

DAFTAR ISI

LEMBAR PENGESAHAN	ii
PERNYATAAN BEBAS PLAGIARISME	iv
HALAMAN PERTANYAAN PUBLIKASI	v
ABSTRAK	vi
ABSTRACT	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xvi
DAFTAR SINGKATAN	xvii
DAFTAR ISTILAH	xviii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Metode Penelitian	3
1.7 Sistematika Penulisan	4
BAB II LANDASAN TEORI	6
2.1 Pengertian Perbandingan	6
2.2 Definisi Router	6
2.3 Definisi <i>Computer Security</i>	7
2.4 Definisi <i>Network Security</i>	8

2.4.1 Firewall	10
2.4.2 IDS	12
2.4.2 ACL	14
2.5 Definisi GNS3	16
2.6 Definisi Oracle VM Virtualbox.....	16
2.7 Definisi Snort	17
BAB III RANCANGAN SIMULASI JARINGAN	18
3.1 Perancangan Simulasi	18
3.1.1 Skenario Perancangan Implementasi Simulasi	18
3.1.2 Skenario proses kinerja Firewall	20
3.1.3 Skenario proses kinerja IDS.....	21
3.1.4 Skenario proses kinerja ACL.....	22
3.2 Kebutuhan Software dan Hardware	23
3.3 Implementasi	24
3.3.1 Instalasi Software GNS3.....	24
3.3.2 Instalasi Software VM Virtualbox.....	27
BAB IV HASIL DAN PEMBAHASAN	31
4.1 Pengujian <i>End to End Device</i>	31
4.1.1 Konfigurasi <i>End to End Device</i>	31
4.1.2 Hasil Pengujian <i>End to End Device</i>	32
4.2 Pengujian Firewall.....	33
4.2.1 Konfigurasi Firewall.....	34
4.2.2 Hasil Pengujian Firewall.....	35
4.3 Pengujian ACL.....	39
4.3.1 Konfigurasi ACL.....	40
4.3.2 Hasil Pengujian ACL	42

4.4 Pengujian IDS	45
4.4.1 Konfigurasi IDS.....	45
4.4.2 Hasil pengujian IDS	50
4.5 Perbandingan antara Firewall, ACL, dan IDS	52
4.5.1 Karakteristik, Kelebihan, dan Kekurangan Firewall	52
4.5.2 Karakteristik, Kelebihan, dan Kekurangan ACL.....	52
4.5.3 Karakteristik, Kelebihan, dan Kekurangan IDS.....	53
BAB V PENUTUP	55
5.1 Kesimpulan	55
5.2 Saran	56
DAFTAR PUSTAKA.....	57
LAMPIRAN.....	59

DAFTAR GAMBAR

Gambar 2.1 Ilustrasi Firewall	10
Gambar 2.2 Ilustrasi Sistem IDS.....	12
Gambar 2.3 Topologi ACL	14
Gambar 2.4 Logo GNS3	16
Gambar 2.5 Logo Virtualbox	16
Gambar 2.6 Logo Snort IDS	17
Gambar 3.1 Skenario <i>Flowchart</i> perancangan simulasi	18
Gambar 3.2 Skenario <i>Flowchart</i> kinerja Firewall.....	20
Gambar 3.3 Skenario <i>Flowchart</i> kinerja IDS	21
Gambar 3.4 Skenario <i>Flowchart</i> kinerja ACL	22
Gambar 3.5 Instalasi GNS3	24
Gambar 3.6 <i>Setup</i> GNS3.....	25
Gambar 3.7 <i>License</i> GNS3	25
Gambar 3.8 <i>Finishing</i> GNS3.....	26
Gambar 3.9 Tampilan utama GNS3.....	26
Gambar 3.10 Instalasi Virtualbox.....	27
Gambar 3.11 Memulai Instalasi	27
Gambar 3.12 Pemilihan tempat lokasi <i>driver</i>	28
Gambar 3.13 Proses <i>Warming</i> pada proses instalasi	28
Gambar 3.14 Proses <i>install</i>	29

