



**UNIVERSITAS INDO GLOBAL MANDIRI**

**IMPLEMENTASI DUA *HONEYPOT* SEBAGAI PENDETEKSI  
SERANGAN PADA *VIRTUAL PRIVATE SERVER (VPS)***

**SKRIPSI**

**Diajukan Sebagai Syarat Untuk Menyelesaikan  
Pendidikan Program Strata - 1  
Pada Program Studi Teknik Informatika**

Oleh :

**Wahyu Nugraha  
2019.11.0026**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS INDO GLOBAL MANDIRI  
2023**

**IMPLEMENTASI DUA *HONEYPOT* SEBAGAI PENDETEKSI  
SERANGAN PADA *VIRTUAL PRIVATE SERVER (VPS)***



**SKRIPSI**

**Diajukan Sebagai Syarat Untuk Menyelesaikan  
Pendidikan Program Strata – 1  
Pada Program Studi Teknik Informatika**

**Oleh:**

**Wahyu Nugraha  
2019.11.0026**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS INDO GLOBAL MANDIRI  
2023**

# LEMBAR PENGESAHAN SKRIPSI

## LEMBAR PENGESAHAN SKRIPSI

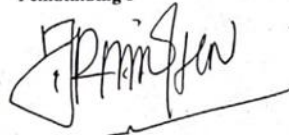
Implementasi Dua Honeypot Sebagai Pendeteksi Serangan  
Pada Virtual Private Server (VPS)

Oleh

Wahyu Nugraha  
NPM : 2019.11.0026

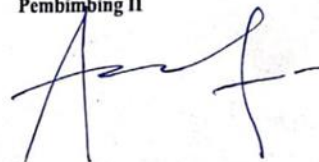
Palembang, 31 Agustus 2023

Pembimbing I



Rudi Heriansyah, S.T., M.Eng. Ph.D  
NIK : 2022.01.0315

Pembimbing II



Lastri Widya Astuti, M.Kom  
NIK: 2003.01.0063

Mengetahui,

Dekan Fakultas Ilmu Komputer

FAKULTAS ILMU KOM & SAINS



Rudi Heriansyah, S.T., M.Eng. Ph.D  
NIK : 2022.01.0315

## LEMBAR PERSETUJUAN DEWAN PENGUJI

### LEMBAR PERSETUJUAN DEWAN PENGUJI

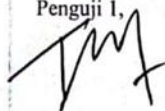
Pada hari Kamis tanggal 24 Agustus 2023 telah dilaksanakan ujian sidang skripsi :

Nama : Wahyu Nugraha  
NPM : 2019.11.0026  
Judul : Implementasi Dua Honeypot Sebagai Pendeteksi Serangan  
Pada Virtual Private Server (VPS)

Oleh Prodi Teknik Informatika Fakultas Ilmu Komputer Universitas Indo Global  
Mandiri Palembang

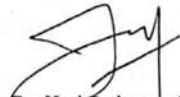
Palembang, 31 Agustus 2023

Penguji 1,



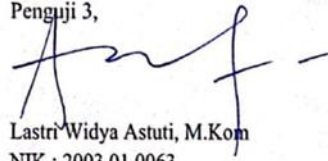
Tasmi, S.Si., M.Kom  
NIK: 2017.01.0230

Penguji 2,



Dr. Heri Setiawan, M.Kom  
NIK: 2003.01.0060

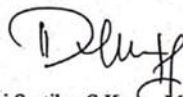
Penguji 3,



Lastri Widya Astuti, M.Kom  
NIK : 2003.01.0063

Menyetujui,

Ka. Prodi Teknik Informatika



Dewi Sartika, S.Kom., M.Kom  
NIK: 2013.01.0015

## SURAT KETERANGAN REVISI SKRIPSI



SURAT KETERANGAN SIAP SIDANG SKRIPSI  
PROGRAM STUDI TEKNIK INFORMATIKA (SI)  
FASILKOM UNIVERSITAS INDO GLOBAL MANDIRI

Kami yang bertanda tangan dibawah ini, menerangkan bahwa :

Nama : Wahyu Nugraha  
NPM : 2019.11.0026  
Judul : Implementasi Dua Honeypot Sebagai Pendeteksi Serangan Pada Virtual Private Server (VPS)

Mahasiswa yang namanya tercantum diatas, telah selesai melakukan penulisan SKRIPSI dan dinyatakan telah memenuhi persyaratan untuk mengikuti sidang SKRIPSI.

