

**IMPLEMENTASI SISTEM PEMANTAUAN KEAMANAN JARINGAN
MENGUNAKAN HONEYPOT DAN ELK STACK (ELASTICSEARCH,
LOGSTASH, KIBANA) UNTUK DETEKSI KEAMANAN SIBER DI
UNJAYA**

TUGAS AKHIR

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



Disusun oleh:

TEGAR FATWA NUGROHO
212104020

**PROGRAM STUDI S-1 TEKNOLOGI INFORMASI
FAKULTAS TEKNIK & TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA
2025**

HALAMAN PENGESAHAN

TUGAS AKHIR

IMPLEMENTASI SISTEM PEMANTAUAN KEAMANAN JARINGAN MENGUNAKAN HONEYPOT DAN ELK STACK (ELASTICSEARCH, LOGSTASH, KIBANA) UNTUK DETEKSI KEAMANAN SIBER DI UNJAYA

Diajukan oleh:

TEGAR FATWA NUGROHO

212104020

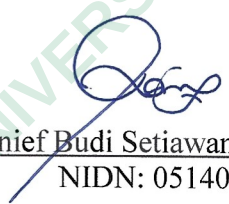
Telah dipertahankan di depan dewan penguji dan dinyatakan sah
sebagai salah satu syarat untuk memperoleh gelar Sarjana
di Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta

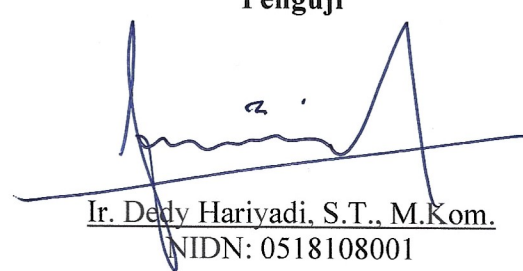
Tanggal: 02 Juli 2025

Mengesahkan:

Pembimbing

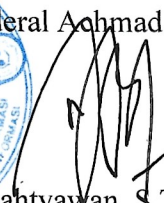
Penguji


Chanief Budi Setiawan., S.T., M.Eng.
NIDN: 0514068101


Ir. Dedy Hariyadi, S.T., M.Kom.
NIDN: 0518108001

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

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul: “Implementasi Sistem Pemantauan Keamanan Jaringan menggunakan Honeypot dan ELK Stack (Elasticsearch, Logstash, Kibana) Untuk Deteksi Keamanan Siber Di UNJAYA”. Penyusunan laporan ini merupakan salah satu persyaratan untuk menyelesaikan studi di Program Studi S-1 Teknologi Informasi Fakultas Teknik & Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta. Laporan ini dapat diselesaikan atas bimbingan, arahan, dan bantuan dari berbagai pihak. Pada kesempatan ini penulis dengan rendah hati mengucapkan terima kasih dengan setulus-tulusnya kepada:

1. Bapak Rama Sahtyawan, S.T., M.Cs.. selaku Ketua Program Studi S-1 Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
2. Bapak Chanief Budi Setiawan, S.T., M.Eng. selaku Dosen Pembimbing Tugas Akhir;
3. Bapak Arief Ikhwan Wicaksono, S. Kom., M.Cs. selaku Dosen Pembimbing Akademik;
4. Para dosen yang telah memberikan banyak bekal ilmu pengetahuan kepada penulis selama menjadi mahasiswa di Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
5. Orang tua penulis, yang telah memberikan dukungan semangat serta doa restu kepada saya, sehingga dapat menyelesaikan studi saya;
6. Rekan-rekan mahasiswa Prodi S-1 Teknologi Informasi Angkatan 21 di Universitas Jenderal Achmad Yani Yogyakarta yang sudah memberi dukungan dan kerja sama selama pembuatan tugas akhir.
7. Untuk diri saya sendiri yang telah berjuang dan bertahan hingga titik ini, melewati berbagai tantangan dengan semangat untuk terus belajar dan berkembang.
8. Untuk seseorang yang selalu menjadi sumber semangat, yang senantiasa memberi dukungan, motivasi, dan keyakinan kepada penulis di setiap langkah perjalanan ini.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari kata sempurna. Maka dari itu dengan segala kerendahan hati penulis sangat menghargai adanya kritik dan saran yang membangun dari semua pihak yang bersedia meluangkan waktu untuk membaca laporan tugas akhir ini.

Yogyakarta, 02 Juli 2025

Tegar Fatwa Nugroho

HALAMAN PERNYATAAN

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

Nama : Tegar Fatwa Nugroho
NPM : 212104020
Program Studi : S-1 Teknologi Informasi
Judul Tugas Akhir : Implementasi Sistem Pemantauan Keamanan Jaringan Menggunakan Honeypot dan ELK Stack (Elasticsearch, Logstash, Kibana) Untuk Deteksi Ancaman Siber Di UNJAYA

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, 02 Juli 2025



Tegar Fatwa Nugroho

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
KATA PENGANTAR.....	iii
HALAMAN PERNYATAAN.....	iv
DAFTAR ISI.....	v
DAFTAR TABEL	viii
DAFTAR GAMBAR.....	ix
DAFTAR LAMPIRAN	x
DAFTAR SINGKATAN	xi
INTISARI	xiii
ABSTRACT	xiv
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	2
1.3 Pertanyaan Penelitian	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Hasil Penelitian	3
1.6 Batasan Penelitian	3
BAB 2 TINJAUAN PUSTAKA DAN LANDASAN TEORI.....	5
2.1 Tinjauan Pustaka	5
2.2 Landasan Teori	10
2.2.1 Keamanan Jaringan	10
2.2.1 <i>Deception Technology</i>	11
2.2.2 Honeypot	11
2.2.3 OpenCanary.....	14
2.2.4 ELK Stack (Elasticsearch, Logstash, Kibana).....	16
2.2.5 NDLC (<i>Network Development Life Cycle</i>).....	18
2.2.6 Server	20

2.2.7	Proxmox	20
2.2.8	Tailscale	21
BAB 3 METODE PENELITIAN		23
3.1	Alat dan Bahan Penelitian	25
3.1.1	Perangkat Keras.....	25
3.1.2	Perangkat Lunak.....	25
3.1.3	Kebutuhan Jaringan.....	27
3.2	Jalan Penelitian	28
3.2.1	Tahap Analisis Kebutuhan	28
3.2.2	Tahap Perancangan.....	29
3.2.3	Tahap Simulasi Prototipe	29
3.2.4	Tahap Implementasi	29
3.2.5	Tahap <i>Monitoring</i>	30
3.2.6	Tahap Manajemen	30
3.3	Perancangan Arsitektur Sistem.....	30
3.4	Pemilihan Jenis Honeypot	32
3.5	Alur Integrasi Sistem	33
3.6	Desain Dashboard.....	35
BAB 4 HASIL PENELITIAN		38
4.1	Ringkasan Hasil Penelitian	38
4.2	Implementasi Sistem.....	39
4.2.1	Pembangunan Perangkat Honeypot.....	39
4.2.2	Implementasi ELK Stack.....	44
4.2.3	Pengujian Sistem	46
4.2.4	Implementasi Pada Jaringan Publik.....	49
4.3	Pembahasan	50
4.3.1	Periode <i>Monitoring</i>	50
4.3.2	Statistik Umum Aktivitas Jaringan.....	51
4.3.3	Visualisasi Data Hasil Monitoring	52
4.3.4	Analisis Pola Serangan	61
4.3.5	Kesimpulan Hasil Monitoring	64
4.4	Manajemen Sistem	65

BAB 5 KESIMPULAN DAN SARAN	68
5.1 Kesimpulan.....	68
5.2 Saran.....	69
DAFTAR PUSTAKA.....	71
LAMPIRAN.....	74

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR TABEL

Tabel 2.1 Ringkasan Tinjauan Pustaka	8
Tabel 3.1 Perbandingan Honeypot	33
Tabel 4.1 Tabel IP Perangkat	47
Tabel 4.2 IP Publik Server OpenCanary	49
Tabel 4.3 Tabel Statistik Umum.....	51
Tabel 4.4 Rekap Harian Aktivitas Serangan	54
Tabel 4.5 Username Pada Upaya Login Tidak Sah.....	57
Tabel 4.6 Sampel Log Berdasarkan Jenis Logtype	59
Tabel 4.7 Tabel IP Negara Penyerang.....	60

DAFTAR GAMBAR

Gambar 2.1 Arsitektur Teknologi Honeypot	13
Gambar 2.2 Arsitektur Fungsional Sistem OpenCanary	15
Gambar 3.1 Metode NDLC	23
Gambar 3.2 Rancangan Arsitektur Sistem	31
Gambar 3.3 Alur Integrasi Sistem	34
Gambar 4.1 Pembangunan Perangkat Honeypot OpenCanary	39
Gambar 4.2 Implementasi ELK Stack	45
Gambar 4.3 Lingkungan Jaringan Uji	47
Gambar 4.4 Hasil Deteksi Pada ELK Stack	48
Gambar 4.5 Dashboard Kibana - Bagian Atas	53
Gambar 4.6 Dashboard Kibana - Bagian Bawah	53
Gambar 4.7 Visualisasi Frekuensi Serangan	55
Gambar 4.8 Visualisasi Grafik Top IP Penyerang	56
Gambar 4.9 Visualisasi Port Tujuan Terbanyak diserang	57
Gambar 4.10 Kategori Log Aktivitas Serangan	58
Gambar 4.11 Negara Penyerang	60
Gambar 4.12 Lokasi Negara Penyerang	61

DAFTAR LAMPIRAN

Lampiran 1 Konfigurasi Sistem	74
Lampiran 2 Log Aktifitas	80
Lampiran 3 Hasil Monitoring Tambahan	88
Lampiran 4 Jadwal Penelitian	91
Lampiran 5 Kartu Bimbingan.....	92
Lampiran 6 Hasil Cek Plagiasi	93

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR SINGKATAN

BSSN	Badan Siber dan Sandi Negara
BIOS	<i>Basic Input Output System</i>
CPU	<i>Central Processing Unit</i>
CT	<i>Contrainers</i>
DDoS	<i>Distributed Denial of Service</i>
DNS	<i>Domain Name System</i>
ELK Stack	<i>Elasticsearch, Logstash, Kibana</i>
FTP	<i>File Transfer Protocol</i>
Git	<i>Group Inclusive Tour</i>
GUI	<i>Graphical User Interface</i>
HTTP	<i>Hypertext Transfer Protocol</i>
IDS	<i>Intrusion Detection System</i>
IP	<i>Internet Protocol</i>
IPS	<i>Intrusion Prevention System</i>
ISO	<i>International Organization for Standardization</i>
JSON	<i>JavaScript Object Notation</i>
KVM	<i>Kernel-based Virtual Machine</i>
LTS	<i>Long Term Support</i>
NAT	<i>Network Address Translation</i>
Nmap	<i>Network Mapper</i>
OpenVZ	<i>Operating-system-level Virtualization</i>
PBX	<i>Private Branch eXchange</i>
SMB	<i>Server Message Block</i>
RAM	<i>Random Access Memory</i>
RDP	<i>Remote Desktop Protocol</i>
SMT	<i>Satisfiability Modulo Theories</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SQL	<i>Structured Query Language</i>
SSH	<i>Secure Shell</i>

Telnet	<i>Teletype Network</i>
VCPU	<i>Virtual Central Processing Unit</i>
VE	<i>Virtual Environment</i>
VM	<i>Virtual Machines</i>
VPN	<i>Virtual Private Network</i>
VPS	<i>Virtual Private Server</i>

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA