

**IMPLEMENTASI SISTEM KEAMANAN BERBASIS WEB
DENGAN PROTOKOL *TLS* PADA *WEBSITE* PENYEDIA JASA
SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh

RAMADIANSYAH NUARI

16.11.0762

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023**

**IMPLEMENTASI SISTEM KEAMANAN BERBASIS WEB
DENGAN PROTOKOL *TLS* PADA *WEBSITE* PENYEDIA JASA**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh

RAMADIANSYAH NUARI

16.11.0762

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA**

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

**IMPLEMENTASI SISTEM KEAMANAN BERBASIS WEB DENGAN
PROTOKOL *TLS* PADA *WEBSITE* PENYEDIA JASA**

yang disusun dan diajukan oleh

Ramadiansyah Nuari

16.11.0762

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal <17 Maret 2023>

Dosen Pembimbing,



Mauid Rafardi, S.Kom., M.Eng

NIK. 190302393

HALAMAN PENGESAHAN
SKRIPSI
IMPLEMENTASI SISTEM KEAMANAN BERBASIS WEB DENGAN
PROTOKOL *TLS* PADA *WEBSITE* PENYEDIA JASA

yang disusun dan diajukan oleh

Ramadiansyah Nuari

16.11.0762

Telah dipertahankan di depan Dewan Penguji
pada tanggal <17 Maret 2023>

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Melwin Syafrizal, S.Kom., M.Eng
NIK. 190302105

Majid Rahardi, S.Kom., M.Eng
NIK. 190302393

Agung Nugroho, M.Kom
NIK. 190302242



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal < 17 Maret 2023 >

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ramadiansyah Nuari
NIM : 16.11.0762

Menyatakan bahwa Skripsi dengan judul berikut:

**IMPLEMENTASI SISTEM KEAMANAN BERBASIS WEB DENGAN
PROTOKOL TLS PADA WEBSITE PENYEDIA JASA**

Dosen Pembimbing : Majid Rahardi, S.Kom., M.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, <17 Maret 2023>

Yang Menyatakan,



Ramadiansyah Nuari

HALAMAN PERSEMBAHAN

Dalam kesempatan ini, saya ingin mengucapkan terima kasih dan memberikan penghargaan kepada beberapa pihak yang telah membantu dan memberikan dukungan selama proses penulisan skripsi ini.

Pertama-tama, saya ingin mengucapkan terima kasih kepada keluarga saya, terutama orangtua dan saudara-saudari saya, yang selalu memberikan doa, dukungan, dan semangat dalam setiap langkah yang saya ambil. Tanpa kehadiran dan cinta kasih mereka, saya mungkin tidak akan bisa menyelesaikan skripsi ini.

Kedua, terima kasih saya sampaikan kepada dosen pembimbing saya, Majid Rahardi, S.Kom.,M.Eng, yang telah memberikan bimbingan, arahan, dan dukungan selama proses penulisan skripsi ini. Terima kasih juga untuk seluruh dosen di Jurusan Teknik Informatika yang telah memberikan ilmu dan pengalaman berharga selama kuliah.

Terakhir, saya menyadari bahwa skripsi ini masih jauh dari sempurna dan masih banyak kekurangan. Oleh karena itu, saya berharap kritik dan saran yang membangun dari semua pihak untuk perbaikan dan pengembangan skripsi ini di masa yang akan datang.

Akhir kata, saya mengucapkan terima kasih sekali lagi kepada semua pihak yang telah membantu dan memberikan dukungan selama proses penulisan skripsi ini. Semoga Allah SWT senantiasa memberikan keberkahan dan kesuksesan dalam setiap langkah kehidupan kita. Amin.

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT, Penulis dapat menyelesaikan penulisan skripsi dengan judul "Implementasi Sistem Keamanan Berbasis Web Dengan Protokol *TLS* Pada *Website* Penyedia Jasa". Skripsi ini bertujuan untuk menganalisis keamanan protokol *TLS* 1.3 dalam menghadapi serangan siber dan mengimplementasikannya pada web pelayanan jasa untuk meningkatkan keamanan data pengguna.

