

DAFTAR ISI

HALAMAN PENGESAHAN.....	i
PERNYATAAN BEBAS PLAGIARISME	iii
HALAMAN PERNYATAAN PUBLIKASI PROYEK AKHIR.....	iv
ABSTRAK.....	v
ABSTRACT.....	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL.....	xiii
DAFTAR ISTILAH.....	xiv
DAFTAR SINGKATAN.....	xv

BAB I PENDAHULUAN

1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	2
1.6 Metodologi Penelitian.....	3
1.7 Sistematika Penulisan.....	3

BAB II LANDASAN TEORI

2.1 Pengertian Keamanan.....	5
2.2 Jaringan Komputer	7
2.3 Keamanan Jaringan Komputer.....	11
2.4 <i>Server</i>	11
2.5 <i>Telegram</i>	11
2.6 <i>Bot Telegram</i>	12
2.7 <i>IPS (Intuction Prevention System)</i>	12
2.8 <i>IDS (Intrusion Detection System)</i>	13
2.9 <i>Snort</i>	15
2.10 <i>Honeypot</i>	16

viii

2.11 <i>Shell-Bot</i>	17
-----------------------------	----

2.12	<i>Internet Control Message Protocol (ICMP)</i>	17
2.13	<i>Transmission Control Protocol (TCP)</i>	17
2.14	<i>User Datagram Protocol (UDP)</i>	17
2.15	<i>Ubuntu</i>	18
2.16	<i>Linux</i>	18
2.17	<i>PuTTY</i>	18
2.18	<i>Zenmap</i>	18
2.19	<i>Command Prompt</i>	18
2.20	<i>SSH Server</i>	19

BAB III PERANCANGAN DAN IMPLEMENTASI

3.1	Analisa Kebutuhan Sistem	20
3.2	Diagram Alur Penelitian.....	21
3.3	Gambar Umum Sistem	22
3.4	Tampilan <i>Ubuntu</i>	26
3.5	<i>Telegram Bot</i> Token dan ID Pengguna.....	26
3.6	Rancangan Pengujian Sistem	27

BAB IV HASIL DAN PEMBAHASAN

4.1	Implementasi Arsitektur Jaringan	29
4.2	Implementasi Perangkat Lunak <i>Snort</i>	30
4.3	Konfigurasi Jaringan dan Aturan File <i>Snort</i>	32
4.4	Memasang <i>Barnyard2</i>	33
4.5	Menambah Peringatan Serangan	34
4.6	Berjalan Sebagai <i>Daemon</i>	36
4.7	<i>Base-GUI WEB</i> untuk <i>Snort</i>	36
4.8	Implementasi Perangkat Lunak <i>Honeypot</i>	38
4.9	Install dan Konfigurasi <i>Kippo Graph (Web Interface Log Kippo)</i>	39
4.10	Aplikasi	40
4.11	Persiapan dan Hasil Pengujian Serangan	40
4.12	Implementasi <i>Telegram Bot</i>	48
4.13	Implementasi Notifikasi <i>Bot Telegram</i>	50
4.14	Notifikasi <i>Bot Telegram</i>	51
4.15	Implementasi <i>Shell-bot</i>	51
4.16	Hasil dan Pengujian <i>Shell-bot</i>	52
4.17	Hasil dan Perbandingan Akurasi IDS	54

