

DAFTAR ISI

	Halaman
HALAMAN JUDUL.....	i
PERSETUJUAN DOSEN PEMBIMBING	ii
PERSETUJUAN TIM PENGUJI SIDANG KERJA PRAKTEK.....	iv
KETERANGAN INSTANSI	iv
ABSTRAK	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Pokok Permasalahan	2
1.3 Pembatasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Metodologi Penelitian	3
1.6 Sistematika Penyajian	7
BAB II LANDASAN TEORI	9
2.1 Karakteristik dan Peranan IDS (<i>Intrusion Detection Sytem</i>)	9
2.1.1 Sejarah Perkembangan IDS.....	9
2.1.2 Karakteristik IDS	12
2.2 Alasan dan Tujuan Penggunaan IDS.....	13
2.3 Macam-macam Teknik IDS dalam Mendeteksi Serangan.....	14
2.3.1 <i>Anomaly detection / Anomaly-based</i> IDS	14
2.3.2 <i>Misuse detection / Signature-based</i> IDS	15
2.3.3 <i>Honey Pot</i> dan <i>Sistem Padded</i>	16
2.4 Tipe-tipe IDS.....	17
2.4.1 <i>Host-based Intrusion Detection System (HIDS)</i>	17
2.4.2 <i>Network Intrusion Detection Systems (NIDS)</i>	19
2.5 Hal-hal yang Dapat Dipantau oleh IDS	21

2.5	Hal-hal yang Dapat Dipantau oleh IDS	21
2.5.1	Tipe-tipe Serangan	21
2.5.2	Strategi yang Dilakukan oleh Penyerang	22
2.5.3	Contoh Serangan	22
BAB III GAMBARAN UMUM PERUSAHAAN		24
3.1	Profil Perusahaan	24
3.1.1	Visi Perusahaan.....	29
3.1.2	Misi dan Nilai yang Dijunjung Tinggi Perusahaan.....	30
3.1.3	Jaringan Kabel PT. Broadband Multimedia, Tbk. di Indonesia....	30
3.2	Struktur Organisasi PT. Broadband Multimedia, Tbk.	31
3.3	Sistem Jaringan Saat Ini	34
3.3.1	Skema Jaringan PT Broadband Multitmedia, Tbk. di Karawaci ...	35
BAB IV ANALISIS DAN PERANCANGAN		37
4.1	Spesifikasi Jaringan yang Dikonfigurasi	37
4.2	Perancangan Penggunaan <i>Snort</i> sebagai IDS	39
4.2.1	Pengenalan Aplikasi <i>Snort</i> dan BASE.....	39
4.2.2	Alasan Penggunaan Aplikasi <i>Snort</i>	40
4.2.3	Lokasi Penempatan Aplikasi <i>Snort</i> pada Jaringan.....	41
4.2.4	Macam-macam Modus pada Aplikasi <i>Snort</i>	41
4.2.5	Komponen Aplikasi <i>Snort</i>	42
4.2.6	Hubungan Antar Aplikasi <i>Snort</i> dengan BASE.....	43
4.2.7	Hal-hal yang Diperlukan untuk Implementasi IDS	44
4.3	Instalasi dan Konfigurasi Aplikasi <i>Snort</i>	45
4.3.1	Instalasi Aplikasi <i>Snort</i> dari RPM <i>Package</i>	45
4.3.2	Instalasi Aplikasi <i>Snort</i> dari <i>Source Code</i>	46
4.4	Struktur dan Konfigurasi <i>Snort Rules</i>	50
4.4.1	Cara Mendapatkan <i>Snort Rules</i>	51
4.4.2	Struktur <i>Snort Rules</i>	52
4.4.3	Membuat <i>Snort Rules</i>	56
4.5	Instalasi dan Konfigurasi BASE	58
4.6	Hasil Instalasi Aplikasi <i>Snort</i> dan BASE.....	60
4.6.1	<i>Troubleshooting Snort</i> dan BASE	61

4.6.2	<i>Test Snort</i> dengan Perintah Nmap.....	61
4.7	Hasil Tampilan pada BASE.....	62
BAB V	KESIMPULAN DAN SARAN	74
5.1	Kesimpulan	74
5.2	Saran	75
DAFTAR PUSTAKA	77
LAMPIRAN	78



DAFTAR GAMBAR

	Halaman
Gambar 2. 1 Sejarah Perkembangan IDS.....	11
Gambar 2. 2 Diagram <i>Anomaly Detection System</i>	15
Gambar 2. 3 Diagram <i>Misuse Detection System</i>	16
Gambar 3. 1 <i>Platform</i> pelayanan PT. Broadband Multimedia, Tbk.....	29
Gambar 3. 2 Jaringan kabel PT. Broadband Multimedia, Tbk.....	31
Gambar 3. 3 Struktur Organisasi Divisi IT.....	34
Gambar 3. 4 Skema Jaringan PT. Broadband Multimedia, Tbk.....	36
Gambar 4. 1 Jaringan yang Dibangun.....	38
Gambar 4. 2 Lokasi Penempatan Aplikasi <i>Snort</i>	41
Gambar 4. 3 Komponen Aplikasi <i>Snort</i>	43
Gambar 4. 4 Diagram Hubungan <i>Snort</i> dengan BASE.....	43
Gambar 4. 5 Alur Hubungan Aplikasi <i>Snort</i> dengan BASE.....	44
Gambar 4. 6 Tahapan Instalasi Aplikasi <i>Snort</i>	50
Gambar 4. 7 Struktur <i>Snort Rule</i>	52
Gambar 4. 8 Struktur <i>Rule Header</i>	52
Gambar 4. 9 Tahapan Instalasi BASE.....	60
Gambar 4. 10 Halaman Utama BASE.....	64
Gambar 4. 11 Contoh <i>Alert TCP</i>	65
Gambar 4. 12 Contoh <i>Alert UDP</i>	66
Gambar 4. 13 Contoh <i>Alert ICMP</i>	67
Gambar 4. 14 Macam-macam <i>Alert</i> Hasil Pantauan.....	68
Gambar 4. 15 Informasi Suatu <i>Alert</i>	70
Gambar 4. 16 Contoh <i>Port</i> Hasil Pantauan.....	71
Gambar 4. 17 Layanan <i>Search</i>	72
Gambar 4. 18 Contoh Grafik.....	73

DAFTAR TABEL

	Halaman
Tabel 1. 1 <i>Time Frame</i>	4
Tabel 4. 1 Macam-macam Perintah <i>Configure</i>	48
Tabel 4. 2 Nomor <i>Port</i>	53
Tabel 4. 3 Macam-macam <i>Rule Option</i>	55
Tabel 4. 4 Macam-macam <i>Flag</i>	55
Tabel 4. 5 Tipe Paket ICMP	56
Tabel 4. 6 Macam-macam Respon.....	56
Tabel 4. 7 Macam-macam SID	68



DAFTAR LAMPIRAN

- A. *Business Requirement*
- B. *Requirement Analysis*
- C. *Project Plan*
- D. Penjelasan Mengenai SID (*Signature ID*) pada *Snort Alert*