Gambar 3.15 <i>Finishing</i> Virtualbox.....	29
Gambar 3.16 Tampilan Utama Virtualbox	30
Gambar 4.1 Proses Penginstalan pada Virtualbox.....	31
Gambar 4.2 Pengaturan IP Address secara manual	32
Gambar 4.3 Ping dari Lubuntu-1 ke Lubuntu-2	32
Gambar 4.4 Ping dari Lubuntu-2 ke Lubuntu-1	33
Gambar 4.5 Topologi untuk Firewall	33
Gambar 4.6 Tampilan Hasil show ip	35
Gambar 4.7 Hasil Ping Inside di R2	35
Gambar 4.8 Tampilan IP <i>route</i> Inside di R2	36
Gambar 4.9 Hasil Ping Outside di R3	36
Gambar 4.10 Hasil Ping R2 ke R3.....	36
Gambar 4.11 Hasil Ping dari R3	37
Gambar 4.12 Hasil Ping di R4.....	37
Gambar 4.13 Hasil Ping di Lubuntu-2	38
Gambar 4.14 Hasil uji Ping 172.18.21.2 di R2	38
Gambar 4.15 Hasil uji Ping R2 dan R3 di Firewall.....	39
Gambar 4.16 Hasil pengujian debug IP ICMP.....	39
Gambar 4.17 Topologi untuk ACL dan IDS.....	40
Gambar 4.18 Hasil tes ACL di R1	42
Gambar 4.19 Hasil tes ACL di R4	42
Gambar 4.20 Hasil tes ACL di Lubuntu-2.....	43
Gambar 4.21 Tampilan hasil show access-lists R1	43
Gambar 4.22 Hasil tes Lubuntu-1	44
Gambar 4.23 Hasil tes <i>interface</i> R4	44
Gambar 4.24 Tampilan hasil show access-lists R4.....	45

Gambar 4.25 versi Snort.....	46
Gambar 4.26 Tampilan snort.conf.....	49
Gambar 4.27 Tampilan local.rules	50
Gambar 4.28 Hasil uji tes notifikasi pesan IDS Client.....	51
Gambar 4.29 Hasil uji test notifikasi pesan di Router R4.....	51

DAFTAR TABEL

Tabel 3.1 Daftar Software yang digunakan	23
Tabel 3.2 Daftar Spesifikasi Hardware Laptop	24
Tabel 4.1 Daftar Alamat IP pada Firewall.....	34
Tabel 4.2 Daftar Alamat IP pada ACL	40
Tabel 4.3 Daftar Alamat IP untuk sistem IDS	45

DAFTAR SINGKATAN

ACL	<i>(Access Control List)</i>
DoS	<i>(Denial of Service)</i>
GUI	<i>(Graphical User Interface)</i>
HIDS	<i>(Host-Based Intrusion Detection System)</i>
ICMP	<i>(Internet Control Message Protocol)</i>
IDS	<i>(Intrusion Detection System)</i>
IPS	<i>(Intrusion Prevention System)</i>
IP	<i>(Internet Protocol)</i>
ISP	<i>(Internet Service Provider)</i>
NAT	<i>(Network Address Translation)</i>
NIDS	<i>(Network-Based Intrusion Detection System)</i>
UDP	<i>(User Datagram Protocol)</i>
VM	<i>(Virtual Machine)</i>

DAFTAR ISTILAH

- ACL** *ACL (Access Control List)* Adalah kumpulan *list* kondisi dari setiap akses. ACL dapat men-filter paket data yang tidak diinginkan dan dapat diimplementasikan sebagai *Access Policy*.
- Router** *Router* adalah sebuah alat yang digunakan untuk mengirim paket dari beberapa 2 buah network berbeda. Router bekerja pada lapisan OSI Layer ke-2 (*Network Layer*). Baik network yang sama maupun yang berbeda (secara fisik dan logika).
- Firewall** Bertugas di pintu gerbang masuk jaringan dan setiap packet yang melaluinya perlu mematuhi *policy firewall* tersebut. Jadi adalah suatu mekanisme untuk melindungi keamanan jaringan komputer dengan menyaring paket data yang keluar dan masuk di jaringan.
- Snort** Snort adalah NIDS yang bekerja dengan menggunakan *signature detection*, berfungsi juga sebagai *sniffer* dan *packet logger*. Snort pertama kali di buat dan dikembangkan oleh Marti Roesh.
- IDS** *Intrusion Detection System(IDS)* merupakan sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan pada sebuah sistem atau jaringan. Jika ditemukan aktivitas yang mencurigakan pada traffic jaringan maka IDS akan memberikan sebuah peringatan terhadap sistem atau administrator jaringan dan melakukan analisis dan mencari bukti dari percobaan penyusupan.
- VM** *Virtual Machine (VM)* adalah program perangkat lunak atau sistem operasi yang tidak hanya menunjukkan perilaku komputer yang terpisah, tetapi juga mampu melakukan tugas-tugas seperti menjalankan aplikasi dan program seperti komputer yang terpisah.