

DAFTAR ISI

HALAMAN JUDUL	ii
LEMBAR PENGESAHAN	iii
PERNYATAAN KEASLIAN PENELITIAN	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL	ix
INTISARI	xi
<i>ABSTRACT</i>	xii
BAB I	1
PENDAHULUAN	1
1.1 Latar belakang	1
1.2 Rumusan Masalah	2
1.3 Alternatif – Alternatif Penyelesaian Masalah	2
1.4 Justifikasi Cara Penyelesaian Masalah	3
1.5 Tujuan dan Manfaat	3
BAB II	4
KAJIAN PUSTAKA	4
2.1 Dasar Teori	7
2.1.1 Security Operation Center (SOC)	7
2.1.2 Security Information and Event Management (SIEM)	8
2.1.3 <i>File Integrity Monitoring (FIM)</i>	9
2.1.4 <i>Virtual Private Server</i>	10
2.1.5 Algoritma <i>Hash</i>	11
2.1.6 Elastic Stack	11
2.1.7 Wazuh	13
2.1.8 <i>Linux Audit System</i>	16
2.1.9 Audit Daemon (Auditd)	18
2.1.10 <i>Secure Shell (SSH)</i>	18



2.1.11 Termius	19
2.1.12 Google Chrome	19
2.2 Hipotesis	23
BAB III	23
BAHAN DAN METODE PENELITIAN	24
3.1 Bahan	24
3.2 Peralatan	25
3.3 Tahapan Penelitian	25
3.5 Perancangan Sistem	27
3.5.1 Perancangan Topologi	27
3.5.2 Perancangan Sistem dan Instalasi	28
3.5.3 Pengujian Sistem	35
BAB IV	37
HASIL PENELITIAN DAN PEMBAHASAN	37
4.1 Hasil Pengujian <i>File Integrity Monitoring</i> Secara <i>Real-time</i>	37
4.2 Hasil Pengujian <i>File Integrity Monitoring</i> Pada Interval Waktu Tertentu	47
4.3 Pengujian untuk Mengetahui <i>User</i> yang Digunakan pada Sistem	53
4.4 Penyajian Data Diagram Peringatan pada <i>Wazuh Dashboard</i>	56
BAB V	58
PENUTUP	59
5.1 Kesimpulan	59
5.2 Saran	60
DAFTAR PUSTAKA	61
LAMPIRAN	64

DAFTAR GAMBAR

Gambar 2. 1 Arsitektur Wazuh	14
Gambar 2. 2 Komponen Wazuh dan <i>Data Flow</i>	15
Gambar 2. 3 Arsitektur Sistem Audit	17
Gambar 3. 1 Diagram alir instalasi	27
Gambar 3. 2 Topologi rancangan sistem	28
Gambar 3. 3 Diagram alir pengujian sistem	36
Gambar 4. 1 Peringatan <i>wazuh server</i> menambahkan <i>file</i> baru	38
Gambar 4. 2 Peringatan <i>file</i> baru melalui <i>wazuh dashboard</i>	39
Gambar 4. 3 Instalasi bahasa pemrograman	39
Gambar 4. 4 Peringatan <i>file</i> baru saat melakukan instalasi	40
Gambar 4. 5 Peringatan <i>whodata file</i> baru pada <i>wazuh server</i>	42
Gambar 4. 6 Peringatan <i>whodata file</i> baru	42
Gambar 4. 7 Peringatan <i>wazuh server</i> modifikasi <i>file</i>	44
Gambar 4. 8 Peringatan <i>wazuh dashboard</i> modifikasi <i>file</i>	45
Gambar 4. 9 Peringatan <i>wazuh server</i> menghapus <i>file</i>	46
Gambar 4. 10 Peringatan <i>wazuh dashboard</i> menghapus <i>file</i>	47
Gambar 4. 11 <i>Running file ossec.log</i> frekuensi <i>scan</i>	48
Gambar 4. 12 Peringatan <i>wazuh dashboard</i> interval waktu 10 menit	49
Gambar 4. 13 <i>Running file ossec.log scan_day</i> dan <i>scan_time</i>	49
Gambar 4. 14 Peringatan <i>wazuh dashboard scan_day</i> dan <i>scan_time</i>	50
Gambar 4. 15 Peringatan <i>wazuh dashboard</i> melakukan <i>scan</i> (10 November 2022)	51
Gambar 4. 16 Peringatan <i>wazuh dashboard</i> melakukan <i>scan</i> (17 November 2022)	51
Gambar 4. 17 Peringatan <i>wazuh dashboard</i> melakukan <i>scan</i> (24 November 2022)	52
Gambar 4. 18 Peringatan <i>wazuh dashboard</i> melakukan <i>scan</i> (1 Desember 2022)	53
Gambar 4. 19 Pembuatan <i>user</i> baru	54
Gambar 4. 20 File informasi <i>user</i>	54
Gambar 4. 21 <i>User aulia</i> membuat dan menghapus <i>file</i> direktori	55
Gambar 4. 22 <i>User Rizky</i> membuat dan menghapus <i>file</i> direktori	55
Gambar 4. 23 Memberikan akses <i>file</i> semua <i>user</i>	55
Gambar 4. 24 <i>User Nabila</i> memodifikasi <i>file</i>	55
Gambar 4. 25 Peringatan pada <i>dashboard</i> identifikasi <i>user</i>	56
Gambar 4. 26 Menambahkan dan menghapus beberapa <i>file</i> secara bersama	56
Gambar 4. 27 Peringatan menambahkan <i>file</i> secara bersamaan	57
Gambar 4. 28 Diagram pada <i>wazuh dashboard</i>	58

DAFTAR TABEL

Tabel 2. 1 Penelitian-penelitian terkait	20
Tabel 3. 1 Spesifikasi <i>wazuh platform</i>	24
Tabel 3. 2 Spesifikasi sistem operasi	24
Tabel 3. 3 Spesifikasi browser	25
Tabel 3. 4 Spesifikasi termius	25
Tabel 3. 5 Spesifikasi penggunaan server	25
Tabel 3. 6 Spesifikasi <i>laptop</i>	25