

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	5
1.3 Tujuan	5
1.4 Batasan masalah	6
1.5 Kerangka pemikiran	7
1.6 Sistematika Penulisan	7
BAB II KAJIAN LITERATUR	10
2.1 Tinjauan Pustaka	10
2.2 Landasan Teori	13
2.2.1 Cloud Computing	13
2.2.2 Networking	13
2.2.3 Internet	14
2.2.4 Domain Name System	15
2.2.5 Server	16
2.2.6 Webserver	16
2.2.7 Cybersecurity	16
2.2.8 DDOS Attack	16
2.2.9 Cloudflare	17
BAB III METODOLOGI PENELITIAN	18
3.1 Gambaran Umum Mengenai Metode OCTAVE	18
3.2 Phase 1: Build Assets Threat Profile	19
3.3 Phase 2: Identify Infrastructure Vulnerabilities	20
3.4 Phase 3: Develops Security Strategy and Plans	21

BAB IV HASIL DAN PEMBAHASAN	22
4.1 Phase 1: Build Assest-Based Threat Profile	22
4.2 Phase 2: Identify Insfrastructure Vulnerabilities	23
4.3 Phase 3: Develops Security Strategy Plans	23
4.4 Konfigurasi keamanan pada CLOUDFLARE	25
4.5 Alur Pengujian Serangan DDOS Attack	30
4.6 Hasil Serangan Terhadap domain APTAPLUS.ONLINE	32
4.6.1 Pengujian 1	32
4.6.2 Pengujian 2	34
4.6.3 Pengujian 3	37
4.6.4 Pengujian 4	39
4.6.5 Pengujian 5	42
4.6.6 Pengujian 6	45
4.7 Hasil Serangan Terhadap domain BYPASS.APTAPLUS.ONLINE	47
4.7.1 Pengujian 7	48
4.7.2 Pengujian 8	50
4.7.3 Pengujian 9	52
BAB V KESIMPULAN	55
5.1 Kesimpulan	55
5.2 Saran	56
DAFTAR PUSTAKA	57
DAFTAR RIWAYAT HIDUP	59

DAFTAR GAMBAR

Gambar 1. 1 Kerangka Pemikiran	7
Gambar 2. 1 Contoh Sebuah Jaringan Komputer	13
Gambar 2. 2 Perubahan Computing Envirovment	14
Gambar 2. 3 Struktur DNS	15
Gambar 2. 4 Skema DDOS Attack	17
Gambar 2. 5 Logo <i>Cloudflare</i>	17
Gambar 3. 1 Metode OCTAVE	18
Gambar 4. 1 Perubahan namerserver domain ke nameserver <i>Cloudflare</i>	25
Gambar 4. 2 Domain berhasil ditambahkan ke <i>Cloudflare</i>	26
Gambar 4. 3 Pengecekan IP Address domain dengan NSLOOKUP	26
Gambar 4. 4 Validasi dengan who.is terhadap IP Address baru	26
Gambar 4. 5 Konfigurasi SSL pada <i>Cloudflare</i>	27
Gambar 4. 6 Konfigurasi DDOS Ruleset	28
Gambar 4. 7 Tampilan beberapa konfigurasi rule dari serangan DDOS	28
Gambar 4. 8 Konfigurasi Security Level	28
Gambar 4. 9 Konfigurasi Browser Integrity Check	29
Gambar 4. 10 Konfigurasi Bot Fight Mode	29
Gambar 4. 11 Topologi Penyerangan	30
Gambar 4. 12 Tampilan interface website aptaplus.online	31
Gambar 4. 13 Tampilan interface website bypass.aptaplus.online	31
Gambar 4. 14 Hasil Monitoring CPU Pengujian 1	33
Gambar 4. 15 Hasil Monitoring Traffic Pengujian 1	33
Gambar 4. 16 Hasil Monitoring Bandwidth Pengujian 1	33
Gambar 4. 17 Metrics kinerja <i>webserver</i> pada Pengujian 1	34
Gambar 4. 18 Activity log pada Pengujian 1	34
Gambar 4. 19 Hasil Monitoring CPU Pengujian 2	35
Gambar 4. 20 Hasil Monitoring Traffic Pengujian 2	35
Gambar 4. 21 Hasil Monitoring bandwidth Pengujian 2	36
Gambar 4. 22 Metrics kinerja <i>webserver</i> pada Pengujian 2	36
Gambar 4. 23 Activity log pada Pengujian 2	36
Gambar 4. 24 Hasil Monitoring CPU Pengujian 3	37
Gambar 4. 25 Hasil Monitoring Traffic Pengujian 3	38
Gambar 4. 26 Hasil Monitoring Bandwidth Pengujian 3	38
Gambar 4. 27 Metrics kinerja <i>webserver</i> pada Pengujian 3	38

