



DAFTAR ISI

DAFTAR TABEL	xi
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN	xii
I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan	2
1.4 Manfaat	2
1.5 Ruang Lingkup	2
II TINJAUAN PUSTAKA	3
2.1 <i>Firewall</i>	3
2.2 <i>Malware</i>	3
2.3 <i>Snort</i>	3
2.4 <i>Maltrail</i>	5
2.5 <i>Crontab</i>	6
III METODE	7
3.1 Lokasi dan Waktu PKL	7
3.2 Prosedur Kerja	7
3.3 Alat dan Bahan	9
IV KEADAAN UMUM PERUSAHAAN	11
4.1 Sejarah	11
4.2 Kegiatan Lembaga	11
4.3 Struktur Organisasi	12
4.4 Tugas dan Fungsi	12
V HASIL DAN PEMBAHASAN/TOPIK PKL	13
5.1 Perencanaan	13
5.2 Implementasi	16
5.3 Pengujian	24
VI SIMPULAN DAN SARAN	30
6.1 Simpulan	30
6.2 Saran	30
DAFTAR PUSTAKA	31
LAMPIRAN	32
RIWAYAT HIDUP	36

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:

- Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
- Pengutipan tidak merugikan kepentingan yang wajar IPB.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.

Hak cipta milik IPB (Institut Pertanian Bogor)

Bogor Agricultural University



Sekolah Vokasi
College of Vocational Studies

DAFTAR TABEL

1	Opsi <i>Rule's Action</i>	4
2	Opsi <i>Rule's Protocol</i>	4
3	Opsi <i>Direction</i>	5
4	Opsi <i>Rule Option</i>	5
5	Beberapa alamat situs yang diuji	9
6	Kebutuhan Perangkat Keras	9
7	Kebutuhan Perangkat Lunak	9
8	<i>Library</i> dan Perangkat lunak prasyarat Snort	10
9	Penjelasan perintah PulledPork	21
10	Keterangan Cronjob pada Crontab	22
11	Keterangan data <i>log</i> Snort	27
12	Keterangan data <i>log</i> Maltrail	28
13	Hasil pengujian <i>Intrusion Detection and Prevention System</i>	29

DAFTAR GAMBAR

1	Format <i>Rules</i> pada Snort (Sumber: Khamphakdee <i>et al</i> 2015)	4
2	Arsitektur Maltrail (Sumber : Github.com/stamparm/maltrail)	5
3	Metode PBM (kiri); Simplifikasi Metode PPDIOO (kanan). (Sumber: www.networkdirection.net)	7
4	Struktur Organisasi Diskominfostandi Kota Bekasi (Sumber: www.diskominfo.bekasikota.go.id)	12
5	Topologi jaringan Diskominfostandi Kota Bekasi	13
6	Ilustrasi kondisi jaringan sebelum diterapkan sistem Snort dan Maltrail	13
7	Ilustrasi rancangan jaringan setelah diterapkan sistem Snort dan Maltrail	14
8	Topologi pada lingkungan pengujian	14
9	<i>Flowchart</i> Snort dan Maltrail	15
10	<i>Flowchart</i> Cronjob untuk Snort dan Maltrail	16
11	Perintah membuat dan membuka file <i>ethtool.service</i>	17
12	Perintah konfigurasi <i>Network Cards</i>	17
13	Perintah untuk mengaktifkan service <i>ethtool</i>	17
14	Perintah instalasi perangkat lunak <i>Snort</i>	18
15	Status dan Versi Snort	18
16	Direktori penyimpanan <i>rules</i> dan <i>log</i> Snort	19
17	Konfigurasi tambahan <i>Snort.lua</i>	19
18	Perintah verifikasi file konfigurasi Snort	20
19	Perintah instalasi PulledPork	20
20	Keluaran versi PulledPork	20
21	Konfigurasi PulledPork	21
22	Perintah untuk menjalankan PulledPork	21
23	Perintah Crontab untuk PulledPork	21



24	Perintah instalasi Splunk	22
25	Perintah untuk membuat direktori dan file konfigurasi Splunk	22
26	Perintah Konfigurasi Splunk	23
27	Tampilan Splunk	23
28	Perintah untuk menjalankan sensor Maltrail	23
29	Perintah untuk menjalankan server Maltrail	23
30	Perintah Crontab untuk menjalankan Maltrail	24
31	Web Interface Maltrail	24
32	Pengujian serangan <i>Ping of Death</i> ; (a) <i>rules</i> yang digunakan; (b) Ping dengan ukuran 1000 <i>bytes</i> berhasil; (c) Ping dengan ukuran 25000 <i>bytes</i> gagal	25
33	Deteksi <i>Ping of Death</i> oleh Snort	25
34	Pengujian serangan SSH Brute Force; (a) <i>rules</i> yang digunakan; (b) Status dan hasil serangan	26
35	Deteksi SSH <i>Brute Force Attack</i>	26
36	Pengujian serangan ICMP <i>Flood</i> ; (a) <i>Rules</i> yang digunakan; (b) Proses dan hasil serangan	26
37	Deteksi ICMP <i>Flood</i>	27
38	Log Snort dalam bentuk JSON	27
39	(a) Visualisasi file <i>log</i> Snort oleh Splunk; (b) Ekspor ke PDF	28
40	Hasil deteksi Maltrail (a) <i>web interface</i> Maltrail; (b) Contoh salah satu ancaman yang terdeteksi; (c) Deteksi potensi <i>Port Scanning</i>	29

DAFTAR LAMPIRAN

1	Instalasi <i>requirement</i> Snort dengan APT	33
2	Perintah instalasi perangkat lunak pendukung Snort	33
3	Instalasi <i>library</i> prasyarat PulledPork	35
4	Konfigurasi Maltrail	35

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber;

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar IPB.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.