

**IMPLEMENTASI LOW-INTERACTION HONEYD PADA  
VIRTUAL ENVIRONMENT UNTUK MENINGKATKAN  
KEAMANAN SERVER**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Informatika



disusun oleh

**MUHAMMAD AMRULLAH**

**18.11.1898**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2023**

**IMPLEMENTASI LOW-INTERACTION HONEYD PADA  
VIRTUAL ENVIRONMENT UNTUK MENINGKATKAN  
KEAMANAN SERVER**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Informatika



disusun oleh

**MUHAMMAD AMRULLAH**

**18.11.1898**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2023**

HALAMAN PERSERUJUAN

SKRIPSI

IMPLEMENTASI LOW-INTERACTION HONEYD PADA VIRTUAL  
ENVIRONMENT UNTUK MENINGKATKAN KEAMANAN SERVER

yang disusun dan dipresentasikan oleh

MURAMMAD AMRULLAH

18111090

sebagai persyaratan untuk memenuhi sebagian  
pada tanggal 22 November 2021

Dosen Pembimbing

  
Sahakhotomullo, S. Kurni, M. Kom  
NID. 190303413

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI LOW-INTERACTION HONEYD PADA VIRTUAL ENVIRONMENT UNTUK MENINGKATKAN KEAMANAN SERVER

yang disusun dan diajukan oleh

Muhammad Anrullah

18.11.1898

Telah dipertahankan di depan Dewan Penguji pada tanggal 22 November 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Haryoko, S.Kom., M. Cs.  
NIK. 190302286

Bayu Setiati, M.Kom  
NIK. 190302216

Subektiingsih, M.Kom  
NIK. 190302413

Skripsi ini telah diterima sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Komputer Tanggal 22 November 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.  
NIK. 190302096

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : **Muhammad Aneeliah**  
NIM : **181121008**

Menyatakan bahwa Skripsi dengan judul berikut:

**IMPLEMENTASI LOW-INTERACTION HONEYD PADA VIRTUAL ENVIRONMENT UNTUK MENINGKATKAN KEAMANAN SERVER**

Dibaca dan disetujui oleh Dosen Pembimbing : **Sobektiingatih, A. Iqbal, M. Kesu**

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau produk orang lain, kecuali secara tertulis dengan nama dan alamatnya sebagai acuan dalam masalah dengan diizinkan nama pengarang dan diterbitkan dalam Daftar Pustaka pada karya tulis ini.
4. Peringkat hasil yang diperoleh dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan prosedur yang berlaku yang sudah ditetapkan, serta sanksi lainnya sesuai dengan aturan yang berlaku di Perguruan Tinggi.

Yogyakarta, 22 November 2023

Yang Menyatakan,

  
Muhammad Aneeliah

## HALAMAN PERSEMBAHAN

Alhamdulillah kupersembahkan kepada Allah SWT, atas segala rahmat dan juga kesempatan dalam menyelesaikan tugas akhir skripsi saya dengan segala kekurangannya. Segala syukur kuucapkan kepada Mu Ya Rabb, karena sudah menghadirkan orang - orang berarti disekeliling saya. Yang selalu memberi semangat dan doa, sehingga skripsi saya ini dapat di selesaikan dengan baik. Oleh karena itu penulis mempersembahkan skripsi ini pada :

