

SKRIPSI

IMPLEMENTASI *HONEYPOT DIONAEA* SEBAGAI UJI KERENTANAN DAN PENUNJANG KEAMANAN JARINGAN



Oleh :

Mohammad Fadhol

NIM : 19083000015

PROGRAM STUDI S1 SISTEM INFORMASI

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS MERDEKA

MALANG

2023

**IMPLEMENTASI *HONEYPOT DIONAEA* SEBAGAI UJI KERENTANAN
DAN PENUNJANG KEAMANAN JARINGAN**



SKRIPSI

Diajukan Sebagai Salah Satu Persyaratan
Untuk Memperoleh Gelar Sarjana Sistem Informasi (S.Kom.)

Oleh :

Mohammad Fadhol

NIM : 19083000015

**PROGRAM STUDI S1 SISTEM INFORMASI
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS MERDEKA
MALANG
2023**

LEMBAR PERSETUJUAN SKRIPSI

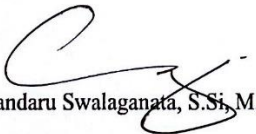
Nama : Mohammad Fadhol
NIM : 19083000015
Universitas : Universitas Merdeka Malang
Fakultas : Teknologi Informasi
Program Studi : S1 Sistem Informasi
Judul Skripsi : Implementasi *Honeypot Dionaea* Sebagai Uji Kerentanan dan Penunjang Keamanan Jaringan

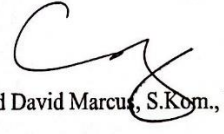
Malang, 18 April 2023

DISETUJUI DAN DITERIMA

Ketua Program Studi
S1 Sistem Informasi

Dosen Pembimbing


Galandaru Swalaganata, S.Si, M.Si


Ronald David Marcus, S.Kom., M.Kom

Dekan Fakultas Teknologi Informasi




Dr. Mardiana Andarwati, M.Si

LEMBAR PENGESAHAN

IMPLEMENTASI *HONEYPOT DIONAEA* SEBAGAI UJI KERENTANAN DAN PENUNJANG KEAMANAN JARINGAN

Dipersiapkan dan disusun oleh

Mohammad Fadhol

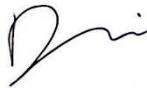
19083000015

Telah dipertahankan di depan Dewan Penguji

Pada Tanggal 25 Juli 2023

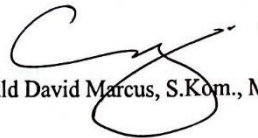
Susunan Dewan Penguji

Ketua Penguji



Nofrian Deny Hendrawan, S.ST., M.Tr.T

Sekretaris Penguji



Ronald David Marcus, S.Kom., M.Kom

Anggota Penguji



Andriyan Rizki Jatmiko, S.Si., M.Kom

Skripsi ini Telah Diterima Sebagai Salah Satu Persyaratan Untuk Memperoleh
Gelar Sarjana Sistem Informasi (S.Kom.)

Malang, 25 Juli 2023

Dekan Fakultas Teknologi Informasi
Universitas Merdeka Malang



Dr. Mardiana Andarwati, M.Si

LEMBAR PERNYATAAN ORISINALITAS


Yang bertanda tangan dibawah ini:

Nama : Mohammad Fadhol
NIM : 19083000015
Program Studi : S1 Sistem Informasi
Bidang Kajian Skripsi : Keamanan Jaringan
Judul Skripsi : IMPLEMENTASI *HONEYPOT DIONAEA*
SEBAGAI UJI KERENTANAN DAN
PENUNJANG KEAMANAN JARINGAN
Alamat Rumah Asal : Jl. Warinoi V No.16, Kota Malang
No. Telp/E-mail : 081230263969 / mfadhol07@gmail.com

Dengan ini menyatakan bahwa saya benar-benar melakukan penelitian dan penulisan skripsi tersebut di atas benar-benar karya saya dan tidak melakukan plagiasi. Jika saya melakukan plagiasi maka saya bersedia untuk dicabut gelar dan akademik saya.

Demikian surat pernyataan ini di buat untuk dipergunakan sebagaimana mestinya.

Malang, 25 Juli 2023

Peneliti,

Mohammad Fadhol

MOTTO

**KEPUTUSAN KECIL DAPAT MEMBERIKAN
DAMPAK YANG SANGAT BESAR DALAM HIDUPMU**

KATA PENGANTAR

Puji syukur penulis haturkan kepada Allah SWT karena berkat Ridha-Nya proposal skripsi ini dapat diselesaikan di waktu yang tepat. Tak lupa shalawat serta salam selalu tercurah kepada junjungan kita Nabi besar Muhammad SAW.

Laporan Skripsi ini penulis susun untuk memenuhi salah satu persyaratan dalam memperoleh gelar Sarjana Sistem Informasi (S.Kom) Universitas Merdeka Malang Tahun ajaran 2019 pada program studi Sistem Informasi.

