

TUGAS AKHIR

**IMPLEMENTASI HONEYPY DENGAN *MALICIOUS TRAFFIC DETECTION SYSTEM* (MALTRAIL)
MENGUNAKAN ANALISIS DESKRIPTIF GUNA
UNTUK MENDETEKSI SERANGAN DOS PADA
SERVER**



HALIM ALFIDZAR

18102195

**PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2022**

TUGAS AKHIR

IMPLEMENTASI HONEYPY DENGAN *MALICIOUS TRAFFIC DETECTION SYSTEM* (MALTRAIL) MENGGUNAKAN ANALISIS DESKRIPTIF GUNA UNTUK MENDETEKSI SERANGAN DOS PADA SERVER

IMPLEMENTATION OF HONEYPY WITH MALICIOUS TRAFFIC DETECTION SYSTEM (MALTRAIL) USING DESCRIPTION ANALYSIS TO DETECT DOS ATTACKS ON SERVERS

Disusun Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer



**HALIM ALFIDZAR
18102195**

**PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2022**

HALAMAN PENGESAHAN PEBIMBING TUGAS AKHIR

IMPLEMENTASI HONEYPY DENGAN *MALICIOUS TRAFFIC DETECTION SYSTEM* (MALTRAIL) MENGGUNAKAN ANALISIS DESKRIPTIF GUNA UNTUK MENDETEKSI SERANGAN DOS PADA SERVER

IMPLEMENTATION OF HONEYPY WITH MALICIOUS TRAFFIC DETECTION SYSTEM (MALTRAIL) USING DESCRIPTION ANALYSIS TO DETECT DOS ATTACKS ON SERVERS

Dipersiapkan dan Disusun Oleh

HALIM ALFIDZAR

18102195

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tugas Akhir
Pada hari Senin, 21 Februari 2022

Pebimbing I



(Bitu Parga'Zen, S.Kom., M.Han)

NIDN. 0603089202

Tugas Akhir ini diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal, 25 Februari 2022

Kaprodi,

(Amalia Beladinna Arifa, S.Pd., M.Cs)

NIK. 0606019201

HALAMAN PENETAPAN PENGUJI TUGAS AKHIR

IMPLEMENTASI HONEYPY DENGAN *MALICIOUS TRAFFIC DETECTION SYSTEM* (MALTRAIL) MENGGUNAKAN ANALISIS DESKRIPTIF GUNA UNTUK MENDETEKSI SERANGAN DOS PADA SERVER

IMPLEMENTATION OF HONEYPY WITH MALICIOUS TRAFFIC DETECTION SYSTEM (MALTRAIL) USING DESCRIPTION ANALYSIS TO DETECT DOS ATTACKS ON SERVERS

Dipersiapkan dan Disusun Oleh

HALIM ALFIDZAR

18102195

**Tugas Akhir Telah diuji dan Dinilai Panitia Penguji Program
Studi Informatika**

Fakultas Informatika

Institut Teknologi Telkom Purwokerto

Pada Tanggal: 21 Februari 2022

Penguji I

Penguji II

(Arif Wirawan Muhammad, S.Kom., M.Kom)
NIDN. 0601098701

(Ipam Fuaddina Adam, S.T., M.Kom)
NIDN. 0614048403

LEMBAR PERNYATAAN KEASLIAAN TUGAS AKHIR

LEMBAR PERNYATAAN KEASLIAAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama Mahasiswa : Halim Alfidzar
NIM : 18102195
Program Studi : Teknik Informatika

Menyatakan bahwa Tugas Akhir dengan judul berikut:
IMPLEMENTASI HONEYPY DENGAN *MALICIOUS TRAFFIC DETECTION SYSTEM (MALTRAIL)* MENGGUNAKAN ANALISIS DESKRIPTIF GUNA UNTUK MENDETEKSI SERANGAN DOS PADA SERVER

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, 16 Februari 2022,
Yang Menyatakan,**

(Halim Alfidzar)

KATA PENGANTAR

Alhamdulillah puji syukur penulis panjatkan atas ke hadirat Allah SWT yang telah melimpahkan rahmat, hidayah dan karunia-Nya. Sholawat dan salam kepada Rasulullah SAW yang menjadi kiblat suri tauladan sepanjang zaman sehingga penulis dapat menyusun serta menyelesaikan Tugas Akhir ini dengan baik, dalam kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Dr. Arfianto Fahmi, S.T., M.T., IPM selaku Rektor Institut Teknologi Telkom Purwokerto.
2. Bapak Auliya Burhanuddin, S.Si., M.Kom selaku Dekan Fakultas Informatika Institut Teknologi Telkom Purwokerto.
3. Ibu Amalia Beladonna Arifa, S.Pd., M. Cs selaku Kepala Program Studi S1 Teknik Informatika Institut Teknologi Telkom Purwokerto.
4. Bapak Bitu Parga Zen, S.Kom., M.Han selaku dosen Pembimbing yang selalu memberikan solusi, ilmu serta membimbing dengan ikhlas dan sabar dalam menyelesaikan penulisan Tugas Akhir ini.
5. Ibu Dr. Tenia Wahyuningrum, S.Kom., M.T selaku Dosen Wali S1IF-06-F yang bersedia memberikan motivasi untuk berkembang lebih baik lagi dalam menyelesaikan penulisan Tugas Akhir ini.
6. Seluruh Bapak/Ibu Dosen Program Studi S1 Informatika Institut Teknologi Telkom Purwokerto yang telah memberikan bekal ilmu kepada penulis.
7. Ibunda tercinta Diah Puspitasari yang selalu memberikan kasih sayang tiada batas serta doa yang selalu dipanjatkan sehingga dalam pengerjaan Tugas Akhir ini diselesaikan dengan baik.
8. Rekan-rekan seperjuangan Kelas IF-06-F yang telah mempercayakan saya sebagai ketua kelas, semoga kalian selalu dalam keadaan yang baik.
9. Penulis menyadari bahwa penulisan Tugas Akhir ini masih jauh dari sempurna dikarenakan keterbatasan pengalaman dan pengetahuan yang dimiliki. Oleh karena itu, penulis mengharapkan adanya bentuk saran dan kritik yang

