

**ANALISIS DAN IMPLEMENTASI HONEYPOT
UNTUK MENDETEKSI SERANGAN DOS (*DENIAL OF
SERVICE*)**

Tugas Akhir

**Diajukan untuk Memenuhi Salah Satu Persyaratan Mencapai Derajat
Sarjana Komputer**



Dibuat Oleh:

AURELL MAYO LEWIDYAS KRISTANTYO

190710483

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ATMA JAYA YOGYAKARTA
2023**

LEMBAR PENGESAHAN

HALAMAN PENGESAHAN

Tugas Akhir Berjudul

ANALISIS DAN IMPLEMENTASI HONEYPOT UNTUK MENDETEKSI SERANGAN DDOS (DISTRIBUTED DENIAL OF SERVICE)

yang disusun oleh

Aurell Mayo Lewidyas Kristantyo

190710483

dinyatakan telah memenuhi syarat pada tanggal 22 Januari 2024

		Keterangan
Dosen Pembimbing 1	: Prof. Ir. Suyoto, M.Sc., Ph.D.	Telah Menyetujui
Dosen Pembimbing 2	: Y. Sigit Purnomo WP., S.T., M.Kom., Ph.D.	Telah Menyetujui
Tim Penguji		
Penguji 1	: Prof. Ir. Suyoto, M.Sc., Ph.D.	Telah Menyetujui
Penguji 2	: Prof. Dr. Ir. Alb. Joko Santoso, M.T.	Telah Menyetujui
Penguji 3	: Wilfridus Bambang Triadi H, ST., M.Cs	Telah Menyetujui

Yogyakarta, 22 Januari 2024

Universitas Atma Jaya Yogyakarta

Teknologi Industri

Dekan

ttd.

Dr. Ir. Parama Kartika Dewa SP., S.T., M.T.

Dokumen ini merupakan dokumen resmi UAJY yang tidak memerlukan tanda tangan karena dihasilkan secara elektronik oleh Sistem Bimbingan UAJY. UAJY bertanggung jawab penuh atas informasi yang tertera di dalam dokumen ini

PERNYATAAN ORISINALITAS & PUBLIKASI ILMIAH

Saya yang bertanda tangan di bawah ini:

Nama Lengkap : Aurell Mayo Lewidyas Kristantyo
NPM : 190710483
Program Studi : Informatika
Fakultas : Teknologi Industri
Judul Penelitian : Analisis dan Implementasi Honeypot untuk Mendeteksi Serangan DoS (*Denial of Service*)

Menyatakan dengan ini:

1. Tugas Akhir ini adalah benar tidak merupakan salinan sebagian atau keseluruhan dari karya penelitian lain.
2. Memberikan kepada Universitas Atma Jaya Yogyakarta atas penelitian ini, berupa Hak untuk menyimpan, mengelola, mendistribusikan, dan menampilkan hasil penelitian selama tetap mencantumkan nama penulis.
3. Bersedia menanggung secara pribadi segala bentuk tuntutan hukum atas pelanggaran Hak Cipta dalam pembuatan Tugas Akhir ini.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 4 Oktober 2023

Yang menyatakan,



Aurell Mayo Lewidyas Kristantyo

190710483

KATA PENGANTAR

Puji dan syukur penulis haturkan kepada Tuhan Yang Maha Esa karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan pembuatan tugas akhir “Analisis dan Implementasi HoneyPot untuk Mendeteksi Serangan DoS (*Denial of Service*)” ini dengan baik.

Penulisan tugas akhir ini bertujuan untuk memenuhi salah satu syarat untuk mencapai derajat sarjana komputer dari Program Studi Informatika, Fakultas Teknologi Industri di Universitas Atma Jaya Yogyakarta.

Penulis menyadari bahwa dalam pembuatan tugas akhir ini penulis telah mendapatkan bantuan, bimbingan, dan dorongan dari banyak pihak. Untuk itu, pada kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Tuhan Yesus Kristus yang selalu membimbing dalam iman-Nya, memberikan berkat-Nya, dan menyertai penulis selalu.
2. Bapak Dr. Ir. Parama Kartika Dewa SP., S.T., M.T., selaku Dekan Fakultas Teknologi Industri, Universitas Atma Jaya Yogyakarta.
3. Bapak Thomas Adi Purnomo Sidhi, S.T., M.T., selaku Ketua Program Studi S1 Informatika.
4. Bapak Prof. Ir. Suyoto, M.Sc., Ph.D., selaku dosen pembimbing I yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.
5. Bapak Y. Sigit Purnomo WP., S.T., M.Kom., Ph.D., selaku dosen pembimbing II yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.
6. Kedua orang tua dan saudara – saudara saya yang selalu mendukung dan memberikan semangat.
7. Hazel Bayu Putra sebagai teman seperjuangan skripsi dan teman bermain di sela - sela pengerjaan skripsi.

