

DAFTAR ISI

HALAMAN JUDUL.....	1
HALAMAN PENGESAHAN.....	ii
HALAMAN PENGESAHAN DEWAN PENGUJI.....	iii
PERNYATAAN BEBAS PLAGIASI.....	iv
HALAMAN PERSEMBAHAN.....	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
DAFTAR SINGKATAN	xiii
INTISARI.....	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian	4
1.4 Batasan Penelitian	4
1.5 Manfaat Penelitian	6
1.6 Sistematika Penulisan	6
1.6.1 BAB I PENDAHULUAN	7
1.6.2 BAB II TINJAUAN PUSTAKA DAN DASAR TEORI	7
1.6.3 BAB III METODOLOGI PENELITIAN.....	7
1.6.4 BAB IV HASIL DAN PEMBAHASAN	7
1.6.5 BAB V KESIMPULAN DAN SARAN.....	7
BAB II TINJAUAN PUSTAKA DAN DASAR TEORI.....	8
2.1 Tinjauan Pustaka	8
2.2 Analisis Perbandingan Metode	20
2.3 Pertanyaan Penelitian	22
2.4 Dasar Teori.....	23
2.3.1 Bash Scripting	23
2.3.2 Forensik Digital.....	23
2.3.3 Regular Expression	24
2.3.4 API (Application Programming Interface).....	25
2.3.5 XSS (Cross-Site Scripting)	26

2.3.6	DDoS (Distributed Denial-of-Service)	27
2.3.7	Access Log	28
2.3.8	Nginx Web Server.....	28
2.3.9	Wordpress dan WooCommerce	29
2.3.10	OSI Layer	29
2.3.11	VPN (Virtual Private Network)	30
BAB III METODE PENELITIAN.....		31
3.1	Alat dan Bahan Penelitian.....	31
3.1.1	Alat Penelitian.....	31
3.1.2	Bahan Penelitian.....	35
3.2	Metode yang Digunakan	36
3.3	Alur Penelitian	38
3.3.1	Studi Literatur dan Perbandingan Alat Serta Identifikasi Kebutuhan	39
3.3.2	Perancangan alat.....	39
3.3.2.1	Rancangan alat	39
3.3.2.2	<i>Flowchart</i> filter <i>access log</i>	41
3.3.2.3	<i>Pseudocode</i> alat untuk filter <i>access log</i>	42
3.3.2.4	<i>Flowchart</i> alat untuk filter negara.....	43
3.3.2.5	<i>Pseudocode</i> alat untuk filter negara	45
3.3.3	Pembuatan kode	46
3.3.3.1	Pembuatan <i>regular expression</i>	46
3.3.3.2	Pembuatan kode untuk filter <i>access log</i>	47
3.3.3.3	Pembuatan kode untuk filter negara.....	47
3.3.3.4	Integrasi dengan API <i>ipdata.co</i>	48
3.3.4	Skenario pengujian alat dan pengumpulan data.....	49
3.3.4.1	Skenario secara umum	49
3.3.4.2	Skenario <i>web server</i> dan situs web	50
3.3.4.3	Skenario serangan	51
3.3.4.4	Skenario forensik	53
3.3.5	Analisis dan penarikan kesimpulan.....	54
BAB IV HASIL DAN PEMBAHASAN		55
4.1	Implementasi Rancangan Alat	55
4.1.1	Implementasi Kode Filter Dari Access Log.....	55
4.1.2	Implementasi Kode Filter Negara	60
4.2	Pengujian Serangan.....	62
4.2.1	Pengujian Serangan XSS.....	62
4.2.2	Pengujian Serangan DDoS dan DoS	68

4.3	Pengujian Penggunaan Alat	71
4.3.1	Proses instalasi	71
4.3.2	Pengujian pada proses digital forensik.....	72
4.4	Beberapa informasi tambahan hasil pengujian	88
4.5	Perbandingan Dengan Alat Sejenis.....	90
4.6	Kelebihan dan kekurangan alat	92
4.7	Kelebihan dan kekurangan penelitian	93
BAB V KESIMPULAN DAN SARAN.....		95
5.1	Kesimpulan	95
5.2	Saran.....	96
DAFTAR PUSTAKA		98
LAMPIRAN		102