

## DAFTAR ISI

HALAMAN PENGESAHAN.....	ii
HALAMAN PERSEMBAHAN .....	iii
KATA PENGANTAR .....	iv
DAFTAR ISI.....	vi
DAFTAR TABEL.....	xi
DAFTAR GAMBAR .....	xii
DAFTAR SINGKATAN.....	xv
Intisari.....	xix
<i>Abstract</i> .....	xx
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	6
1.3 Batasan Masalah.....	6
1.4 Tujuan Penelitian.....	7
1.5 Manfaat Penelitian.....	7
1.6 Metodologi Penelitian.....	8
1.7 Sistematika Penelitian.....	9
BAB 2 TINJAUAN PUSTAKA DAN DASAR TEORI.....	10
2.1 Tinjauan Pustaka.....	10

2.1.1 Penelitian Terkait <i>honeypot</i> kontemporer.....	10
2.1.2 Penelitian Terkait <i>honeypot</i> berbasis <i>platform</i> .....	11
2.2 Dasar Teori.....	14
2.2.1 <i>Honeypot</i> .....	14
2.2.2 <i>Modern Honey Network : MHN</i> .....	16
2.2.3 <i>Honeymap</i> .....	18
2.2.4 Sensor.....	19
2.2.4.1 <i>Snort</i> .....	20
2.2.4.2 <i>Suricata</i> .....	20
2.2.4.3 <i>Conpot</i> .....	21
2.2.4.4 <i>Kippo</i> .....	22
2.2.4.5 <i>Amun</i> .....	23
2.2.4.6 <i>Glastopf</i> .....	25
2.2.4.7 <i>Wordpot</i> .....	25
2.2.4.8 <i>Shockpot</i> .....	25
2.2.4.9 <i>p0f</i> .....	26
2.2.4.10 <i>Dionaea</i> .....	26
2.2.5 <i>Mnemosyne</i> .....	28
2.2.6 <i>Hpfeeds</i> .....	36
2.2.7 ELK ( <i>Elasticsearch, Logstash, Kibana</i> ).....	39

BAB 3 METODE PENELITIAN.....	42
3.1 Bahan Penelitian.....	42
3.2 Alat Penelitian.....	42
3.2.1 Perangkat Keras .....	42
3.2.2 Perangkat Lunak.....	45
3.2.3 Arsitektur Perangkat Lunak dan Perangkat Keras.....	49
3.3 Alur Penelitian.....	51
3.3.1 Identifikasi Masalah .....	52
3.3.2 Instalasi Server MHN [2].....	52
3.3.3 Konfigurasi Sensor <i>Honeypot</i> .....	53
3.3.4 Implementasi Sensor dengan Server MHN.....	55
3.3.5 Uji Coba Server MHN.....	56
3.3.6 Implementasi MHN dengan <i>platform</i> ELK.....	56
3.3.7 Analisis Data.....	59
3.3.8 Penulisan Laporan.....	59
BAB 4 HASIL DAN PEMBAHASAN.....	60
4.1 Pengembangan Server MHN.....	60
4.1.1 Instalasi dan Konfigurasi <i>Backend</i> Server MHN.....	60
4.1.2 <i>Honeymap</i> pada Server MHN.....	64
4.1.3 <i>Dashboard</i> Server MHN.....	65
4.1.3.1 Konfigurasi Akses <i>Login</i> pada <i>Dashboard</i> .....	67

4.1.3.2 Pengembangan Sensor Melalui <i>Dashboard</i> .....	68
4.1.3.3 Halaman <i>Attack Report</i> .....	69
4.1.4 Ringkasan Pengembangan Server MHN.....	70
4.2 Pengembangan Sensor/ <i>Honeypot</i> .....	71
4.2.1 Pengembangan Sensor Publik.....	72
4.2.1.1 Pengembangan Sensor <i>Kippo</i> .....	72
4.2.1.2 Pengembangan Sensor <i>Dionaea</i> .....	81
4.2.2 Pengembangan Sensor <i>Private</i> .....	103
4.2.2.1 Pengembangan Sensor <i>p0f</i> .....	103
4.2.2.2 Pengembangan Sensor <i>Snort</i> .....	106
4.2.3 Analisis Perbandingan Sensor Publik dan Sensor <i>Private</i> .....	112
4.2.4 Ringkasan Pengembangan Sensor/ <i>Honeypot</i> .....	116
4.2.5 Rekomendasi Pemasangan Sensor.....	117
4.3 Implementasi ELK ( <i>Elasticsearch, Logstash, Kibana</i> ).....	118
4.3.1 Hasil Konfigurasi ( <i>back-end</i> ).....	118
4.3.1.1 Analisis Instalasi <i>Elasticsearch</i> .....	123
4.3.1.2 Analisis Instalasi <i>Kibana</i> .....	124
4.3.1.3 Analisis Instalasi <i>Logstash</i> .....	125
4.3.1.4 Analisis Konfigurasi ELK.....	126
4.3.2 Konfigurasi <i>Widget</i> dan <i>Dashboard</i> ( <i>front-end</i> ).....	141
4.3.2.1 Inisiasi <i>Dashboard Kibana</i> .....	141

4.3.2.2 Visualisasi <i>Widget</i> pada <i>Dashboard Kibana</i> .....	143
4.3.3 Analisis Data <i>Malicious Activity (Threat)</i> .....	145
4.3.4 Ringkasan Implementasi Server MHN dan <i>Platform ELK</i> .....	161
4.3.5 Uji Coba Perbandingan <i>Dashboard Utama</i> dan <i>Dashboard Kibana</i> .....	163
4.3.6 Rekomendasi Hasil Analisis Data <i>Malicious Activity (Threat)</i> .....	165
BAB 5 SARAN DAN KESIMPULAN.....	167
5.1 Kesimpulan.....	167
5.2 Saran.....	168
DAFTAR PUSTAKA.....	171
LAMPIRAN.....	173