

## DAFTAR ISI

<b>HALAMAN JUDUL</b>	
<b>LEMBAR PENGESAHAN</b>	
<b>LEMBAR PERNYATAAN</b>	
<b>ABSTRAK.....</b>	<b>i</b>
<b>ABSTRACT .....</b>	<b>ii</b>
<b>KATA PENGANTAR.....</b>	<b>iii</b>
<b>UCAPAN TERIMA KASIH.....</b>	<b>iv</b>
<b>DAFTAR ISI .....</b>	<b>vi</b>
<b>DAFTAR GAMBAR.....</b>	<b>ix</b>
<b>DAFTAR TABEL .....</b>	<b>xi</b>
<b>DAFTAR SINGKATAN .....</b>	<b>xii</b>
<b>DAFTAR ISTILAH .....</b>	<b>xiii</b>
<b>DAFTAR LAMPIRAN .....</b>	<b>xiv</b>
<b>BAB I PENDAHULUAN</b>	
1.1 Latar Belakang .....	1
1.2 Tujuan.....	2
1.3 Rumusan Masalah .....	2
1.4 Batasan Masalah .....	2
1.5 Metode Penelitian.....	3
1.6 Sistematika Penulisan.....	4
<b>BAB II DASAR TEORI</b>	
2.1 Definisi <i>Honeypot</i> .....	5
2.2 Penelitian Awal <i>Honeypot</i> .....	5
2.2.1 Kelemahan Sistem yang Telah Ada.....	5
2.2.2 <i>Honeynet</i> .....	6
2.2.3 Hasil dari <i>Honeynet</i> Project .....	8
2.2.4 Perbandingan dari Beberapa <i>Honeypot</i> .....	10
2.3 Lokasi Penempatan <i>Honeypot</i> .....	10
2.4 Kelebihan dan Kekurangan <i>Honeypot</i> .....	13
2.5 Kategori <i>Honeypot</i> .....	14

2.6 Level of Involvement .....	15
2.6.1 <i>Low Involvement Honeypot</i> .....	15
2.6.2 <i>Mid Involvement Honeypot</i> .....	16
2.6.3 <i>High Involvement Honeypot</i> .....	16
2.6.2 Perbandingan Karakteristik <i>Level of Involvement</i> .....	17
2.7 <i>Intrusion Detection System(IDS)</i> .....	17
2.8 <i>Firewall</i> .....	18
2.9 Snort IDS dan IPTables .....	19
2.9.1 Snort IDS .....	19
2.9.2 IPTables .....	20
2.10 Voice over Internet Procotol .....	21
2.10.1 <i>Session Initiation Protocol</i> .....	21
2.10.2 Arsitektur SIP .....	21
2.10.3 Format <i>Message SIP</i> .....	22
2.10.4 Model <i>Security SIP</i> .....	24
2.10.5 <i>Attack Vector</i> pada SIP .....	26
<b>BAB III PERANCANGAN DAN IMPLEMENTASI</b>	
3.1 Skenario Perancangan Sistem .....	27
3.2 Sistem Kerja <i>Honeypot</i> .....	29
3.3 Perangkat yang Diperlukan .....	30
3.3.1 Perangkat Lunak .....	30
3.3.2 Perangkat Keras .....	33
3.4 Instalasi dan Konfigurasi .....	35
3.5 <i>Tool Attack</i> .....	38
3.5.1 <i>Attack Vector</i> .....	38
3.5.2 Tool Penguji <i>Firewall</i> .....	39
3.5.3 Tool Penguji Snort .....	39
3.5.4 Tool Penguji Artemisa .....	40
<b>BAB IV PENGUJIAN DAN ANALISIS HASIL IMPLEMENTASI</b>	
4.1 Gambaran Analisis .....	41
4.2 Analisis Pengujian terhadap Keamanan VoIP .....	41

4.2.1 Analisis Pengujian terhadap Keamanan VoIP Berdasarkan Vektor <i>Attack pada SIP</i> .....	41
4.2.1.1 Pengumpulan Informasi, <i>Footprinting</i> , dan Enumerasi.....	41
4.2.1.2 Monitoring Trafik dan <i>Eavesdrooping</i> .....	43
4.2.1.3 <i>Attacking Authentication</i> .....	45
4.2.1.4 <i>Denial of Service Attack (DoS)</i> .....	47
4.2.2 Analisis Pengujian <i>Firewall</i> terhadap Keamanan VoIP .....	50
4.2.2.1 Pengujian Firewall dengan Menggunakan <i>Scanning</i> .....	50
4.2.2.2 Pengujian Firewall dengan Menggunakan Denial of Service.....	51
4.2.3 Analisis Pengujian Keamanan VoIP Berdasarkan Kemampuan <i>Fingerprint Honeypot</i> .....	54
4.2.3.1 <i>Sipvicious</i> .....	54
4.2.3.2 <i>PROTOS</i> .....	56
4.2.3.3 <i>Invite Flooding</i> .....	56
4.2.3.4 <i>SIPp</i> .....	57
4.2.3.5 <i>SIPScan</i> .....	58
4.2.3.6 <i>SIPSak</i> .....	58
4.2.3.7 <i>SMAP</i> .....	59
4.2.4 Analisis Pengujian <i>Snort</i> terhadap Keamanan VoIP .....	60
4.2.4.1 <i>Denial of Service</i> .....	61
4.2.4.2 <i>Arpspoofing</i> .....	61
4.2.4.3 <i>Portscanning</i> .....	62
4.2.4.1 <i>False Negative dan False Positif Snort</i> .....	62

## **BAB V KESIMPULAN DAN SARAN**

5.1 Kesimpulan .....	66
5.2 Saran.....	68

## **DAFTAR PUSTAKA**

### **LAMPIRAN A**

### **LAMPIRAN B**

### **LAMPIRAN C**

### **LAMPIRAN D**

### **LAMPIRAN E**