



**SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI**

**PERANCANGAN DAN ANALISA EFEKTIFITAS *HONEYPOT*  
MENGUNAKAN *DIONEAE* DALAM JARINGAN  
KOMPUTER SIMULASI**

**TUGAS AKHIR**

**RAKHA DIASRY**

**0110216075**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**DEPOK**

**JULI 2021**



**SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI**

**PERANCANGAN DAN ANALISA EFEKTIFITAS *HONEYPOT*  
MENGUNAKAN *DIONEAE* DALAM JARINGAN  
KOMPUTER SIMULASI**

**TUGAS AKHIR**

**RAKHA DIASRY**

**0110216075**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**DEPOK**

**JULI 2021**

## HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah karya penulis,  
dan semua sumber baik yang dikutip maupun dirujuk  
telah saya nyatakan dengan benar.

Nama : Rakha Diasry

NIM : 0110216075

Tanda Tangan : 

Tanggal : 15 Juli 2021

## HALAMAN PENGESAHAN

Skripsi / Tugas Akhir ini diajukan oleh :

Nama : Rakha Diasry

NIM : 0110216075

Program Studi : Teknik Informatika

Judul Skripsi : Perancangan Dan Analisa Efektifitas Honeypot Menggunakan Dionaea Dalam Jaringan Komputer Simulasi

**Telah berhasil dipertahankan dihadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri**

### DEWAN PENGUJI

Pembimbing

(Tubagus Rizky Dharmawan, S.T, M.Sc.)

Penguji 1

Penguji 2

(Henry Saptono, S.Si., M.Kom.)

(Aditya Putra, S.T., M.T.)

Ditetapkan di : Depok

Tanggal : 15 Juli 2021

## KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan skripsi/Tingkat Akhir ini. Penulisan skripsi/Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana computer Program Studi Teknik Informatika pada Sekolah Tinggi Teknologi Terpadu Nurul Fikri. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi/tugas akhir ini.

Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Allah SWT.
2. Seluruh keluarga di rumah yang selalu melangitkan doanya untuk kemudahan dan kelancaran proses studi penulis.
3. Bapak Drs. Lukman Rosyidi, S.T, M.M, M.T selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
4. Bapak Ahmad Rio Adriansyah, S.Si, M.Si selaku Ketua Program Studi Teknik Informatika Sekolah Tinggi Teknologi Terpadu Nurul Fikri
5. Bapak Zaki Imaduddin S.T, M.Kom selaku Dosen Pembimbing Akademik yang telah membimbing penulis selama berkuliah di Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
6. Bapak Tubagus Rizky Dharmawan, S.T, M.Sc. selaku Dosen Pembimbing Tugas Akhir penulis dalam menyelesaikan penulisan ilmiah ini.
7. Para Dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.

8. Bapak Slamet Santoso, S.Kom. selaku Dosen & Mentor yang membantu penulis dalam pembuatan Tugas Akhir.

9. Serta support dari teman-teman yang tidak dapat penulis sebutkan satu-persatu agar penulis dapat menyelesaikan Tugas Akhir.

Dalam penulisan ilmiah ini tentu saja masih banyak terdapat kekurangan yang mungkin disebabkan oleh keterbatasan kemampuan dan pengetahuan yang penulis miliki. Walaupun demikian, penulis telah berusaha menyelesaikan penulisan ilmiah ini sebaik mungkin. Oleh karena itu apabila terdapat kekurangan didalam penulisan ilmiah ini, dengan rendah hati penulis menerima kritik dan saran dari pembaca.

Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa mandaat bagi pengembangan ilmu.

Depok, 15 Juli 2021

Penulis

STT - NF

## HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPERNTINGAN AKADEMIS

Sebagai sivitas akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri, saya yang bertanda tangan di bawah ini:

Nama : Rakha Diasry  
NIM : 0110216075  
Program Studi : Teknik Informatika  
Jenis Karya : Skripsi / Tugas Akhir

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada STT-NF **Hak Bebas Royalti Noneksklusif (Non-exclusive Royalty – Free Right)** atas karya ilmiah saya yang berjudul:

PERANCANGAN DAN ANALISA EFEKTIFITAS HONEYPOT MENGGUNAKAN DIONEAE DALAM JARINGAN KOMPUTER SIMULASI.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini STT-NF berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

