ANALISIS KERENTANAN PENGGUNAAN OPENSSL MENGGUNAKAN METODE SNIFFING TERHADAP ANCAMAN SERANGAN SSL HIJACKING

Kholis Munajat, Adkhan Sholeh, Chanief Budi Setiawan

INTISARI

Latar Belakang: Keamanan data dalam komunikasi jaringan merupakan aspek yang sangat penting di era digital saat ini. OpenSSL adalah perpustakaan perangkat lunak untuk aplikasi yang menyediakan komunikasi aman melalui jaringan komputer dari protokol SSL/TLS. Namun, OpenSSL tidak sepenuhnya kebal terhadap berbagai ancaman, termasuk serangan SSL *hijacking* yang dapat mengancam integritas dan kerahasiaan data yang ditransmisikan.

Tujuan: Penelitian ini bertujuan untuk menganalisis kerentanan penggunaan OpenSSL dengan metode *sniffing* terhadap ancaman serangan SSL *hijacking*.

Metode: Metode *sniffing* digunakan untuk menangkap dan menganalisis lalu lintas jaringan guna mengidentifikasi kelemahan didalam OpenSSL.

Hasil: Hasil dari penelitian ini menunjukkan bahwa kerentanan dalam penggunaan OpenSSL dapat dieksploitasi melalui metode *sniffing*, yang memungkinkan serangan SSL *hijacking*.

Kesimpulan: Penelitian ini mengungkapkan bahwa penggunaan OpenSSL untuk mengamankan koneksi HTTPS pada *localhost* memiliki kelemahan signifikan terhadap serangan *sniffing*. Data yang dikirim melalui *https://localhost* tidak terdeteksi oleh metode *sniffing* karena *browser* menampilkan peringatan sertifikat tidak valid, sementara *website* dengan sertifikat valid tetap rentan terhadap serangan *sniffing*. Oleh karena itu, penting untuk memastikan sertifikat dikeluarkan oleh *Certificate Authority* (CA) yang terpercaya dan mengonfigurasi *server* dengan protokol keamanan terbaru untuk melindungi data dari ancaman *sniffing* dan serangan SSL *Hijacking*.

Kata-kunci: OpenSSL, SSL/TLS, *Sniffing*, SSL *Hijacking*, Keamanan Jaringan, Kerentanan, Serangan Siber.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

ANALYSIS OF VULNERABILITIES IN THE USE OF OPENSSL USING SNIFFING METHODS AGAINST SSL HIJACKING ATTACK THREATS

Kholis Munajat, Adkhan Sholeh, Chanief Budi Setiawan

ABSTRACT

Background: *Data security in network communication is a critical aspect in today's digital era. OpenSSL is a software library for applications that provide secure communication over computer networks using the SSL/TLS protocol. However, OpenSSL is not entirely immune to various threats, including SSL hijacking attacks that can compromise the integrity and confidentiality of transmitted data.*

Objective: *This study aims to analyze the vulnerabilities of using OpenSSL with sniffing methods against the threat of SSL hijacking attacks.*

Method: *The sniffing method was used to capture and analyze network traffic to identify weaknesses within OpenSSL.*

Results: *The results of this study indicate that vulnerabilities in the use of OpenSSL can be exploited through sniffing methods, enabling SSL hijacking attacks.*

Conclusion: *This research reveals that using OpenSSL to secure HTTPS connections on localhost has significant weaknesses against sniffing attacks. Data transmitted through https://localhost is not detected by sniffing methods because browsers display an invalid certificate warning, while websites with valid certificates remain vulnerable to sniffing attacks. Therefore, it is crucial to ensure that certificates are issued by a trusted Certificate Authority (CA) and to configure servers with the latest security protocols to protect data from sniffing threats and SSL hijacking attacks.*

Keywords: *OpenSSL, SSL/TLS, Sniffing, SSL Hijacking, Network Security, Vulnerability, Cyber Attack.*

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA