

ABSTRAK

Dave Handoko Priatmojo.

Skripsi

Analisis dan Implementasi *Distributed Denial of Service (DDoS) Attack* Terhadap *Website* dan *Server XYZ*

Dalam era digital saat ini, menjaga keamanan situs web dan infrastruktur server adalah hal yang sangat krusial untuk memastikan keamanan data dan kelancaran layanan yang disediakan secara *online*. Skripsi ini menggali analisis mendalam dan aplikasi praktis dari serangan *DDoS* yang terdistribusi pada infrastruktur *website* dan *server* milik instansi terkait. Skripsi ini bertujuan untuk memperdalam pemahaman tentang mekanisme serangan *DDoS* dan mengembangkan metode mitigasi yang efisien. Melalui penelitian ini, ditemukan berbagai pola serangan yang sering terjadi, dilakukan evaluasi terhadap kerentanan yang ada pada sistem, dan diusulkan strategi pencegahan serta tanggapan yang sistematis. Pengujian dilakukan pada implementasi strategi pertahanan yang beragam, termasuk penggunaan *firewall* yang lebih maju, sistem pendeteksian intrusi yang efektif, dan struktur arsitektur jaringan yang kuat, untuk menilai kemampuan mereka dalam menangkal serangan *DDoS*. Selama penelitian dilakukan, peneliti telah mengevaluasi berbagai strategi menyerang serta bertahan, dan hasilnya menunjukkan variasi yang menarik. Beberapa percobaan serangan membuahkan hasil yang cukup memuaskan, sementara percobaan lainnya masih memerlukan penyesuaian lebih lanjut. Hasil dari penelitian ini diharapkan akan memberikan wawasan baru dalam bidang keamanan siber dan menjadi panduan bagi administrator sistem untuk melindungi aset digital mereka dari ancaman yang selalu berkembang.

Kata Kunci:

Attack, DDoS, DoS, Website, Server, GoldenEye, Kali Linux, Etherape, Ubuntu, Slowloris, Proxychains, TOR, Hping3, Wireshark, TCP Syn Flood, Ping Flood, ICMP Flood

ABSTRACT

Dave Handoko Priatmojo.

Undergraduate Thesis

Analysis and Implementation of Distributed Denial of Service (DDoS) Attack on XYZ Website and Server

In today's digital era, maintaining the security of websites and server infrastructure is crucial to ensure data security and the smooth running of services provided online. This thesis explores the in-depth analysis and practical application of distributed DDoS attacks on websites and server infrastructures belonging to related institutions. This thesis aims to deepen the understanding of DDoS attack mechanisms and develop efficient mitigation methods. Through this research, frequent attack patterns were discovered, vulnerabilities in the system were evaluated, and systematic prevention and response strategies were proposed. Tests were conducted on the implementation of various defense strategies, including the use of more advanced firewalls, effective intrusion detection systems, and robust network architecture structures, to assess their ability to counteract DDoS attacks. During the course of the research, researchers have evaluated various attacking as well as defensive strategies, and the results show interesting variations. Some of the attack experiments yielded satisfactory results, while others still require further fine-tuning. The results of this research will hopefully provide new insights into the field of cybersecurity and serve as a guide for system administrators to protect their digital assets from ever-evolving threats.

Keywords:

Attack, DDoS, DoS, Website, Server, GoldenEye, Kali Linux, Etherape, Ubuntu, Slowloris, Proxymchains, TOR, Hping3, Wireshark, TCP Syn Flood, Ping Flood, ICMP Flood

DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PENGESAHAN.....	ii
LEMBARAN PERSETUJUAN PUBLIKASI.....	iii
KATA PENGANTAR.....	iv
ABSTRAK.....	v
ABSTRACT.....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	ix
1. PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian.....	3
1.5 Ruang Lingkup.....	3
1.6 Metodologi Penelitian.....	5
1.7 Sistematika Penulisan.....	5
2. TEORI PENUNJANG.....	6
2.1 Keamanan Website (Mulyawan, R., 2021).....	6
2.2 GoldenEye (Johan, 2023.).....	7
2.3 Etherape (Lynix Networks, 2023).....	8
2.4 Kali Linux (Rudiharto, 2023).....	9
2.5 Distributed Denial of Service(DDoS) Attack (Napizahni, M., 2022).....	10
2.6 Slowloris DDoS Attack (Donesrom, 2023).....	12
2.7 TOR Proxychains.....	15
2.8 Virtual Private Network (VPN) (A., F., 2022).....	16
2.9 Website XYZ.....	19
2.10 Wireshark (Cybersecuritysector1, 2022).....	20
2.11 Hping3 (Halil, D., 2023).....	21
2.12 TCP Syn Flood (Imperva, n.d.).....	22
2.13 Ping Flood (ICMP Flood) (, 2023).....	25
3. METODOLOGI PENELITIAN.....	27
3.1. Analisa Permasalahan.....	27
3.2. Alur Pengujian Skripsi.....	27
3.2.1. Persiapan & Planning.....	28

3.2.2. Implementasi Distributed Denial of Service (DDoS) Attack.....	29
3.2.3. Strategi Bertahan dan Perbaikan Sesuai Rekomendasi Oleh Perusahaan.....	30
3.2.4. Membuat Laporan Akhir Kesimpulan Pengujian.....	31
4. IMPLEMENTASI.....	32
4.1. Perencanaan.....	32
4.1.1. Instalasi Goldeneye Pada Kali Linux.....	33
4.1.2. Instalasi Slowloris Pada Kali Linux.....	37
4.1.3. Instalasi TOR Proxychains Pada Kali Linux.....	41
4.1.4. Instalasi Goldeneye Pada Linux Ubuntu.....	47
4.1.5. Instalasi Slowloris Pada Linux Ubuntu.....	49
4.1.6. Instalasi Wireshark Pada Kali Linux.....	51
4.1.7. Instalasi Hping3 Pada Kali Linux.....	55
5. PENGUJIAN.....	57
5.1. Analisis dan Penyelidikan.....	57
5.1.1. Nmap.....	57
5.2. Implementasi Serangan DDoS (Distributed Denial of Service) Attack.....	66
5.2.1. DDoS Attack dengan Menggunakan Goldeneye dan Etherape.....	66
5.2.2. DDoS Attack dengan Menggunakan Goldeneye Pada Ubuntu Server.....	71
5.2.3. Slowloris DDoS Attack dengan Menggunakan Slowloris, Goldeneye, dan Etherape..	73
5.2.4. DDoS Attack dengan Menggunakan Goldeneye dan Etherape yang Dibantu dengan Proxychains.....	83
5.2.5. TCP Syn Flood dengan Menggunakan Hping3 dan Wireshark Pada Kali Linux.....	86
5.2.6. Ping Flood (ICMP Flood) dengan Menggunakan Hping3 dan Wireshark Pada Linux Ubuntu dan Kali Linux.....	91
5.3. Pemantauan dan Penyesuaian.....	95
6. KESIMPULAN DAN SARAN.....	97
6.1. Kesimpulan.....	97
6.2. Saran.....	98
DAFTAR REFERENSI.....	100