Palembang, 31 Agustus 2023

Pembimbing I,

Rudi Heriansyah, S.T., M.Eng., Ph.D  
NIK. 2022.01.0315

Pembimbing II,

Lastr Widya Astuti, M.Kom  
NIK. 2003.01.0063

Menyetujui,  
Ka. Prodi Teknik Informatika

Dewi Sartika, S.Kom., M.Kom  
NIK. 2013.01.0015

# **IMPLEMENTASI DUA *HONEYPOT* SEBAGAI PENDETEKSI SERANGAN PADA *VIRTUAL PRIVATE SERVER (VPS)***

## **ABSTRAK**

*Internet memberikan dampak positif seperti kemudahan dalam berkomunikasi dan berbagi informasi yang cepat dan akurat, namun juga terdapat dampak negatif yang perlu kita waspadai. Dampak negatif dapat berakibat serius jika data yang dicuri digunakan untuk kepentingan tertentu yang dapat merugikan pengguna. Oleh karena itu, perlu kesadaran dan tindakan dari setiap individu dalam menjaga dan melindungi data pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Honeypot mulai dari Low Interaction Honeypot, tipe honeypot yang dibuat untuk mensimulasikan service (layanan) seperti pada server yang asli. Misalnya FTP, SSH, HTTP, dan service lainnya. Lalu selanjutnya ada High Interaction Honeypot, tipe honeypot yang menggunakan keseluruhan resource sistem, dimana honeypot yang dibangun nanti benar-benar persis seperti sistem yang asli. Honeypot jenis ini bisa berupa satu keseluruhan sistem operasi beserta aplikasi yang berjalan didalamnya Dengan adanya honeypot dapat mendeteksi apabila ada serangan yang terjadi pada server Dengan mencoba banyak serangan sehingga tau setiap jenis serangan yang dapat terjadi, sehingga dapat menentukan jenis honeypot yang tepat untuk digunakan pada server.*

Kata Kunci : Virtual Private Server, Honeypot, Server

**IMPLEMENTASI DUA *HONEYPOT* SEBAGAI PENDETEKSI  
SERANGAN PADA *VIRTUAL PRIVATE SERVER (VPS)***

**ABSTRACT**

*The internet has positive impacts such as ease of communication and sharing of fast and accurate information, but there are also negative impacts that we need to be aware of. Negative impacts can have serious consequences if stolen data is used for certain interests that can harm users. Therefore, there needs to be awareness and action from every individual in protecting and safeguarding personal data from being misused by irresponsible parties. Honeypots range from Low Interaction Honeypots, which are designed to simulate services such as those on real servers, such as FTP, SSH, HTTP, and other services. Then there are High Interaction Honeypots, which use the entire system resources, where the honeypot built is exactly like the original system. This type of honeypot can be a whole operating system along with the applications running within it. With honeypots, we can detect if there are attacks happening on the server by trying out many attacks to know each type of attack that can occur, so that we can determine the appropriate type of honeypot to use on the server.*

*Keyword : Virtual Private Server, Honeypot, server*

## KATA PENGANTAR

Puji dan syukur saya ucapkan atas kehadiran Allah Subhanahu Wata'ala berkat rahmat dan hidayahnya akhirnya penulis dapat menyelesaikan penelitian ini dengan baik tepat pada waktunya, tidak lupa shalawat serta salam selalu dilimpahkan kepada junjungan kita Nabi besar Nabi Muhammad SAW beserta keluarga sahabat para pengikut dan insyaallah kita semua hingga akhir zaman.

Skripsi yang penulis buat dengan judul “Implementasi Dua Honeypot sebagai pendeteksi serangan pada Virtual Private Server (VPS) ” disusun guna memenuhi syarat kelulusan dalam memperoleh gelar Sarjana (S1) pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Indo Global Mandiri (UIGM) Palembang.