4.18	Hasil Akurasi Notifikasi Telegram.....	55
------	--	----

4.19	Informasi Serangan yang di Terima <i>Bot Telegram</i>	55
4.20	Hasil Pengujian Sistem	56

BAB V PENUTUP

5.1	Kesimpulan	57
5.2	Saran	57

DAFTAR PUSTAKA	58
-----------------------------	-----------

LAMPIRAN	59
-----------------------	-----------

DAFTAR GAMBAR

Gambar 2.1 Skema <i>Main In The Middle Attack</i>	5
Gambar 2.2 Skema bentuk dari <i>Denial of service Attack</i>	6
Gambar 2.3 <i>Sniffer Attack</i>	6
Gambar 2.4 Skema serangan <i>Brute Force</i>	7
Gambar 2.5 Bentuk jaringan PAN	8
Gambar 2.6 Bentuk jaringan LAN	8
Gambar 2.7 Bentuk jaringan MAN	9
Gambar 2.8 Bentuk jaringan WAN	10
Gambar 2.9 Logo <i>Telegram</i>	11
Gambar 2.1 Logo <i>Snort</i>	15
Gambar 3.1 Diagram Alur Penelitian	21
Gambar 3.2 Implementasi IDS dan IPS	22
Gambar 3.3 Alur informasi pengiriman serangan ke <i>Telegram</i>	22
Gambar 3.4 Alur informasi pengiriman serangan ke <i>kippo graph</i>	23
Gambar 3.5 Diagram <i>Snort & IPS User Use Case</i> Sistem.....	23
Gambar 3.6 Diagram <i>Honeypot & IPS User Case</i> Sistem	24
Gambar 3.7 <i>Flowchart Snort</i> Deteksi Serangan.....	25
Gambar 3.8 <i>Flowchart Honeypot</i> Deteksi Serangan.....	25
Gambar 3.9 Flowchart IPS Pengamanan.....	25
Gambar 3.10 Versi <i>Ubuntu</i>	26
Gambar 3.11 <i>Flowchart set Telegram Bot Token</i>	27
Gambar 3.12 Skenario pengujian Sistem.....	27
Gambar 4.1 Versi <i>Snort</i>	30
Gambar 4.2 Versi <i>barnyard2</i>	33
Gambar 4.3 Peringatan di dalam <i>Local.rules</i>	34
Gambar 4.4 Penyesuaian <i>barnyard2</i> dengan <i>local.rules</i>	35
Gambar 4.5 <i>Base-Gui web snort</i>	38
Gambar 4.6 Tampilan Perubahan <i>ssh_port</i>	39
Gambar 4.7 Pengiriman paket berupa <i>ping</i> ke <i>ip address</i>	41
Gambar 4.8 Serangan menuju ICMP terdeteksi dalam <i>BASE Snort</i>	42
Gambar 4.9 Scan port TCP dengan <i>zenmap</i>	43
Gambar 4.10 Scan port TCP Terdeteksi di <i>Base snort</i>	43
Gambar 4.11 Scan port UDP dengan <i>Zenmap</i>	44
Gambar 4.12 Scan port UDP Terdeteksi di <i>Base snort</i>	44
Gambar 4.13 Analisa ip adres dan port dengan <i>PutTY</i>	45

Gambar 4.14 Sistem <i>Brute force</i>	46
Gambar 4.15 Melakukan kegiatan di dalam SSH	46
Gambar 4.16 Pendeteksi dalam bentuk <i>Web</i>	47
Gambar 4.17 Pendeteksi dalam bentuk Terminal	47
Gambar 4.18 Memulai <i>bot Telegram</i>	48
Gambar 4.19 Membuat <i>Bot Telegram</i>	49
Gambar 4.20 Mendapat <i>token Telegram Bot</i>	49
Gambar 4.21 Mendapat <i>ID chat</i>	50
Gambar 4.22 <i>load.php</i>	50
Gambar 4.23 Notifikasi <i>Bot Telegram</i>	51
Gambar 4.24 Pemblokiran Ip.....	52
Gambar 4.25 Pengecekan Ip yang terblokir	52
Gambar 4.26 <i>Unblock ip</i>	53
Gambar 4.27 Hasil dari ip yang di blok.....	54

DAFTAR TABEL

Tabel 4.1 Konfigurasi <i>IP Address</i> IDS	29
Tabel 4.2 Konfigurasi <i>IP Address attacker</i>	29
Tabel 4.3 Akurasi waktu terdeteksi.....	55
Tabel 4.4 Akurasi waktu notifikasi <i>telegram</i>	56
Tabel 4.5 Informasi serangan terdeteksi	56
Tabel 4.6 Hasil Pengujian Sistem.....	57

DAFTAR SINGKATAN

IPS	: <i>Intrusion Prevention System</i>
HIPS	: <i>Host-based Intrusion Prevention System</i>
NIPS	: <i>Network-based Intrusion Prevention System</i>
IDS	: <i>Intrusion Detection System</i>
HIDS	: <i>Host Intrusion Detection System</i>
NIDS	: <i>Network Intrusion Detection System</i>
PAN	: <i>Personal Area Network</i>
LAN	: <i>Local Area Network</i>
MAN	: <i>Metropolitan Area Network</i>
WAN	: <i>Wide Area Network</i>
DOS	: <i>Denial Of Service</i>
DDOS	: <i>Distributed Denial Of Service</i>
INTERNET	: <i>Interconnection Network</i>
API	: <i>Application Programing Interface</i>
ICMP	: <i>Internet Control Message Protocol</i>
TCP	: <i>Transmission Control Protocol</i>
UDP	: <i>User Datagram Protocol</i>
CMD	: <i>Comannd Prompt</i>
SSH	: <i>Secure Shell</i>
FTP	: <i>File Transfer Protocol</i>

DAFTAR ISTILAH

Attacker : Penyerang

Administrator : Selaku *admin* yang menjalankan atau mengamankan *server*

Server : Sistem komputer yang menyediakan jenis layanan dalam sebuah jaringan komputer

Notifikasi : Pemberitahuan