Buletin Ilmiah
Ilmu Komputer dan Multimedia

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 2, No. 4, November Tahun 2024
ISSN 3024-8248 (media online)
Hal 735-738

HTTPS Dibandingkan HTTP dalam Pengambilan Data Login Melalui Metode "*Packet Sniffing*"

Lusius Dian Margareta[1], Munaldi[2*]

[1,2]Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1]dianmargaretndr@gmail.com, [2*]dosen01573@unpam.ac.id
(* : coressponding author)

Abstrak−HTTP (*Hypertext Transfer Protoco*l) dan HTTPS (*Hypertext Transfer Protocol Secure*) adalah dua protokol yang paling umum digunakan dalam komunikasi web untuk mengakses dan mentransfer data. Namun, perbedaan mendasar antara keduanya terletak pada tingkat keamanan, terutama saat menangani data sensitif seperti informasi login. HTTP mentransmisikan data dalam bentuk teks biasa (*plaintext*), sehingga membuat data rentan terhadap serangan seperti *packet sniffing*, di mana pihak ketiga dapat dengan mudah membaca dan mencuri data yang ditransmisikan. Sebaliknya, HTTPS mengenkripsi data menggunakan protokol keamanan seperti SSL/TLS, yang secara signifikan meningkatkan perlindungan terhadap akses tidak sah.

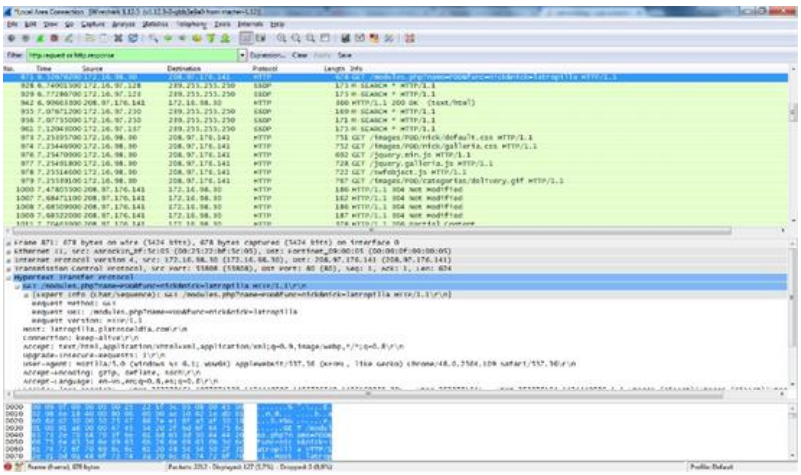
Kata Kunci: Keamanan Jaringan, Sistem Komputer, Perangkat Keras, *Malware*, *Ransomware*, Mitigasi Risiko

Abstract−*HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) are two of the most commonly used protocols in web communication for accessing and transferring data. However, the fundamental difference between them lies in their level of security, particularly when handling sensitive. information such as login credentials. HTTP transmits data in plaintext, making it vulnerable to attacks such as *packet sniffing*, where third parties can easily read and steal transmitted data. In contrast, HTTPS encrypts data using security protocols like SSL/TLS, significantly enhancing protection against unauthorized access.*

Keywords*: Network Security, Computer Systems, Hardware, Malware, Ransomware, Risk Mitigation.*

1. PENDAHULUAN

HTTP (*Hypertext Transfer Protocol*) merupakan protokol komunikasi standar yang digunakan untuk mentransfer data antara klien (seperti browser web) dan server. Protokol ini menjadi fondasi utama dalam pengaksesan halaman web, mulai dari memuat konten sederhana hingga transaksi data yanglebih kompleks. Namun, salah satu kelemahan utama HTTP adalah kurangnyamekanisme keamanan. Data yang dikirim melalui HTTP tidak dienkripsi, yangberarti informasi sensitif seperti username, password, atau data pribadi lainnyadapat ditransmisikan dalam bentuk teks biasa (plaintext). Hal ini membuat HTTP rentan terhadap berbagai ancaman keamanan, seperti packet sniffing, dimana pihak ketiga yang tidak berwenang dapat menangkap dan membaca datayang sedang ditransmisikan.



