

DAFTAR GAMBAR

Gambar 3.1 Tahapan Pengerjaan	11
Gambar 3.2 Gambaran Umum.....	13
Gambar 3.3 Gambaran Umum Proses	13
Gambar 3.4 <i>Flowchart Regular Expression</i>	14
Gambar 3.5 <i>Flowchart ELK Stack</i>	15
Gambar 3.6 DFD <i>Level 0</i>	15
Gambar 3.7 DFD <i>Level 1 Regular Expression</i>	16
Gambar 3.8 DFD <i>Level 1 ELK Stack</i>	16
Gambar 3.9 DFD <i>Level 2 ELK Stack</i>	17
Gambar 4.1 Proses <i>String Matching</i>	23
Gambar 4.2 Hasil <i>Logs String Matching</i>	24
Gambar 4.3 Perintah <i>Install Java</i>	25
Gambar 4.4 Perintah pengecekan versi Java	25
Gambar 4.5 <i>GNU Privacy Guard (GPG) Elastic</i>	26
Gambar 4.6 Perintah <i>Update Sistem</i>	26
Gambar 4.7 <i>Repository Elastic</i>	26
Gambar 4.8 Perintah <i>Install ELK Stack</i>	26
Gambar 4.9 <i>Repository Metricbeat Dan Perintah Instalasi Metricbeat</i>	26
Gambar 4.10 <i>File Konfigurasi Directory Elasticsearch</i>	27
Gambar 4.11 Konfigurasi <i>Elasticsearch</i>	27
Gambar 4.12 Perintah Menjalankan <i>Elasticsearch</i>	27
Gambar 4.13 Perintah <i>Curl Elasticsearch</i>	27
Gambar 4.14 Perintah Ekstraksi dan <i>Move Geolitecity2</i>	28
Gambar 4.15 Perintah Konfigurasi <i>Logstash</i>	28
Gambar 4.16 <i>Input.conf</i>	29
Gambar 4.17 <i>Filter.conf Diona</i>	29
Gambar 4.18 <i>Filter.conf Cowrie</i>	30
Gambar 4.19 <i>Output.conf</i>	31
Gambar 4.20 Perintah Menjalankan <i>Logstash</i>	31
Gambar 4.21 <i>File Konfigurasi Directory Kibana</i>	31

Gambar 4.22 Konfigurasi Kibana.yml.....	32
Gambar 4.23 Perintah Menjalankan Kibana.....	32
Gambar 4.24 <i>Performance</i> CPU ELK Stack	37
Gambar 4.25 <i>Performance I/O operation</i> ELK Stack	38
Gambar 4.26 <i>Ram Usage</i> ELK Stack	38
Gambar 4.27 Visualisasi <i>Log</i> IoT Honeypot Dst IP	39
Gambar 4.28 Visualisasi <i>Log</i> IoT Honeypot Dst <i>Port</i>	39
Gambar 4.29 Visualisasi <i>Log</i> IoT Honeypot Src IP.....	40
Gambar 4.30 Visualisasi <i>Log</i> IoT Honeypot Src <i>Port</i>	40
Gambar 4.31 Visualisasi <i>Log</i> IoT Honeypot <i>Username</i>	41
Gambar 4.32 Visualisasi <i>Log</i> IoT Honeypot <i>Password</i>	41
Gambar 4.33 Visualisasi <i>Dionaea Pattern 1 Remote Hostname</i>	42
Gambar 4.34 Visualisasi <i>Dionaea Pattern 2 Remote Hostname</i>	42
Gambar 4.35 Visualisasi <i>Dionaea Pattern 1 Remote port</i>	43
Gambar 4.36 Visualisasi <i>Dionaea Pattern 2 Remote_port</i>	43
Gambar 4.37 Visualisasi <i>Dionaea Pattern 1 Local Port</i>	44
Gambar 4.38 Visualisasi <i>Dionaea Pattern 2 Local Port</i>	44
Gambar 4.39 Visualisasi <i>Dionaea Pattern 1 Connection Transport</i>	45
Gambar 4.40 Visualisasi <i>Dionaea Pattern 1 Concection Type</i>	45
Gambar 4.41 Visualisasi <i>Dionaea Pattern 1 Concection Type</i>	46
Gambar 4.42 Visualisasi <i>Cowrie Pattern 1 Src IP</i>	46
Gambar 4.43 Visualisasi <i>Cowrie Pattern 2 Src IP</i>	47
Gambar 4.44 Visualisasi <i>Cowrie paterrn 2 Dst Port</i>	47
Gambar 4.45 Visualisasi <i>Cowrie Paterrn 2 Src Port</i>	48
Gambar 4.46 Visualisasi <i>Cowrie Pattern 1 Username</i>	48
Gambar 4.47 Visualisasi <i>Cowrie Pattern 1 Password</i>	49