

DAFTAR GAMBAR

Gambar 2. 1 Keamanan Jaringan	6
Gambar 2. 2 Distributed Denial of Service	7
Gambar 2. 3 Intrusion Detection System	7
Gambar 2. 4 Network Intrusion Detection System.....	8
Gambar 2. 5 Host Intrusion Detection System	8
Gambar 2. 6 Virtual Private Server	9
Gambar 2. 7 Firewall	9
Gambar 2. 8 Python Programming [21].....	12
Gambar 2. 9 AAPanel	13
Gambar 2. 10 Putty.....	13
Gambar 3. 1 Rangkaian Proses.....	14
Gambar 3. 2 Perintah Ifconfig	16
Gambar 3. 3 Suricata HOME_NET	16
Gambar 3. 4 Suricata interface	16
Gambar 3. 5 Suricata rule-files	16
Gambar 3. 6 Putty Confirmation.....	17
Gambar 3. 7 Rancangan Jaringan	20
Gambar 4. 1 Status Suricata.....	22
Gambar 4. 2 Website Normal.....	23
Gambar 4. 3 CPU Normal (Server Target)	23
Gambar 4. 4 Log Suricata Kosong (Server Target)	24
Gambar 4. 5 Serangan Berhasil (GoldenEye - Botnet 1).....	25
Gambar 4. 6 Tanda Serangan Gagal (GoldenEye - Botnet 1)	25
Gambar 4. 7 Serangan Gagal (GoldenEye - Botnet 5).....	26
Gambar 4. 8 Website Tidak Normal	27
Gambar 4. 9 CPU Penuh (Server Target).....	27
Gambar 4. 10 Log Suricata Mendeteksi Serangan (Server Target)	28
Gambar 4. 11 Pengumpulan Data Dengan Suricata (Server Target)	28
Gambar 4. 12 Grafik Serangan Yang Diluncurkan Setiap 5 Menit (Tanpa Solusi)	30
Gambar 4. 13 Grafik Jumlah Serangan Terdeteksi Suricata (Tanpa Solusi)	31
Gambar 4. 14 Penggunaan CPU (VPS Target - Tanpa Solusi).....	31
Gambar 4. 15 Rangkaian Jaringan (Solusi Firewall)	32

Gambar 4. 16 CPU Kembali Normal (Server Target - Solusi Firewall).....	33
Gambar 4. 17 Log Suricata Masih Mendeteksi Serangan (Server Target - Solusi Firewall).....	34
Gambar 4. 18 Website Normal (Solusi Firewall).....	34
Gambar 4. 19 CPU Penuh (Server Target - Hapus Solusi Firewall).....	35
Gambar 4. 20 Log Suricata Mendeteksi Serangan (Server Target - Hapus Solusi Firewall).....	35
Gambar 4. 21 Website Tidak Bisa Diakses (Hapus Solusi Firewall).....	36
Gambar 4. 22 Grafik Jumlah Serangan Setiap 5 Menit (Solusi Firewall)	37
Gambar 4. 23 Jumlah Serangan Terdeteksi Suricata (Solusi Firewall)	38
Gambar 4. 24 Penggunaan CPU (VPS Target - Solusi Firewall)	38
Gambar 4. 25 Rangkaian Jaringan (Solusi DNS Cloudflare).....	39
Gambar 4. 26 Pilih Domain (DNS Cloudflare)	40
Gambar 4. 27 Pilih Menu Record (Cloudflare)	40
Gambar 4. 28 Menyalakan Proxy Status (Cloudflare)	41
Gambar 4. 29 Menu Overview (Cloudflare).....	41
Gambar 4. 30 Mengaktifkan Under Attack Mode (DNS Cloudflare).....	42
Gambar 4. 31 Penggunaan CPU Kembali Normal (Server Target - Solusi DNS Cloudflare).....	42
Gambar 4. 32 Halaman Keamanan Cloudflare (Solusi DNS Cloudflare)	43
Gambar 4. 33 Website Normal (Solusi DNS Cloudflare)	43
Gambar 4. 34 Log Suricata Tidak Mendeteksi Serangan Terbaru (Server Target - Solusi DNS Cloudflare).....	44
Gambar 4. 35 Grafik Jumlah Serangan Setiap 5 Menit (Solusi DNS Cloudflare) 45	
Gambar 4. 36 Jumlah Serangan Terdeteksi Suricata (Solusi DNS Cloudflare)...	46
Gambar 4. 37 Penggunaan CPU (VPS Target - Solusi DNS Cloudflare).....	46
Gambar 4. 38 Hasil Jumlah Serangan Terdeteksi	47
Gambar 4. 39 Penggunaan CPU (VPS Target - Perbandingan)	47