

DAFTAR ISI

HALAMAN COVER.....	i
LEMBAR PENGESAHAN	3
PERNYATAAN BEBAS PLAGIASI.....	4
KATA PENGANTAR.....	5
DAFTAR ISI.....	1
DAFTAR GAMBAR.....	4
DAFTAR TABEL	5
INTISARI	12
ABSTRACT	13
BAB I PENDAHULUAN.....	14
1.1 Latar Belakang	14
1.2 Rumusan Masalah	15
1.3 Batasan Masalah.....	16
1.4 Tujuan Penelitian	16
1.5 Manfaat Penelitian	16
1.6 Sistematika Penulisan	17
BAB II TINJAUAN PUSTAKA	18
2.1 <i>Intrusion Detection System (IDS)</i>	22
2.2 <i>Wazuh OpenSource Security Platform</i>	23
2.3 Elastic.....	26
2.4 Kibana	26
2.5 Hydra	26
2.6 Crowbar.....	27
2.7 NMAP	27
2.8 NGINX.....	27

2.9 Realtime.....	27
2.10 Hipotesis	28
BAB III METODE PENELITIAN	29
3.1 Waktu dan Tempat.....	29
3.2 Alat Penelitian.....	29
3.3 Bahan Penelitian	30
3.4 Tahapan Penelitian.....	32
3.5 Perancangan Sistem dan Instalasi	34
3.5.1 Perancangan Topologi	34
3.6 Instalasi dan Konfigurasi Server	35
3.6.1 Instalasi Docker.....	35
3.6.2 Instalasi Docker-compose.....	35
3.6.3 Instalasi Portainer	36
3.6.4 Instalasi Wazuh.....	36
3.6.5 Instalasi Wazuh Agent	37
3.7 Tahap Pengujian.....	38
3.7.1 Dashboard Wazuh	38
3.7.2 Dashboard Portainer	39
3.7.3 Penambahan Wazuh Agent.....	40
3.7.4 Percobaan Serangan	40
BAB IV HASIL DAN ANALISIS.....	44
4.1 Hasil dan Analisis Pengujian Response Time Wazuh.....	44
4.1.1 Response Time terhadap serangan SSH bruteforce	44
4.1.2 Response Time terhadap Port Scanning.....	48
4.2 Pengujian Penggunaan Resource CPU Wazuh server	51
4.2.1 Penggunaan resource CPU pada Wazuh All-in-One Server	51

4.2.2	Penggunaan resource CPU pada Wazuh Distributed Server	53
4.3	Pengujian Resource Memory pada Wazuh Server	54
4.3.1	Penggunaan resource Memory pada Wazuh All-in-One Server	54
4.3.2	Penggunaan resource Memory pada Wazuh Distributed Server	56
BAB V PENUTUP.....		58
5.1	Kesimpulan	58
5.2	Saran	58
DAFTAR PUSTAKA.....		59
LAMPIRAN.....		61

DAFTAR GAMBAR

Gambar 2. 1 Gambar Struktur NIDS bekerja	22
Gambar 2. 2 Struktur HIDS bekerja	23
Gambar 3. 1 Diagram Alir Penelitian	34
Gambar 3. 2 Topologi Sistem Wazuh All-in-One deployment	35
Gambar 3. 3 Topologi Wazuh Distributed deployment	36
Gambar 3. 4 Halaman Dashboard Wazuh	40
Gambar 3. 5 Halaman Dashboard Portainer	40
Gambar 3. 6 Halaman Dashboard Wazuh Agents	41
Gambar 3. 7 Topologi Pengujian Serangan SSH Bruteforce	42
Gambar 3. 8 Dashboard Security Events Wazuh	43
Gambar 3. 9 Topologi Pengujian Port Scanning	43
Gambar 3. 10 Dashboard Security Events Wazuh	44
Gambar 4. 1 Grafik Response Time terhadap serangan SSH bruteforce pada Wazuh All-in-one server	47
Gambar 4. 2 Grafik Response Time terhadap serangan SSH bruteforce pada Wazuh Distributed server	49
Gambar 4. 3 Grafik Response Time terhadap Port Scanning pada Wazuh All-in-One server	50
Gambar 4. 4 Grafik Response Time terhadap Port Scanning pada Wazuh Distributed server	52
Gambar 4. 5 Grafik Penggunaan Resource CPU Wazuh server All-in-One	53
Gambar 4. 6 Grafik Penggunaan Resource CPU Wazuh server Distributed	55
Gambar 4. 7 Penggunaan Resource Memory Wazuh All-in-One server	56
Gambar 4. 8 Penggunaan Resource Memory Wazuh Distributed server	57

DAFTAR TABEL

Tabel 2. 1 Ringkasan sumber jurnal penelitian	20
Tabel 3. 1 Spesifikasi Laptop	29
Tabel 3. 2 Spesifikasi Server Development PT. Emporia Digital Raya	29
Tabel 3. 3 Spesifikasi Docker	30
Tabel 3. 4 Spesifikasi Kibana	31
Tabel 3. 5 Spesifikasi Elasticsearch	31
Tabel 3. 6 wazuh-manager	31
Tabel 3. 7 Spesifikasi Wazuh-agent.....	31
Tabel 3. 8 Spesifikasi Parrot Security OS.....	32
Tabel 4. 1 Nilai response time terhadap serangan SSH bruteforce pada Wazuh All-in-one server	45
Tabel 4. 2 Nilai response time terhadap serangan SSH bruteforce pada Wazuh Distributed server	47
Tabel 4. 3 Nilai response time terhadap Port Scanning pada Wazuh All-in-One server.....	49
Tabel 4. 4 Response Time Port Scanning pada Wazuh Distributed server	50
Tabel 4. 5 Nilai Penggunaan Resource CPU pada Wazuh server All-in-One	52
Tabel 4. 6 Nilai penggunaan Resource CPU Time pada Wazuh Distributed.....	53
Tabel 4. 7 Penggunaan Resource Memory pada Wazuh server All-in-One.....	55
Tabel 4. 8 Penggunaan Resource Memory pada Wazuh Distributed server	56