

## DAFTAR ISI

HALAMAN JUDUL.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN .....	iv
KATA PENGANTAR .....	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR .....	ix
DAFTAR TABEL.....	xi
INTISARI.....	xii
<i>ABSTRACT</i> .....	xiii
BAB I. PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
1.6 Sistematika Penulisan.....	4
BAB II. TINJAUAN PUSTAKA.....	6
2.1 Aktivitas <i>Blackhat</i> dalam Jaringan.....	6
2.1.1 Fase <i>Hacking</i> yang Dilakukan oleh <i>Blackhat</i> .....	6
2.1.2 Serangan <i>Port</i> sebagai Jalan Masuk <i>Blackhat</i> .....	7
2.2 <i>Malware</i> .....	8
2.2.1 <i>Hashing</i> untuk <i>Fingerprint Malware</i> .....	9
2.2.2 <i>Scanning Malware</i> Menggunakan <i>Engine Antivirus</i> .....	9
2.3 <i>Honeypot</i> sebagai Sensor dan <i>Logging</i> Aktivitas <i>Blackhat</i> .....	12
2.3.1 <i>Honeypot</i> Berdasarkan Level Interaksi Penyerangan.....	12
2.3.2 <i>Dionaea</i> sebagai Alat Mengumpulkan Informasi Serangan .....	17
2.4 <i>Honeypot</i> Terdistribusi .....	19
2.5 Analisis <i>Log</i> Serangan Menggunakan Data <i>Mining</i> .....	20
2.5.1 <i>Clustering</i> untuk Mengelompokkan Data .....	21

2.5.2 Penggunaan <i>K-Means Clustering</i> dalam Partisi Data Serangan .	21
2.6 Deteksi Aktivitas <i>Blackhat</i> Dengan Visualisasi Pola Serangan .....	23
2.7 Hipotesis .....	23
<b>BAB III. BAHAN DAN METODE PENELITIAN</b> .....	<b>25</b>
3.1 Bahan .....	25
3.2 Peralatan .....	25
3.3 Tahapan Penelitian .....	25
3.3.1 Menjalankan Sistem MHN .....	27
3.3.2 Integrasi <i>Honeypot</i> Dionaea sebagai Sensor .....	28
3.3.3 Pengembangan dan Instalasi <i>Tools</i> HoneynetMiner .....	30
3.3.4 Pengambilan dan Pemisahan Data Serangan .....	33
3.3.5 Analisis dan Visualisasi Data .....	35
3.4 Rancangan Topologi Jaringan .....	45
<b>BAB IV. HASIL PENELITIAN DAN PEMBAHASAN</b> .....	<b>47</b>
4.1 Hasil Tampilan HoneynetMiner .....	47
4.1.1 Hasil Tampilan <i>Dashboard</i> .....	48
4.1.2 Hasil Tampilan Detil Koneksi Serangan .....	49
4.1.3 Hasil Tampilan Propagasi Serangan .....	50
4.1.4 Hasil Tampilan Sumber Lokasi Serangan .....	52
4.2 Hasil Analisis Alamat IP Teratas .....	53
4.2.1 Hasil Identifikasi Pola Distribusi Serangan 110.172.171.126.....	56
4.2.2 Hasil Identifikasi Pola Distribusi Serangan 5.235.235.107.....	58
4.2.3 Hasil Identifikasi Pola Distribusi Serangan 62.210.101.115.....	60
4.2.4 Hasil Identifikasi Pola Distribusi Serangan 94.136.40.37.....	62
4.2.5 Hasil Identifikasi Pola Distribusi Serangan 94.136.40.103.....	64
4.3 Hasil Analisis <i>Clustering</i> Serangan <i>Port</i> .....	66
4.4 Hasil Analisis <i>Hash Malware</i> .....	68
4.4.1 Hasil Identifikasi Varian <i>Worm</i> .....	70
4.4.2 Hasil Identifikasi Varian Trojan .....	71
4.4.3 Hasil Identifikasi Varian <i>Malware Generic</i> .....	72
4.4.4 Hasil Identifikasi Varian <i>Backdoor</i> .....	73
4.4.5 Hasil Identifikasi Varian Virus .....	74



4.4.5 Hasil Identifikasi Varian <i>Adware</i> .....	75
BAB V. PENUTUP.....	77
5.1 Kesimpulan.....	77
5.2 Saran.....	78
DAFTAR PUSTAKA .....	79
LAMPIRAN	