STT - NF

Dibuat di : Depok

Pada tanggal : 15 July 2021

Yang menyatakan



(Rakha Diasry)

## ABSTRAK

Nama : Rakha Diasry

NIM : 0110216075

Program Studi : Teknik Informatika

Judul : Perancangan dan Analisa Efektifitas Honeypot Menggunakan Dionaea Dalam Jaringan Komputer Simulasi

Perkembangan teknologi seputar informasi pada jaringan komputer saat ini sudah semakin maju dan berkembang sangat pesat serta sudah dapat di aplikasikan di segala bidang. Alasan inilah yang mendorong banyak pihak bergantung pada kewanaman sistem jaringan komputer, namun di sisi lain sistem jaringan komputer masih memiliki beberapa masalah. Salah satunya adalah terkait faktor keamanan. Peran faktor kewanaman menjadi penting tidak semua data atau informasi yang tersedia bersifat terbuka untuk umum dan tak semua orang juga berhak untuk mengaksesnya. Oleh karena itu, informasi akan menjadi aset yang sangat berharga baik bagi perseorangan, pemerintah maupun pihak swasta. Salah satu alat yang dapat membantu untuk meningkatkan sistem keamanan komputer adalah *Honeypot*. Dengan penggunaan *Honeypot* kita dapat merekam segala aktivitas ilegal yang dilakukan oleh penyerang dapat digunakan oleh *administrator* sebagai informasi tambahan tentang penyerangan untuk menganalisis serta mempelajari aktivitas-aktivitas yang cenderung membahayakan sistem.

Kata kunci : Keamanan jaringan, *Dionaea*, *Honeypot*, Informasi

STT - NF



## ***ABSTRACT***

*Name* : Rakha Diasry

*NIM* : 0110216075

*Study Program* : *Informatics Engineering*

*Title* : *Design and Network Simulation of Honeypot Dionaea on Computer Network*

*The development of technology around information on computer networks is now increasingly advanced and growing very rapidly and can be applied in all fields. this is what encourages many parties but is supported on computer network system security, the reason on the other side of the computer network system still has some problems. One of them is related to the safety factor. The role of security factors is important, not all available data or information is open to the public and not everyone has the right to access it. Therefore, information will become a very valuable asset for individuals, government and private sectors. One of the tools that can help to improve computer security system is Honeypot. With the use of Honeypot, we can record all illegal activities carried out by attackers which can be used by administrators as additional information about attacks to analyze and study activities that harm the system.*

*Key* : *Network security, Dionaea, Honeypot, Information*

STT - NF

## DAFTAR ISI

|                                       |      |
|---------------------------------------|------|
| HALAMAN PERNYATAAN ORISINALITAS ..... | ii   |
| HALAMAN PENGESAHAN .....              | iii  |
| KATA PENGANTAR .....                  | iv   |
| HALAMAN PERNYATAAN .....              | vi   |
| ABSTRAK.....                          | vii  |
| <i>ABSTRACT</i> .....                 | viii |
| DAFTAR ISI.....                       | ix   |
| DAFTAR GAMBAR .....                   | xii  |
| DAFTAR TABEL.....                     | xiv  |
| BAB I PENDAHULUAN.....                | 1    |
| 1.1 Latar Belakang.....               | 1    |
| 1.2 Rumusan Masalah.....              | 3    |
| 1.3 Tujuan Penelitian.....            | 3    |
| 1.4 Manfaat Penelitian.....           | 3    |
| 1.5 Batasan Masalah .....             | 4    |
| 1.6 Sitematika Penulisan.....         | 4    |
| BAB II LANDASAN TEORI.....            | 6    |
| 2.1 Honeypot.....                     | 6    |