Tidak lupa penulis mengucapkan terimakasih atas bantuan yang diberikan selama penyusunan skripsi ini kepada

1. Dr. Marzuki Alie, SE.,MM, selaku Rektor Universitas Indo Global Mandiri Palembang.
2. Rudi Heriansyah, ST., M.Eng. Ph.D selaku Dekan Fakultas Ilmu Komputer Universitas Indo Global Mandiri.
3. Dewi Sartika, M.Kom, sebagai Ketua Program Studi Teknik Informatika Universitas Indo Global Mandiri dan Dosen Pembimbing Akademik.
4. Rudi Heriansyah, ST., M.Eng. Ph.D, sebagai Dosen Pembimbing I.
5. Latri Widya Astuti, M.Kom, sebagai Dosen Pembimbing II.
6. Bapak/Ibu Dosen Fakultas Ilmu Komputer dan Karyawan/Karyawati Universitas Indo Global Mandiri.
7. Kedua Orang Tua saya dan Keluarga yang telah memberikan dukungan moril maupun materil, serta Do'a sehingga penulis bisa menyelesaikan skripsi ini.
8. Semua teman-teman seperjuangan Teknik Informatika Angkatan 2019.



Dengan segala kerendahan hati penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna, oleh karena itu dibutuhkan kritik dan saran untuk perbaikan dan pengembangan skripsi ini sangat diharapkan. Akhir kata, semoga skripsi ini bermanfaat bagi semua pihak terima kasih.

Palembang, April 2023

Penulis

Wahyu Nugraha

2019.11.0026

## DAFTAR ISI

<b>HALAMAN JUDUL LUAR</b> .....	<b>i</b>
<b>HALAMAN JUDUL DALAM</b> .....	<b>i</b>
<b>LEMBAR PENGESAHAN SKRIPSI</b> .....	<b>ii</b>
<b>LEMBAR PERSETUJUAN DEWAN PENGUJI</b> .....	<b>iii</b>
<b>SURAT KETERANGAN REVISI SKRIPSI</b> .....	<b>iv</b>
<b>ABSTRAK</b> .....	<b>v</b>
<b>ABSTRACT</b> .....	<b>vi</b>
<b>KATA PENGANTAR</b> .....	<b>vii</b>
<b>DAFTAR ISI</b> .....	<b>ix</b>
<b>DAFTAR GAMBAR</b> .....	<b>xiii</b>
<b>DAFTAR TABEL</b> .....	<b>xvi</b>
<b>DAFTAR LAMPIRAN</b> .....	<b>xvii</b>
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Sistematika Penulisan.....	3
<b>BAB II LANDASAN TEORI</b> .....	<b>5</b>
2.1 <i>OSI Layer</i> .....	5
2.1.1 Physical Layer .....	5
2.1.2 Data Link.....	6
2.1.3 Network Layer .....	7

2.1.4	Transport Layer .....	7
2.1.5	Session Layer .....	7
2.1.6	Presentation Layer.....	8
2.1.7	Application Layer.....	9
2.2	Topologi Jaringan.....	9
2.2.1	Topologi Star.....	10
2.2.2	Topologi <i>Mesh</i> .....	11
2.2.3	Topologi <i>Tree</i> .....	12
2.2.4	Topologi <i>ring</i> .....	13
2.3	IP Address .....	14
2.3.1	IP <i>Public</i> .....	14
2.3.2	IP Private.....	15
2.3.3	Jenis-Jenis <i>IP Address</i> .....	15
2.4	Linux .....	17
2.5	Debian .....	17
2.6	<i>Honeypot</i> .....	18
2.6.1	Dionaea .....	19
2.6.2	Cowrie.....	19
2.7	Virtual Private Server .....	20
2.8	Virtual Box .....	20
2.9	Secure Socket Shell (SSH) .....	21
2.10	Web Server .....	21
2.11	Apache.....	21
2.12	Basis Data.....	22
2.13	<i>MySQL</i> .....	22
2.14	<i>Port</i> .....	22
2.15	Jenis serangan.....	23

