

**OPTIMALISASI MONITORING SERANGAN
BRUTE FORCE PADA SSH MENGGUNAKAN
WAZUH BERBASIS OPEN SOURCE**

PRAKTEK KERJA LAPANGAN



Disusun oleh:

ENGIE RAMADHANI (22082010029)

**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL
"VETERAN" JAWA TIMUR SURABAYA
2025**

HALAMAN PENGESAHAN

Judul : OPTIMALISASI MONITORING SERANGAN BRUTE FORCE PADA SSH MENGGUNAKAN WAZUH BERBASIS OPEN SOURCE

Oleh : ENGIE RAMADHANI NPM. 22082010029

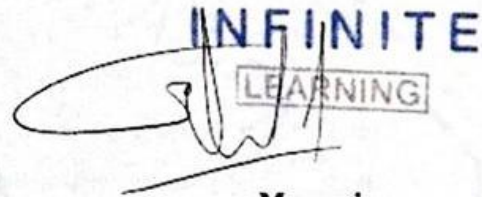
Menyetujui,

Dosen Pembimbing

Pembimbing Lapangan



Rizka Hadiwiyanti, S.Kom, M.Kom
NIP. 19860727 2018032 001



Marsani

Mengetahui,

Dekan

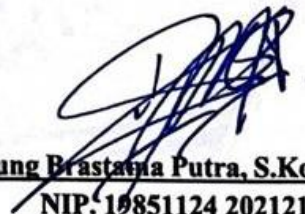
Koordinator

Fakultas Ilmu Komputer

Program Studi Sistem Informasi



Prof. Dr. Ir. Novirina Hendrasarie, MT.
NIP. 19681126 1994032 001



Agung Brastama Putra, S.Kom., M.Kom
NIP. 19851124 2021211 003

ABSTRAK

Keamanan server merupakan aspek krusial dalam pengelolaan sistem informasi, terutama dalam menghadapi serangan brute force yang sering menargetkan layanan *Secure Shell (SSH)*. Untuk mengoptimalkan monitoring terhadap serangan semacam ini, *Wazuh* sebuah platform keamanan *open source* dapat dimanfaatkan guna mendeteksi ancaman secara *real time*. Dalam implementasinya, *Wazuh* dikonfigurasi untuk mengenali percobaan login yang mencurigakan dan secara otomatis mengirimkan notifikasi kepada administrator. Pengujian menunjukkan bahwa *Wazuh* mampu memantau aktivitas *login SSH* secara efektif dan mengidentifikasi pola serangan *brute force* dengan tingkat akurasi yang tinggi. Dengan fitur seperti *alerting*, analisis *log*, dan integrasi dengan sistem keamanan lainnya, *Wazuh* menjadi solusi monitoring yang efisien. Hasil implementasi menunjukkan bahwa *Wazuh* layak digunakan sebagai bagian dari sistem pertahanan server karena mampu memberikan monitoring yang efisien, real-time, serta fleksibel tanpa biaya lisensi.

Kata Kunci: *Wazuh, brute force, SSH, monitoring, open source, keamanan server*

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat, taufik, dan hidayah-Nya sehingga penyusunan laporan praktek kerja lapangan (PKL) dapat diselesaikan dengan baik. Laporan ini disusun berdasarkan kegiatan Program Magang dan Studi Independen Bersertifikat di PT Kinema Systrans Multimedia (*Infinite Learning*) yang berjudul **Optimalisasi Monitoring Serangan Brute Force pada SSH Menggunakan Wazuh Berbasis Open Source**.

Adapun maksud dan tujuan penyusunan laporan Praktek Kerja Lapangan (PKL) ini adalah agar nantinya bermanfaat dalam penerapan ilmu pengetahuan di masa mendatang serta membantu mempersiapkan diri memasuki dunia kerja yang sebenarnya.

Penyusunan laporan ini tidak akan berhasil tanpa bantuan, bimbingan, arahan, serta doa dari banyak pihak yang memberikan dukungan penuh sepanjang proses berlangsung. Sebagai bentuk rasa hormat dan terima kasih yang tulus, ucapan terima kasih disampaikan kepada :

1. Kedua Orang tua tercinta, yang selalu menjadi sumber kekuatan dan inspirasi. Terimakasih atas dukungan materi, moril dan doa.
2. Bapak Mohamad Irwan Afandi, ST, M.Sc selaku Dosen Wali yang telah mendukung untuk mengikuti kegiatan studi independen baik rekomendasi maupun dengan memberikan saran serta nasihat yang bersifat membangun.
3. Ibu Rizka Hadiwiyanti, S.Kom, M.Kom, MBA, selaku Dosen Pembimbing Laporan Praktek Kerja Lapangan atas bantuan, bimbingan, serta arahan yang membangun dalam penyusunan Laporan PKL selama pelaksanaan kegiatan studi independen.
4. Tim Program Magang dan Studi Independen Bersertifikat di PT Kinema Systrans Multimedia (*Infinite Learning*) yang telah memberikan kesempatan kepada untuk magang dan studi independen periode tahun 2025 selama kurang lebih 5 bulan.

5. Kepada seluruh rekan-rekan Studi Independen di PT Kinema Systrans Multimedia (*Infinite Learning*) periode tahun 2025, terkhusus pada bidang *Computer Network & Security* dan Grup 3 *Massive* yang selalu memberikan semangat, serta pengalaman yang amat berharga.
6. Dan semua pihak yang tidak dapat disebutkan satu-persatu yang telah memberikan bantuan dan dukungan dalam Praktek Kerja Lapangan ini.

Penyusunan laporan ini masih terdapat banyak kekurangan. Oleh karena itu, kritik dan saran yang bersifat membangun diharapkan untuk penyempurnaan di masa mendatang. Akhir kata, semoga laporan ini dapat memberikan manfaat sebagaimana mestinya.

Surabaya, 10 Juni 2025



Engie Ramadhani

DAFTAR ISI

ABSTRAK.....	iii
KATA PENGANTAR	iv
DAFTAR ISI.....	vi
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN.....	xi
BAB I.....	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan PKL.....	2
1.4 Manfaat PKL.....	3
BAB II.....	4
2.1 Profil Organisasi	4
2.2 Tujuan Organisasi	6
2.3 Struktur Organisasi	7
2.4 Lingkup Organisasi.....	9
BAB III PELAKSANAAN PKL.....	11
3.1 Tinjauan Pustaka.....	11
3.1.1 Keamanan Jaringan Komputer.....	11
3.1.2 Serangan Brute Force.....	12
3.1.3 Protokol SSH (Secure Shell).....	13
3.1.4 Deteksi intrusi dan sistem monitoring keamanan	14
3.1.5 Wazuh	15

3.1.6	Analisis Log dan Manajemen Alert	17
3.1.7	Siklus Keamanan Siber Berdasarkan NIST Cybersecurity Framework	19
3.2	Waktu dan tempat pelaksanaan PKL	22
3.2.1	Tempat dan waktu penelitian	22
3.2.2	Pelaksanaan Praktek Kerja Lapangan	23
BAB IV HASIL DAN PEMBAHASAN		27
4.1	Studi Kasus	27
4.2	Arsitektur dan Lingkungan Pengujian	28
4.2.1	VM 1 (Attacker & Manager)	28
4.2.2	VM 2 (Target & Agent)	28
4.3	Implementasi Monitoring dan Simulasi Serangan	29
4.3.1	Instalasi dan Verifikasi Hydra	29
4.3.2	Simulasi Serangan SSH menggunakan Hydra	30
4.4	Instalasi dan Aktivasi Wazuh.....	30
4.4.1	Proses Instalasi	30
4.4.2	Verifikasi Layanan.....	33
4.5	Hasil Monitoring pada Wazuh Dashboard.....	35
4.5.1	Percobaan login SSH menggunakan username yang tidak dikenal.....	36
4.5.2	Kegagalan login yang berulang dalam waktu singkat	37
4.5.3	Indikasi upaya login yang tidak sah melalui sistem autentikasi PAM (Pluggable Authentication Modules)	38
4.6	Hasil dan Analisis Alert	40
4.6.1	Hasil Monitoring	40
4.6.2	Analisis Alert	41
4.6.3	Interpretasi Gabungan	42
4.7	Integrasi Siklus Proyek Cybersecurity (NIST CSF)	42

