

**TUGAS AKHIR**

**ANALISIS UNJUK KERJA TELER SEBAGAI *REAL TIME INTRUSION DETECTION* DAN *THREAT ALERT* MENGGUNAKAN *WEB LOG* DALAM MENDETEKSI SERANGAN *DIRECTORY BRUTEFORCE* PADA *WEBSITE***



**RIO DARMAWAN**

**18102283**

**PROGRAM STUDI S1 TEKNIK INFORMATIKA  
FAKULTAS INFORMATIKA  
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

**2022**

**TUGAS AKHIR**

***ANALISIS UNJUK KERJA TELER SEBAGAI REAL  
TIME INTRUSION DETECTION DAN THREAT ALERT  
BERDASARKAN WEB LOG DALAM MENDETEKSI  
SERANGAN DIRECTORY BRUTEFORCE PADA  
WEBSITE***

***ANALYSIS OF TELER PERFORMANCE AS REAL  
TIME INTRUSION DETECTION AND THREAT ALERT  
BASED ON WEB LOG IN DETECTING DIRECTORY  
BRUTEFORCE ATTACKS ON WEBSITES***

Disusun Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Komputer



**RIO DARMAWAN**

**18102283**

**PROGRAM STUDI S1 TEKNIK INFORMATIKA  
FAKULTAS INFORMATIKA  
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

**2022**

## LEMBAR PENGESAHAN PEMBIMBING

**ANALISIS UNJUK KERJA TELER SEBAGAI *REAL TIME INTRUSION DETECTION* DAN *THREAT ALERT* DALAM MENDETEKSI SERANGAN *DIRECTORY BRUTEFORCE* PADA *WEBSITE***

***ANALYSIS OF TELER PERFORMANCE AS REAL TIME INTRUSION DETECTION AND THREAT ALERT IN DETECTING DIRECTORY BRUTEFORCE ATTACKS ON WEBSITES***

Dipersiapkan dan Disusun oleh  
**Rio Darmawan**  
18102283

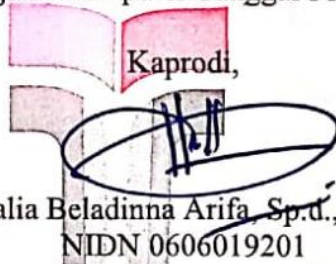
Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tugas Akhir  
Pada hari Rabu, 31 Agustus 2022

Pembimbing I



(Bita Parga Zen, S.Kom., M.Han.)  
NIDN 0603089202

Tugas Akhir ini diterima sebagai salah satu persyaratan untuk memperoleh gelar  
Sarjana Komputer Tanggal 31 Agustus 2022



(Amalia Beladinna Arifa Sp.d., M.Sc.)  
NIDN 0606019201

## LEMBAR PENETAPAN PENGUJI

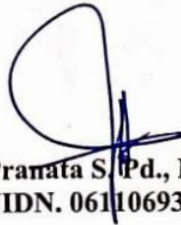
**ANALISIS UNJUK KERJA TELER SEBAGAI *REAL TIME*  
*INTRUSION DETECTION* DAN *THREAT ALERT*  
BERDASARKAN *WEB LOG* DALAM MENDETEKSI  
SERANGAN *DIRECTORY BRUTEFORCE* PADA *WEBSITE***

***ANALYSIS OF TELER PERFORMANCE AS REAL TIME  
INTRUSION DETECTION AND THREAT ALERT BASED ON  
WEB LOG IN DETECTING DIRECTORY BRUTEFORCE  
ATTACKS ON WEBSITES***

Dipersiapkan dan Disusun oleh  
**Rio Darmawan**  
18102283

Tugas Akhir Telah Diuji dan Dinilai Panitia Penguji  
Program Studi Teknik Informatika  
Fakultas Informatika Institut Teknologi Telkom Purwokerto  
Pada Tanggal : 31 Agustus 2022

**Penguji I**



(Mega Pranata S.Pd., M. Kom.)  
NIDN. 0611069301

**Penguji II**



(Trihastuti Yuniati, S.Kom., M.T.)  
NIDN . 0602068902

**Penguji III**



(Agi Prasetiadi, S.T., M. Eng.)  
NIDN. 0617098802

## HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama mahasiswa : Rio Darmawan  
NIM : 18102283  
Program Studi : S1 Teknik Informatika

Menyatakan bahwa Tugas Akhir dengan judul berikut:

**ANALISIS UNJUK KERJA TELER SEBAGAI *REAL TIME INTRUSION DETECTION* DAN *THREAT ALERT* BERDASARKAN *WEB LOG* DALAM MENDETEKSI SERANGAN *DIRECTORY BRUTEFORCE* PADA WEBSITE**

Dosen Pembimbing Utama : Bitu Parga Zen, S.Kom., M.Han.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Institut Teknologi Telkom Purwokerto maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan, dan penelitian Saya Sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim 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 tanggungjawab Saya, bukan tanggungjawab Institut Teknologi Telkom Purwokerto.
5. Pernyataan ini Saya buat dengan sesungguhnya, apabila dikemudian 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.