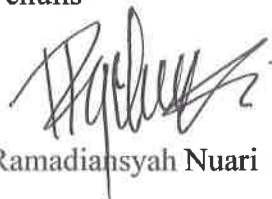
Penulisan skripsi ini tidaklah mudah, namun berkat bantuan dan dukungan dari banyak pihak, akhirnya Penulis dapat menyelesaikannya. Penulis ingin mengucapkan terima kasih kepada dosen pembimbing Majid Rahardi, S.Kom., M.Eng yang telah memberikan bimbingan dan arahan sepanjang penulisan skripsi ini. Penulis juga mengucapkan terima kasih kepada keluarga, teman, dan rekan yang telah memberikan dukungan moral dan motivasi.

Penulis menyadari bahwa penulisan skripsi ini masih jauh dari sempurna dan masih banyak kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat Penulis harapkan agar dapat menjadi bahan perbaikan dan pengembangan di masa yang akan datang.

Akhir kata, semoga hasil penelitian yang dilakukan dalam skripsi ini dapat memberikan manfaat dan kontribusi positif bagi perkembangan ilmu pengetahuan dan teknologi informasi. Wassalamu'alaikum wr.wb.

Yogyakarta, <15 Ferbruari 2023>

Penulis



Ramadiansyah Nuari

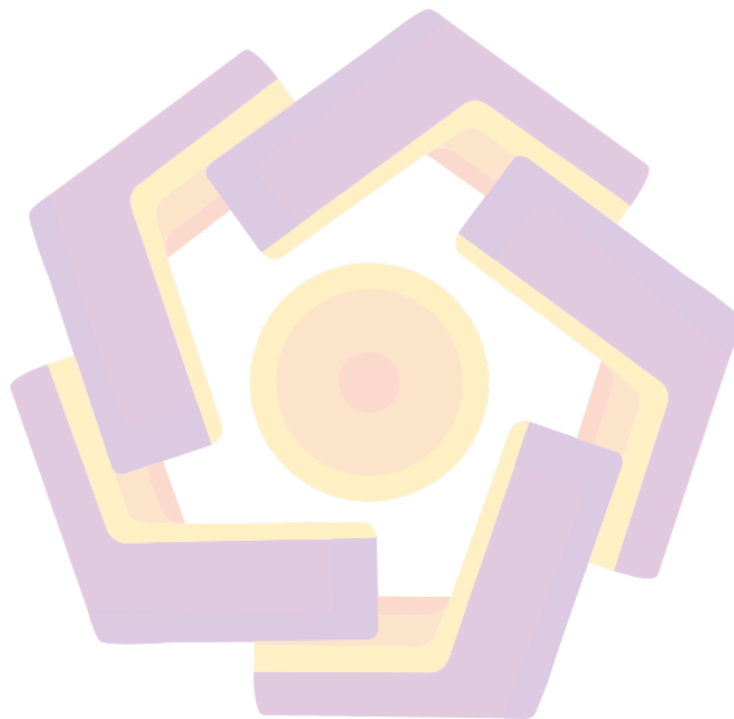
DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI	vii
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN	xi
INTISARI	xii
<i>ABSTRACT</i>	xiii
BAB I PENDAHULUAN	14
1.1 Latar Belakang	14
1.2 Rumusan Masalah	15
1.3 Batasan Masalah	15
1.4 Tujuan Penelitian	15
1.5 Manfaat Penelitian	16
1.6 Sistematika Penulisan	17
BAB II TINJAUAN PUSTAKA	19
2.1 Studi Literatur	19
2.2 Dasar Teori	31

2.2.1 Website	31
2.2.2 HTTP (<i>Hypertext Transfer Protocol</i>)	33
2.2.3 HTTPS (<i>Hypertext Transfer Protocol Secure</i>)	34
2.2.4 TLS (<i>Transport Layer Security</i>)	34
2.2.5 MitM (<i>Man in the Middle</i>)	35
BAB III METODE PENELITIAN	37
3.1 Objek Penelitian	37
3.2 Alur Penelitian	37
3.2.1 Tahap Persiapan	37
3.2.2 Tahap Pengujian	38
3.2.3 Tahap Analisis	38
3.2.4 Tahap Evaluasi	39
3.2.5 Tahap Tindak Lanjut	39
3.2.6 Tahap Uji Coba Ulang	39
3.3 Alat dan Bahan	41
BAB IV HASIL DAN PEMBAHASAN	43
4.1 Pengujian	43
4.1.1 Tahap Planning	43
4.1.2 Tahap Discovery	44
4.1.3 Tahap Attacking	52
4.1.4 Tahap Reporting	56
4.2 Analisis	61
4.3 Evaluasi	63
BAB V PENUTUP	65
5.1 Kesimpulan	65
5.2 Saran	65
REFERENSI	66
LAMPIRAN	69