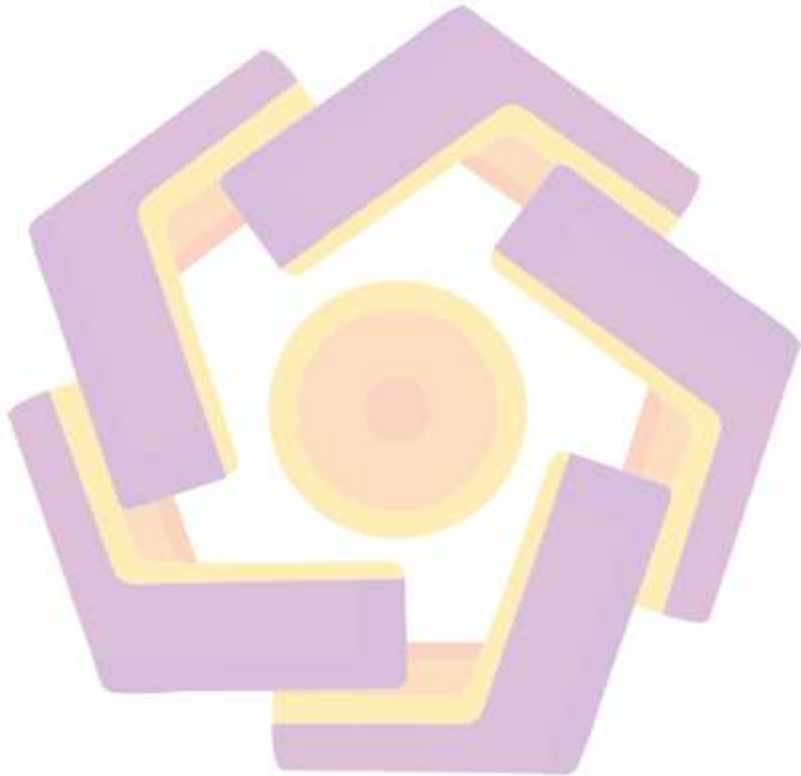
Teristimewa khususnya kepada Orang tua yang selalu mendukung, memberi doa restu, cinta dan kasih sayang kepada anaknya. Untuk karya yang sederhana ini, Apa yang saya dapatkan hari ini, belum mampu membayar semua kebaikan, keringat, dan juga air mata bagi saya. Terimakasih atas segala dukungan kalian, baik dalam bentuk materi maupun moril. Karya ini saya persembahkan untuk kalian, sebagai wujud rasa terima kasih atas pengorbanan dan jerih payah kalian sehingga saya dapat menggapai cita-cita. Kelak cita-cita saya ini akan menjadi persembahan yang paling mulia untuk papah dan mamah, dan semoga dapat membahagiakan kalian.

Kepada yang kuhormati dan kubanggakan kepada Ibu Dosen Subektiningsih, S.Kom, M.Kom selaku dosen pembimbing saya yang paling baik dan bijaksana, terima kasih atas bantuan, nasihat, dan ilmunya yang selama ini dilimpahkan pada saya dengan rasa tulus dan ikhlas. dan almamaterku. Ilmu dan dedikasi yang sedemikian besar bagi kampus dan pendidikan terutama dalam Jurusan Informatika.

Kepada sahabat dan teman seperjuangan saya dalam kelas Informatika IF 02 . Dari awal perkuliahan banyak sekali cerita yang telah terekam, segala bentuk dukungan, kekompakan, keluh kesah sedih senang bersama sama hingga keterbatasan perkuliahan karena pandemi, hingga akhirnya saya dapat menyelesaikan skripsi. Selalu semangat untuk teman - teman yang masih berjuang. Serta tidak lupa saya ucapkan terima kasih untuk teman-teman baik saya yang selalu mensupport saya dan menemani mengerjakan skripsi ini yaitu Denny, Bima,

Galih, Dimas, Iqbal dan yang lainnya yang tidak bisa saya sebut satu persatu. maaf jika banyak salah dengan kata yang tak terucap. Terima kasih untuk support dan luar biasa, sampai saya bisa menyelesaikan skripsi ini dengan baik.

Kepada Qurrata Ayna, yang telah menemani dan mendukung saya secara penuh sehingga skripsi ini dapat selesai.





## KATA PENGANTAR

Puji syukur penulis ucapkan kepada Allah SWT, yang mana telah memberikan kesehatan dan karunia-Nya kepada penulis serta kekuatan untuk menyelesaikan skripsi yang berjudul **IMPLEMENTASI LOW-INTERACTION HONEYD PADA VIRTUAL ENVIRONMENT UNTUK MENINGKATKAN KEAMANAN SERVER**. Tidak lupa penulis mengucapkan shalawat dan salam kepada junjungan Nabi Besar Muhammad SAW. Penyelesaian tulisan ini terlepas bantuan dari berbagai pihak yang terkait secara langsung maupun tidak langsung, terutama dan teristimewa dipersembahkan kepada kedua orang tua tercinta yang senantiasa memberikan rasa sayang, didikan, serta doa yang selalu di panjatkan pada Allah kepada penulis.

Skripsi ini dapat terselesaikan dengan bantuan berbagai pihak, maka dari itu penulis menyatakan rasa hormat dan terimakasih kepada:

1. Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas AMIKOM Yogyakarta.
2. Bapak Hanif Al Fatta, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Ibu Windha Mega Pradnya D, M.Kom selaku ketua Program Studi Informatika Universitas AMIKOM Yogyakarta.
4. Ibu Subektiningsih, S.Kom., M.Kom. selaku pembimbing yang senantiasa memberikan masukan serta nasihat dalam penulisan skripsi ini.
5. Dosen penguji, terima kasih atas saran dan kritiknya sehingga penelitian ini menjadi lebih baik lagi.