4.7.1	Identify (Mengidentifikasi)	43
4.7.2	Protect (Melindungi)	43
4.7.3	Detect (Mendeteksi)	44
4.7.4	Respond (Merespons)	45
4.7.5	Recover (Pulih)	45
4.8	Evaluasi dan Optimalisasi Monitoring.....	46
4.8.1	Evaluasi.....	46
4.8.2	Optimalisasi	47
4.9	Ringkasan Hasil Uji Keamanan <i>Brute Force SSH</i> Menggunakan <i>Wazuh</i>	48
BAB V PENUTUP		49
5.1	Kesimpulan	49
5.2	Saran	49
DAFTAR PUSTAKA		50
LAMPIRAN.....		52

DAFTAR TABEL

Tabel 3. 1 Timeline Pelaksanaan Praktek Kerja Lapangan	23
Tabel 3. 2 Logbook Kegiatan Praktek Kerja Lapangan	25
Tabel 4. 1 Timestamps per 30 menit	40

DAFTAR GAMBAR

Gambar 2. 1 Logo Infinite Learning.....	4
Gambar 2. 2 Struktur Organisasi Infinite Learning.....	7
Gambar 3. 1 Siklus Proyek Cybersecurity.....	19
Gambar 3. 2 Challenge Cycle.....	23
Gambar 3. 3 Challenge Journey	24
Gambar 4. 1 Ilustrasi Konfigurasi Hydra	29
Gambar 4. 2 Proses Instalasi Wazuh	31
Gambar 4. 3 Verifikasi Status Layanan Wazuh	32
Gambar 4. 4 Tampilan awal Wazuh Dashboard melalui antarmuka.....	33
Gambar 4. 5 Status Layanan dalam keadaan active (running)	34
Gambar 4. 6 Status Layanan Filebeat dalam keadaan active (running)	35
Gambar 4. 7 Alert “sshd: Attempt to login using a non-existent user” pada wazuh dashboard.....	36
Gambar 4. 8 Alert “PAM: User Login Failed” akibat login gagal secara berulang pada Wazuh.....	37
Gambar 4. 9 Log Wazuh yang menunjukkan kegagalan autentifikasi PAM sebagai indikasi Brute Force	38
Gambar 4. 10 Timestamp per 30 menit.....	41
Gambar 4. 11 Siklus Proyek Cybersecurity.....	42

DAFTAR LAMPIRAN

Lampiran 1 Surat Keterangan PKL (LoA)	52
Lampiran 2 Nilai Magang dan Studi Independen.....	53
Lampiran 3 Kode Konfigurasi Wazuh V1	54
Lampiran 4 Kode Konfigurasi Wazuh VM2.....	55
Lampiran 5 Kode Konfigurasi PowerShell/CMD untuk Akses ke Ubuntu VM....	56
Lampiran 6 Log Hasil Monitoring	57
Lampiran 7 Perintah-perintah instalasi (Script bash/automation Wazuh).....	59
Lampiran 8 Tampilan Dashboard Wazuh status agent.....	61
Lampiran 9 Tampilan Status API Connection pada Wazuh.....	61
Lampiran 10 Proses Instalasi, Konfigurasi, dan akses wazuh dashboard via browser	62
Lampiran 11 Sesi Mentoring dengan pembimbing	62
Lampiran 12 Kegiatan Magang Bersama Tim	63