

Daftar Isi

Lembar Pernyataan.....	ii
Lembar Pengesahan	iii
Abstrak	iv
<i>Abstract</i>	v
Kata Pengantar	vi
Lembar Persembahan	vii
Daftar Isi.....	viii
Daftar Gambar.....	x
Daftar Tabel	xi
1. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan masalah	2
1.3 Tujuan.....	2
1.4 Hipotesa.....	3
1.5 Metodologi Penyelesaian Masalah	3
2. LANDASAN TEORI.....	4
2.1 <i>Network Forensic</i>	4
2.1.1 Definisi <i>Network Forensic</i>	4
2.1.2 Proses <i>Network Forensic</i>	4
2.2 <i>Traditional Forensic</i>	4
2.3 <i>Live Forensic</i>	5
2.4 <i>Data Volatile</i>	6
2.5 <i>Network Forensic Tools</i>	7
2.5.1 Dampak <i>Tools</i> Terhadap Sistem	8
2.5.2 TCPView.....	8
2.5.3 Openports	9
2.6 Parameter Pengujian.....	9
2.6.1 <i>Memory Footprint</i>	9
2.6.2 <i>Time and File System Impact</i>	10
3. PERANCANGAN SISTEM	10
3.1 Spesifikasi Sistem.....	11
3.1.1 Spesifikasi Kebutuhan Perangkat Lunak dan Keras	11
3.1.2 Perancangan Sistem	11
3.2 Perancangan Aplikasi <i>Retrieve and Analysis Data (RAD)</i>	11
3.2.1 Ilustrasi Fungsi dari Aplikasi RAD.....	12
3.2.2 <i>Tools</i> yang Digunakan pada Aplikasi RAD.....	12
3.2.3 Skema Penanganan Aplikasi RAD.....	13
3.2.4 Perancangan Antar Muka Aplikasi RAD.....	18
3.3 Inisialisasi Lingkungan Pengujian.....	18
3.3.1 Instalasi Lingkungan Pengujian	19
3.4 Inisialisasi Simulasi Kasus	20
3.4.1 Kasus 1: Exploit via command line menggunakan Metasploit.....	20
3.4.2 Kasus 2: <i>VNC Remote Control & Stealth</i>	21
3.4.3 Kasus 3: <i>Ping Flood</i>	22
3.4.4 Kasus 4: <i>Malicious Software Backdoor</i>	22
3.5 Skema Penanganan Kasus dan Pengujian <i>Tools</i>	23

3.6	Perancangan Proses <i>Profiling</i> pada <i>Tools</i> (TCPView dan Openports) ..	23
3.6.1	<i>Profiling Tools</i>	23
4.	PENGUJIAN DAN ANALISIS SISTEM	25
4.1	Pengujian Sistem	25
4.1.1	Tujuan Pengujian Aplikasi RAD	25
4.1.2	Tujuan Pengujian Performansi TCPView dan Openports	25
4.2	Analisa Pengujian.....	25
4.2.1	Kasus 1: <i>Exploit Via Command Line</i>	25
4.2.2	Kasus 2: VNC Remote Control and Stealth.....	28
4.2.3	Kasus 3: <i>Ping Flood</i>	31
4.2.4	Kasus 4: <i>Malicious Software Backdoor</i>	34
4.3	Perbandingan Performansi Metode dari Kasus yang Dihadapi.....	37
4.3.1	Perbandingan Penggunaan <i>Physical memory</i>	37
4.3.2	Perbandingan Akurasi	39
4.3.3	Perbandingan Penulisan dan Penggunaan File Sistem.....	40
4.3.4	Perbandingan Jumlah Penggunaan <i>File library</i>	40
4.3.5	Perbandingan <i>Elapsed Time</i>	41
4.4	<i>Tools</i> dan Metode Terbaik.....	41
5.	KESIMPULAN DAN SARAN	43
5.1	Kesimpulan.....	43
5.2	Saran	43
6.	DAFTAR PUSTAKA	44
7.	LAMPIRAN A: <i>SCREENSHOT</i> PENGUJIAN.....	45
8.	LAMPIRAN B: HASIL PENGUJIAN PARAMETER <i>MEMORY FOOTPRINT</i>	49