BAB 5
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Penelitian ini mengungkapkan bahwa penggunaan OpenSSL untuk mengamankan koneksi HTTPS pada lingkungan lokal (*localhost*) memiliki kelemahan signifikan terhadap serangan *sniffing*. Dalam skenario pengujian, data yang dikirim melalui *https://localhost* tidak terdeteksi oleh metode *sniffing* karena browser menampilkan peringatan bahwa sertifikat tidak valid dan tidak memperbolehkan koneksi yang tidak aman. Namun, ketika mengakses *website* lain dengan sertifikat yang valid, serangan *sniffing* dapat berhasil dilakukan, dan data yang seharusnya terenkripsi dapat terungkap.

Hal ini menunjukkan bahwa penggunaan sertifikat *self-signed* pada *localhost* mengakibatkan koneksi dianggap tidak aman oleh *browser*, sehingga melindungi data dari serangan *sniffing*. Sebaliknya, situs web dengan sertifikat yang valid tetap rentan terhadap serangan *sniffing* jika pengaturan keamanan tidak tepat. Salah satu mitigasi serangan adalah untuk tidak menggunakan *proxy mitmproxy* dan tidak menginstal sertifikat *mitmproxy.*

Oleh karena itu, penting untuk memastikan bahwa sertifikat yang digunakan dikeluarkan oleh *Certificate Authority* (CA) yang terpercaya dan mengonfigurasi *server* dengan protokol keamanan terbaru untuk melindungi data dari ancaman *sniffing* dan serangan SSL *Hijacking.*

5.2 SARAN

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, terdapat beberapa saran yang dapat diambil untuk meningkatkan keamanan dan efektivitas dalam melakukan penelitian serupa di masa mendatang:

1. Gunakan Sertifikat CA Terpercaya

   Disarankan untuk menghindari penggunaan sertifikat *self-signed* pada lingkungan penelitian. Gunakan sertifikat SSL/TLS yang dikeluarkan oleh *Certificate Authority* (CA) terpercaya untuk

memastikan bahwa sertifikat tersebut diakui oleh *browser* dan perangkat klien. Hal ini akan menghilangkan peringatan "*Not Secure*" dan memungkinkan koneksi HTTPS yang aman.

2. Hindaran Penggunaan *Localhost* dalam Penelitian Keamanan

   Untuk penelitian keamanan yang lebih valid dan relevan, sebaiknya tidak menggunakan *localhost* sebagai domain penelitian. Menggunakan domain yang valid dan diakui oleh CA dapat memberikan hasil yang lebih akurat terkait kerentanan dan serangan yang mungkin terjadi pada lingkungan penelitian yang sebenarnya. lapisan keamanan tambahan terhadap serangan.

3. Edukasi Pengguna dan Administrator

   . Disarankan untuk memberikan edukasi bagi pengguna dan administrator mengenai pentingnya keamanan sertifikat dan pengaturan *proxy*. Memahami risiko memasang sertifikat yang tidak terpercaya dan menggunakan *proxy* yang tidak diketahui dapat membantu meningkatkan keselamatan dan keamanan data.