Penulis menyadari masih ada kekurangan dan kelemahan dalam pembuatan skripsi ini. Maka penulis mengharapkan adanya kritik dan saran dari segala pihak agar menambah kesempurnaan dalam skripsi ini.

Yogyakarta, 5 November 2023

Muhammad Amrullah

NIM 18.11.1898

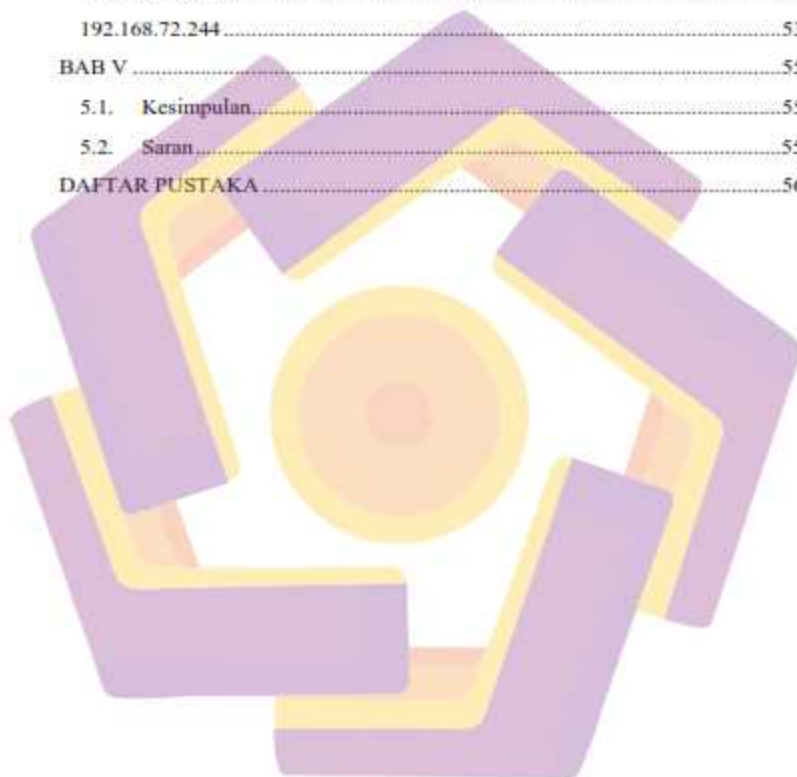


## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PERSETUJUAN SKRIPSI.....	ii
HALAMAN PENGESAHAN .....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....	iii
HALAMAN PERSEMBAHAN .....	v
KATA PENGANTAR .....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL.....	xiii
INTISARI.....	xiv
<i>ABSTRAK</i> .....	xv
<b>BAB I</b> .....	<b>1</b>
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	4
1.3. Batasan Masalah .....	4
1.4. Tujuan Penelitian.....	4
1.5. Manfaat Penelitian.....	5
<b>BAB II</b> .....	<b>6</b>
2.1. Tinjauan Pustaka .....	6
2.2. Literature Review .....	8
2.3. Dasar Teori.....	12
2.3.1. Jaringan Komputer .....	12
2.3.2. Jenis-jenis jaringan komputer .....	13
2.3.3. Tipe jaringan komputer.....	13
2.3.4. Layanan server pada jaringan komputer .....	14
2.3.5. TCP / IP.....	15
2.3.6. Port Pada Jaringan Komputer .....	16
2.4. Sistem Keamanan Jaringan .....	18
2.4.1. Strategi Keamanan Data/Informasi dalam Jaringan.....	18

2.5.	Serangan dan Ancaman Pada Sistem Keamanan Jaringan.....	19
2.5.1.	Serangan Terhadap Sistem Keamanan Jaringan .....	19
2.5.2.	Bentuk-bentuk Ancaman .....	20
2.6.	Honeypot.....	21
2.6.1.	Jenis Interaksi Honeypot.....	22
2.6.2.	Jenis Honeypot.....	24
2.6.3.	Honeyd.....	25
BAB III	.....	26
3.1.	Objek Penelitian.....	26
3.2.	Alur Penelitian.....	26
3.2.1.	Analisis ( <i>Analysis</i> ).....	27
3.2.2.	Desain ( <i>Design</i> ) .....	28
3.2.3.	Simulasi ( <i>Simulation Prototyping</i> ) .....	29
3.2.4.	Melakukan penerapan hasil ( <i>Implementation</i> ).....	30
3.2.5.	Melakukan Pemantauan ( <i>Monitoring</i> ).....	31
3.2.6.	Melakukan pengelolaan ( <i>Management</i> ).....	31
3.3.	Alat dan Bahan.....	32
BAB IV	.....	34
4.1.	<i>Prototyping Simulation</i> .....	34
4.2.	<i>Implementation</i> .....	37
4.3.	<i>Monitoring</i> .....	47
4.4.	<i>Management</i> .....	52
No.	.....	53
IP Honeyd Lama.....		53
IP Honeyd Baru.....		53
1.....		53
192.168.72.251.....		53
192.168.72.247.....		53
2.....		53
192.168.72.250.....		53
192.168.72.246.....		53

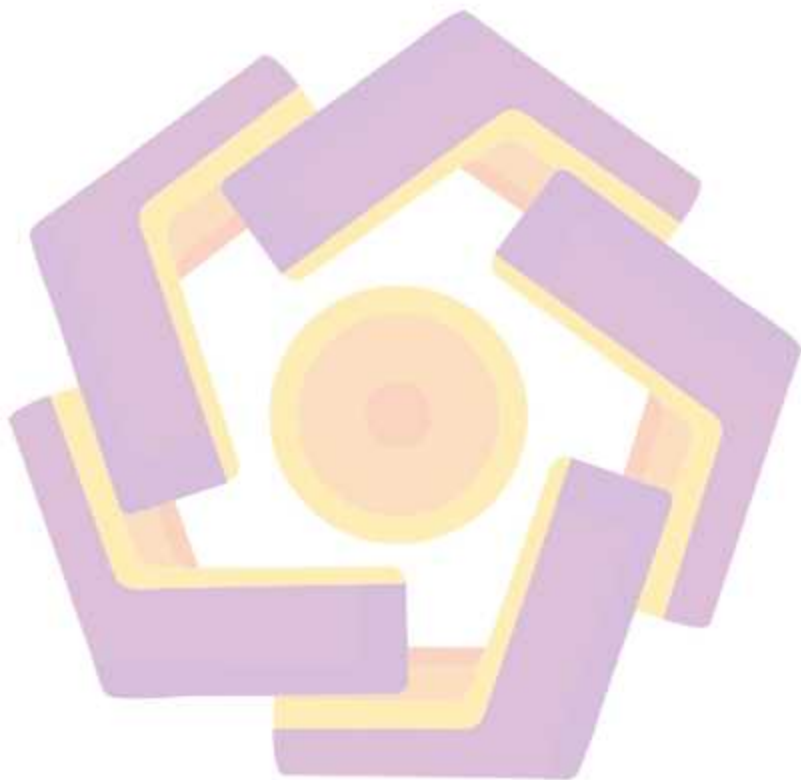
3.....	53
192.168.72.249.....	53
192.168.72.245.....	53
4.....	53
192.168.72.248.....	53
192.168.72.244.....	53
<b>BAB V</b> .....	<b>55</b>
5.1. Kesimpulan.....	55
5.2. Saran.....	55
<b>DAFTAR PUSTAKA</b> .....	<b>56</b>



## DAFTAR GAMBAR

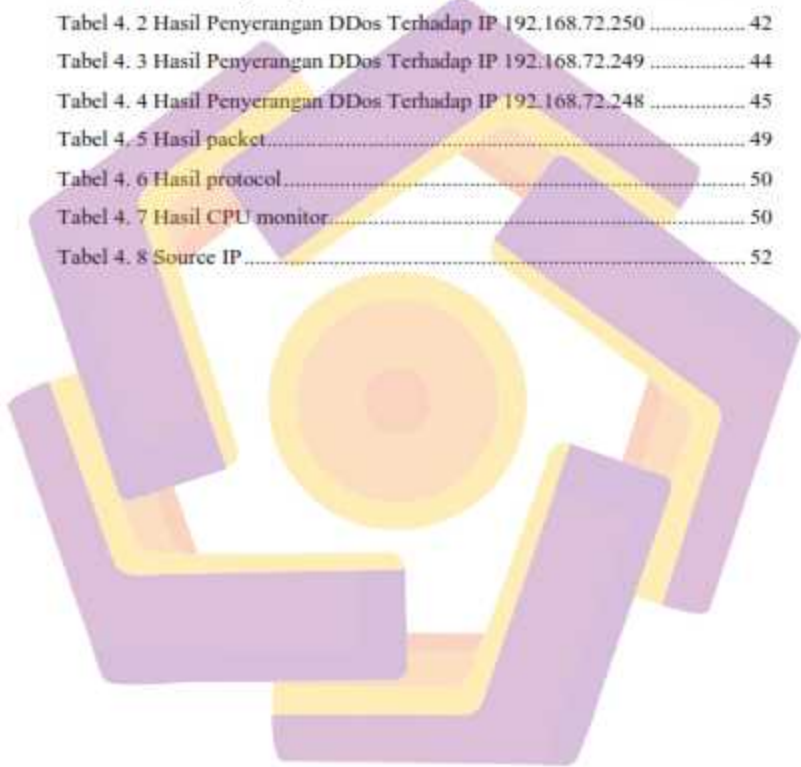
Gambar 3.1	Tahapan NDLC [17].....	27
Gambar 3.2	Web Server.....	27
Gambar 3.3	Topologi Jaringan.....	29
Gambar 3.4	Tahapan Simulasi.....	30
Gambar 3.5	Tahapan Impelementasi.....	31
Gambar 4.1	Tampilan Virtual Box.....	34
Gambar 4.2	Tampilan IP Adress.....	35
Gambar 4.3	DHCP Server.....	35
Gambar 4.4	Mengunduh repository.....	36
Gambar 4.5	Berpindah direktori.....	36
Gambar 4.6	Instal sistem Honeyd.....	36
Gambar 4.7	Web server.....	37
Gambar 4.8	Konfigurasi Honeyd.....	37
Gambar 4.9	Konfigurasi Honeyd.....	38
Gambar 4.10	Perintah menjalankan honeyd.....	39
Gambar 4.11	Hasil Scanning melalui Aplikasi Zenmap.....	39
Gambar 4.12	Respon Honeyd setelah dilakukan scanning.....	40
Gambar 4.13	Serangan DDoS.....	40
Gambar 4.14	Tanggapan Honeyd IP 192.168.72.251 terhadap serangan DDoS.....	42
Gambar 4.15	Tanggapan Honeyd IP 192.168.72.250 terhadap serangan DDoS.....	43
Gambar 4.16	Tanggapan Honeyd IP 192.168.72.249 terhadap serangan DDoS.....	45
Gambar 4.17	Tanggapan Honeyd IP 192.168.72.248 terhadap serangan DDoS.....	46
Gambar 4.18	Log Source Sawmill.....	47
Gambar 4.19	Packet yang masuk sebelum penyerangan.....	48
Gambar 4.20	Packet yang masuk setelah penyerangan.....	48
Gambar 4.21	Protocol setelah penyerangan.....	49
Gambar 4.22	Protocol sebelum penyerangan.....	49
Gambar 4.23	CPU monitor sebelum penyerangan.....	50
Gambar 4.24	CPU monitor setelah penyerangan.....	50
Gambar 4.25	Source IP setelah penyerangan.....	51

Gambar 4. 26 Soure IP sebelum penyerangan .....	51
Gambar 4. 27 Perintah untuk menggunakan layanan.....	52
Gambar 4. 29 Honeyd baru .....	53
Gambar 4. 28 Honeyd lama.....	53



## DAFTAR TABEL

Tabel 2.1 Literature Review .....	8
Tabel 2.2 Daftar Port (Sumber :[11]).....	17
Tabel 3.1 Alat dan Bahan.....	32
Tabel 4. 1 Hasil Penyerangan DDos Terhadap IP 192.168.72.251 .....	41
Tabel 4. 2 Hasil Penyerangan DDos Terhadap IP 192.168.72.250 .....	42
Tabel 4. 3 Hasil Penyerangan DDos Terhadap IP 192.168.72.249 .....	44
Tabel 4. 4 Hasil Penyerangan DDos Terhadap IP 192.168.72.248 .....	45
Tabel 4. 5 Hasil packet.....	49
Tabel 4. 6 Hasil protocol.....	50
Tabel 4. 7 Hasil CPU monitor.....	50
Tabel 4. 8 Source IP.....	52





## INTISARI

Jaringan komputer telah menjadi sarana berbagi informasi di seluruh dunia, teknologi internet saat ini telah digunakan dari berbagai kalangan baik untuk jejaring sosial maupun kebutuhan lainnya. Maraknya kasus *Cybercrime* yang terjadi terutama di Indonesia mengindikasikan adanya penyalahgunaan sistem keamanan jaringan, untuk dapat menghindari kejahatan yang mungkin dilakukan oleh pihak tertentu, dibutuhkannya sebuah solusi untuk dapat meningkatkan sistem keamanan yang dapat mendeteksi serangan serta dapat menjebak penyerang. HoneyPot merupakan salah satu sistem jaringan yang bisa diimplementasikan untuk mengantisipasi terjadinya *Cyber Crime*. Honeyd adalah sebuah produk honeyPot yang ditulis oleh Niels Provos, ini dari honeyd yaitu sistem ini akan mensimulasikan tingkah laku sebuah komputer beserta sistem operasinya.