membangun dari segala pihak. Semoga laporan Tugas Akhir ini dapat bermanfaat dan menambah wawasan bagi pembaca.

Purwokerto, 16 Februari 2022,

Yang Menyatakan,

A handwritten signature in black ink, appearing to read 'Halim Alfidzar', written over a light pink rectangular background.

(Halim Alfidzar)

DAFTAR ISI

HALAMAN SAMPUL DALAM	ii
HALAMAN PENGESAHAN PEMBIMBING TUGAS AKHIR.....	iii
HALAMAN PENETAPAN PENGUJI TUGAS AKHIR.....	iv
LEMBAR PERNYATAAN KEASLIAAN TUGAS AKHIR	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	x
DAFTAR GAMBAR	xi
ABSTRAK	xii
ABSTRACT.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian.....	3
1.4 Batasan Masalah.....	3
1.5 Manfaat Penelitian.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1 Penelitian Sebelumnya	5
2.2 Dasar Teori	6
2.2.1 Insiden Keamanan Jaringan	6
2.2.2 DoS.....	9
2.2.3 Server	9
2.2.4 Honeypot.....	9
2.2.5 HoneyPy	11
2.2.6 Maltrail.....	11
2.2.7 VirtualBox.....	12

2.2.8	Linux	12
BAB III METODE PENELITIAN.....		14
3.1	Subjek dan Objek Penelitian	14
3.2	Diagram Alir Penelitian.....	14
3.2.1	Studi Literatur	14
3.2.2	Metode Penelitian.....	15
3.3	Pengumpulan Kebutuhan	15
3.4	Perancangan Konfigurasi	15
3.5	Implementasi	15
3.6	Pengujian Sistem	16
3.7	Analisis Hasil	17
3.8	Jadwal Penelitian.....	19
BAB IV HASIL DAN PEMBAHASAN		21
4.1	Hasil Pengumpulan Data	21
4.1.1	Pengelolaan Jaringan.....	21
4.1.2	Pengecekan IP	22
4.1.3	Konfigurasi.....	24
4.1.4	Hasil Serangan	25
4.2	Pembahasan	29
4.2.1	Perbandingan Hasil Serangan Yang Di Tangkap Maltrail.....	30
4.2.2	Hasil Keseluruhan Yang Di Tangkap Maltrail.....	31
BAB V KESIMPULAN DAN SARAN.....		35
5.1	Kesimpulan.....	35
5.2	Saran.....	35
DAFTAR PUSTAKA		36

DAFTAR TABEL

Tabel 3.1 Jadwal Penelitian.....	20
----------------------------------	----

DAFTAR GAMBAR

Gambar 2.1 Alur Perbedaan LIH dan HIH	11
Gambar 3.1 Diagram Alir Penelitian	14
Gambar 3.2 Diagram Alir Pengujian	16
Gambar 3.3 Simulasi Gambar	18
Gambar 4.1 Arsitektur.....	21
Gambar 4.2 Pengelolaan Jaringan.....	22
Gambar 4.3 IP Kali Linux.....	23
Gambar 4.4 IP CentOS	23
Gambar 4.5 IP Linux Mint.....	24
Gambar 4.6 Menjalankan Sensor.py	24
Gambar 4.7 Menjalankan Server.py.....	25
Gambar 4.8 Menjalankan Setup.py.....	25
Gambar 4.9 Nmap IP CentOS	26
Gambar 4.10 Nmap IP Linux Mint	26
Gambar 4.11 Ping IP CentOS.....	27
Gambar 4.12 Ping IP Linux Mint.....	27
Gambar 4.13 Hping3 CentOS.....	28
Gambar 4.14 Hping3 Linux Mint	28
Gambar 4.15 Nmap IP Linux Mint Yang Sudah Menggunakan HoneyPy.....	29
Gambar 4.16 Hasil Tanpa HoneyPY.....	30
Gambar 4.17 Hasil Menggunakan HoneyPy.....	31
Gambar 4.18 Hasil Gabungan	31
Gambar 4.19 Threats.....	32
Gambar 4.20 Events	32
Gambar 4.21 Severity.....	33
Gambar 4.22 Sources	33
Gambar 4.23 Trails.....	34