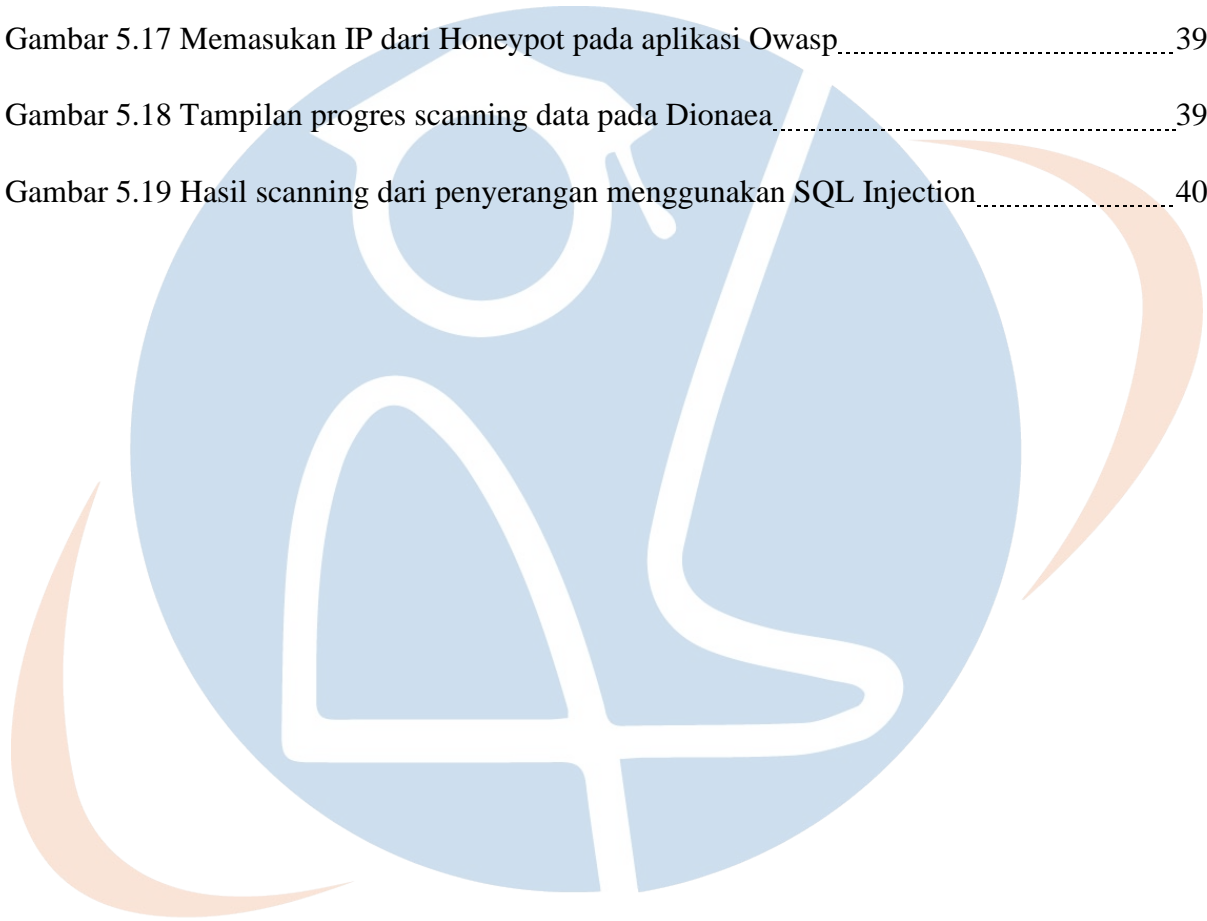
|                                            |                                    |           |
|--------------------------------------------|------------------------------------|-----------|
| 2.1.1                                      | Klasifikasi Honeypot .....         | 7         |
| 2.2                                        | Dionaea.....                       | 8         |
| 2.3                                        | Metasploit.....                    | 9         |
| 2.4                                        | Advanced Port Scanner .....        | 10        |
| 2.5                                        | OWASP ZAP .....                    | 10        |
| 2.6                                        | Metasploit Framework .....         | 11        |
| 2.7                                        | Perangkat Jaringan Komputer .....  | 11        |
| 2.8                                        | Penelitian Terkait .....           | 13        |
| <b>BAB III METODOLOGI PENELITIAN .....</b> |                                    | <b>16</b> |
| 3.1                                        | Jenis Metode Penelitian.....       | 16        |
| 3.2                                        | Metode Pengumpulan Data .....      | 16        |
| 3.3                                        | Prosedur Penelitian.....           | 17        |
| 3.3.1                                      | Analisis Kebutuhan.....            | 17        |
| 3.3.2                                      | Perancangan Sistem .....           | 18        |
| 3.3.3                                      | Implementasi.....                  | 18        |
| 3.3.4                                      | Pengujian.....                     | 18        |
| 3.3.5                                      | Pembuatan Laporan Penelitian ..... | 18        |
| 3.4                                        | Lingkungan Penelitian.....         | 19        |
| 3.5                                        | Alat dan Utilitas .....            | 19        |
| 3.6                                        | Jadwal Penelitian.....             | 20        |