DAFTAR GAMBAR

Gambar 2.1 Tampilan Daftar Command yang Ada Pada Goldeneye.....	20
Gambar 2.2 Tampilan Cara Kerja Distributed Denial of Service (DDoS) Attack.....	24
Gambar 2.3 Tampilan Cara Kerja Pivoting Menggunakan Proxychains.....	28
Gambar 2.4 Tampilan Cara Kerja Virtual Private Network (VPN).....	31
Gambar 2.5 Contoh Cara Kerja Serangan TCP Syn Flood.....	35
Gambar 2.6 Cara Kerja Serangan ICMP Flood.....	38
Gambar 3.1 Tahapan Desain Sistem.....	41
Gambar 4.1 Website yang akan Menjadi Target Serangan.....	46
Gambar 4.2 Melakukan Pencarian Git Goldeneye Pada Firefox di Kali Linux.....	46
Gambar 4.3 Melakukan Instalasi Goldeneye Pada Kali Linux dengan Command “git clone”	47
Gambar 4.4 Melakukan Pengecekan Hasil Instalasi dengan Command “ls”	48
Gambar 4.5 Masuk ke dalam Folder Goldeneye dan Lihat Isi dari Folder Goldeneye.....	48
Gambar 4.6 Buka Etherape dengan Command “sudo etherape” Pada Terminal Baru.....	49
Gambar 4.7 Contoh Melakukan Serangan DDoS Menggunakan Goldeneye dan Etherape.....	50
Gambar 4.8 Melakukan Pencarian Git Slowloris Pada Firefox Di Kali Linux.....	51
Gambar 4.9 Membuat Folder Baru dengan Nama “Slowloris” Pada Kali Linux.....	52
Gambar 4.10 Melakukan Instalasi Slowloris Pada Kali Linux dengan Command “git clone”	53
Gambar 4.11 Tampilan Setelah Membuka Konfigurasi Slowloris dan Menyimpan Alamat IP yang Dimiliki Ke Dalam File Baru.....	53
Gambar 4.12 Contoh Tampilan Melakukan Serangan Dengan Menggunakan Slowloris Pada Kali Linux.....	54
Gambar 4.13 Tampilan Untuk Melakukan Instalasi TOR Proxychains Pada Kali Linux.....	55
Gambar 4.14 Command Untuk Membuka Konfigurasi TOR Proxychains.....	56

Gambar 4.15 Gambar Fitur Konfigurasi TOR Proxychains.....	58
Gambar 4.16 Tampilan Pada Saat TOR Proxychains Dijalankan.....	58
Gambar 4.17 Contoh Pertama Hasil DNS Leak Test Menggunakan TOR Proxychains Pada Kali Linux...	59
Gambar 4.18 Contoh Kedua Hasil DNS Leak Test Menggunakan TOR Proxychains Pada Kali Linux...	60
Gambar 4.19 Tampilan Hasil Pembuatan Folder Baru Pada Ubuntu.....	61
Gambar 4.20 Goldeneye yang Ada Pada Github.....	61
Gambar 4.21 File Goldeneye yang Sudah Di Donlot Ke Dalam Folder Goldeneye Dari Google.....	62
Gambar 4.22 Command yang Diperlukan Untuk Menginstal Slowloris Pada Ubuntu.....	63
Gambar 4.23 Link Github yang Berisi Segala Informasi Mengenai Slowloris.....	64
Gambar 4.24 Command yang Diperlukan Untuk Melakukan Instalasi Wireshark Pada Kali Linux....	64
Gambar 4.25 Tampilan yang Akan Muncul Setelah Melakukan Langkah Kedua.....	65
Gambar 4.26 Tampilan yang Akan Muncul Untuk Mengubah Pengaturan Default dari Wireshark...	66
Gambar 4.27 Tampilan Aplikasi Wireshark.....	67
Gambar 4.28 Cara Menjalankan Default Network Interface Pada Wireshark.....	68
Gambar 4.29 Command yang Diperlukan Untuk Menginstal Hping3 Pada Kali Linux.....	69
Gambar 4.30 Tampilan Daftar Command Serta Fungsi yang Disediakan Oleh Hping3.....	69
Gambar 5.1 Hasil Scan Pada Target yang Menampilkan TCP Ports Target Dengan Menggunakan Zenmap.....	71
Gambar 5.2 Topologi Jaringan yang dimiliki oleh Target.....	72
Gambar 5.3 Hasil Scan yang Menampilkan Informasi Detil dari Host atau Target Dengan Menggunakan Zenmap.....	73
Gambar 5.4 Hasil Scan Pada Target Untuk Menemukan Port yang Dibuka Menggunakan Nmap Pada Kali Linux.....	74

