

DAFTAR ISI

HALAMAN PENGESAHAN	i
HALAMAN PERSEMBAHAN	ii
KATA PENGANTAR	iii
DAFTAR ISI	vii
DAFTAR TABEL	viii
DAFTAR GAMBAR	ix
Abstrak	x
<i>Abstract</i>	xi
I LATAR BELAKANG	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Hipotesis	2
1.5 Tujuan Penelitian	2
1.6 Metode Penyelesain Masalah	3
1.7 Sistematika Penulisan	4
II TINJAUAN PUSTAKA DAN DASAR TEORI	5
2.1 Telegram Bot	5
2.2 <i>Intrusion Detection System (IDS)</i>	5
2.2.1 <i>Network Intrusion Detection System (NIDS)</i>	5
2.2.2 <i>Host Intrusion Detection System (HIDS)</i>	6
2.2.3 <i>System Integrity Verifier (SIV)</i>	6
2.2.4 <i>Log File Monitor (LFM)</i>	6
2.3 <i>Distributed Denial of Service (DDoS)</i>	6
2.4 <i>Brute Force Attack</i>	7
2.5 <i>Scanning</i>	7

2.5.1	<i>Host Discovery</i>	7
2.5.2	<i>Port Detections</i>	7
2.5.3	<i>Service Scanning</i>	7
2.5.4	<i>Host Detection</i>	8
2.5.5	<i>Scapy</i>	8
III METODOLOGI PENELITIAN		9
3.1	Gambaran Umum	9
3.1.1	<i>(Capture Network)</i>	9
3.1.2	<i>Deteksi Anomali</i>	9
3.1.3	<i>Repost Telegram</i>	9
3.2	Gambaran Khusus	10
3.2.1	<i>Capture Packet</i>	11
3.2.2	<i>Pengolahan Rule</i>	11
3.2.3	<i>Pemindain Rule</i>	11
3.2.4	<i>Blocking</i>	11
3.2.5	<i>Repost Telegram</i>	11
3.2.6	<i>Pembuatan Rule Baru</i>	11
3.3	<i>Capture Packet</i>	12
3.4	<i>Pengolahan Traffik</i>	12
3.5	Dataset	12
3.5.1	<i>Transmission Control Protocol (TCP)</i>	13
3.5.2	<i>Internet Control Message Protocol (ICMP)</i>	14
3.5.3	<i>Internet Protocol Address (IP)</i>	15
3.5.4	<i>User Datagram Protocol (UDP)</i>	15
3.6	<i>Autonomous System</i>	16
3.7	<i>Telegram Command and Control (CNC)</i>	17
3.8	<i>Attacking Tools</i>	18
3.8.1	NMAP	18
3.8.2	NESSUS	18
3.8.3	METASPLOIT AUXILIARY	18
3.8.4	TCP Scanning	18
3.8.5	HYDRA dan Medusa	19
3.8.6	Zero Brute	19
3.8.7	Metasploit SynFlood	19

3.8.8	Slowloris	19
3.8.9	HULK	19
3.8.10	PyLoris	19
3.9	Alat dan Bahan	20
3.9.1	Perangkat Keras	20
3.9.2	Perangkat Lunak	20

IV HASIL DAN PEMBAHASAN 21

4.1	Kebutuhan Pengujian	21
4.1.1	<i>Scanning Tools</i>	21
4.1.2	<i>Brute Force Tools</i>	21
4.1.3	<i>DDoS Tools</i>	22
4.2	Pengujian Akurasi Masing-Masing Tools	22
4.2.1	NMAP	22
4.2.2	NESSUS	23
4.2.3	Metasploit Auxiliary	23
4.2.4	TCP Scanning Tools	24
4.2.5	Hydra	24
4.2.6	Medusa	25
4.2.7	Metasploit Auxiliary	25
4.2.8	Zero Brute	26
4.2.9	Nmap Script Enggine	26
4.2.10	Metasploit SynFlood	27
4.2.11	Slowloris	27
4.2.12	TCP Flood	28
4.2.13	HULK	28
4.2.14	PyLoris	29
4.3	Pengujian Akurasi	29
4.3.1	Skenario Pertama	29
4.3.2	Skenario Kedua	39
4.3.3	Skenario Ketiga	48
4.3.4	Skenario Keempat	54
4.3.5	Skenarion Kelima	55

V KESIMPULAN DAN SARAN	57
5.1 Kesimpulan	57
5.2 Saran	57
DAFTAR PUSTAKA	58