DAFTAR ISI

KATA PENGANTAR iii
ABSTRAK v
ABSTRACT vi
DAFTAR TABEL ix
DAFTAR GAMBAR x
DAFTAR ISTILAH xi
BAB 1. PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 4
1.4 Tujuan Penelitian 5
1.5 Manfaat Penelitian 5
1.6 Sistematika Penulisan 6
BAB 2. TINJAUAN PUSTAKA 8
2.1 Intrusion Detection System 8
2.1.1 Peletakan IDS pada Jaringan 10
2.1.2 Perbandingan IDS Signature-based dan Anomaly-based 12
2.1.3 Snort IDS 13
2.2 Firewall 18
2.2.1 Sistematika Firewall 19
2.2.2 IPTables 21
2.3 Intrusion Prevention System 37
2.3.1 Konsep Umum IPS 37
2.4 Honeypot 38
2.4.1 Peletakan Honeypot pada Jaringan 41
2.4.2 Honeyweb 44
BAB 3. METODOLOGI PENELITIAN 46
3.1 Alat dan Bahan Penelitian 46
3.1.1 Alat Penelitian 46
3.1.2 Bahan Penelitian 47
3.2 Desain Penelitian 48
3.2.1 Model Proses 49

BAB 4. PEMBAHASAN DAN HASIL PENELITIAN 59
4.1 Pembahasan 59
4.1.1 Desain Topologi 59
4.1.2 Desain Umum SmartIPS 60
4.1.3 Pengamanan Dasar Sistem 61
4.1.4 Instalasi dan Konfigurasi Snort 63
4.1.5 Pengembangan BlockIt 66
4.1.6 Instalasi dan Konfigurasi Honeyweb 71
4.2 Hasil Penelitian 73
4.2.1 Networking & Performance Testing 73
4.2.2 Proteksi Terhadap Bruteforce SSH 75
4.2.3 Deteksi Malicious pada IDS 76
4.2.4 Redirect Traffic dan Blokir ICMP dari IP Address Malicious 80
4.2.5 Jumlah Serangan pada Host 82
4.2.6 Melihat Detail Penyerang 85
4.2.7 Rekaman Aktifitas pada Honeyweb 87
BAB 5. KESIMPULAN DAN SARAN 92
5.1 Kesimpulan 92
5.2 Saran 95
DAFTAR PUSTAKA 97
LAMPIRAN 98
RIWAYAT HIDUP 108

DAFTAR TABEL

TABEL 2.1 PERBANDINGAN IDS SIGNATURE-BASED DAN ANOMALY-BASED 12
TABEL 2.2 DAFTAR COMMAND PADA IPTABLES 23
TABEL 2.3 DAFTAR GENERIC MATCH PADA IPTABLES 26
TABEL 2.4 DAFTAR TCP MATCHES PADA IPTABLES 28
TABEL 2.5 DAFTAR TARGET/JUMP PADA IPTABLES 32
TABEL 4.1 KONFIGURASI KEAMANAN TIAP NODE 61
TABEL 4.2 HASIL NETWORKING & PERFORMANCE TESTING 74
TABEL 4.3 AKTIFITAS INISIALISASI KONEKSI SSH DALAM INTERVAL < 60 DETIK PADA SERVER 75
TABEL 4.4 REKAP HASIL SERANGAN TERHADAP SERVER 77
TABEL 4.5 INTERAKSI CLIENT-SERVER SEBELUM DAN SETELAH TERDETEKSI MELAKUKAN INTRUSI 81
TABEL 4.6 JUMLAH SERANGAN HOST TERTENTU 83
TABEL 4.7 HOST TERDETEKSI LEBIH DARI BATAS TOLERANSI 83
TABEL 4.8 HOST BLACKLIST 84
TABEL 4.9 INFORMASI DETAIL HOST PENYERANG 85
TABEL 4.10 LOG AKTIFITAS HOST TERTENTU PADA HONEYWEB 88

DAFTAR GAMBAR

GAMBAR 1.1 GRAFIK INTRUSI YANG BIASA TERJADI PADA WEB 1
GAMBAR 2.1 PELETAKAN IDS BERSAMA DENGAN JARINGAN YANG DI PROTEKSI 10
GAMBAR 2.2 PELETAKAN IDS IN-LINE PADA ROUTER 11
GAMBAR 2.3 PELETEKAN IDS DI DEPAN FIREWALL 12
GAMBAR 2.4 SISTEMATIKA KERJA SNORT MEMANFAATKAN LIBPCAP 14
GAMBAR 2.5 FLOWCHART KERJA DETEKSI SNORT BERBASIS SIGNATURE 18
GAMBAR 2.6 TUMPUKAN HEADER PADA SISTEM KOMUNIKASI BERBASIS TCP/IP 20
GAMBAR 2.7 SISTEMATIKA IPTABLES 22
GAMBAR 2.8 PENEMPATAN HONEYPOT PADA BORDER TERLUAR JARINGAN 42
GAMBAR 2.9 PENEMPATAN HONEYPOT DI BELAKANG FIREWALL 42
GAMBAR 2.10 PENEMPATAN HONEYPOT PADA AREA DMZ 43
GAMBAR 3.1 DESAIN PENELITIAN 48
GAMBAR 3.2 TAHAP-TAHAP PENELITIAN 49
GAMBAR 3.3 FLOWCHART MEKANISME UMUM KERJA SMARTIPS 55
GAMBAR 4.1 DESAIN TOPOLOGI 59
GAMBAR 4.2 PROSES DNAT TRAFFIC 72
GAMBAR 4.3 PROSES SNAT TRAFFIC 72

UNIVERSITAS PENDIDIKAN INDONESIA
PERPUSTAKAAN