

DAFTAR ISI

PERNYATAAN.....	ii
PRAKATA.....	iv
ARTI LAMBANG DAN SINGKATAN	vi
ABSTRACT.....	vii
INTISARI.....	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xiii
DAFTAR TABEL.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	4
1.3 Tujuan Penelitian.....	4
1.4 Batasan Masalah.....	5
1.5 Keaslian Penelitian	5
1.6 Manfaat Penelitian.....	8
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI	10
2.1 Tinjauan Pustaka	10
2.2 Landasan Teori	13
2.2.1 <i>Wireless Local Area Network (WLAN)</i>	13
2.2.2 Sistem keamanan WLAN.....	14
2.2.3 Sistem Operasi Android	16
2.2.4 Backtrack 5 ARM	17
2.2.5 Honeypot.....	18
2.2.6 Kategori Honeypot.....	19
2.2.6.1 Jenis Honeypot.....	19
2.2.6.2 Kelebihan dan Kekurangan Honeypot.....	22
2.2.6.3 Kegunaan Honeypot	23
2.2.6.4 Penempatan Honeypot.....	24
2.2.7 Mobile Honeypot	27

2.2.8	Dionaea	27
2.2.9	Serangan Jaringan Komputer	28
2.2.10	Jenis-jenis Serangan	29
2.3	Pertanyaan Penelitian	30
BAB III METODE PENELITIAN		31
3.1	Bahan Penelitian	31
3.2	Alat Penelitian	31
3.3	Alur Penelitian	32
3.3.1	Perancangan sistem Mobile HoneyPot	33
3.3.2	Implementasi sistem Mobile HoneyPot	34
3.3.3	Pengujian Performa Mobile HoneyPot	35
3.3.3.1	Skenario Pengujian Performa	35
3.3.3.1.1	Skenario serangan Scanning	36
3.3.3.1.2	Skenario serangan Eksploitasi untuk pengujian menangkap Malware.	37
3.3.3.2	Performa sistem Mobile HoneyPot	38
3.3.4	Pengumpulan data pada publik WLAN	38
3.3.5	Analisis	40
BAB IV HASIL DAN PEMBAHASAN		41
4.1	Perancangan sistem Mobile HoneyPot	41
4.2	Implementasi Sistem Mobile HoneyPot	42
4.2.1	Instalasi Backtrack 5 ARM	42
4.2.2	Instalasi Dionaea	46
4.3	Pengujian Performa Mobile HoneyPot	54
4.2.3	Skenario Pengujian Performa	54
4.2.3.1	Pengujian Performa dengan Skenario Serangan Scanning	54
4.2.3.1.1	Scanning Samsung Galaxy S3 sebelum menjalankan paket aplikasi Mobile HoneyPot	56
4.2.3.1.2	Scanning Samsung Galaxy S3 setelah menjalankan Backtrack 5 ARM	58

4.2.3.1.3	Scanning Samsung Galaxy S3 setelah menjalankan Dionaea.....	60
4.2.3.2	Pengujian Performa dengan Skenario Serangan Eksploitasi ...	62
4.2.3.2.1	Eksploitasi pada <i>vulnerability</i> MS10-061 Microsoft Print Spooler Service Impersonation.....	64
4.2.4	Performa Mobile Honeykot	67
4.2.4.1	Hasil Pengujian Performa dengan Skenario Serangan Scanning.	68
4.2.4.1.1	Daftar jumlah serangan berdasarkan port	71
4.2.4.1.2	Daftar jumlah serangan berdasarkan alamat IP penyerang	72
4.2.4.1.3	Daftar jumlah serangan berdasarkan sistem operasi yang digunakan penyerang	73
4.2.4.1.4	Daftar alamat IP yang menyerang port 445	74
4.2.4.1.5	Daftar port yang diserang oleh IP 192.168.3.13 dan jumlah serangannya.....	74
4.2.4.2	Hasil Pengujian Performa dengan Skenario Serangan Eksploitasi.....	75
4.4	Pengumpulan data pada publik WLAN.....	78
4.4.1	Log pada WLAN UGM Hot-Spot Gedung Teknik Elektro	78
4.4.2	Log pada WLAN UGM Hot-Spot Gedung Kantor Pusat Fakultas Teknik	82
4.4.3	Log pada WLAN UGM Hot-Spot Gedung Perpustakaan Pusat	86
4.5	Analisis	89
4.5.1	Performa Mobile Honeykot	89
4.5.2	Pengumpulan data pada publik WLAN	92
4.5.3	Perbandingan dengan Mobile Honeykot yang sudah ada	94
BAB V KESIMPULAN DAN SARAN.....		98
5.1	Kesimpulan.....	98
5.2	Saran.....	98
DAFTAR PUSTAKA		100

LAMPIRAN	L-1
A. Dionaea.conf	L-1
B. Isi file 'bootbt' yang diedit untuk Smasung Galaxy S3	L-2
C. Listing Perintah Instalasi Backtrack 5 ARM	L-4
D. Listing Instalasi Dionaea.....	L-5
E. Listing Perintah NMAP	L-10
F. Listing Perintah Eksploitasi	L-11
G. Listing <i>Query</i> SQLITE3.....	L-12