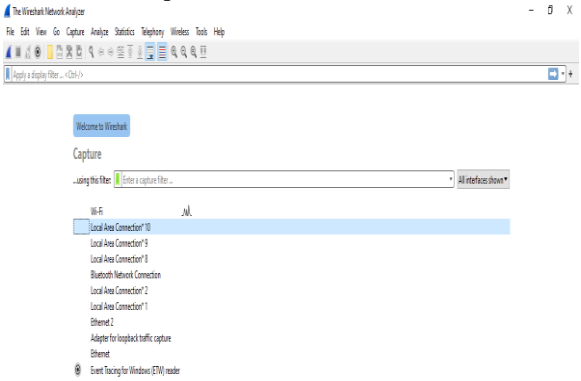
Gambar 1. *Snifiing*

a. Proses sniffing dimulai saat sniffer diaktifkan. Sniffer dapat berupa program perangkat keras atau perangkat lunak.
b. Mengumpulkan dan mempelajari literatur, buku-buku, *ebook* dan artikel untuk menunjang penelitian.
c. Sniffer menangkap semua lalu lintas jaringan yang melewati antar mukanya. Hal ini dapat dilakukan pada mode promiscuous yang artinya sniffer menangkap semua trafik, atau pada mode terfilter yang artinya sniffer hanya menangkap trafik yang memenuhi kriteria tertentu.
d. Sniffer menganalisis paket yang didekodekan. Hal ini dapat melibatkan pencarian pola atau kata kunci tertentu dalam muatan data, atau penghitungan statistik tentang lalu lintas.
e. Sniffer dapat mencatat paket yang dianalisis ke file atau database. Ini dapat digunakan untuk analisis atau pemecahan masalah nanti.
f. Menarik kesimpulan untuk memutuskan sebuah saran yang bisa digunakan untuk mengamankan *website* terhadap proses *sniffing* melihat dari sisi pengguna.

4. HASIL DAN PEMBAHASAN

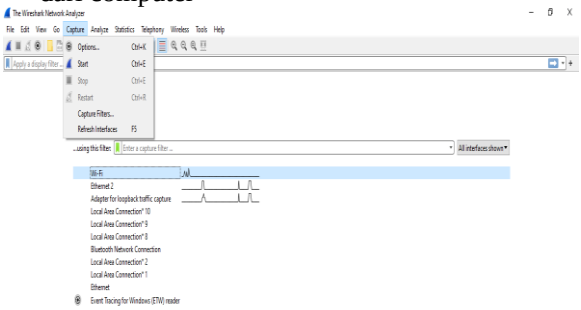
Hasil analisis keamanan data pada website dengan wireshark, pertama akan melakukan analisis dengan website yang menggunakan http untuk melakukan sniffing menggunakan wireshark agar mendapatkan username dan password, Dengan melakukan beberapa langkah dibawah ini :

1. Jalankan Aplikasi Wireshark



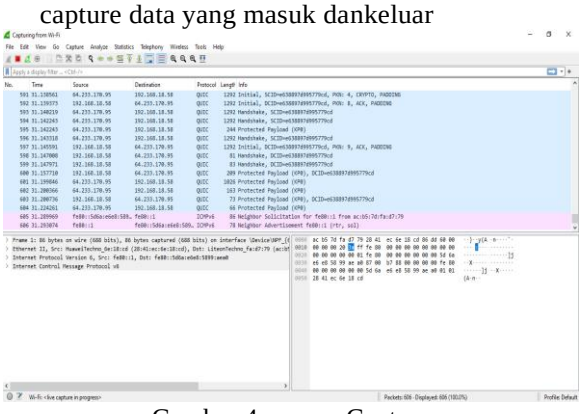
Gambar 2. Tampilan Wireshark

2. Kemudian pilih wifi sebagai interfacenya dan klik capture dan pilih start untuk memulai perekaman data internet yang masuk dan keluar dari computer



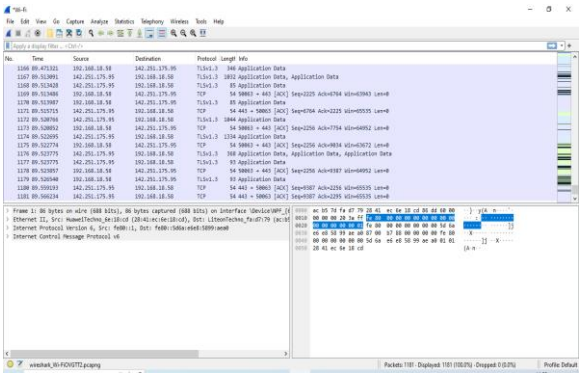
Gambar 3. Capture

3. Setelah itu Wireshark akan melakukan proses capture data yang masuk dankeluar



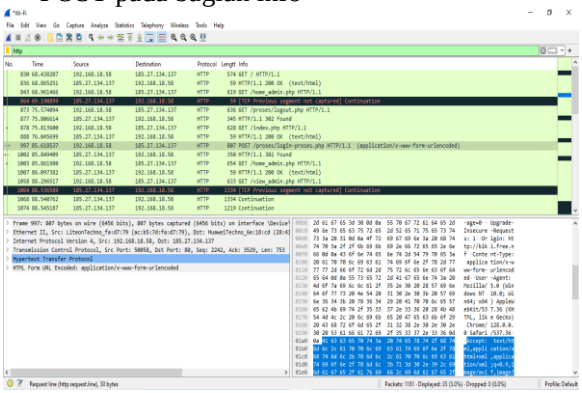
Gambar 4. proses Capture

4. Selanjutnya buka websitenya dan masukan username dan password dalam websitenya.
5. Kembali ke wireshark dan stop capture yang sedang berjalan



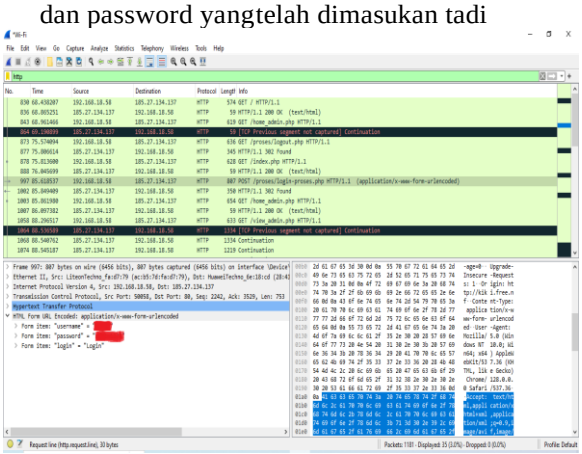
Gambar 5. stop capture

6. Ketikan perintah HTTP pada filter dan pilih POST pada bagian info



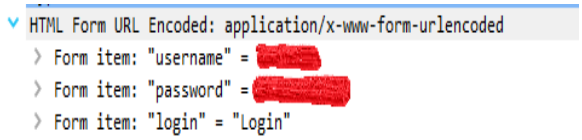
Gambar 6. filter http

7. Pada data POST terdapat informasi seperti alamat IP192.168.18.58 source dan 185.27.134.137 destination, kemudian didalam HTTP terdapat berbagai informasi kemudian pilih HTML form untuk mengetahui username dan password yangtelah dimasukan tadi



Gambar 7. HTML form

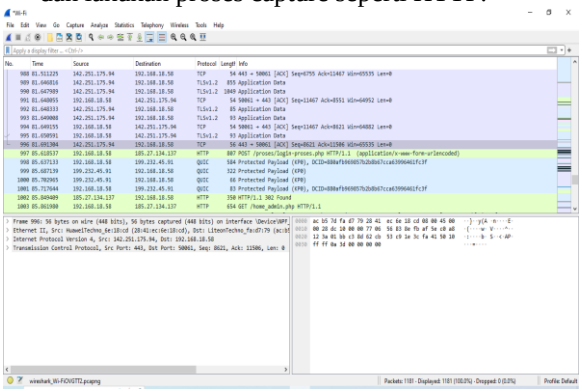
1. Sniffing username dan password menggunakan Wireshark berhasil. Dengan hasil capture yang di analisa melalui jaringan pada jaringan terpilih bisa diketahui username dan password pada paket data POST.