|                                                     |    |
|-----------------------------------------------------|----|
| BAB IV ANALISIS KEBUTUHAN DAN PERANCANGAN .....     | 21 |
| 4.1    Analisa Sistem.....                          | 21 |
| 4.2    Perancangan Sistem.....                      | 22 |
| 4.3    Perancangan Pengujian .....                  | 24 |
| 4.3.1    Port Scanning .....                        | 24 |
| 4.3.2    Metasploit .....                           | 25 |
| 4.3.3    SQL INJECTION .....                        | 26 |
| BAB V IMPLEMENTASI DAN PENGUJIAN .....              | 27 |
| 5.1    Implementasi Sistem .....                    | 27 |
| 5.2    Pengujian Sistem.....                        | 32 |
| 5.2.1    Scanning ke Server Honeypot.....           | 32 |
| 5.2.2    Pengujian Serangan Jaringan Exploit5 ..... | 35 |
| 5.2.3    Pengujian Serangan SQL Injection .....     | 38 |
| BAB VI PENUTUP .....                                | 43 |
| 6.1    Kesimpulan.....                              | 43 |
| 6.2    Saran.....                                   | 44 |
| DAFTAR PUSTAKA .....                                | 45 |
| LAMPIRAN.....                                       | 47 |

## DAFTAR GAMBAR

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Gambar 2.1 Alur kerja Honeypot.....                                     | 6  |
| Gambar 2.2 Arsitektur Metasploit.....                                   | 9  |
| Gambar 2.3 Contoh Struktur Local Area Network.....                      | 12 |
| Gambar 2.4 Contoh Struktur Metropolitan Area Network.....               | 13 |
| Gambar 2.5 Contoh Struktur Wide Area Network.....                       | 13 |
| Gambar 3.1 Alur Kegiatan Penelitian.....                                | 17 |
| Gambar 4.1 Skema perancangan arsitektur jaringan.....                   | 23 |
| Gambar 4.2 Hasil port scanning menggunakan advanced port scanning.....  | 24 |
| Gambar 4.3 Hasil port scanning menggunakan advanced port scanning.....  | 25 |
| Gambar 4.4 Hasil pembacaan eksploit yang dilakukan oleh metasploit..... | 26 |
| Gambar 5.1 Pemilihan lokasi penginstalan aplikasi Honeypot.....         | 27 |
| Gambar 5.2 Tampilan fitur Honeypot yang akan diinstal.....              | 28 |
| Gambar 5.3 Hasil penginstalan aplikasi Honeypot.....                    | 29 |
| Gambar 5.4 Penyetingan jaringan Honeypot.....                           | 29 |
| Gambar 5.5 Penyetingan alamat IP pada virtual box computer.....         | 30 |
| Gambar 5.6 Pengecekan Dionaea.....                                      | 30 |
| Gambar 5.7 Konfigurasi DionaeaFR.....                                   | 31 |
| Gambar 5.8 Pemanggilan tools nmap untuk port scanning DionaeaFR.....    | 31 |
| Gambar 5.9 Hasil koneksi antara komputer dan Honeypot.....              | 32 |
| Gambar 5.10 Hasil koneksi komputer dengan Honeypot.....                 | 33 |
| Gambar 5.11 Pengecekan website DionaeaFR.....                           | 33 |

