

DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS	ii
LEMBAR PENGESAHAN	iii
ABSTRAK	iv
<i>ABSTRACT</i>	v
KATA PENGANTAR	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	xiv
DAFTAR TABEL	xvi
DAFTAR LAMPIRAN	xix
DAFTAR SINGKATAN	xx
DAFTAR ISTILAH	xxi
Bab I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	2
I.3 Tujuan Penelitian	2
I.4 Batasan Penelitian	3
I.5 Manfaat Penelitian	3
Bab II TINJAUAN PUSTAKA	5
II.1 <i>Security Information and Event Management (SIEM)</i>	5
II.2 IBM QRadar	5
II.3 <i>Threat</i>	6
II.4 <i>Port Scanning</i>	6
II.5 <i>Brute Force</i>	6
II.6 <i>Distributed Denial of Service (DDoS)</i>	7

II.7	<i>Network Attack</i>	7
II.8	<i>Vulnerability</i>	7
II.9	Eksplorasi.....	8
II.10	Fungsi Kontrol	8
II.11	Fungsi Deteksi	9
II.12	<i>Profiling</i>	9
II.13	Data Flow Diagram (DFD)	9
II.14	Metrik <i>Response Time</i>	10
II.15	Metrik <i>Granularity</i>	10
II.16	Penelitian Terdahulu	10
Bab III	METODOLOGI PENELITIAN	14
III.1	Model Konseptual	14
III.2	Sistematika Penyelesaian Masalah	15
III.2.1	Tahap Awal (Perumusan Masalah).....	17
III.2.2	Tahap Hipotesis.....	17
III.2.3	Tahap Desain.....	17
III.2.4	Tahap Pengujian.....	18
III.2.5	Tahap Analisis.....	18
III.2.6	Tahap Akhir	19
III.3	Pengumpulan Data	19
III.4	Pengolahan Data	19
III.5	Metode Evaluasi.....	19
Bab IV	EKSPERIMEN DAN DATA EKSPERIMEN	20
IV.1	Platform Eksperimen	20
IV.1.1	Spesifikasi Perangkat Keras	21
IV.1.2	Spesifikasi Perangkat Lunak	22

IV.2	Kelompok Pengujian.....	26
IV.3	Skenario Pengujian	26
IV.3.1	Skenario Eksperimen Penyerangan.....	26
IV.3.1.1	Skenario Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan</i>	28
IV.3.1.2	Skenario Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan plus UDP</i>	29
IV.3.1.3	Skenario Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan, All TCP Ports</i>	30
IV.3.1.4	Skenario Pengujian <i>Brute Force</i> Menggunakan Hydra.....	32
IV.3.1.5	Skenario Pengujian <i>Brute Force</i> Menggunakan Brutespray .	33
IV.3.1.6	Skenario Pengujian <i>Brute Force</i> Menggunakan Medusa	35
IV.3.1.7	Skenario Pengujian DDoS Menggunakan Hping 3	36
IV.3.1.8	Skenario Pengujian DDoS Menggunakan LOIC	37
IV.3.1.9	Skenario Pengujian DDoS Menggunakan Slowloris.....	39
IV.4	Implementasi Pengujian.....	41
IV.4.1	Implementasi Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan</i>	41
IV.4.2	Implementasi Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan plus UDP</i>	42
IV.4.3	Implementasi Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan, All TCP Ports</i>	43
IV.4.4	Implementasi Pengujian <i>Brute Force</i> Menggunakan Hydra.....	45
IV.4.5	Implementasi Pengujian <i>Brute Force</i> Menggunakan Brutespray	46
IV.4.6	Implementasi Pengujian <i>Brute Force</i> Menggunakan Medusa	48
IV.4.7	Implementasi Pengujian DDoS Hping 3	49

IV.4.8	Implementasi Pengujian DDoS Menggunakan LOIC.....	50
IV.4.9	Implementasi Pengujian DDoS Menggunakan Slowloris.....	52
IV.5	Parameter dan Data Hasil Pengujian.....	53
IV.5.1	Parameter Penyerangan dan Data Hasil Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan</i>	53
IV.5.2	Parameter Penyerangan dan Data Hasil Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan plus UDP</i>	54
IV.5.3	Parameter Penyerangan dan Data Hasil Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan, All TCP Ports</i>	56
IV.5.4	Parameter Penyerangan dan Data Hasil Pengujian <i>Brute Force</i> Menggunakan Hydra.....	57
IV.5.5	Parameter Penyerangan dan Data Hasil Pengujian <i>Brute Force</i> Menggunakan Brutespray	58
IV.5.6	Parameter Peyerangan dan Data Hasil Pengujian <i>Brute Force</i> Menggunakan Medusa.....	60
IV.5.7	Parameter Penyerangan dan Data Hasil Pengujian DDoS Hping 3	61
IV.5.8	Parameter Penyerangan dan Data Hasil Pengujian DDoS LOIC.....	62
IV.5.9	Parameter Penyerangan dan Data Hasil Pengujian DDoS Slowloris	63
Bab V	INDIKATOR DAN ANALISIS	65
V.1	Analisa Indikator rules Serangan	65
V.1.1	Indikator <i>Rules Port Scanning</i>	65
V.1.2	Indikator <i>Rules Brute Force</i>	71
V.1.3	Indikator <i>Rules DDoS</i>	76