Gambar 1. *Wireshark Debugging* HTTP/HTTPS

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 2, No. 4, November Tahun 2024
ISSN 3024-8248 (media online)
Hal 735-738

Di sisi lain, HTTPS (Hypertext Transfer Protocol Secure) dirancang untuk mengatasi kekurangan keamanan yang dimiliki oleh HTTP. HTTPS menggunakan protokol SSL/TLS (Secure Sockets Layer/Transport Layer Security) untuk mengenkripsi data selama proses transmisi. Dengan enkripsi ini, data yang dikirimkan melalui HTTPS tidak dapat dibaca oleh pihak yang tidak memiliki kunci enkripsi, meskipun data tersebut berhasil ditangkap oleh alat seperti Wireshark. Selain itu, HTTPS juga menyediakan mekanisme autentikasi untuk memastikan bahwa data dikirimkan ke server yang sah,sehingga mengurangi risiko serangan seperti man-in-the-middle attack.

Keamanan komunikasi web menjadi semakin penting seiring dengan meningkatnya penggunaan internet untuk aktivitas yang melibatkan data sensitif, seperti login, pembayaran online, dan transaksi keuangan. Dengan semakin banyaknya ancaman siber yang muncul, memahami perbedaan antaraHTTP dan HTTPS, serta bagaimana protokol ini melindungi atau gagal melindungi data pengguna, menjadi sangat penting. Studi ini berfokus pada perbandingan keamanan antara HTTP dan HTTPS dengan melakukan simulasipengambilan data login menggunakan alat packet sniffing seperti Wireshark.

Dengan pendekatan ini, artikel ini bertujuan untuk memberikan pemahaman mendalam mengenai pentingnya migrasi ke HTTPS dalam memastikan privasidan keamanan pengguna.

2. METODE PENELITIAN

2.1 Kerangka Teoritis

Keamanan data dalam komunikasi web merupakan salah satu aspek yang sangat penting, terutama di era digital saat ini. Protokol HTTP (Hypertext Transfer Protocol) telah lama digunakan sebagai standar untuk pertukaran informasi di internet. Namun, protokol ini memiliki kelemahan mendasar, yaitutransmisi data dalam bentuk teks biasa (plaintext). Hal ini membuat data yang dikirim melalui HTTP, seperti informasi login dan data pribadi lainnya, dapat dengan mudah diakses oleh pihak ketiga menggunakan teknik packet sniffing.

HTTPS (Hypertext Transfer Protocol Secure) hadir sebagai solusi atas kelemahan tersebut dengan mengintegrasikan protokol SSL/TLS (Secure Sockets Layer/Transport Layer Security). SSL/TLS menyediakan mekanisme enkripsi data, autentikasi server, dan integritas data, sehingga data yang dikirimkan tidak hanya terlindungi dari pengintaian tetapi juga dijamin keasliannya. Ketika HTTPS digunakan, data yang ditangkap menggunakan alatseperti Wireshark akan terlihat dalam bentuk terenkripsi, sehingga hampir tidakmungkin dibaca tanpa kunci enkripsi.

Dalam konteks keamanan data, pendekatan berbasis teori kriptografi menjadi dasar utama dari protokol HTTPS. Protokol ini memanfaatkan algoritma enkripsi simetris untuk transmisi data yang cepat dan algoritma asimetris untuk proses pertukaran kunci yang aman. Kombinasi keduanya menciptakan lapisan keamanan yang sulit ditembus, terutama dibandingkan dengan protokol HTTP yang sama sekali tidak menggunakan enkripsi.