8. Teman – teman saya yang telah memberikan masukan dan supportnya.
9. Serta semua pihak yang telah membantu dalam penyelesaian tugas akhir ini yang tidak dapat disebutkan satu per satu.

Demikian laporan tugas akhir ini dibuat, dan penulis mengucapkan terima kasih kepada semua pihak. Semoga laporan ini dapat bermanfaat bagi pembaca.

Yogyakarta, 4 Oktober 2023



Aurell Mayo Lewidyas Kristantyo

190710483

DAFTAR ISI

LEMBAR PENGESAHAN	i
PERNYATAAN ORISINALITAS & PUBLIKASI ILMIAH	ii
KATA PENGANTAR.....	iii
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL.....	x
INTISARI.....	xi
BAB I	1
PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	2
C. Batasan Masalah.....	3
D. Tujuan Penelitian.....	3
E. Metode Penelitian.....	3
F. Sistematika Penulisan	5
BAB II.....	9
TINJAUAN PUSTAKA.....	9
BAB III	16
LANDASAN TEORI	16
A. DoS.....	16
B. Honeypot.....	20
C. Ethical Hacking.....	22
BAB IV	26

PERANCANGAN SISTEM	26
A. Topologi Jaringan.....	26
B. Skenario Serangan DoS (<i>Denial of Service</i>).....	28
C. Kerangka Pemodelan	29
D. Persiapan Tools dan Device	31
BAB V.....	41
HASIL ANALISIS DAN PEMBAHASAN.....	41
A. Simulasi Serangan DoS (<i>Denial of Service</i>)	41
1. Slowloris	42
2. LOIC (Low Orbit Ion Cannon)	42
3. Hasil Serangan DoS	44
B. Implementasi Honeypot	52
1. Slowloris #2	56
2. LOIC (Low Orbit Ion Cannon) #2	59
C. Hasil Pengujian Honeypot	63
BAB VI.....	71
PENUTUP.....	71
A. Kesimpulan	71
B. Saran.....	72
DAFTAR PUSTAKA	73

DAFTAR GAMBAR

Gambar 1. 1 Metode Penelitian.....	4
Gambar 4. 1 Topologi Jaringan.....	27
Gambar 4. 2 Skenario Serangan DoS.....	28
Gambar 4. 3 Flowchart Skenario Serangan.....	30
Gambar 4. 4 Kali Linux 2023	32
Gambar 4. 5 Instalasi mono-complete	32
Gambar 4. 6 Download LOIC.....	33
Gambar 4. 7 Unzip File LOIC.....	33
Gambar 4. 8 Instalasi Slowloris	34
Gambar 4. 9 Nmap	35
Gambar 4. 10 Linux Ubuntu 22.04 LTS.....	36
Gambar 4. 11 Instalasi Apache2 Web Server	36
Gambar 4. 12 Download Pentbox	37
Gambar 4. 13 Ekstrak File Pentbox	38
Gambar 4. 14 Pentbox.....	39
Gambar 4. 15 Apache2 Web Server	40
Gambar 5. 1 Nmap 192.168.2.106	41
Gambar 5. 2 Slowloris DoS Attack.....	42
Gambar 5. 3 LOIC Menu	43
Gambar 5. 4 LOIC DoS Attack.....	44
Gambar 5. 5 Kinerja Web Server melambat	45
Gambar 5. 6 Slowloris Traffic Statistic.....	45
Gambar 5. 7 Slowloris Network Traffic pada Wireshark.....	46
Gambar 5. 8 Slowloris Open Connection	46
Gambar 5. 9 Traffic dari Port 33444	47
Gambar 5. 10 Three-way Handshake Port 33444	47
Gambar 5. 11 Slowloris ACK-PSH Flood	48
Gambar 5. 12 LOIC Traffic Statistic.....	48