Gambar 4. 28 Activity log pada Pengujian 3	39
Gambar 4. 29 Hasil Monitoring CPU Pengujian 4	40
Gambar 4. 30 Hasil Monitoring Traffic Pengujian 4	40
Gambar 4. 31 Hasil Monitoring Bandwidth Pengujian 4	40
Gambar 4. 32 Metrics kinerja <i>webservice</i> pada Pengujian 4	40
Gambar 4. 33 Activity log pada Pengujian 4	41
Gambar 4. 34 Hasil Monitoring CPU Pengujian 5	42
Gambar 4. 35 Hasil Monitoring Traffic Pengujian 5	43
Gambar 4. 36 Hasil Monitoring Bandwidth Pengujian 5	43
Gambar 4. 37 Metrics kinerja <i>webservice</i> pada Pengujian 5	43
Gambar 4. 38 Activity log pada Pengujian 5	44
Gambar 4. 39 Hasil Monitoring CPU Pengujian 6	45
Gambar 4. 40 Hasil Monitoring Traffic Pengujian 6	46
Gambar 4. 41 Hasil Monitoring Bandwidth Pengujian 6	46
Gambar 4. 43 Activity log pada Pengujian 6	47
Gambar 4. 44 Hasil Monitoring CPU Pengujian 7	49
Gambar 4. 45 Hasil Monitoring Traffic Pengujian 7	49
Gambar 4. 46 Hasil Monitoring Bandwidth Pengujian 7	49
Gambar 4. 47 Metrics kinerja <i>webservice</i> pada Pengujian 7	49
Gambar 4. 48 Hasil Monitoring CPU Pengujian 8	51
Gambar 4. 49 Hasil Monitoring Traffic Pengujian 8	51
Gambar 4. 50 Hasil Monitoring Bandwidth Pengujian 8	51
Gambar 4. 51 Metrics kinerja <i>webservice</i> pada Pengujian 8	51
Gambar 4. 52 Hasil Monitoring CPU Pengujian 9	53
Gambar 4. 53 Hasil Monitoring Traffic Pengujian 9	53
Gambar 4. 54 Hasil Monitoring Bandwidth Pengujian 9	53
Gambar 4. 55 Metrics kinerja <i>webservice</i> pada Pengujian 9	53

DAFTAR TABEL

Tabel 3.1 Contoh Action Plan Phase 3	21
Tabel 4. 1 Hasil identifikasi phase 1	22
Tabel 4. 2 Hasil identifikas phase 2	23
Tabel 4. 3 Hasil identifikasi phase 3	23
Tabel 4. 5 Test Case Pengujian 1	32
Tabel 4. 6 Test Case Pengujian 2	35
Tabel 4. 7 Test Case Pengujian 3	37
Tabel 4. 8 Test Case Pengujian 4	39
Tabel 4. 9 Test Case Pengujian 5	42
Tabel 4. 10 Test Case Pengujian 6	45
Tabel 4. 11 Test Case Pengujian 7	48
Tabel 4. 12 Test Case Pengujian 8	50
Tabel 4. 13 Test Case Pengujian 9	52