2.2 Pengembangan Hipotesis

Berdasarkan teori di atas, penelitian ini mengembangkan hipotesis berikut:

- Hipotesis 1 (H1): Data login yang ditransmisikan melalui HTTP lebihmudah ditangkap dan dibaca menggunakan teknik packet sniffingdibandingkan data yang ditransmisikan melalui HTTPS.
- Hipotesis 2 (H2): Penggunaan HTTPS secara signifikan mengurangi risiko kebocoran data login karena proses enkripsi membuat data tidakdapat dibaca oleh pihak yang tidak memiliki kunci enkripsi.
- Hipotesis 3 (H3): Data login yang ditransmisikan melalui HTTP lebihrentan terhadap serangan man-in-the-middle dibandingkan dengan data yang ditransmisikan melalui HTTPS.
- Relevansi Hipotesis dengan Penelitian
- Hipotesis yang diajukan relevan dengan penelitian ini karenamemberikan kerangka untuk mengevaluasi efektivitas HTTPS dibandingkan HTTP dalam melindungi data pengguna.

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 2, No. 4, November Tahun 2024
ISSN 3024-8248 (media online)
Hal 735-738

3. ANALISA DAN PEMBAHASAN

Penelitian ini menggunakan metode eksperimental untuk membandingkan tingkat keamanan antara HTTP dan HTTPS dalam melindungi data login dari ancaman packet sniffing. Eksperimen dilakukan dengan mensimulasikan proses pengambilan data login pada kedua protokol menggunakan alat analisis jaringan, yaitu Wireshark. Penelitian ini bertujuan untuk mengevaluasi perbedaan tingkat kerentanan data terhadap serangan berdasarkan protokol yang digunakan.

3.1 Lingkungan Eksperimen

Eksperimen dilakukan pada jaringan lokal (LAN) untuk mengurangi faktoreksternal yang dapat memengaruhi hasil penelitian. Lingkungan eksperimen mencakup:

- Server Web: Menyediakan halaman login sederhana yang diaksesmenggunakan HTTP dan HTTPS.
- Klien: Komputer yang digunakan untuk mengakses halaman login danmengirimkan data login.
- Alat Penangkap Paket: Wireshark digunakan untuk menangkap danmenganalisis paket data yang dikirimkan melalui jaringan.

3.2 Prosedur Penelitian

Tahap Persiapan:

- Membuat halaman login sederhana dengan form input username danpassword.
- Mengonfigurasi server untuk mendukung akses melalui HTTP danHTTPS.
- Menyiapkan Wireshark untuk menangkap lalu lintas data padajaringan.

Pengujian HTTP:

- Klien mengakses halaman login melalui protokol HTTP.
- Data login (username dan password) dimasukkan pada form login.
- Wireshark digunakan untuk menangkap lalu lintas data selama proses pengiriman data login.
- Hasil tangkapan dianalisis untuk melihat apakah data login dapatdibaca dalam bentuk plaintext.

Pengujian HTTPS:

- Klien mengakses halaman login yang sama melalui protokol HTTPS.
- Data login dimasukkan pada form login.
- Wireshark kembali digunakan untuk menangkap lalu lintas data selamapengiriman.
- Hasil tangkapan dianalisis untuk mengevaluasi pola enkripsi danapakah data login dapat dibaca.

Analisis Data:

- Membandingkan hasil tangkapan paket antara HTTP dan HTTPS.
- Mengevaluasi kerentanan data login pada kedua protokol berdasarkan kemampuan membaca data yang ditangkap.

3.3 Instrumen Penelitian

Alat:

- Komputer/laptop dengan Wireshark terinstal.
- Server web lokal (XAMPP atau Nginx).
- Browser web (Google Chrome atau Mozilla Firefox).

Bahan:

- Halaman login berbasis HTML dan PHP.
- Sertifikat SSL/TLS untuk pengujian HTTPS.

3.4 Analisis Data

Data yang diperoleh dari tangkapan Wireshark akan dianalisis secara kualitatif untuk melihat apakah data login dapat dibaca dalam bentuk plaintext(pada HTTP) atau dalam bentuk terenkripsi (pada HTTPS). Hasil analisis akandigunakan untuk mengukur perbedaan tingkat keamanan antara kedua protokol.