Gambar 5. 13 LOIC Network Traffic pada Wireshark.....	49
Gambar 5. 14 LOIC Open Connection	50
Gambar 5. 15 Traffic dari Port 44116	50
Gambar 5. 16 Three-way Handshake Port 44116	51
Gambar 5. 17 LOIC ACK-PSH Flood	51
Gambar 5. 18 PenTBox Menu	52
Gambar 5. 19 Setting Honeypot.....	53
Gambar 5. 20 Implementasi Honeypot pada Port 21 (kiri) dan Port 23 (kanan) ..	54
Gambar 5. 21 Implementasi Honeypot pada Port 80	55
Gambar 5. 22 Nmap 192.168.2.106 #2	56
Gambar 5. 23 Slowloris DoS Attack pada Port 21 (atas) dan Port 23 (bawah)	57
Gambar 5. 24 Slowloris DoS Attack pada Port 80.....	58
Gambar 5. 25 Proteksi Honeypot pada Port 21 (kiri) dan Port 23 (kanan).....	58
Gambar 5. 26 Proteksi Honeypot pada Port 80.....	59
Gambar 5. 27 LOIC DoS Attack pada Port 21	60
Gambar 5. 28 Proteksi Honeypot pada Port 21	60
Gambar 5. 29 LOIC DoS Attack pada Port 23	61
Gambar 5. 30 Proteksi Honeypot pada Port 23	61
Gambar 5. 31 LOIC DoS Attack pada Port 80.....	62
Gambar 5. 32 Proteksi Honeypot pada Port 80.....	62
Gambar 5. 33 Slowloris Traffic Statistic #2.....	63
Gambar 5. 34 Slowloris Network Traffic pada Wireshark #2.....	63
Gambar 5. 35 Slowloris Open Connection #2	64
Gambar 5. 36 Traffic dari Port 39028 #2	64
Gambar 5. 37 Three-way Handshake Port 39028 #2	65
Gambar 5. 38 Slowloris ACK-PSH Flood #2	65
Gambar 5. 39 Honeypot Reply dengan Packet "PSH, ACK"	66
Gambar 5. 40 LOIC Network Statistic #2.....	66
Gambar 5. 41 LOIC Network Traffic pada Wireshark #2.....	67
Gambar 5. 42 LOIC Open Connection #2	67
Gambar 5. 43 Traffic dari Port 56292 #2	68

Gambar 5. 44 Three-way Handshake Port 56292 #2	68
Gambar 5. 45 LOIC ACK-PSH Flood #2	69
Gambar 5. 46 Honeypot TCP ZeroWindow	69

DAFTAR TABEL

Tabel 2. 1 Tabel Perbandingan Penelitian Terdahulu	13
Tabel 4. 1 IP Address pada Topologi Jaringan	27
Tabel 4. 2 Port yang Terproteksi oleh Honeypot.....	31

INTISARI

ANALISIS DAN IMPLEMENTASI HONEYPOT UNTUK MENDETEKSI SERANGAN DOS (*DENIAL OF SERVICE*)

Intisari

Aurell Mayo Lewidyas Kristantyo
190710483

Perkembangan internet yang berkembang pesat membuat semakin banyak kegiatan yang dapat dilakukan secara online. Hal ini dapat meningkatkan potensi kejahatan *cyber* yang dilakukan di internet. Salah satu *cyber attack* yang dilakukan melalui jaringan seperti internet yaitu serangan DoS. Serangan DoS (*Denial of Service*) merupakan serangan yang dilakukan dengan membanjiri *traffic* dari banyak sumber ke sebuah situs web atau server yang mengakibatkan layanan pada situs web atau server tersebut menjadi lambat ataupun menjadi *offline* sehingga tidak dapat diakses oleh pengguna yang sah. Oleh karena itu, diperlukan adanya solusi yang efektif untuk mengatasi DoS *attack*.

Salah satu solusi yang dapat digunakan adalah dengan menggunakan honeypot. Honeypot merupakan sebuah sistem keamanan yang berfungsi sebagai jebakan bagi para *hacker* yang memancing *hacker* untuk menyerang sistem yang memang sengaja dibuat untuk diserang. Dengan menggunakan honeypot, serangan dari *hacker* dapat dideteksi dan diamati sehingga membantu pemilik layanan dalam mengidentifikasi dan mengatasi serangan DoS yang menyerang situs web atau server.

Hasil dari implementasi honeypot yang telah dilakukan yaitu honeypot dapat digunakan untuk menghentikan serangan DoS. Honeypot juga dapat mengelabui *attacker* untuk menyerang *open port* yang sudah disiapkan oleh honeypot sehingga port yang asli dapat terus menyediakan *service*.

Kata Kunci: Internet, *Computer Network*, *Cyber Security*, DoS, Honeypot

Dosen Pembimbing I : Prof. Ir. Suyoto, M.Sc., Ph.D.

Dosen Pembimbing II : Y. Sigit Purnomo WP., S.T., M.Kom., Ph.D.

Jadwal Sidang Tugas Akhir : 15 Januari 2024