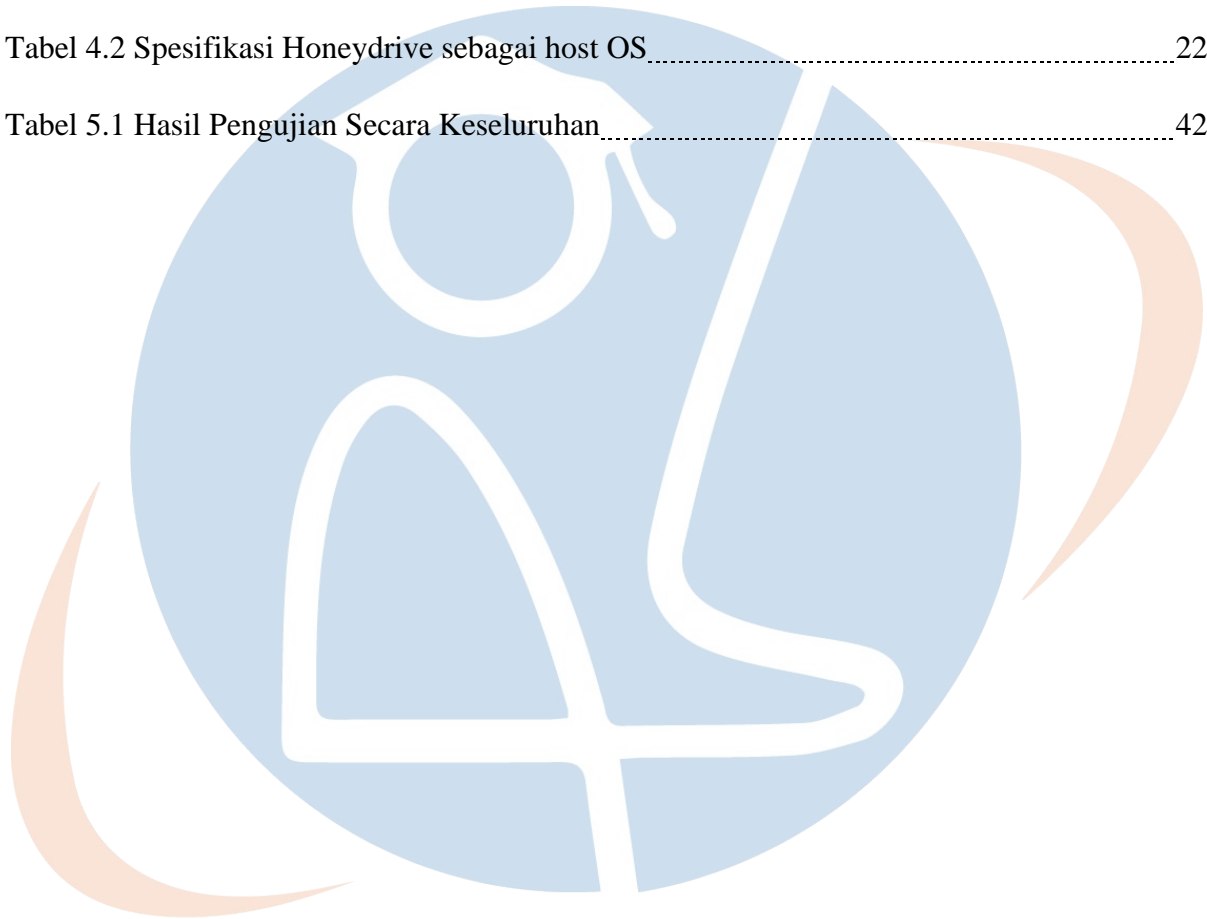
|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| Gambar 5.12 Pengaturan alamat IP yang akan diserang.....                          | 34 |
| Gambar 5.13 Pengaturan alamat IP penyerang.....                                   | 35 |
| Gambar 5.14 Tampilan awal Metasploit Framework.....                               | 36 |
| Gambar 5.15 Proses serangan menggunakan Metasploit Framework.....                 | 37 |
| Gambar 5.16 Hasil serangan jaringan exploit menggunakan Metasploit Framework..... | 38 |
| Gambar 5.17 Memasukan IP dari Honeypot pada aplikasi Owasp.....                   | 39 |
| Gambar 5.18 Tampilan progres scanning data pada Dionaea.....                      | 39 |
| Gambar 5.19 Hasil scanning dari penyerangan menggunakan SQL Injection.....        | 40 |



STT - NF

## DAFTAR TABEL

|                                                        |    |
|--------------------------------------------------------|----|
| Tabel 2.1 Penelitian Terkait .....                     | 13 |
| Tabel 3.1 Jadwal Penelitian .....                      | 20 |
| Tabel 4.1 Spesifikasi Windows sebagai host OS .....    | 22 |
| Tabel 4.2 Spesifikasi Honeydrive sebagai host OS ..... | 22 |
| Tabel 5.1 Hasil Pengujian Secara Keseluruhan .....     | 42 |



STT - NF