2.16	Penelitian Terdahulu.....	26
<b>BAB III METODOLOGI PENELITIAN .....</b>		<b>33</b>
3.1	Metode Penelitian.....	33
3.2	Studi Literatur.....	33
3.3	Persiapan <i>Software</i> dan <i>Hardware</i> .....	34
3.3.1	<i>Hardware</i> (Perangkat Keras) .....	34
3.3.2	<i>Software</i> (perangkat lunak) .....	35
3.4	Analisa Masalah .....	35
3.5	Desain.....	36
3.5.1	Instalasi dan Konfigurasi <i>Honeypot</i> .....	36
3.6	Pengujian Serangan .....	36
3.6.1	Pengujian <i>Port Scanning</i> .....	37
3.6.2	Pengujian Distributed Denial Of service attack (DDoS) .....	38
3.6.3	Pengujian Brute Force Attack .....	40
3.7	Komparasi Hasil .....	42
3.8	Variabel Penelitian .....	42
3.9	Hasil dan Kesimpulan Penelitian .....	43
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>		<b>44</b>
4.1	Implementasi .....	44
4.1.1	Implementasi <i>Honeypot Cowrie</i> .....	45
4.1.2	Implementasi <i>Honeypot Dionaea</i> .....	58
4.2	Pengujian Serangan .....	62
4.2.1	Hasil pengujian <i>port scanning</i> pada <i>honeypot Dionaea</i> .....	62
4.2.2	Hasil Pengujian <i>Port Scanning</i> pada <i>Honeypot Cowrie</i> .....	66
4.2.3	Hasil Pengujian DDoS pada <i>honeypot Dionaea</i> .....	71
4.2.4	Hasil Pengujian <i>Bruteforce</i> pada <i>Honeypot cowrie</i> .....	74
4.2.5	Hasil Pengujian <i>Bruteforce</i> pada <i>Honeypot cowrie</i> .....	76

4.3	Perbandingan kedua <i>honeypot</i> .....	78
4.4	Hasil dan Pembahasan.....	79
<b>BAB V KESIMPULAN DAN SARAN .....</b>		<b>82</b>
5.1	Kesimpulan.....	82
5.2	Saran.....	82
<b>DAFTAR PUSTAKA .....</b>		<b>83</b>
<b>LAMPIRAN.....</b>		<b>88</b>

## DAFTAR GAMBAR

Gambar 2.1 Topologi <i>Star</i> .....	10
Gambar 2.2 Topologi <i>mesh</i> .....	11
Gambar 2.3 Topologi <i>Tree</i> .....	12
Gambar 2.4 Topologi Ring .....	13
Gambar 3.1 Diagram Alir Penelitian .....	33
Gambar 3.2 Topologi <i>Honeypot</i> .....	36
Gambar 3.3 Diagram Alir Port Scanning .....	38
Gambar 3.4 Diagram Alir DDoS .....	39
Gambar 3.5 Diagram Alir DDoS .....	40
Gambar 3.6 Diagram Alir Bruteforce Attack.....	41
Gambar 3.7 Diagram Alir Bruteforce Attack.....	42
Gambar 4.1 Konfigurasi repositori lokal menjadi repo aktif .....	45
Gambar 4.2 Update Repository .....	46
Gambar 4.3 <i>Konfigurasi SSH</i> .....	46
Gambar 4.4 <i>Restart service SSH</i> .....	47
Gambar 4.5 Install Paket Pendukung .....	48
Gambar 4.6 <i>Download Python</i> .....	48
Gambar 4.7 Mengkonfigurasi dan optimisasi <i>python</i> .....	49
Gambar 4.8 Build Python.....	50
Gambar 4.9 Proses Install Python .....	50
Gambar 4.10 Instalasi <i>packet honeypot cowrie</i> .....	51
Gambar 4.11 Pembuatan User.....	51
Gambar 4.12 instalasi <i>packet honeypot cowrie</i> .....	52
Gambar 4.13 <i>Clone File Cowrie</i> .....	52
Gambar 4.14 Mengaktifkan <i>enviroment python</i> dan instalasi <i>pip</i> .....	53
Gambar 4.15 Mengaktifkan <i>enviroment python</i> dan instalasi <i>pip</i> .....	53
Gambar 4.16 Mengubah Port SSH.....	53

