

BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Keamanan dalam komunikasi digital adalah salah satu isu paling krusial dalam era informasi saat ini (Aulia et al., 2023). Protokol SSL (*Secure Sockets Layer*) yang kemudian berevolusi menjadi TLS (*Transport Layer Security*), merupakan teknologi yang digunakan untuk mengamankan transmisi data di internet dengan cara mengenkripsi data yang dikirimkan antara klien dan *server*. Salah satu implementasi dari teknologi ini adalah OpenSSL, sebuah *toolkit* yang digunakan secara luas untuk menerapkan protokol SSL/TLS dalam berbagai aplikasi (Mujiastuti & Prasetyo, 2021).

OpenSSL adalah perpustakaan perangkat lunak yang menyediakan fungsi kriptografi untuk mengamankan koneksi *internet*. Sebagai proyek *open-source*, OpenSSL menjadi pilihan utama dalam berbagai aplikasi *web* dan layanan *online* karena kemudahan akses dan fleksibilitasnya (Istiana, 2022). Namun, sebagai perangkat lunak *open-source*, OpenSSL juga menghadapi tantangan besar dalam hal keamanan, termasuk kerentanan terhadap serangan (Ramadhan et al., 2022).

Meskipun SSL/TLS dirancang untuk memberikan keamanan, bukan berarti kebal terhadap serangan (Affandi, 2022). Serangan seperti SSL *Hijacking*, di mana penyerang mengambil alih sesi SSL yang sah, dapat mengekspos data sensitif. Metode serangan ini sering kali memanfaatkan teknik *sniffing* untuk menangkap dan memanipulasi data yang dikirim antara pengguna dan *server* (Susanto & Raharja, 2021).

Metode *sniffing* digunakan untuk menganalisis dan mengidentifikasi celah didalam protokol SSL/TLS (Akbar et al., 2022). Dengan *sniffing*, peneliti dapat menangkap lalu lintas data dan menganalisis bagaimana data tersebut dikirim, di mana potensi kelemahan berada, dan bagaimana serangan dapat dilakukan. Metode ini memungkinkan pemahaman yang mendalam tentang mekanisme

serangan dan pertahanan yang diperlukan untuk melindungi sistem dari ancaman (Sahara et al.,2022).

Oleh karena itu, penelitian ini bertujuan untuk menganalisis kerentanan penggunaan OpenSSL terhadap ancaman serangan SSL *Hijacking* menggunakan metode *sniffing*. Penelitian ini diharapkan dapat memberikan wawasan yang lebih mendalam mengenai titik-titik lemah dalam penggunaan OpenSSL dan menyarankan langkah-langkah mitigasi yang tepat untuk meningkatkan keamanan komunikasi digital.

1.1.1 Perumusan Masalah

Penelitian ini ingin menjawab pertanyaan tentang bagaimana metode *sniffing* dapat digunakan untuk mengidentifikasi dan mengeksploitasi kerentanan dalam implementasi OpenSSL, serta bagaimana kerentanan tersebut mempengaruhi keamanan data yang ditransmisikan. Selain itu, penelitian ini berusaha mengidentifikasi kerentanan spesifik dalam OpenSSL yang rentan terhadap serangan SSL *Hijacking* dan mengevaluasi dampak potensial dari serangan tersebut terhadap integritas dan kerahasiaan data.

1.1.2 Manfaat Hasil Penelitian

Dengan melakukan penelitian ini diharapkan menjadi manfaat bagi penulis dan pengelola jaringan. Manfaat yang didapat seperti :

1. Membantu mengidentifikasi dan memahami kerentanan dalam penggunaan OpenSSL terhadap serangan SSL *Hijacking*.
2. Menyediakan panduan praktis dan langkah-langkah mitigasi yang dapat diterapkan untuk mencegah serangan SSL *Hijacking*.
3. Memberikan manfaat langsung bagi pengembang perangkat lunak, administrator jaringan, dan organisasi dalam mengkonfigurasi dan menggunakan OpenSSL dengan lebih aman.

1.2 TUJUAN PENELITIAN

Penelitian ini bertujuan untuk menganalisis kerentanan penggunaan OpenSSL terhadap ancaman serangan SSL *Hijacking* yang dilakukan

menggunakan metode *sniffing*. Fokus utama dari metode sniffing adalah mengidentifikasi dan mengeksploitasi kelemahan dalam implementasi OpenSSL, serta dampak dari kerentanan tersebut terhadap keamanan data yang ditransmisikan. Penelitian ini juga mengeksplorasi langkah-langkah mitigasi yang dapat diterapkan untuk mengurangi risiko serangan SSL *Hijacking*, dengan harapan dapat memberikan solusi praktis dan efektif bagi pengembang perangkat lunak dan administrator jaringan untuk meningkatkan keamanan sistem mereka.

UNIVERSITAS JENDERAL ACHMAD YANI
PERPUSTAKAAN
YOGYAKARTA