

**ANALISIS KERENTANAN PENGGUNAAN OPENSLL MENGGUNAKAN
METODE SNIFFING TERHADAP ANCAMAN SERANGAN SSL HIJACKING**

TUGAS AKHIR

Diajukan sebagai salah satu syarat memperoleh gelar Sarjana
Program Studi S-1 Teknologi Infomasi



Disusun oleh:

KHOLIS MUNAJAT
182104015

**PROGRAM STUDI S-1 TEKNOLOGI INFORMASI
FAKULTAS TEKNIK & TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA
2024**

HALAMAN PENGESAHAN

TUGAS AKHIR

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

Diajukan oleh:

KHOLIS MUNAJAT

182104015

Telah dipertahankan di depan dewan penguji dan dinyatakan sah
sebagai salah satu syarat untuk memperoleh gelar Sarjana
di Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta

Tanggal: 11 Juli 2024

Mengesahkan:

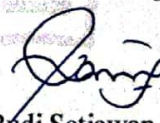
Pembimbing I



Adkhan Sholeh, S.Si., M.Cs.

NIDN: 0510127501

Pembimbing II



Chanief Budi Setiawan, S.T., M.Eng.

NIDN: 0514068101

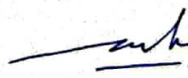
Penguji I



Rama Sahtyawan, S.T., M.Cs.

NIDN: 0518058001

Penguji II



Arief Ikhwan Wicaksono, S.Kom., M.Cs.

NIDN: 0512128401

Ketua Program Studi S-1 Teknologi Informasi
Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta



Rama Sahtyawan, S.T., M.Cs.

NPP: 2019.13.0150

PERNYATAAN

Saya yang bertanda tangan di bawah ini, adalah mahasiswa Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta,

Nama : Kholis Munajat
NPM : 182104015
Program Studi : S-1 Teknologi Informasi
Judul Tugas Akhir : Analisis Kerentanan Penggunaan OpenSSL Menggunakan Metode Sniffing Terhadap Ancaman Serangan SSL Hijacking

Menyatakan bahwa hasil penelitian dengan judul tersebut di atas adalah asli karya saya sendiri dan bukan hasil plagiarisme. Semua referensi dan sumber terkait yang dikutip dalam karya ilmiah ini telah ditulis sesuai kaidah penulisan ilmiah yang berlaku. Dengan ini, saya menyatakan untuk menyerahkan hak cipta penelitian kepada Universitas Jenderal Achmad Yani Yogyakarta guna kepentingan ilmiah.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya tanpa ada paksaan dari pihak mana pun. Apabila terdapat kekeliruan atau ditemukan adanya pelanggaran akademik di kemudian hari, maka saya bersedia menerima konsekuensi yang berlaku sesuai ketentuan akademik.

Yogyakarta, 24 Juli 2024



Kholis Munajat

KATA PENGANTAR

Puji syukur kehadiran Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Kerentanan Penggunaan OpenSSL Menggunakan Metode Sniffing terhadap Ancaman Serangan SSL Hijacking”. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana di Program Studi Teknologi Informasi, Fakultas Teknik dan Teknologi Informasi, Universitas Jenderal Achmad Yani Yogyakarta.

Penulisan skripsi ini tidak terlepas dari bantuan dan dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Rama Sahtyawan, S.T., M.Cs., selaku Ketua Program Studi Teknologi Informasi, Fakultas Teknik dan Teknologi Informasi, Universitas Jenderal Achmad Yani Yogyakarta, yang telah memberikan kesempatan dan dukungan dalam penelitian ini.
2. Adkhan Sholeh, S.Si., M.Cs., selaku dosen pembimbing yang telah memberikan bimbingan, saran, dan dukungan selama penulisan skripsi ini.
3. Orang Tua dan Keluarga, yang selalu memberikan doa, dukungan, dan motivasi yang tiada henti.
4. Teman-Teman dan Rekan Mahasiswa Program Studi Teknologi Informasi, yang telah memberikan bantuan, semangat, dan kerjasama yang baik selama penulisan skripsi ini.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat kekurangan dan keterbatasan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk perbaikan di masa mendatang. Semoga skripsi ini dapat bermanfaat bagi pengembangan ilmu pengetahuan dan menjadi referensi bagi pembaca dan peneliti lainnya.

Akhir kata, penulis mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dalam penyelesaian skripsi ini.

