ANALISIS KERENTANAN PENGGUNAAN OPENSSL 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 OPENSSL 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	Pembimbing II
Adkhan Sholeh, S.Si., M.Cs.	Chanief Budi Setiawan, S.T., M.Eng.
NIDN: 0510127501	NIDN: 0514068101

Penguji I	Penguji II
Rama Sahtyawan, S.T., M.Cs.	Arief Ikhwan Wicaksono, S.Kom., M.Cs.
NIDN: 0518058001	NIDN: 0512128401

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

KETUA PROGRAM STUDI

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 kehadirat 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

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR SINGKATAN

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