Judul yang penulis ajukan yaitu **“Implementasi *Honeypot Dionaea* Sebagai Uji Kerentanan dan Penunjang Keamanan Jaringan”**.

Selama penyusunan karya tulis ini, penulis banyak sekali mendapatkan pelajaran berharga, dukungan serta motivasi, bantuan berupa bimbingan moral dan material yang sangat berharga dari berbagai pihak, mulai dari pelaksanaan hingga akhir penyusunan laporan skripsi ini.

Pada kesempatan ini penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada orang-orang yang penulis hormati dan cintai yang hingga saat ini pun tidak ada lelahnya dalam memberikan arahan dan bimbingan yang paling besar terhadap kehidupan penulis baik di dalam maupun di luar kehidupan perkuliahan, Terima kasih yang tak terhingga terutama kepada keluarga yang tercinta, Kapten CBA Waloejo Bagoes Rachmanoe, Kapten CBA (K) Purwanti, Citra Dewi Rachmawanti Sang Dyah Pitaloka S.E, dan Najwa Haura Zahra yang selalu memberikan doa dan arahan sehingga kelak ilmu yang penulis dapatkan selama mengenyam pendidikan ini dapat berguna bagi sesama manusia yang membutuhkannya, serta memberikan semangat yang luar biasa dan memberikan dukungan moril maupun materil.

Selama proses penyusunan dan penulisan skripsi ini banyak pihak yang telah berpartisipasi, sebagai rasa syukur dan trima kasih dalam kesempatan ini penulis dengan senang hati ingin mengucapkan terima kasih kepada :

1. Bapak Rektor Universitas Merdeka Malang, Prof. Dr. Anwar Sanusi, S.E., M.Si.
2. Ibu Dekan Fakultas Teknologi Informasi Universitas Merdeka Malang, Dr. Mardiana Andarwati, S.E., M.Si.
3. Bapak Wakil Dekan 1 Fakultas Teknologi Informasi Universitas Merdeka Malang, Ahmad Rofiqul Muslikh, S.Kom., M.Kom.
4. Bapak Wakil Dekan 2 Fakultas Teknologi Informasi Universitas Merdeka Malang, Aditya Galih Sulaksono, S.Kom., M.Kom.
5. Bapak Ketua Prodi Jurusan S1 Sistem Informasi, Galandaru Swalaganata, S.Si, M.Si.
6. Dosen Pembimbing, Bapak Ronald David Marcus, S.Kom., M.Kom.
7. Dosen Penguji, Bapak Andriyan Rizki Jatmiko, S.Si., M.Kom dan Bapak Nofrian Deny Hendrawan, S.ST., M.Tr.T.
8. Untuk seluruh teman Angkatan 2019 prodi S1 dan D3 Sistem Informasi, serta sahabat dan teman seperjuanganku Alwi, Dewa, Taufiq, Alex di Universitas Merdeka Malang Jurusan S1 Sistem Informasi
9. Dan yang terakhir tak lupa ucapan terima kasih sebesar-besarnya kepada Pelatih, Atlit Senior, dan Junior di UKM Taekwondo Universitas Merdeka Malang.

Untuk mereka semua yang telah berbaik hati, hanya ungkapan terimakasih serta doa yang tuluslah yang dapat saya persembahkan, semoga segala yang telah mereka berikan kepada saya, kelak dapat menjadi tabungan pahala di akhirat nantinya.

Akhirnya, dengan segala bentuk keterbatasan dan kekurangan, saya persembahkan hasil karya tulis ini kepada siapapun yang membutuhkannya sebagai sumber pengetahuan serta referensi dalam penelitiannya. Kritik dan saran dari semua pihak yang bersifat membangun sangat saya harapkan untuk penyempurnaan kualitas penyusunan karya – karya saya selanjutnya.

Terimakasih,

DAFTAR ISI

LEMBAR PERSETUJUAN SKRIPSI	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN ORISINALITAS	iv
MOTTO	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xii
DAFTAR LAMPIRAN	xiii
ABSTRAK	xiv
ABSTRACT.....	xv
DAFTAR RIWAYAT HIDUP	xvi
BAB I.....	1
PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	4
1.3. Tujuan.....	5
1.4. Manfaat Penelitian.....	6
1.5. Batasan Penelitian	6
BAB II	8
KAJIAN PUSTAKA.....	8
2.1. Landasan Teori	8
2.2. Penelitian Terdahulu	14
BAB III.....	16
METODE PENELITIAN	16
3.1. Kerangka Penelitian	16