DAFTAR TABEL

Tabel 2.1. Perbandingan penelitian	23
Tabel 3.1 Alat yang digunakan dalam penelitian	46
Tabel 4.1 Tabel Pengujian serangan <i>MitM</i>	62

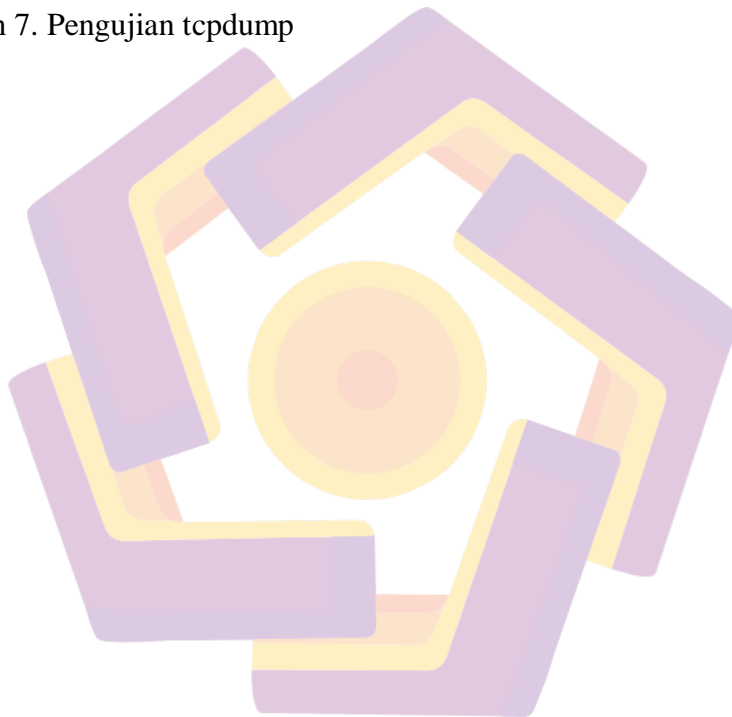


DAFTAR GAMBAR

Gambar 2.1	<i>TLS 1.3 full handshake</i>	40
Gambar 3.1	Alur Penelitian	45
Gambar 4.1	Tampilan depan <i>Website</i> pelayanan jasa	48
Gamabr 4.2	ping domain gerbakomputer.com	50
Gambar 4.3	Hasil Whois gerbakomputer.com	51
Gambar 4.4	Hasil zone transfer gerbakomputer.com	51
Gambar 4.5	hasil dari ssl scan	52
Gambar 4.6	Sertifikat TLS valid	53
Gambar 4,7	Tingkat Enkripsi pada www.gerbakomputer.com	53
Gambar 4.8	Serangan Xerosploit pada http://www.gerbakomputer.com	54
Gambar 4.9	Serangan Bettercap pada http://www.gerbakomputer.com	55
Gambar 4.10	Serangan Ettercap pada http://www.gerbakomputer.com	55
Gambar 4.11	Serangan Netsniffer-Ng http://www.gerbakomputer.com	56
Gambar 4.12	Serangan tcpdump pada http://www.gerbakomputer.com	57
Gambar 4.13	Tampilan log xeraspolit saat melakukan penyerangan	58
Gambar 4.14	Serangan Xerosploit pada https://www.gerbakomputer.com	58
Gambar 4.15	Serangan Bettercap pada https://www.gerbakomputer.com	59
Gambar 4.16	Serangan Ettercap pada https://www.gerbakomputer.com	60
Gambar 4.17	Serangan Netsniff-ng pada https://www.gerbakomputer.com	60
Gambar 4.18	Serangan TCPCDump pada https://www.gerbakomputer.com	61

