

DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PENGESAHAN.....	iii
PERNYATAAN BEBAS PLAGIASI	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL.....	x
INTISARI.....	xi
<i>ABSTRACT</i>	xii
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	3
1.6. Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	5
2.1. <i>Honeypot</i>	5
2.2. <i>Application Programming Language</i> (API).....	6
2.3. Migrasi Data	7
2.4. Hipotesis.....	11
BAB III METODE PENELITIAN	12
3.1. Peralatan	12
3.2. Bahan	13
3.3. Tahapan Penelitian.....	14
3.4. Tahap Pemasangan dan Konfigurasi Sistem	16
3.2.1. Perancangan Sistem Pengambilan Data pada <i>Honeypot</i> <i>Dionaea</i>	16
3.2.2. Perancangan Topologi	20
3.2.3. Pemasangan MHN pada OpenStack	21
3.2.4. Pemasangan <i>Honeypot</i> pada Raspberry Pi.....	23
3.2.5. Pemasangan <i>Server</i> Sebagai Penerima Log pada OpenStack	25
3.2.6. Persiapan Penyerangan pada <i>Honeypot</i>	25

3.2.7.	Pembuatan API pada <i>Honeypot</i>	29
3.2.8.	Pembuatan Program Pengambilan Data pada <i>Server</i>	30
3.2.9.	Konfigurasi Pengiriman <i>Malware</i> pada <i>Server</i>	32
3.5.	Metode Pengujian Sistem Pengambilan Data	33
BAB IV HASIL PENELITIAN DAN PEMBAHASAN		35
4.1.	Hasil Log Berbentuk JSON pada <i>Honeypot</i>	35
4.2.	Hasil Serangan pada <i>Honeypot</i>	36
4.2.1.	Modul “exploit/windows/smb/ms10_061_spools”.....	36
4.2.2.	Modul “auxiliary/scanner/http/dir_listing”	38
4.2.3.	Modul “auxiliary/admin/mysql/mysql_sql”	38
4.2.4.	Modul “auxiliary/scanner/ftp/ftp_version”	39
4.2.5.	Menggunakan <i>Random Login</i> Melalui FTP	40
4.3.	Hasil Pengambilan Data Serangan Melalui <i>Server</i>	40
4.4.	Hasil Pengambilan <i>Malware</i> pada <i>Honeypot</i>	41
4.5.	Analisa Hasil Pengujian	43
BAB V PENUTUP		44
5.1.	Kesimpulan.....	44
5.2.	Saran	44
DAFTAR PUSTAKA		45
LAMPIRAN		47