3.2.	Alur Kerja Penelitian	17
3.3.	Spesifikasi Kebutuhan	18
3.4.	Spesifikasi Mesin <i>Virtual</i>	19
3.5.	Arsitektur Jaringan	21
3.6.	<i>Honeypot Dionaea</i>	22
3.7.	Tahapan Penetrasi	22
3.8.	<i>Port Scanning</i>	22
BAB IV	23
HASIL PENELITIAN DAN PEMBAHASAN	23
4.1.	Penentuan <i>IP Address</i>	23
4.2.	Implementasi Honeypot	24
4.3.	Proses penyerangan <i>Honeypot</i> menggunakan <i>Kali Linux</i>	29
BAB V	35
PENUTUP	35
5.1.	Kesimpulan.....	35
5.2.	Saran	36
DAFTAR PUSTAKA	37
LAMPIRAN	39
Lampiran 1.	Surat Persetujuan Pengajuan Seminar Proposal	39
Lampiran 2.	Persetujuan Pengajuan Seminar Hasil	40
Lampiran 3.	Surat Keterangan Pemeriksaan Kemiripan	41

DAFTAR GAMBAR

Gambar 1. Alur Penelitian 1	16
Gambar 2. Alur Kerja 1	17
Gambar 3. Desain perancangan jaringan 1	21
Gambar 4. IP Address Kali Linux 1	23
Gambar 5. IP Address Honeydrive 1	24
Gambar 6. Mengaktifkan Dionaea 1	24
Gambar 7. Proses Aktivasi Dionaea 1	25
Gambar 8. Kondisi sebelum diaktifkan 1	25
Gambar 9. Aktivasi web server DionaeaFR 1	26
Gambar 10. CLI log aktivitas DionaeaFR 1	26
Gambar 11. Pengumpulan data statis 1	27
Gambar 12. Web monitoring DionaeaFR 1	27
Gambar 13. Menu connection web DionaeaFR 1	28
Gambar 14. Monitoring CLI DionaeaFR 1	28
Gambar 15. Aktivasi Dionaea.sh 1	29
Gambar 16. Sebelum layanan Dionaea aktif 1	29
Gambar 17. kondisi setelah Dionaea aktif 1	30

Gambar 18. Aktivasi Metasploit 1	31
Gambar 19. Input port untuk di eksploit 1	31
Gambar 20. Eksploitasi port ms06_040_net 1	31
Gambar 21. Eksploitasi port ms04_011_lsa 1	32
Gambar 22. Eksploitasi port ms03_026_dcom 1	32
Gambar 23. Monitoring serangan 1	33
Gambar 24. Menu connection DionaeaFR 1	34
Gambar 25. Slide 2 menu connection 1	34

DAFTAR TABEL

Tabel 1. Spesifikasi Host 1	19
Tabel 2. Spesifikasi Honeydrive3 1	20
Tabel 3. Spesifikasi Kali linux 1	20

DAFTAR LAMPIRAN

Lembar Persetujuan 1	ii
Lembar Pengesahan 1	iii
Lembar Pernyataan 1	iv

ABSTRAK

Perkembangan sumber daya ilmu pengetahuan yang berkembang pesat dalam dunia teknologi informasi memberikan manfaat yang besar terhadap kemajuan sumber daya manusia ini sendiri. Namun tidak sedikit juga masalah yang ditimbulkan oleh kemajuan ilmu pengetahuan teknologi informasi yang sangat pesat ini, salah satunya penyalahgunaan ilmu tersebut untuk meretas, merusak, dan mencuri sumber daya dari sebuah celah kerentanan *port* komputer *server*.

Honeypot merupakan sistem yang sengaja digunakan untuk menjadi target sasaran penyerangan dari peretas. *Honeypot* akan menggunakan sumber daya *port* manipulasi sebagai sebuah cara untuk menjebak dan merekam informasi penetrasi dan serangan yang masuk. Implementasi *Honeypot Dionaea* ini sangat penting untuk meningkatkan potensi bertahan dari berbagai jenis serangan yang masuk melalui *port* komputer *server*.

Dengan diimplementasikan sistem *Honeypot* tersebut, sebuah port manipulasi dapat melayani serangan yang dilakukan oleh peretas dalam melakukan penetrasi terhadap komputer yang diduga sebagai server tersebut. Sehingga komputer server akan lebih terjaga keamanannya dari segala celah-celah yang ada khususnya celah kerentanan dari sebuah *port*.

Kata Kunci: Peretas, Honeypot, Dionaea, Kerentanan Port, Komputer Server, Teknologi Informasi.

ABSTRACT

The development of rapidly growing scientific resources in the world of information technology provides great benefits to the progress of human resources themselves. However, there are also not a few problems caused by the rapid progress of information technology science, one of which is the misuse of this knowledge to hack, destroy, and steal resources from a server computer port vulnerability gap.

Honeypot is a system that is deliberately used to become the target of attacks from hackers. Honeypots will use port manipulation resources as a way to trap and record incoming penetration and attack information. Implementation of the Dionaea Honeypot is very important to increase the potential to survive various types of attacks that enter through the server computer port.

By implementing the Honeypot system, a port manipulation can serve attacks carried out by hackers in penetrating the computer suspected of being the server. So that the server computer will be more secure from all the gaps that exist, especially the vulnerability gap of a port.

Keyword: *Hackers, Honeypot, Dionaea, Port Vulnerability Gap, Server Computer, Information Technology.*