Gambar 4.17 Mengaktifkan Service Telnet .....	54
Gambar 4.18 Menyalin File Config .....	54
Gambar 4.19 Mengubah Hak Akses User.....	55
Gambar 4.20 Proses konfigurasi file cowrie .....	55
Gambar 4.21 Proses menjalankan <i>service cowrie</i> .....	56
Gambar 4.22 proses menyalin data login user .....	56
Gambar 4.23 pengkonfigurasian userdb.txt .....	57
Gambar 4.24 proses menjalankan <i>service cowrie</i> .....	57
Gambar 4.25 Proses mengecek <i>log cowrie</i> .....	58
Gambar 4.26 Membuat usermod.....	58
Gambar 4.27 Clone File Dionaea.....	58
Gambar 4.28 Install Paket Pendukung .....	59
Gambar 4.29 Membuat file system Dionaea.....	59
Gambar 4.30 Proses <i>make system</i> .....	60
Gambar 4.31 Proses <i>make install</i> .....	60
Gambar 4.32 Proses mengaktifkan <i>dionaea</i> .....	61
Gambar 4.33 Proses mengecek <i>port honeypot</i> yang aktif .....	61
Gambar 4. 34 Topologi Penyerangan Port Scanning .....	62
Gambar 4. 35 Pengujian teknik <i>TCP Connect Scan honeypot Dionaea</i> .....	63
Gambar 4.36 Perintah dan waktu penyerangan <i>honeypot Dionaea</i> .....	64
Gambar 4.37 Hasil dari Pengujian Menggunakan Teknik TCP Connect Scan.....	64
Gambar 4.38 Pengujian Teknik <i>TCP SYN Scan honeypot Dionaea</i> .....	65
Gambar 4.39 Perintah dan waktu penyerangan honeypot Dionaea .....	66
Gambar 4.40 Hasil pengujian menggunakan Teknik <i>TCP SYN Scan</i> .....	66
Gambar 4.41 Pengujian Teknik <i>TCP Connect Scan honeypot Cowrie</i> .....	67
Gambar 4.42 Waktu dan perintah <i>honeypot Cowrie</i> .....	68
Gambar 4.43 Hasil Pengujian Teknik <i>TCP Connect Scan honeypot Cowrie</i> .....	68
Gambar 4.44 Hasil Pengujian Teknik <i>TCP Connect Scan honeypot Cowrie</i> .....	69
Gambar 4.45 Perintah dan Waktu Teknik <i>TCP Connect Scan honeypot Cowrie</i> .	70
Gambar 4.46 Hasil Pengujian Teknik TCP Connect Scan honeypot Cowrie .....	70

Gambar 4.47 Topologi Pengujian DDoS .....	71
Gambar 4.48 Proses Penyerangan Menggunakan <i>LOIC</i> .....	72
Gambar 4.49 Hasil <i>DDoS attack</i> ke <i>Honeypot Dionaea</i> .....	72
Gambar 4.50 pengujian <i>DDos attack</i> menggunakan <i>LOIC</i> ke <i>Honeypot cowrie</i> .	73
Gambar 4.51 Hasil <i>DDos attack</i> dari <i>DDoS Attack</i> ke <i>Honeypot cowrie</i> .....	73
Gambar 4.52 Pengujian serangan menggunakan hydra .....	75
Gambar 4.53 Hasil <i>Bruteforce Attack</i> ke <i>Honeypot cowrie</i> .....	76
Gambar 4.54 Topologi Pengujian Bruteforce .....	76
Gambar 4.55 Pengujian serangan menggunakan hydra attack.....	77
Gambar 4.56 Hasil <i>Bruteforce Attack</i> ke <i>Honeypot dionaea</i> .....	78



## DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu .....	26
Tabel 3.1 Spesifikasi <i>Server</i> .....	34
Tabel 3.2 Spesifikasi <i>Laptop Client</i> .....	34
Tabel 3.3 Daftar <i>Software</i> Yang Digunakan .....	35
Tabel 4.1 Hasil Traffic Penyerangan .....	79

## DAFTAR LAMPIRAN

Lampiran 1. Biografi Penulis.....	36
Lampiran 2. Kartu Bimbingan Skripsi.....	37
Lampiran 3. Pernyataan Tidak Plagiat.....	38