

## DAFTAR GAMBAR

Gambar	Halaman
1.1 Peningkatan jumlah serangan jaringan komputer	1
2.1 Struktur NIDS	7
2.2 Struktur HIDS	8
2.3 Misuse Detection Model	8
2.4 Anomaly Detection Model	9
2.5 Sistem IDS standart	9
2.6 Ilustrasi Algoritma K-means	12
2.7 Ilustrasi Kelemahan Algoritma K-means	12
3.1 Diagram Alir Perancangan	18
3.2 Topologi Jaringan	20
3.3 Inisialisasi awal snort	23
3.4 <i>Sniffing mode</i>	23
3.5 Mode <i>sniffing</i> , <i>logger</i> , dan NIDS	25
3.6 Diagram alir proses pengklasteran	25
3.7 Daftar database log snort	24
3.8 Data Hasil Seleksi	27
3.9 Diagram Blok Sistem	27
3.10 Tampilan Awal Program	28
3.11 Penghitungan klaster	28
3.12 Tampilan awal melakukan <i>port scanning</i>	31
3.13 Tampilan awal ping attack	32
3.14 Tampilan Awal Serangan <i>syn</i>	32
3.15 Tampilan awal penyerangan TCP dan UDP	32
3.16 Tampilan awal <i>ettercap</i>	33
4.1 Hasil klaster dengan data training	35
4.2 Rule yang ditulis oleh program	35
4.3 Grafik hasil klaster percobaan pertama	36
4.4 Grafik data training percobaan kedua	38
4.5 Grafik data training percobaan ketiga	40
4.6 Grafik data <i>error</i> percobaan keempat	42

4.7	Pengujian dengan <i>scanner</i>	44
4.8	Koneksi awal ke server dengan <i>port scan</i>	45
4.9	Koneksi pasca banned IP	45
4.10	Informasi pada sistem setelah penyerangan <i>scanning</i>	46
4.11	Pengujian dengan <i>ping attack</i>	46
4.12	Proses <i>ping attack</i> ke server	47
4.13	Informasi banned IP penyerang <i>ping attack</i>	47
4.14	Proses <i>banned IP</i> terhadap penyerang <i>ping attack</i>	48
4.15	Pengujian dengan <i>syn attack</i>	49
4.16	Proses penyerangan dengan <i>syn attack</i>	49
4.17	Informasi banned IP penyerang <i>syn attack</i>	50
4.18	Proses <i>banned IP</i> terhadap penyerang <i>syn attack</i>	50
4.19	Pengujian dengan TCP dan UDP <i>attack</i>	51
4.20	Proses penyerangan dengan TCP dan UDP <i>attack</i>	51
4.21	Informasi banned IP penyerang TCP dan UDP <i>attack</i>	52
4.22	Proses <i>banned IP</i> terhadap penyerang TCP dan UDP <i>attack</i>	52
4.23	Pengujian dengan ARP <i>Poisoning</i>	53
4.24	Proses penyerangan dengan ARP <i>Poisoning</i>	53
4.25	Deteksi sistem terhadap ARP <i>Poisoning</i>	54