UNIVERSITAS GADJAH MADA
Analisis Performa High Availability Security Operation Center Menggunakan Docker Swarm dengan Teknik Failover di PT. Emporia Digital Raya
STEPHANI A DHEA N, Hidayat Nur Isnianto S.T., M.Eng.
Universitas Gadjah Mada, 2022 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN PENGESAHAN iii
PERNYATAAN BEBAS PLAGIASI iv
KATA PENGANTAR v
DAFTAR ISI vii
DAFTAR GAMBAR x
DAFTAR TABEL xi
INTISARI xii
ABSTRACT xiii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Tujuan Penelitian 2
1.4 Batasan Masalah 3
1.5 Manfaat Penelitian 3
1.6 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 5
2.1 Tinjauan Pustaka 5
2.2 Dasar Teori 10
2.2.1 Virtualisasi 10
2.2.2 *High Availability* 10
2.2.3 *Failover* 11
2.2.4 Docker *Container* 11
2.2.5 Docker Swarm 12
2.2.6 Wazuh *Security Platform* 13
2.2.7 ELK *Stack* 14
2.3 Hipotesis 14
BAB III BAHAN DAN METODE PENELITIAN 15
3.1 Waktu dan Tempat Penelitian 15
3.2 Alat Penelitian 15
3.3 Bahan Penelitian 15
3.4 Metode Penelitian 16
3.5 Perancangan Sistem 17

UNIVERSITAS
GADJAH MADA
**Analisis Performa High Availability Security Operation Center Menggunakan Docker Swarm dengan Teknik
Failover di PT. Emporia Digital Raya**
STEPHANI A DHEA N, Hidayat Nur Isnianto S.T., M.Eng.
Universitas Gadjah Mada, 2022 | Diunduh dari http://etd.repository.ugm.ac.id/

3.5.1 Rancangan Topologi 18
3.6 Instalasi dan Konfigurasi Jaringan 21
3.6.1 Membuat Virtual Server pada Virtualbox 21
3.6.2 Melakukan Instalasi Sistem Operasi pada Virtual Server 24
3.6.3 Melakukan Instalasi Docker dan Docker *Compose* 25
3.6.4 Menjalankan Docker Swarm pada Sistem *High Availability Security Operation Center* pada Docker Swarm 26
3.6.5 Melakukan Instalasi dan Konfigurasi pada Sistem *Security Operation Center*…… 26
3.6.6 Melakukan Instalasi dan Konfigurasi pada Sistem *High Availability Security Operation Center* pada Docker Swarm 27
3.6.7 Melakukan Pemasangan Wazuh-*Agent* pada Virtual Server 27
3.7 Skenario Pengujian 28
3.7.1 Pengujian Fungsional 28
3.7.2 Pengujian Failover 31
3.7.3 Pengujian *Resource* 34
3.7.4 Perhitungan Data Pengujian 35
BAB IV HASIL PENELITIAN DAN PEMBAHASAN 36
4.1 Pengujian Fungsional 36
4.1.1 Pengujian Validasi 36
4.1.2 Pengujian Serangan 37
4.2 Pengujian *Failover* 40
4.3 Pengujian *Resource* 42
4.3.1 Pengujian *Resource* CPU 43
4.3.2 Pengujian *Resource Memory* 46
BAB V PENUTUP 51
5.1 Kesimpulan 51
5.2 Saran 51
DAFTAR PUSTAKA 52
Lampiran 1. File .yml Docker Compose Wazuh 56
Lampiran 2. File .yml Docker Stack Portainer 59
Lampiran 3. Dashboard Wazuh 61
Lampiran 4. Dashboard Portainer Mode Swarm 62
Lampiran 5. Serangan brute-force SSH 63

UNIVERSITAS
GADJAH MADA
**Analisis Performa High Availability Security Operation Center Menggunakan Docker Swarm dengan Teknik
Failover di PT. Emporia Digital Raya**
STEPHANI A DHEA N, Hidayat Nur Isnianto S.T., M.Eng.
Universitas Gadjah Mada, 2022 | Diunduh dari http://etd.repository.ugm.ac.id/

Lampiran 6. Serangan port-scanning 64
Lampiran 7. Tampilan Monitoring Glances 65

UNIVERSITAS
GADJAH MADA
**Analisis Performa High Availability Security Operation Center Menggunakan Docker Swarm dengan Teknik
Failover di PT. Emporia Digital Raya**
STEPHANI A DHEA N, Hidayat Nur Isnianto S.T., M.Eng.
Universitas Gadjah Mada, 2022 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR GAMBAR

Gambar 2.1 Virtualisasi (openclipart.org, 2021) 10
Gambar 2.2 Docker *Container* (Docker.com, 2022) 12
Gambar 2.3 Docker Swarm (Fawzy, 2018) 13
Gambar 2.4 Skema Arsitektur Wazuh (wazuh.com, 2021) 13
Gambar 2.5 Skema ELK Stack (Raj, 2020) 14
Gambar 3.1 Diagram Alir Penelitian 16
Gambar 3.2 Topologi *Security Operation Center* 18
Gambar 3.3 Topologi *High Availability Security Operation Center* 20
Gambar 3.4 Menentukan nama dan sistem operasi 22
Gambar 3.5 Pengaturan besaran memori 22
Gambar 3.6 Membuat virtual hardisk baru 23
Gambar 3.7 Menentukan tipe harddisk 23
Gambar 3.8 Menentukan ukuran virtual harddisk 24
Gambar 3.9 Versi Sistem Operasi Centos 24
Gambar 3.10 Versi Sistem Operasi Ubuntu 25
Gambar 3.11 *Node Cluster* Swarm 26
Gambar 3.12 Skema Penyerangan SOC 29
Gambar 3.13 Skema Penyerangan HA-SOC 30
Gambar 3.13 Skema Pengujian *Failover* 32
Gambar 3.14 *Dashboard* HA-SOC Swarm *Leader* 33
Gambar 3.15 *Dashboard* HA-SOC Swarm *Worker* 1 34
Gambar 3.16 *Dashboard* HA-SOC Swarm *Worker* 2 34
Gambar 3.17 *Cluster Visualizer* Portainer HA-SOC 35
Gambar 4.1 Rata-rata *Response Time* Serangan *Brute-force* SSH 38
Gambar 4.2 *Response Time* Serangan *Port Scanning* 40
Gambar 4.3 Pengujian *Failover Worker-1* Mati 42
Gambar 4.4 Pengujian *Failover Worker-2* Mati 42
Gambar 4.5 Penggunaan CPU Serangan *Brute-force* SSH 44
Gambar 4.6 Penggunaan CPU Serangan *Port Scanning* 46
Gambar 4.7 Penggunaan *Memory* Serangan *Brute-force SSH* 48
Gambar 4.8 Penggunaan *Memory* Serangan *Port Scanning* 50

UNIVERSITAS
GADJAH MADA
**Analisis Performa High Availability Security Operation Center Menggunakan Docker Swarm dengan Teknik
Failover di PT. Emporia Digital Raya**
STEPHANI A DHEA N, Hidayat Nur Isnianto S.T., M.Eng.
Universitas Gadjah Mada, 2022 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR TABEL

Tabel 2.1 Ringkasan Jurnal Penelitian 8
Tabel 2.1 (Lanjutan) Ringkasan Jurnal Penelitian..... 9
Tabel 3.1 Spesifikasi Laptop 15
Tabel 3.2 Spesifikasi Server 21
Tabel 4.1 Data Hasil Pengujian Validasi..... 36
Tabel 4.2 *Response Time* Serangan *Brute-force SSH*..... 37
Tabel 4.2 (Lanjutan) *Response Time* Serangan *Brute-force SSH* 38
Tabel 4.3 *Response Time* Serangan *Port Scanning* 39
Tabel 4.4 Pengujian *Failover* 41
Tabel 4.5 Penggunaan CPU Serangan *Brute-force SSH*..... 43
Tabel 4.6 Penggunaan CPU Serangan *Port Scanning*..... 45
Tabel 4.7 Penggunaan *Memory* Serangan *Brute-force SSH* 47
Tabel 4.8 Penggunaan *Memory* Serangan *Port Scanning* 49