Yogyakarta, 24 Juli 2024



Kholis Munajat

PERPUSTAKAAN
JENDERAL ACHMAD YOHANIS
UNIVERSITAS JENDERAL ACHMAD YOHANIS
YOGYAKARTA

DAFTAR ISI

Halaman Judul	i
Halaman Pengesahan.....	ii
Halaman Pernyataan	iii
Kata Pengantar	iv
Daftar Isi	vi
Daftar Tabel.....	viii
Daftar Gambar	ix
Daftar Lampiran	x
Daftar Singkatan	xi
Intisari.....	xii
Abstract.....	xiii
Bab 1 Pendahuluan	1
1.1 Latar Belakang	1
1.1.1 Perumusan Masalah.....	2
1.1.2 Manfaat Hasil Penelitian	2
1.2 Tujuan Penelitian	2
Bab 2 Tinjauan Pustaka dan Landasan Teori.....	4
2.1 Tinjauan Pustaka	4
2.2 Landasan Teori.....	7
2.2.1 SSL/TLS	7
2.2.2 OpenSSL	8
2.2.3 Sniffing.....	8
2.2.4 SSL Hijacking	10
2.3 Pertanyaan Penelitian	12
Bab 3 Metode Penelitian.....	13
3.1 Desain Penelitian.....	13
3.2 Pengumpulan Data	14
3.3 Analisis Data	15

3.4	Bahan dan Alat Penelitian.....	15
3.4.1	Perangkat Keras.....	15
3.4.2	Perangkat Lunak.....	16
3.5	Jalan Penelitian.....	17
3.5.1	Persiapan Lingkungan Penelitian	17
3.5.2	Konfigurasi Server	18
3.5.3	Analisis Kerentanan	18
3.5.4	Evaluasi Hasil.....	18
Bab 4	Hasil Penelitian.....	19
4.1	Ringkasan Hasil Penelitian	19
4.2	Konfigurasi Server Menggunakan Openssl dan Node.Js.....	19
4.2.1	Instalasi OpenSSL	19
4.2.2	Instalasi Node.js	21
4.2.3	Pembuatan Sertifikat SSL	22
4.2.4	Konfigurasi Server Node.js.....	22
4.3	Analisis Kerentanan	24
4.3.1	Permasalahan Sertifikat CA Tidak Valid	24
4.3.2	Instalasi Mitmproxy	25
4.3.3	Simulasi Serangan SSL Hijacking Menggunakan Metode Sniffing .	26
4.3.4	Uji Coba Serangan Pada Halaman Web Lain	27
4.4	Evaluasi Hasil Uji Coba	30
4.4.1	Hasil Pengamatan.....	30
4.4.2	Rekomendasi Keamanan	30
4.4.3	Langkah Mitigasi.....	30
Bab 5	Kesimpulan dan Saran	31
5.1	Kesimpulan	31
5.2	Saran.....	31
	Daftar Pustaka.....	33
	Lampiran	36

DAFTAR TABEL

Tabel 2. 1 Perbandingan Tinjauan Pustaka	6
---	---

PERPUSTAKAAN
JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR GAMBAR

Gambar 2. 1 Mekanisme Kerja SSL/TLS.....	7
Gambar 2. 2 <i>Active Session Hijacking</i>	11
Gambar 2. 3 <i>Passive Session Hijacking</i>	11
Gambar 3. 1 Topologi jaringan	13
Gambar 3. 2 Jalan penelitian	17
Gambar 4. 1 Unduh OpenSSL.....	20
Gambar 4. 2 Menambahkan <i>Path Variable</i>	20
Gambar 4.3 Versi OpenSSL	21
Gambar 4. 4 Unduh Node.js	21
Gambar 4. 5 <i>JavaScript server.js</i>	23
Gambar 4. 6 <i>Login.html</i>	24
Gambar 4. 7 <i>Node server.js</i>	24
Gambar 4. 8 Tampilan web server.....	25
Gambar 4. 9 <i>Setting proxy browser user</i>	26
Gambar 4. 10 Tampilan <i>capture data mitmproxy</i>	27
Gambar 4. 11 Halaman <i>https://pordik.unjaya.ac.id</i>	28
Gambar 4. 12 Sertifikat SSL <i>double</i>	28
Gambar 4. 13 <i>Mitmproxy membaca https://pordik.unjaya.ac.id</i>	29
Gambar 4. 14 <i>Mitmproxy menangkap username dan password</i>	29

DAFTAR LAMPIRAN

Lampiran 1 Surat Izin Penelitian.....	36
Lampiran 2 Kartu Bimbingan Tugas Akhir	37
Lampiran 3 Jadwal Penelitian	38
Lampiran 4 Hasil Cek Plagiarisme.....	39

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR SINGKATAN

CA	<i>Certificate of Authority</i>
CSP	<i>Content Security Policy</i>
DOS	<i>Denial of Service</i>
HSTS	<i>HTTP Strict Transport Security</i>
HTML	<i>Hypertext Markup Language</i>
HTTP	<i>Hypertext Transfer Protocol</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
IDS	<i>Intrusion Detection System</i>
MITM	<i>Man In The Middle</i>
SSH	<i>Secure Shell</i>
SSL	<i>Secure Sockets Layer</i>
TLS	<i>Transport Layer Security</i>
VPN	<i>Virtual Private Network</i>