V.2	Analisa Mekanisme Deteksi Serangan Berdasarkan Data <i>Flow</i> Diagram	81
V.2.1	Analisa Mekanisme Deteksi Serangan Nmap - Zenmap GUI <i>Profile Intense Scan</i> Oleh IBM QRadar Berdasarkan DFD	82
V.2.2	Analisa Mekanisme Deteksi Serangan Nmap - Zenmap GUI <i>Profile Intense Scan Plus UDP</i> Oleh IBM QRadar Berdasarkan DFD	84
V.2.3	Analisa Mekanisme Deteksi Serangan Nmap - Zenmap GUI <i>Profile Intense Scan, All TCP Ports</i> Oleh IBM QRadar Berdasarkan DFD.....	87
V.2.4	Analisa Mekanisme Deteksi Serangan Hydra Oleh IBM QRadar Berdasarkan DFD	89
V.2.5	Analisa Mekanisme Deteksi Serangan Brutespray Oleh IBM QRadar Berdasarkan DFD	92
V.2.6	Analisa Mekanisme Deteksi Serangan Medusa Oleh IBM QRadar Berdasarkan DFD	94
V.2.7	Analisa Mekanisme Deteksi Serangan Hping 3 Oleh IBM QRadar Berdasarkan DFD	97
V.2.8	Analisa Mekanisme Deteksi Serangan LOIC Oleh IBM QRadar Berdasarkan DFD	99
V.2.9	Analisa Mekanisme Deteksi Serangan Slowloris Oleh IBM QRadar Berdasarkan DFD	102
V.3	Deskripsi <i>Field Output</i> IBM QRadar.....	104
V.3.1	Hasil <i>Output</i> Serangan Nmap - Zenmap GUI Profile Intense Scan..	107
V.3.2	Hasil <i>Output</i> Serangan Nmap - Zenmap GUI Profile Intense Scan plus UDP.....	110
V.3.3	Hasil <i>Output</i> Serangan Nmap - Zenmap GUI Profile Intense, All TCP Ports.....	113
V.3.4	Hasil <i>Output</i> Serangan Hydra	116
V.3.5	Hasil <i>Output</i> Serangan Brutespray.....	119

V.3.6	Hasil <i>Output</i> Serangan Medusa.....	121
V.3.7	Hasil <i>Output</i> Serangan Hping 3	124
V.3.8	Hasil <i>Output</i> Serangan LOIC	126
V.3.9	Hasil <i>Output</i> Serangan Slowloris	129
V.4	Analisis Fungsi Kontrol SIEM IBM QRadar Berdasarkan Hasil Output Serangan	132
V.4.1	Analisis Fungsi Kontrol <i>Output</i> Serangan Nmap - Zenmap GUI Profile Intense Scan	134
V.4.2	Analisis Fungsi Kontrol <i>Output</i> Serangan Nmap - Zenmap GUI Profile Intense Scan Plus UDP.....	136
V.4.3	Analisis Fungsi Kontrol <i>Output</i> Serangan Nmap - Zenmap GUI Profile Intense Scan, All TCP Ports.....	138
V.4.4	Analisis Fungsi Kontrol Output Serangan Hydra	140
V.4.5	Analisis Fungsi Kontrol <i>Output</i> Serangan Brutespray.....	142
V.4.6	Analisis Fungsi Kontrol <i>Output</i> Serangan Medusa.....	144
V.4.7	Analisis Fungsi Kontrol <i>Output</i> Serangan Hping 3	146
V.4.8	Analisis Fungsi Kontrol Output Serangan LOIC	148
V.4.9	Analisis Fungsi Kontrol <i>Output</i> Serangan Slowloris.....	149
V.5	Hasil Analisis <i>Output</i> Rule IBM QRadar Dengan Metrik <i>Response Time</i> dan <i>Granularity</i>	151
V.6	Analisis Perbandingan Metrik <i>Response Time</i>	151
V.7	Analisis Perbandingan Metrik <i>Granularity</i>	153
V.8	Ringkasan Analisa	154
V.8.1	Ringkasan Analisa Fungsi Kontrol <i>Output</i> Kategori Serangan ..	155
V.8.2	Ringkasan Analisa Perbandingan Metrik <i>Response Time</i>	156
V.8.3	Ringkasan Analisa Perbandingan Metrik <i>Granularity</i>	157
Bab VI	KESIMPULAN DAN SARAN	158

VI.1 Kesimpulan	158
VI.2 Saran	159
DAFTAR PUSTAKA	160
LAMPIRAN.....	163