

DAFTAR GAMBAR

Gambar III. 1 Model Konseptual	14
Gambar III. 2 Sistematika Penelitian	16
Gambar IV.1 Platform Eksperimen	20
Gambar IV.2 Skenario Eksperimen Penyerangan.....	27
Gambar IV.3 Skenario Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan</i>	28
Gambar IV.4 Skenario Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan plus UDP</i>	29
Gambar IV.5 Skenario Pengujian <i>Port Scanning</i> Menggunakan Nmap - Zenmap GUI <i>Profile Intense Scan, All TCP Ports</i>	31
Gambar IV.6 Skenario Pengujian <i>Brute Force</i> Menggunakan Hydra	32
Gambar IV.7 Skenario Pengujian <i>Brute Force</i> Menggunakan Brutespray	34
Gambar IV.8 Skenario Pengujian <i>Brute Force</i> Menggunakan Medusa	35
Gambar IV.9 Skenario Pengujian DDoS Menggunakan Hping 3	37
Gambar IV.10 Skenario Pengujian DDoS Menggunakan LOIC	38
Gambar IV.11 Skenario Pengujian DDoS Menggunakan Slowloris	40
Gambar IV.12 Proses Pengujian Nmap - Zenmap GUI <i>Profile Intense Scan</i>	41
Gambar IV.13 Tampilan <i>Log Monitoring</i> IBM QRadar Mendeteksi Serangan <i>Port Scanning</i> dengan Nmap - Zenmap GUI <i>Intense Scan</i>	42
Gambar IV.14 Proses Pengujian Nmap - Zenmap GUI <i>Profile Intense Scan plus UDP</i>	43
Gambar IV.15 Tampilan <i>Log Monitoring</i> IBM QRadar Mendeteksi Serangan <i>Port Scanning</i> dengan Nmap - Zenmap GUI <i>Intense Scan plus UDP</i>	43
Gambar IV.16 Proses Pengujian Nmap - Zenmap GUI <i>Profile Intense Scan, All TCP Ports</i>	44
Gambar IV.17 Tampilan <i>Log Monitoring</i> IBM QRadar Mendeteksi Serangan <i>Port Scanning</i> dengan Nmap - Zenmap GUI <i>Intense Scan, All TCP Ports</i>	44
Gambar IV.18 Proses Pengujian <i>Brute Force</i> Menggunakan Hydra.....	45
Gambar IV.19 Tampilan <i>Log Monitoring</i> IBM QRadar Mendeteksi Serangan <i>Brute Force</i> Menggunakan Hydra	46
Gambar IV.20 Proses Pengujian <i>Brute Force</i> Menggunakan Brutespray	47

Gambar IV.21 Tampilan <i>Log Monitoring</i> IBM QRadar Mendeteksi Serangan <i>Brute Force</i> Menggunakan Brutespray	47
Gambar IV.22 Proses Pengujian Brute Force Menggunakan Medusa.....	48
Gambar IV.23 Tampilan <i>Log Monitoring</i> IBM QRadar Mendeteksi Serangan <i>Brute Force</i> Menggunakan Medusa.....	48
Gambar IV.24 Proses Pengujian DDoS Menggunakan Hping 3	49
Gambar IV.25 Tampilan <i>Log Monitoring</i> IBM QRadar Mendeteksi Serangan DDoS menggunakan Hping 3	50
Gambar IV.26 Proses Pengujian DDoS menggunakan LOIC	51
Gambar IV.27 Tampilan <i>Log Monitoring</i> IBM QRadar Mendeteksi Serangan DDoS menggunakan LOIC	51
Gambar IV.28 Proses Pengujian DDoS menggunakan Slowloris	52
Gambar IV.29 Tampilan <i>Log Monitoring</i> IBM QRadar Mendeteksi Serangan DDoS menggunakan Slowloris.....	53
Gambar V.1 Analisa Mekanisme Deteksi Serangan Nmap - Zenmap GUI <i>Profile Intense Scan</i> Oleh IBM QRadar Berdasarkan DFD.....	82
Gambar V.2 Analisa Mekanisme Deteksi Serangan Nmap - Zenmap GUI <i>Profile Intense Scan Plus UDP</i> Oleh IBM QRadar Berdasarkan DFD	85
Gambar V.3 Analisa Mekanisme Deteksi Serangan Nmap - Zenmap GUI <i>Profile Intense Scan, All TCP Ports</i> Oleh IBM QRadar Berdasarkan DFD	87
Gambar V.4 Analisa Mekanisme Deteksi Serangan Hydra Oleh IBM QRadar Berdasarkan DFD.....	90
Gambar V.5 Analisa Mekanisme Deteksi Serangan Brutespray Oleh IBM QRadar Berdasarkan DFD.....	92
Gambar V.6 Analisa Mekanisme Deteksi Serangan Medusa Oleh IBM QRadar Berdasarkan DFD.....	95
Gambar V.7 Analisa Mekanisme Deteksi Serangan Hping 3 Oleh IBM QRadar Berdasarkan DFD.....	97
Gambar V.8 Analisa Mekanisme Deteksi Serangan LOIC Oleh IBM QRadar Berdasarkan DFD.....	100
Gambar V.9 Analisa Mekanisme Deteksi Serangan Slowloris Oleh IBM QRadar Berdasarkan DFD.....	102