**Purwokerto, 18 Agustus 2022**

**Yang Menyatakan,**



**(Rio Darmawan)**



## KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah Subhanahu Wa Ta'ala, atas berkat rahmat dan karunia-Nya yang telah dilimpahkan kepada penulis sehingga penulis dapat menyelesaikan penyusunan laporan proposal Tugas Akhir dengan baik. Penulis menyadari bahwa dalam penulisan Tugas Akhir ini tidak lepas dari bimbingan, doa serta dukungan berbagai pihak yang telah membantu dalam penyusunan laporan Tugas Akhir, untuk itu dalam kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Allah Subhanahu Wa Ta'ala yang telah memberikan keschatan, rahmat dan hidayahnya.
2. Almh. Salamah selaku ibu tercinta yang selalu mendukung secara moral dan materil dalam menyelesaikan tugas akhir ini.
3. Bapak Dr. Arfianto Fahmi selaku Rektor Institut Teknologi Telkom Purwokerto.
4. Bapak Auliya Burhanuddin, S.Si., M. Kom. selaku Dekan Fakultas Informatika Institut Teknologi Telkom Purwokerto
5. Ibu Amalia Beladinna Arifa, S.Pd., M.Cs. selaku Ketua Program Studi Teknik Informatika Fakultas Informatika Institut Teknologi Telkom Purwokerto.
6. Bapak Bitu Parga Zen, S.Kom., M.Han selaku Dosen Pembimbing pertama yang telah memberikan bimbingan dan pengarahan pada saat penyusunan proposal skripsi.
7. Dwi Siswanto & Fariq Fadillah Gusti Insani selaku sahabat yang memberikan dukungan dalam menyelesaikan tugas akhir ini serta semua pihak yang tidak dapat penulis sebutkan satu persatu.

Purwokerto, 18 Agustus 2022



Rio Darmawan

## DAFTAR ISI

TUGAS AKHIR.....	i
LEMBAR PENGESAHAN PEMBIMBING.....	ii
LEMBAR PENETAPAN PENGUJI .....	iii
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR .....	iv
KATA PENGANTAR .....	v
DAFTAR ISI.....	vi
DAFTAR TABEL.....	ix
DAFTAR GAMBAR .....	x
ABSTRAK .....	xi
<i>ABSTRACT</i> .....	xii
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1 Tinjauan Pustaka .....	5
2.2 Landasan Teori .....	10
2.2.1 <i>Cyber Attack</i> .....	10
2.2.2 <i>Teler</i> .....	10
2.2.3 <i>Directory Bruteforce attack</i> .....	10
2.2.4 <i>RealTime System</i> .....	10
2.2.3 <i>Apache2</i> .....	11
2.2.4 <i>Damn Vulnerable Web Application</i> .....	11
2.2.5 <i>DirSearch</i> .....	11
2.2.6 <i>Go Language</i> .....	11
2.2.7 <i>Mysql</i> .....	12

2.2.8	<i>Telegram</i> .....	12
2.2.9	<i>Discord</i> .....	12
2.2.10	<i>Slack</i> .....	12
BAB III METODOLOGI PENELITIAN.....		13
3.1	Objek dan Subjek Penelitian .....	13
3.2	Alat dan Bahan Penelitian .....	13
3.3	Diagram Alur Penelitian.....	14
3.3.1	Identifikasi Masalah dan Studi Literature .....	14
3.3.2	Pengumpulan data .....	15
3.3.3	Perancangan dan Implementasi <i>TELER</i> .....	15
3.3.4	Pengujian Teler .....	16
3.3.5	Evaluasi Hasil.....	16
3.3.6	Penulisan Laporan .....	16
BAB IV PENGUJIAN DAN ANALISIS .....		17
4.1	Arsitektur sistem.....	17
4.2	Tahapan Proses Pada Aplikasi Dirsearch .....	17
4.3	Instalasi Aplikasi Pendukung .....	18
4.3.1	Instalasi Aplikasi Apache2.....	18
4.3.2	Instalasi Aplikasi Mysql.....	19
4.3.3	Instalasi Aplikasi PHP .....	19
4.3.4	Instalasi Aplikasi Golang .....	20
4.4	Tampilan Halaman Utama Website Vuln Pada Webserver .....	20
4.5	Tahapan Proses Pada Aplikasi Teler .....	21
4.5.1	Konfigurasi <i>Log Format</i> Pada Aplikasi Teler.....	22
4.5.2	Konfigurasi autentikasi Telegram , Slack dan Discord.....	23
4.5.3	Script Bash Tambahan Untuk Menjalankan Teler .....	23
4.6	Pengujian Menggunakan Metode <i>Directory Bruteforce</i> .....	24
4.7	Pengujian Sistem IDS terhadap serangan directory bruteforce .....	24
4.7.1	Tampilan command line teler pada saat insiden penyerangan menggunakan metode <i>directory bruteforce</i> .....	24