DAFTAR LAMPIRAN

Lampiran 1. Tampilan <i>Website</i> gerbakomputer.com	74
Lampiran 2. Tampilan pengaktifan <i>TLS</i> 1.3	77
Lampiran 3. Pengujian Xerosploit	78
Lampiran 4. Pengujian BetterCap	80
Lampiran 5. Pengujian Ettercap	82
Lampiran 6. Pengujian netsniff-ng	84
Lampiran 7. Pengujian tcpdump	86



INTISARI

Dalam dunia teknologi informasi, serangan *MITM* adalah salah satu ancaman yang paling serius bagi keamanan data dan privasi pengguna. Serangan *MITM* terjadi ketika pihak yang tidak bertanggung jawab berhasil memasuki jalur komunikasi antara klien dan server, sehingga mereka dapat memata-matai dan mengubah informasi yang dikirimkan. Ini membuat informasi yang dikirimkan tidak lagi dapat dipercaya dan dapat membahayakan keamanan dan privasi pengguna. Untuk mengatasi masalah ini, implementasi *TLS 1.3* pada keamanan *Website* pelayanan jasa service komputer keliling menjadi solusi yang penting. *TLS 1.3* adalah versi terbaru dari protokol keamanan jaringan yang digunakan untuk menjaga integritas dan privasi data yang dikirimkan melalui internet. Implementasi *TLS 1.3* akan membantu mengenkripsi semua data yang dikirimkan antara klien dan server, sehingga pihak yang tidak bertanggung jawab tidak dapat memata-matai informasi tersebut. Secara umum, implementasi keamanan *Website* pelayanan jasa menggunakan *TLS 1.3* adalah langkah penting untuk memastikan bahwa bisnis berbasis *Website* pelayanan jasa berjalan dengan aman dan lancar serta memberikan perlindungan yang baik bagi informasi pribadi dan data sensitif klien. Penulis melakukan implementasi protokol *TLS 1.3* pada server web dan konfigurasi klien untuk mengamankan komunikasi antara server dan klien dengan enkripsi. Selanjutnya, penulis melakukan pengujian sistem keamanan dengan menggunakan serangan *MITM* untuk menguji kehandalan sistem keamanan yang diimplementasikan. Hasil pengujian menunjukkan bahwa sistem keamanan yang diimplementasikan dapat mencegah serangan *MITM*. Dalam evaluasi performa dan keamanan sistem, penulis menunjukkan bahwa penggunaan protokol *TLS 1.3* pada *Website* www.gerbakomputer.com dapat meningkatkan keamanan dan kinerja sistem. Kecepatan respon *Website* meningkat dan tidak terdapat kerentanan pada sistem keamanan yang dapat dimanfaatkan oleh penyerang.

Kata kunci: *TLS*, *Website*, Keamanan, Jasa, *MitM*.

ABSTRACT

In the world of information technology, MITM attacks are one of the most serious threats to user data and privacy. MITM attacks occur when unauthorized parties successfully enter the communication path between a client and a server, allowing them to eavesdrop and alter transmitted information. This makes the transmitted information no longer trustworthy and can endanger user security and privacy. To address this issue, implementing TLS 1.3 in the security of computer service Websites is an important solution. TLS 1.3 is the latest version of network security protocol used to maintain integrity and privacy of data transmitted over the internet. Implementing TLS 1.3 will help encrypt all data transmitted between clients and servers, preventing unauthorized parties from eavesdropping on the information. In general, implementing Website service security using TLS 1.3 is an important step in ensuring that service-based businesses run safely and smoothly, while also providing good protection for personal information and sensitive client data. The author implemented the TLS 1.3 protocol on the web server and configured the client to secure communication between the server and the client with encryption. Furthermore, the author tested the security system using MITM attacks to test the reliability of the implemented security system. The test results showed that the implemented security system can prevent MITM attacks. In the performance and security system evaluation, the author demonstrated that using the TLS 1.3 protocol on the Website www.gerbakomputer.com can improve the security and performance of the system. The Website response speed increased and there were no vulnerabilities in the security system that could be exploited by attackers.

Keyword: *TLS, Website, Keamanan, Jasa, MitM*