Gambar 8. username dan password

Setelah melakukan snifing pada HTTP selanjutnya kita menggunakan HTTPS, untuk perintahnya seperti dibawah ini :

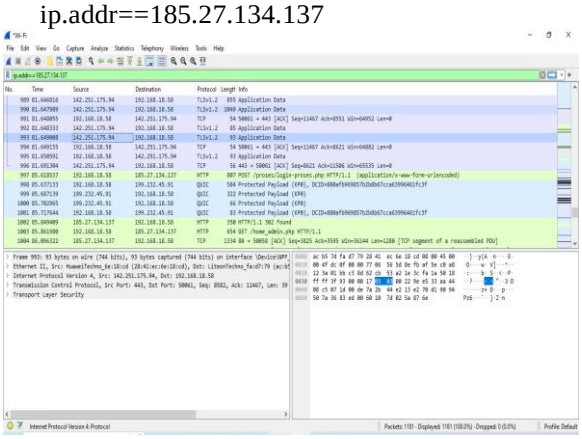
2. Buka wireshark dan akan muncul jendela sotware wireshark, kemudian sambungkan dengan wifi dan lakukan proses capture seperti HTTP.



Gambar 9. Jendela Wireshark

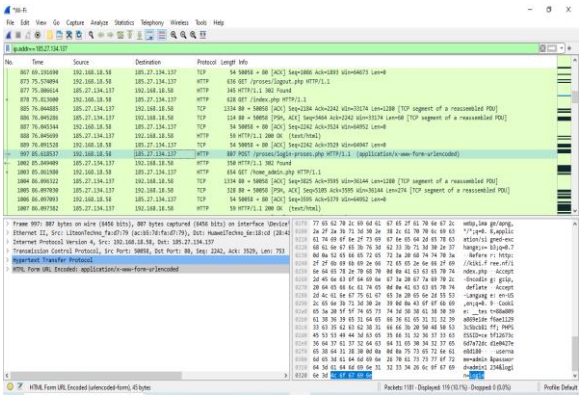
3. Kemudian untuk mengecek website yang diakses lakukan ping pada command prompt untuk mengetahui Ip websitenya.

4. Setelah melakukan ping websitenya dan didapati ipnya yaitu 185.27.134.137, Selanjutnya cari dengan software Wireshark pada bagian filter tulis ip.addr==185.27.134.137



Gambar 10. Mencari Ip

5. Maka akan terlihat ip dari website pada software wireshark.



Gambar 11. Analisis Paket

4.1 Hasil Analisis

Tabel 1. Hasil Analisis

Aspek	Hasil Analisis	Metode	Implikasi Keamanan
Analisis HTTP	Username dan password berhasil didapatkan melalui sniffing	Wireshark, filter HTTP POST	Koneksi HTTP sangat rentan terhadap serangan sniffing
Analisis HTTPS	Alamat IP website terlihat, namun konten terenkripsi	Wireshark, ping, filter IP	HTTPS meningkatkan keamanan, tapi beberapa informasi masih dapat diakses
Kerentanan Sistem	Protokol HTTP memungkinkan akses mudah ke informasi sensitif	Penetration testing dengan teknik sniffing	Risiko tinggi terhadap kerahasiaan data pegawai
Perbedaan HTTP vs HTTPS	HTTP : data terbaca jelas HTTPS : data terenkripsi	Perbandingan hasil sniffing pada HTTP dan HTTPS	HTTPS memberikan lapisan keamanan tambahan yang signifikan
Informasi yang Terekspos (HTTP)	1. User Login ID 2. Password 3. Alamat IP sumber dan tujuan	Analisis paket data POST	Potensi penyalahgunaan akun dan serangan terhadap sistem
Informasi yang Terekspos (HTTPS)	Alamat IP website	Ping dan filter Wireshark	Risiko lebih rendah, namun masih ada potensi serangan berbasis IP
Rekomendasi Keamanan	1. Peningkatan kontrol autentikasi 2. Penerapan enkripsi data yang lebih kuat 3. Implementasi audit log 4. Penerapan kebijakan privasi ketat	Analisis hasil dan best practices keamanan	Peningkatan keamanan sistem secara menyeluruh
Implikasi untuk BKAD Kota Medan	Kebutuhan mendesak untuk meningkatkan keamanan sistem absensi	Evaluasi hasil penetration testing	Perlunya investasi dalam keamanan sistem untuk melindungi data pegawai