4.7.2	Tampilan GUI teler pada saat insiden penyerangan menggunakan metode <i>directory bruteforce</i> .....	25
4.8	Analisa Hasil Pengujian .....	26
4.8.1	Pengujian Telegram sebagai media penerima informasi hasil serangan <i>directory bruteforce</i> .....	26
4.8.2	Pengujian Discord sebagai media penerima informasi hasil serangan <i>directory bruteforce</i> .....	29
4.8.3	Pengujian Slack sebagai media penerima informasi hasil serangan <i>directory bruteforce</i> .....	32
4.8.4	Hasil Pengujian Rentang Waktu Dari Telegram , Discord, Slack ..	34
BAB V KESIMPULAN DAN SARAN.....		35
5.1	Kesimpulan.....	35
5.2	Saran.....	35
DAFTAR PUSTAKA .....		36
LAMPIRAN.....		39

## DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu .....	8
Tabel 3. 1 Kebutuhan Perangkat Lunak .....	13
Tabel 4. 1 Pengujian Skenario .....	26
Tabel 4. 2 Analisa Hasil rentang waktu serangan pada aplikasi telegram .....	27
Tabel 4. 3 Analisa Hasil rentang waktu serangan pada aplikasi Discord .....	29
Tabel 4. 4 Analisa Hasil rentang waktu serangan pada aplikasi slack.....	32

## DAFTAR GAMBAR

Gambar 3. 1 Diagram Alur Penelitian .....	14
Gambar 3. 2 Perancangan dan Implementasi .....	15
Gambar 4. 1 arsitektur sistem pada pengujian teler .....	17
Gambar 4. 2 Penggunaan Dirsearch.....	18
Gambar 4. 3 instalasi Apache2 digunakan untuk <i>webserver</i> .....	19
Gambar 4. 4 proses instalasi Mysql digunakan untuk <i>database</i> pada <i>web dummy</i> .....	19
Gambar 4. 5 Instalasi PHP untuk mengeksekusi <i>web</i> pada <i>webserver</i> .....	20
Gambar 4. 6 Instalasi Golang untuk aplikasi pendukung tools TELER .....	20
Gambar 4. 7 Tampilan awal web Ketika diakses.....	21
Gambar 4. 8 <i>Clone</i> Repositori Teler dari Github.....	21
Gambar 4. 9 <i>Build Teler</i> .....	22
Gambar 4. 10 Konfigurasi Format Log pada Teler.....	22
Gambar 4. 11 Konfigurasi Autentikasi <i>Telegram, Slack</i> dan <i>Discord</i> sebagai penerima informasi. ....	23
Gambar 4. 12 Script Bash untuk menjalankan Teler dengan kondisi <i>Webserver</i> akan mati ketika terjadi serangan .....	23
Gambar 4. 13 Pengujian serangan menggunakan metode <i>directory bruteforce</i> .....	24
Gambar 4. 14 Log dari pengujian serangan menggunakan metode <i>directory bruteforce</i> .	24
Gambar 4. 15 Teler Mendeteksi serangan .....	25
Gambar 4. 16 Tampilan Dashboard teler saat terjadi serangan <i>directory bruteforce</i> .....	25
Gambar 4. 17 Wordlist yang digunakan pada pengujian skenario 1.....	26
Gambar 4. 18 notifikasi hasil pengujian <i>directory bruteforce</i> pada aplikasi telegram.....	28
Gambar 4. 19 Wordlist yang digunakan pada pengujian skenario 2.....	29
Gambar 4. 20 notifikasi hasil pengujian <i>directory bruteforce</i> pada aplikasi Discord .....	31
Gambar 4. 21 Wordlist yang digunakan pada pengujian skenario 3.....	32
Gambar 4. 22 notifikasi hasil pengujian <i>directory bruteforce</i> pada aplikasi Slack.....	34
Gambar 4. 23 hasil pengujian rentang waktu dari telegram , discord dan slack.....	34