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 2, No. 4, November Tahun 2024
ISSN 3024-8248 (media online)
Hal 735-738

3.5 Hasil Penelitian

Hasil eksperimen menunjukkan perbedaan yang signifikan antara keamanan HTTP dan HTTPS dalam melindungi data login dari ancaman *packet sniffing*. Berikut adalah temuan utama:

1. **Hasil pada Protokol HTTP**
   - Data login, termasuk *username* dan *password*, yang ditransmisikan melalui protokol HTTP ditangkap oleh Wireshark dalam bentuk teksbiasa (*plaintext*).
   - Informasi login dapat langsung dibaca tanpa usaha tambahan, sehingga sangat rentan terhadap penyusupan.
2. **Hasil pada Protokol HTTPS**
   - Data login yang ditransmisikan melalui protokol HTTPS tidak dapat dibaca oleh Wireshark.
   - Wireshark hanya menangkap data dalam bentuk terenkripsi, yang tidak dapat diuraikan tanpa kunci enkripsi yang valid.
   - Tidak ditemukan informasi login dalam bentuk yang dapat dimengerti, menunjukkan efektivitas enkripsi SSL/TLS dalam melindungi data.
3. **Perbandingan Keamanan**
   - Pada HTTP, ancaman terhadap privasi pengguna sangat tinggi karena data ditransmisikan tanpa perlindungan.
   - HTTPS, dengan dukungan enkripsi, secara signifikan meningkatkan keamanan dengan mencegah akses pihak ketiga terhadap data yang sensitif.

3.6 Tabel Perbandingan Hasil

Tabel 1. Perbandingan Hasil

Aspek	HTTP	HTTPS
Bentuk Data Tertangkap	Teks biasa (*plaintext*)	Data terenkripsi
Kerentanan terhadap Serangan	Sangat rentan	Sangat rendah
Kebutuhan Dekripsi	Tidak diperlukan	Memerlukan kunci dekripsi

4. KESIMPULAN

Eksperimen ini secara jelas menunjukkan bahwa protokol HTTPS jauh lebih aman dibandingkan dengan HTTP dalam melindungi data login dari ancaman packet sniffing. Hal ini disebabkan oleh penggunaan mekanisme enkripsi pada HTTPS, yang membuat data tidak dapat dibaca oleh pihak yang tidak memiliki kunci enkripsi, bahkan jika data tersebut berhasil ditangkap.

HTTPS adalah solusi yang efektif untuk melindungi data dari ancaman keamanan dengan menggunakan teknologi SSL/TLS untuk mengenkripsi data selama proses transmisi.

Penerapan HTTPS sangat direkomendasikan, terutama untuk situs web yang menangani informasi sensitif seperti login, pembayaran, dan data pribadi pengguna. Penelitian ini menekankan pentingnya migrasi dari HTTP ke HTTPS untuk memastikan keamanan komunikasi web. Dengan adopsi protokol HTTPS, pengguna dan pengembangweb dapat memberikan perlindungan yang lebih baik terhadap privasi dan data sensitif.

REFERENCES

Dierks, T., & Rescorla, E. "*The Transport Layer Security (TLS) Protocol Version 1.2. IETFRFC 5246.*" (2008).

Documentation, Wireshark. "*Wireshark User's Guide. Retrieved from www.wireshark.org.*"(2023).

Kurose, J. F., & Ross, K. W. "*Computer Networking: A Top-Down Approach* (8th ed.). Pearson Education." (2021).

Lab., Kaspersky. "*HTTP vs. HTTPS: What's the Difference*?" Retrieved from www.kaspersky.com." (2020).

Rescorla, E. "*SSL and TLS: Designing and Building Secure Systems. Addison-Wesley*"(2000).

Stallings, W. "*Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education*" (2017).