5. KESIMPULAN

Berdasarkan penelitian yang dilakukan, dapat disimpulkan bahwa sistem informasi absensi berbasis web di BKAD Kota Medan memiliki kerentanan keamanan yang signifikan, terutama ketika menggunakan protokol *HTTP*. Analisis menggunakan metode penetration testing dengan teknik sniffing melalui aplikasi Wireshark menunjukkan bahwa informasi sensitif seperti username dan password dapat dengan mudah diakses pada koneksi *HTTP*. Meskipun penggunaan *HTTPS* meningkatkan keamanan, masih ada potensi kebocoran informasi seperti alamat IP. Untuk meningkatkan keamanan sistem, direkomendasikan beberapa langkah perbaikan, antara lain: meningkatkan kontrol autentikasi pengguna, menerapkan enkripsi data yang lebih kuat, implementasi audit log untuk pemantauan aktivitas, serta penerapan kebijakan privasi yang ketat untuk data absensi. Dengan menerapkan langkah-langkah keamanan yang komprehensif, diharapkan sistem informasi absensi BKAD dapat memberikan layanan yang andal, terpercaya, serta menjaga kerahasiaan dan integritas data pegawai.

DAFTAR PUSTAKA

[1] A. Lubis and A. P. U. Siahaan, "Network Forensics Application in General Cases," IOSR J. Comput. Eng., vol. 18, no. 6, pp. 41–44, 2016.

[2] R. M. Ijtihadie, B. C. Hidayanto, A. Affandi, Y. Chisaki, and T. Usagawa, "Dynamic content synchronization between learning management systems over limited bandwidth network," Human-centric Comput. Inf. Sci., vol. 2, no. 1, p. 17, 2012.

[3] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," Int. J. Electr. Comput. Eng., vol. 8, no. 5, p. 3991, 2018.

[4] M. Denis, C. Zena, and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," in 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2016, pp. 1–6

[5] Zebua, "Bab II Landasan Teori," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 8–24, 2017.

[6] G. J. Simons, "Faktor-Faktor Yang Mempengaruhi Etika Sistem Informasi: Moral, Isu Sosial Dan Etika Masyarakat (Literature Review Sim)," *J. Manaj. Pendidik. Dan Ilmu Sos.*, vol. 3, no. 2, pp. 520–529, 2018, doi: 10.38035/jmpis.v3i2.1115.

[7] E. B. and K. B. Setiawan, "Sistem Informasi Absensi Pegawai Menggunakan Metode RAD dan Metode LBS Pada Koordinat Absensi," *J. Media Inform. Budidarma*, vol. 4, no. 1, p. 59, 2015, doi: 10.30865/mib.v4i1.1445.

[8] K. et Al, "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder," *J. Manaj. dan Pemasar. Digit.*, vol. 1, no. 2, pp. 73–83, 2018.

[9] F. Huzaenia, "Analisis Keamanan Data Pada Website Dengan Wireshark," *JES (Jurnal Elektro Smart)*, 2021.

[10] A. I. Auliyah, "Aplikasi Enkripsi Gambar Menggunakan Metode (Rivest Shamir Adleman) Rsa," *J. Sintaks Log.*, vol. 2, no. 3, pp. 39–45, 2020, doi: 10.31850/jsilog.v2i3.1850.

[11] A. et Al., "Bab ii kajian pustaka bab ii kajian pustaka 2.1.," *Bab Ii Kaji. Pustaka 2.1*, vol. 12, no. 2004, pp. 6–25, 2015.

[12] and A. C. M. Z. Hussain, M. Z. Hasan, M. Taimoor, A. Chughtai, M. Taimoor, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 2, p. 113, 2017, doi: 10.24843/jim.2020.v08.i02.p05.

[13] D. Intern , "Apa Perbedaan HTTP dan HTTPS? Lengkap Beserta Penjelasannya," 2020. [Online]