Gambar 5.5 Hasil Scan Pertama Pada Target Untuk Menemukan Sistem Operasi yang Digunakan Oleh Target Menggunakan Nmap Pada Kali Linux.....	75
Gambar 5.6 Hasil Scan Ke-2 Pada Target Untuk Menemukan Sistem Operasi yang Digunakan Oleh Target Menggunakan Nmap Pada Kali Linux.....	76
Gambar 5.7 Hasil Scriptscan Untuk Menemukan Kerentanan yang Dimiliki Oleh Target Menggunakan Nmap.....	77
Gambar 5.8 Hasil DDoS Attack Pertama Menggunakan Goldeneye dan Etherape Pada Linux.....	80
Gambar 5.9 Hasil DDoS Attack Ke-2 Menggunakan Goldeneye dan Etherape Pada Linux.....	80
Gambar 5.10 Hasil DDoS Attack Ke-3 Menggunakan Goldeneye dan Etherape Pada Kali Linux.....	81
Gambar 5.11 Hasil DDoS Attack Ke-4 Menggunakan Goldeneye dan Etherape Pada Kali Linux.....	82
Gambar 5.12 Hasil DDoS Attack Ke-5 Menggunakan Goldeneye dan Etherape.....	83
Gambar 5.13 Hasil DDoS Attack Pertama Menggunakan Goldeneye Pada Ubuntu Server.....	85
Gambar 5.14 Hasil DDoS Attack Ke-2 Menggunakan Goldeneye Pada Ubuntu Server.....	85
Gambar 5.15 Hasil DDoS Attack Pertama Menggunakan Goldeneye, Slowloris, dan Etherape Pada Kali Linux.....	87
Gambar 5.16 Hasil DDoS Attack Ke-2 Menggunakan Goldeneye, Slowloris, dan Etherape Pada Kali Linux.....	88
Gambar 5.17 Hasil DDoS Attack Ke-3 Menggunakan Goldeneye, Slowloris, dan Etherape Pada Kali Linux.....	89
Gambar 5.18 Hasil DDoS Attack Ke-4 Menggunakan Goldeneye, Slowloris, dan Etherape Pada Kali Linux.....	90
Gambar 5.19 Hasil DDoS Attack Ke-5 Menggunakan Goldeneye, Slowloris, dan Etherape Pada Kali Linux.....	91
Gambar 5.20 Hasil DDoS Attack Ke-6 Menggunakan Goldeneye, Slowloris, dan Etherape Pada Kali Linux.....	92

Gambar 5.21 Hasil DDoS Attack Ke-7 Menggunakan Goldeneye, Slowloris, dan Etherape Pada Kali Linux.....	93
Gambar 5.22 Hasil DDoS Attack Ke-8 Menggunakan Goldeneye, Slowloris, dan Etherape Pada Kali Linux.....	94
Gambar 5.23 Hasil DDoS Attack Ke-9 Menggunakan Goldeneye, Slowloris, dan Etherape Pada Kali Linux.....	95
Gambar 5.24 Hasil DDoS Attack Pertama Menggunakan Goldeneye, TOR Proxychains, dan Etherape	97
Gambar 5.25 Hasil DDoS Attack Ke-2 Menggunakan Goldeneye, TOR Proxychains, dan Etherape...	98
Gambar 5.26 Hasil DDoS Attack Ke-3 Menggunakan Goldeneye, TOR Proxychains, dan Etherape...	99
Gambar 5.27 Hasil Serangan TCP Syn Flood Pertama Menggunakan Hping3 dan Wireshark Pada Kali Linux.....	100
Gambar 5.28 Hasil Serangan TCP Syn Flood Kedua Menggunakan Hping3 dan Wireshark Pada Kali Linux.....	101
Gambar 5.29 Hasil Serangan TCP Syn Flood Ketiga Menggunakan Hping3 dan Wireshark Pada Kali Linux.....	102
Gambar 5.30 Hasil Serangan TCP Syn Flood Keempat Menggunakan Hping3 dan Wireshark Pada Kali Linux.....	103
Gambar 5.31 Hasil Serangan Ping Flood Pertama Menggunakan Hping3 dan Wireshark Pada Linux Ubuntu.....	105
Gambar 5.32 Hasil Serangan Ping Flood Pertama Menggunakan Hping3 dan Wireshark Pada Linux Ubuntu 2.0.....	106
Gambar 5.33 Hasil Serangan Ping Flood Menggunakan Hping3 dan Wireshark Pada Kali Linux.....	107