Honeyd berperan sebagai server bayangan yang menyerupai server sesungguhnya, yang memiliki beberapa layanan disertai port yang sengaja dibuka untuk diserang. Ada beberapa alat yang digunakan untuk konfigurasi dalam implementasi HoneyPot, salah satu alat yang digunakan yaitu virtual environment yang mencakup Virtual Box, yang mana Virtual Box dapat mengubah sistem operasi virtualisasi menjadi sebuah bentuk nyata. Metode yang digunakan dalam penelitian ini adalah metode Network Development Life Cycle (NDLC), dimana metode ini merupakan sebuah metode yang bergantung pada proses pengembangan sebelumnya. Hasil dari penelitian ini memperlihatkan kinerja honeyd yang berhasil mengelabui penyerang dengan server bayangan, saat penyerang melakukan scanning maka honeyd memutuskan koneksi (Killing attempted connection: tcp), sehingga IP Server asli tidak terdeteksi.

Honeyd pada *Virtual Environment* terbukti dapat meningkatkan keamanan server melalui pengujian serangan DDoS sebanyak 36 kali. Server Asli dengan IP Address 192.168.72.253 tetap terlindungi dengan tidak terdeteksi saat proses scanning. Hal ini dikarenakan server asli dilindungi oleh keberadaan 4 server bayangan honeyd dengan IP 192.168.72.251, 192.168.72.250, 192.168.72.249, 192.168.72.248 Sehingga, serangan DDoS hanya berhasil pada server bayangan dan tidak mencapai server asli. Setelah terjadi penyerangan, honeyd perlu dimatikan (set off) untuk mempertahankan kinerja. Saat keempat server bayangan honeyd dimatikan dan dinyalakan kembali maka akan muncul IP baru. Hal ini bertujuan untuk mengantisipasi serangan DDoS kembali. Penelitian ini selanjutnya dapat dilakukan dengan pengujian dan implementasi honeyd tidak hanya dilakukan pada *virtual environment*, akan tetapi juga di implementasikan dalam kehidupan nyata.

**Kata Kunci :** HoneyPot, Honeyd, Sistem Jaringan, Internet



## **ABSTRAK**

Computer networks have become a means of sharing information around the world, internet technology is currently used from various circles both for social networking and other needs. The rise of Cybercrime cases that occur especially in Indonesia indicates the misuse of network security systems, to be able to avoid crimes that may be committed by certain parties, a solution is needed to be able to improve security systems that can detect attacks and can trap attackers. Honeypot is one of the network systems that can be implemented to anticipate cyber crime. Honeyd is a honeypot product written by Niels Provos, the essence of honeyd is that this system will simulate the behavior of a computer and its operating system.

Honeyd acts as a shadow server that resembles a real server, which has several services along with ports that are deliberately opened for attack. There are several tools used for configuration in the implementation of Honeypot, one of the tools used is a virtual environment that includes Virtual Box, which Virtual Box can turn a virtualized operating system into a real form. The method used in this research is the Network Development Life Cycle (NDLC) method, which is a method that depends on the previous development process. The results of this study show the performance of honeyd which successfully tricked the attacker with a shadow server, when the attacker scanned then honeyd broke the connection (Killing attempted connection: tcp), so that the original Server IP was not detected.

Honeyd in the Virtual Environment is proven to increase server security through testing DDoS attacks 36 times. The Original Server with IP Address 192.168.72.253 remains protected by not being detected during the scanning process. This is because the original server is protected by the existence of 4 honeyd shadow servers with IP 192.168.72.251, 192.168.72.250, 192.168.72.249, 192.168.72.248 So, DDoS attacks only succeed on shadow servers and do not reach the original server. After the attack, honeyd needs to be set off to maintain performance. When the four honeyd shadow servers are turned off and turned on again, a new IP will appear. This aims to anticipate DDoS attacks again. Further research can be done by testing and implementing honeyd not only in a virtual environment, but also implemented in real life.

**Keywords:** *Honeypot, Honeyd, Network System, Internet*