PERANCANGAN ATURAN PENCEGAHAN TERHADAP SERANGAN *DENIAL OF SERVICE* MENGGUNAKAN METODE *INTRUSION PREVENTION SYSTEM* (IPS) (STUDI KASUS : TEKNIK INFORMATIKA UNIVERSITAS PASUNDAN BANDUNG)

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan

Program Strata 1, Program Studi Teknik Informatika,

Universitas Pasundan Bandung

oleh :

Ujang Sodikin

12.304.0215

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS PASUNDAN BANDUNG

SEPTEMBER 2016

DAFTAR ISI

DAFTAR ISTILAH

No	Daftar Istilah	Pengertian
1	Intrusion Prevention System	merupakan suatu perangkat lunak atau sistem perangkat keras yang bekerja secara otomatis untuk memonitor kejadian pada jaringan computer dan dapat menganalisa masalah keamanan jaringan
2	Intrusion Detecetion System	adalah pendekatan yang sering digunakan untuk membangun *system* keamanan komputer, IPS mengkombinasikan teknik firewall dan metode *Intrusion Detection System* (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor
3	Denial of Service	Salah satu ancaman keamanan jaringan yang membuat suatu layanan jaringan jadi tersendat, serangan yang membuat jaringan tidak bisa diakses atau serangan yang membuat sistem tidak bisa memproses atau merespon permintaan layanan terhadap object dan *resource* jaringan.
4	*Availability*	User yang mempunyai hak akses (*authorized user*) diberi akses tepat waktu dan tidak terkendala apapun.
5	Network Intrusion Prevention System (NIPS)	Memonitor lalu lintas jaringan untuk segmen jaringan tertentu atau perangkat dan analisis jaringan dan aplikasi dan protocol aplikasi untuk mengidentifikasi aktivitas yang mencurigakan, hal ini dapat berfungsi mengidentifikasi berbagai jenis peristiwa yang menarik
6	Ping Of Death	Dengan menggunakan tool khusus, penyerang dapat mengirimkan paket ping yang oversize yang banyak kepada korban. Ping of death tidak lebih dari semacam serangan buffer overflow. Serangan ini dapat menyebabkan crash sistem, freeze atau reboot.
7	Snort	Snort merupakan sebuah *tool analysis* diantaranya *sniffer,packet logger*, forensic data analysis tool, dan network intrusion detection system, yang dikembangakan pertama kali oleh Martin Roesh,
8	Msg	pesan alert untuk mencetak informasi bersama dengan sebuah paket dump
9	Refernce	Keyword *reference* memungkinkan rule – rule untuk memasukan referensi – referensi ke sistem – sitem pengidentitikasi serangan eksternal.
10	GID	Keyword *gid* digunakan untuk mengenali event saat rule tertentu diaktikan.
11	SID	Keyword *SID* digunakan untuk mengenali rule snort secara unik
12	Rev	Rev digunakan untuk mengidentifikasi revisi – revisi atas rule – rule snort
13	Classtype	Classtype digunakan untuk mengkategorikan sebuah rule sebagai pendeteksi sebuah serangan, yang menjadi bagian dari jenis serangan kelas lebih umum
14	Priority	Sebagaimana diidikasikan namanya, tag priority memberi pembagian level prioritas atas rule – rule.

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN