

**PERANCANGAN SISTEM MONITORING KEAMANAN *CYBER*  
BERBASIS WEBSITE**

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Informatika



disusun oleh

**WAHYU ARIF PURNOMO**

**16.11.0746**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2023**

**PERANCANGAN SISTEM MONITORING KEAMANAN *CYBER*  
BERBASIS WEBSITE**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Informatika



disusun oleh

**WAHYU ARIF PURNOMO**

**16.11.0746**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA**

**YOGYAKARTA**

**2023**

HALAMAN PERSETUJUAN

SKRIPSI

PERANCANGAN SISTEM MONITORING KEAMANAN *CYBER*  
BERBASIS WEBSITE

yang disusun dan diajukan oleh

**Wahyu Arif Purnomo**

**16.11.0746**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 4 Agustus 2023

Dosen Pembimbing,



Lukman, M.Kom  
NIK/190302151

HALAMAN PENGESAHAN  
SKRIPSI  
PERANCANGAN SISTEM MONITORING KEAMANAN *CYBER*  
BERBASIS WEBSITE

yang disusun dan diajukan oleh

**Wahyu Arif Purnomo**

16.11.0746

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 4 Agustus 2023

Susunan Dewan Penguji

Nama Penguji

Lukman, M.Kom  
NIK. 190302151

Uvock Anggoro Saputro, M.Kom  
NIK. 190302419

Theopilus Bayu Sasongko, S.Kom, M.Eng  
NIK. 190302375

Tanda Tangan

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 4 Agustus 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 : Wahyu Arif Purnomo  
NIM : 16.11.0746

Menyatakan bahwa Skripsi dengan judul berikut:

### PERANCANGAN SISTEM MONITORING KEAMANAN *CYBER* BERBASIS WEBSITE

Dosen Pembimbing : Lukman M.Kom

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 pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan 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 pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 04 Agustus 2023

Yang Menyatakan,



Wahyu Arif Purnomo

## KATA PENGANTAR

Penulis mengucapkan terima kasih kepada Allah SWT, Yang Maha Esa, atas semua rahmat dan bimbinganNya sehingga penulis dapat menyelesaikan skripsi berjudul "PERANCANGAN SISTEM MONITORING KEAMANAN *CYBER* BERBASIS WEBSITE" ini tepat waktu. Skripsi ini memenuhi syarat untuk mendapatkan gelar Sarjana Informatika dari Universitas Amikom Yogyakarta.

Penulis menyampaikan penghargaan dan terima kasih kepada banyak orang yang membantu mereka menyelesaikan studi dan menulis skripsi ini, baik secara langsung maupun tidak langsung.

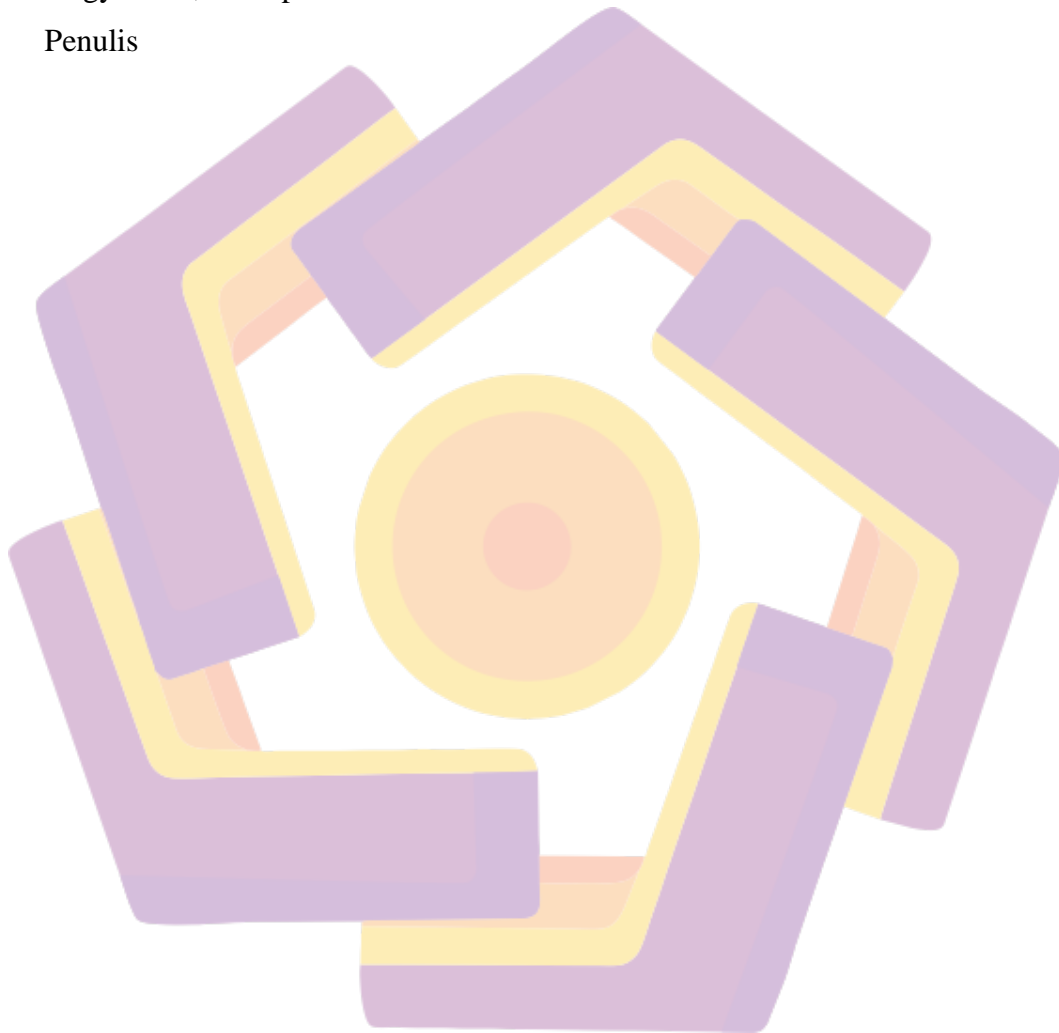
1. Prof. Dr. M. Suyanto, M.M., selaku Rektor Universitas Amikom Yogyakarta.
2. Hanif Al Fatta, S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Robert Marco, M.T., selaku Dosen Wali yang telah memberikan bimbingan dan bantuan selama penulis menempuh studi di Universitas Amikom Yogyakarta.
4. Lukman M.Kom., selaku Dosen Pembimbing yang telah meluangkan waktu ditengah kesibukan beliau, memberikan kritik, saran dan pengarahan kepada Penulis dalam proses penulisan skripsi ini.
5. Uyock Anggoro Saputro, M.Kom., dan Theopilus Bayu Sasongko, S. Kom., M. Eng., selaku Dosen Penguji skripsi yang telah meluangkan waktunya untuk memberikan arahan dalam penulisan skripsi ini serta untuk menguji skripsi ini serta menguji skripsi penulis
6. Dan, semua pihak yang telah membantu dan tidak dapat disebutkan satu persatu.

Semoga segala kebaikan dan bantuan datang dari Allah SWT. Akhirnya, saya menyadari bahwa karena keterbatasan pengetahuan saya, skripsi ini masih jauh

dari kata sempurna. Untuk alasan ini, saya dengan rendah hati mengharapkan kritik dan saran yang konstruktif dari semua pihak yang terlibat dalam proses pembuatan laporan penelitian ini.

Yogyakarta, 25 September 2023

Penulis

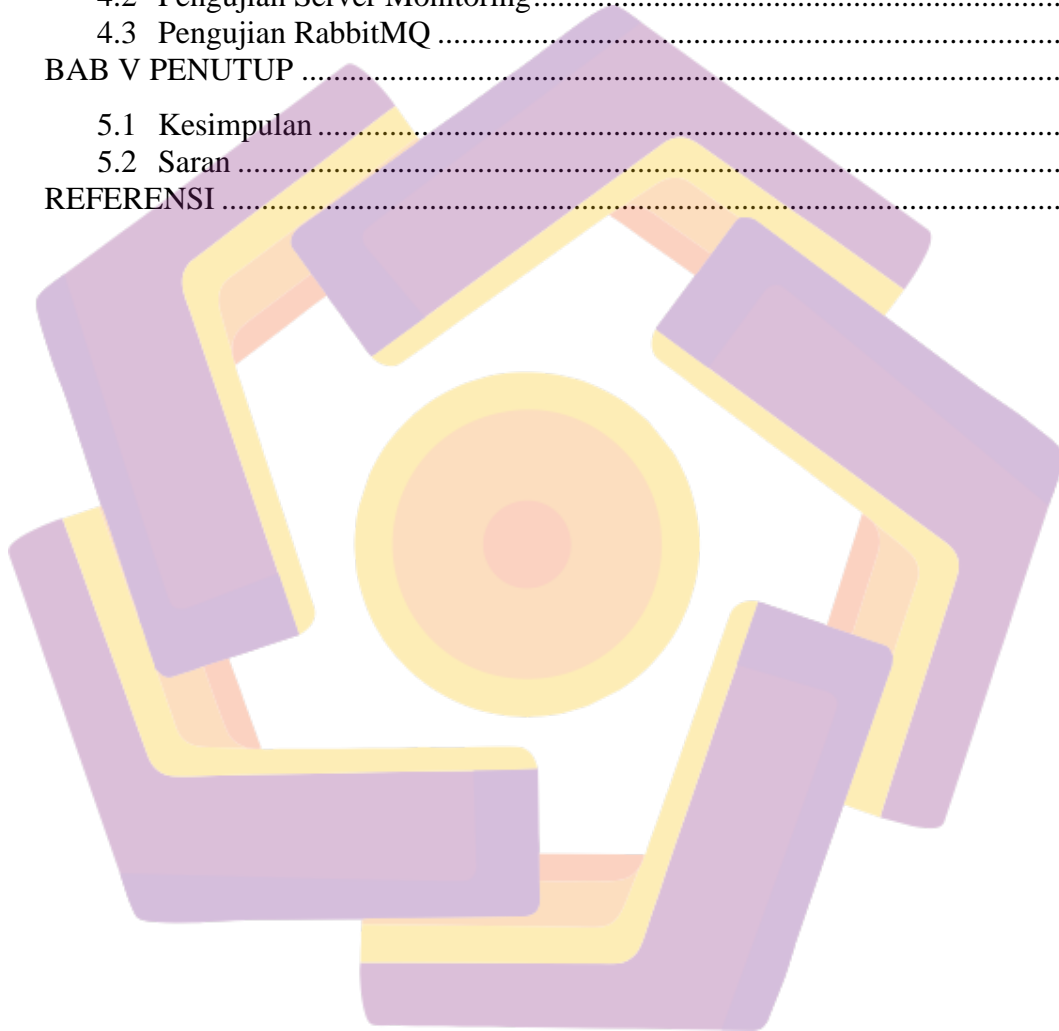


## DAFTAR ISI

|  |           |
|--|-----------|
| HALAMAN JUDUL .....                        | i         |
| HALAMAN PERSETUJUAN.....                   | ii        |
| HALAMAN PENGESAHAN .....                   | iii       |
| HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....  | iv        |
| KATA PENGANTAR .....                       | v         |
| DAFTAR ISI.....                            | vii       |
| DAFTAR TABEL.....                          | ix        |
| DAFTAR GAMBAR .....                        | x         |
| DAFTAR LAMBANG DAN SINGKATAN .....         | xii       |
| INTISARI .....                             | xiii      |
| ABSTRACT.....                              | xiv       |
| <b>BAB I PENDAHULUAN.....</b>              | <b>1</b>  |
| 1.1 Latar Belakang .....                   | 1         |
| 1.2 Rumusan Masalah.....                   | 2         |
| 1.3 Batasan Masalah .....                  | 2         |
| 1.4 Tujuan Penelitian .....                | 3         |
| 1.5 Manfaat Penelitian .....               | 3         |
| 1.6 Sistematika Penulisan .....            | 4         |
| <b>BAB II TINJAUAN PUSTAKA .....</b>       | <b>5</b>  |
| 2.1 Keamanan Cyber.....                    | 5         |
| 2.2 Konsep Keamanan CIA Triad.....         | 5         |
| 2.3 Sistem Monitoring Keamanan Cyber ..... | 6         |
| 2.4 Peran Teknologi Machine Learning ..... | 6         |
| 2.5 Definisi Mongo Database .....          | 7         |
| 2.6 Definisi PostgreSQL.....               | 7         |
| 2.7 Definisi Laravel .....                 | 7         |
| 2.8 Definisi Docker.....                   | 7         |
| 2.9 Definisi Nmap.....                     | 8         |
| 2.10 Definisi Nginx.....                   | 9         |
| 2.11 Definisi RabbitMQ .....               | 9         |
| 2.12 Definisi SMTP .....                   | 11        |
| 2.13 Definisi Port.....                    | 12        |
| 2.14 Definisi Fast API .....               | 13        |
| 2.15 Lingkungan Pengembangan.....          | 13        |
| <b>BAB III METODE PENELITIAN .....</b>     | <b>14</b> |
| 3.1 Objek Penelitian.....                  | 14        |

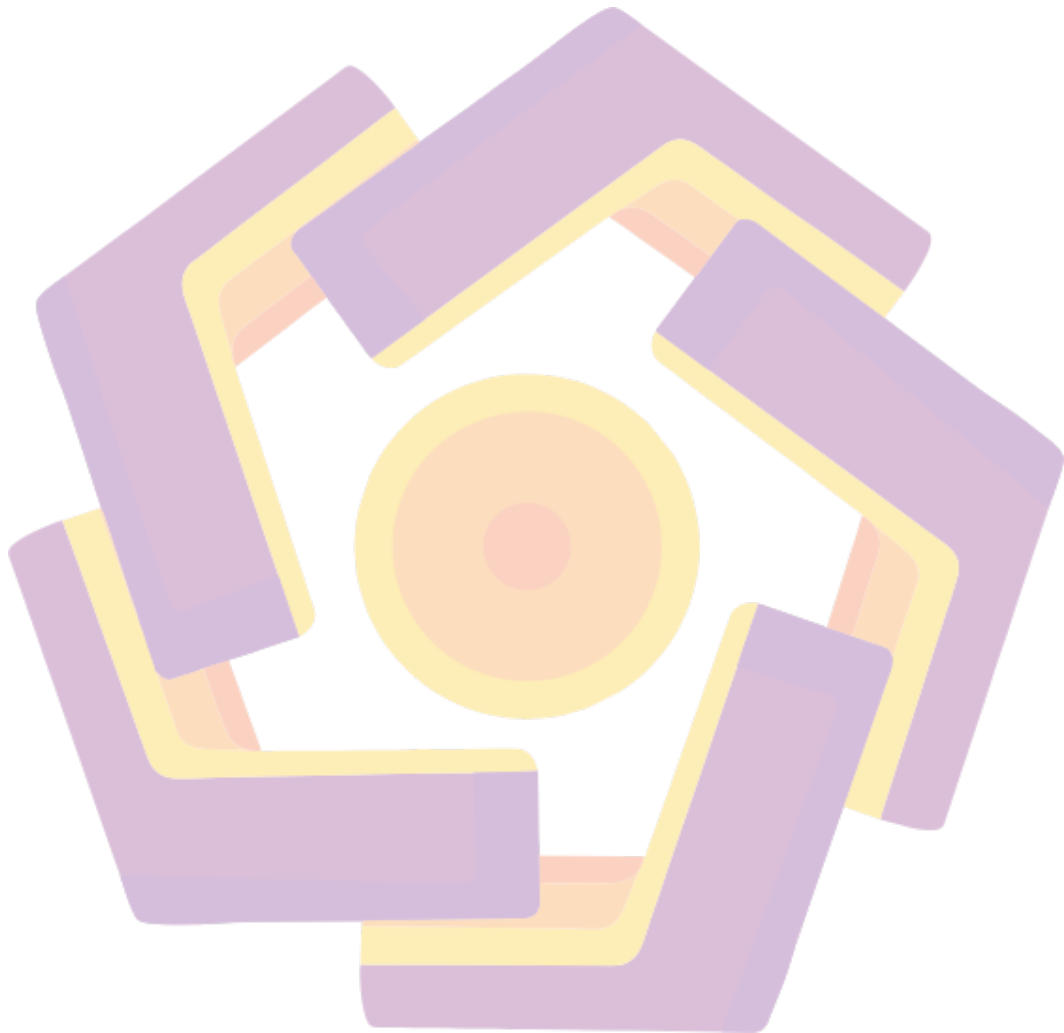


|  |           |
|--|-----------|
| 3.2 Alur Penelitian .....                | 17        |
| 3.3 Perancangan Uji Pemindai.....        | 19        |
| 3.5 Perancangan Notifikasi Laporan.....  | 21        |
| 3.6 Perancangan Antrian.....             | 22        |
| 3.7 Perancangan Laporan.....             | 23        |
| <b>BAB IV HASIL DAN PEMBAHASAN .....</b> | <b>25</b> |
| 4.1 Hasil.....                           | 25        |
| 4.2 Pengujian Server Monitoring.....     | 61        |
| 4.3 Pengujian RabbitMQ .....             | 62        |
| <b>BAB V PENUTUP .....</b>               | <b>66</b> |
| 5.1 Kesimpulan .....                     | 66        |
| 5.2 Saran .....                          | 67        |
| <b>REFERENSI .....</b>                   | <b>68</b> |



## DAFTAR TABEL

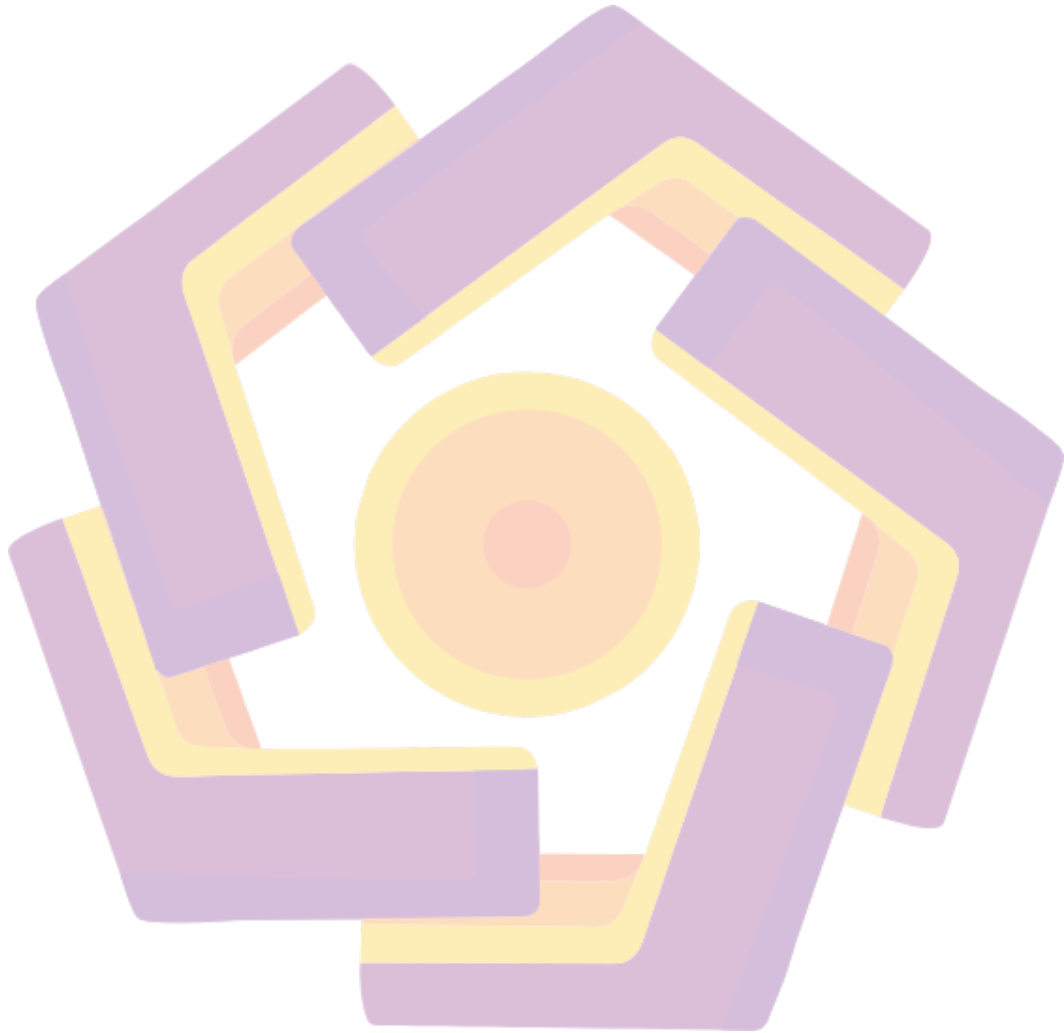
|                                |    |
|--------------------------------|----|
| Tabel 5. 1 Infrastruktur ..... | 66 |
|--------------------------------|----|



## DAFTAR GAMBAR

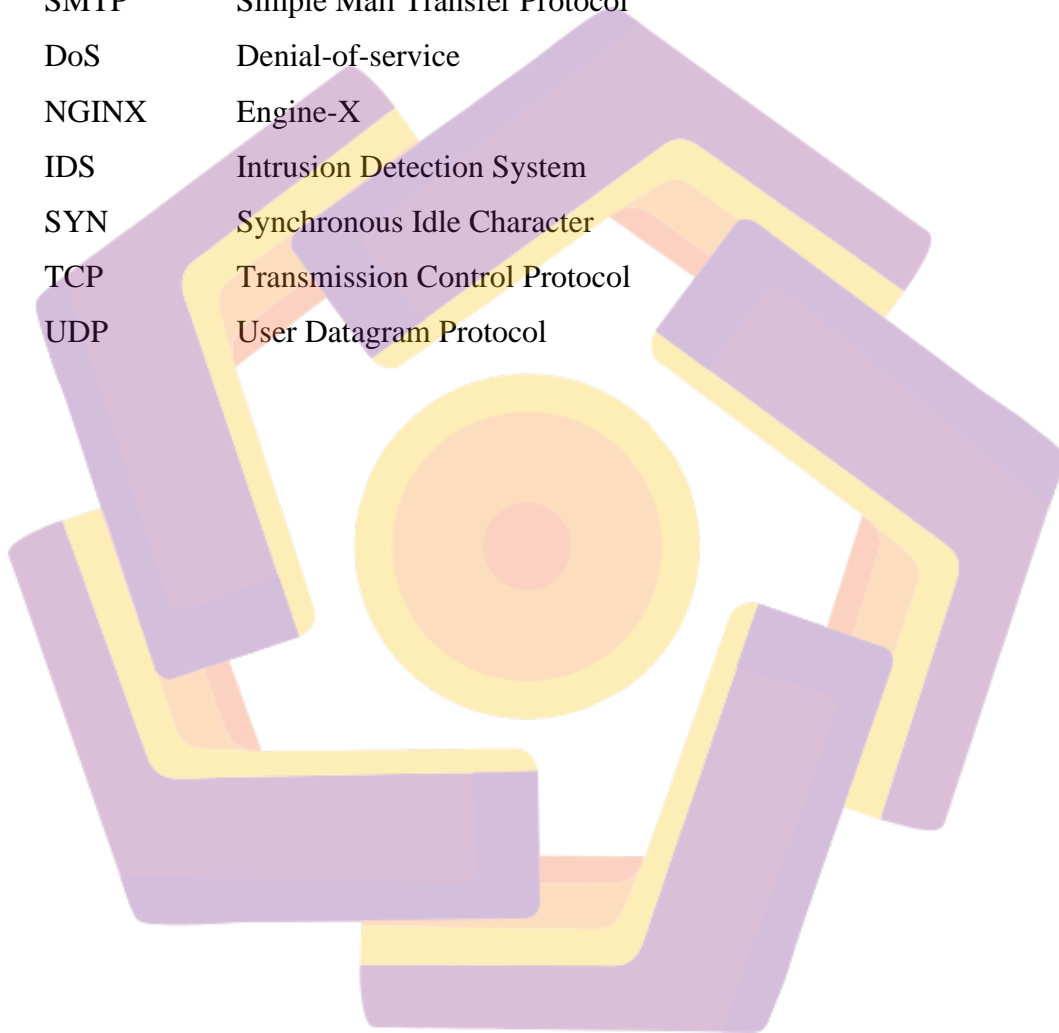
|   |    |
|---|----|
| Gambar 3. 1 Skenario Objek.....                             | 14 |
| Gambar 3. 2 Flowchart Penelitian.....                       | 18 |
| Gambar 3. 3 Flowchart Port Scan .....                       | 19 |
| Gambar 3. 4 Flowchart MongoDB Brute Force Login.....        | 20 |
| Gambar 3. 5 Flowchart Notifikasi Laporan .....              | 21 |
| Gambar 3. 6 Flowchart Kontrol Antrian.....                  | 22 |
| Gambar 3. 7 Flowchart Laporan .....                         | 23 |
| <br>  |    |
| Gambar 4. 1 Halaman Login.....                              | 25 |
| Gambar 4. 2 Halaman Dashboard .....                         | 25 |
| Gambar 4. 3 Menu Virtual Machine .....                      | 33 |
| Gambar 4. 4 Lihat Virtual Machine .....                     | 35 |
| Gambar 4. 5 Halaman Port Scan.....                          | 37 |
| Gambar 4. 6 Tabel Port Scan .....                           | 38 |
| Gambar 4. 7 Menu MongoDB Brute Force Login.....             | 39 |
| Gambar 4. 8 Tabel MongoDB Brute Force Login.....            | 40 |
| Gambar 4. 9 Menu Equipment Port Scan .....                  | 42 |
| Gambar 4. 10 Hasil Pemindaian Equipment Port Scan .....     | 43 |
| Gambar 4. 11 Menu Equipment HTTP Status .....               | 43 |
| Gambar 4. 12 Hasil Equipment HTTP Status .....              | 44 |
| Gambar 4. 13 Equipment IP Geo Location Lookup .....         | 45 |
| Gambar 4. 14 Hasil Equipment IP GEO Location Lookup .....   | 46 |
| Gambar 4. 15 Equipment Reverse IP Address.....              | 47 |
| Gambar 4. 16 Hasil Equipment Reverse IP Address .....       | 48 |
| Gambar 4. 17 Halaman Laporan Analisa.....                   | 49 |
| Gambar 4. 18 Tabel Halaman Laporan Analisa.....             | 49 |
| Gambar 4. 19 Dialog Konfirmasi Pengiriman Laporan.....      | 51 |
| Gambar 4. 20 Dialog Berhasil Pengiriman Laporan.....        | 51 |
| Gambar 4. 21 Pesan Laporan Google Mail.....                 | 52 |
| Gambar 4. 22 Detail Pesan Laporan Google Mail .....         | 52 |
| Gambar 4. 23 Halaman Login Laporan .....                    | 53 |
| Gambar 4. 24 Halaman Login Laporan Email Tidak Sesuai ..... | 53 |
| Gambar 4. 25 Halaman Detail Laporan .....                   | 54 |
| Gambar 4. 26 Halaman Dashboard Log.....                     | 55 |
| Gambar 4. 27 Tabel Halaman Dashboard Log .....              | 56 |
| Gambar 4. 28 Halaman User Log .....                         | 57 |
| Gambar 4. 29 Tabel Halaman User Log .....                   | 58 |
| Gambar 4. 30 Halaman Akun .....                             | 59 |
| Gambar 4. 31 Halaman Pengaturan .....                       | 59 |
| Gambar 4. 32 Informasi Server Development .....             | 61 |
| Gambar 4. 33 Informasi Server Staging .....                 | 61 |
| Gambar 4. 34 RabbitMQ Streams.....                          | 62 |

Gambar 4. 35 Node Instance RabbitMQ.....62  
Gambar 4. 36 Antrian MongoDB Brute Force Login.....64  
Gambar 4. 37 Antrian Port Scan .....65



## DAFTAR LAMBANG DAN SINGKATAN

|       |                               |
|-------|-------------------------------|
| CPU   | Central Processing Unit       |
| VPS   | Virtual Private Server        |
| VM    | Virtual Machine               |
| SMTP  | Simple Mail Transfer Protocol |
| DoS   | Denial-of-service             |
| NGINX | Engine-X                      |
| IDS   | Intrusion Detection System    |
| SYN   | Synchronous Idle Character    |
| TCP   | Transmission Control Protocol |
| UDP   | User Datagram Protocol        |



## INTISARI

Meskipun kemajuan teknologi informasi dan internet telah membawa banyak manfaat bagi manusia, mereka juga membawa tantangan baru dalam hal keamanan siber. Ancaman keamanan siber seperti serangan peretasan, malware, dan pencurian data telah menjadi masalah besar dan mengancam banyak orang, mulai dari individu hingga perusahaan besar. Oleh karena itu, sangat penting untuk merancang sistem pemantauan keamanan siber yang efisien untuk melindungi sistem informasi dari serangan siber.

Tujuan penelitian ini adalah untuk membuat sistem pemantauan keamanan siber berbasis web yang dapat dipantau dan melindungi infrastruktur teknologi informasi dari berbagai serangan. Gerakan yang mencurigakan, perilaku abnormal, dan perilaku tidak sah akan dideteksi oleh sistem ini. Pendekatan berbasis web memungkinkan pengguna mengakses data keamanan secara real-time dan mengambil tindakan cepat jika terjadi ancaman.

Hasil penelitian ini diharapkan dapat membantu meningkatkan keamanan siber, khususnya bagi organisasi yang menggunakan teknologi informasi dalam aktivitas sehari-hari. Dengan adanya sistem pemantauan keamanan siber berbasis web, pengguna diharapkan lebih aman dan terlindungi dari ancaman siber.

**Kata kunci:** Sistem Monitoring, Keamanan Cyber, Website, Analisis Log, Machine Learning.

## ABSTRACT

*Although advances in information technology and the internet have brought many benefits to humans, they have also brought new challenges in terms of cybersecurity. Cyber security threats such as hacking attacks, malware and data theft have become a big problem and threaten many people, from individuals to large companies. Therefore, it is very important to design an efficient cyber security monitoring system to protect information systems from cyber attacks.*

*The purpose of this research is to create a web-based cybersecurity monitoring system that can monitor and protect information technology infrastructure from various attacks. Suspicious movements, abnormal behavior and unauthorized behavior will be detected by this system. The web-based approach allows users to access data security in real-time and take quick action in case of a threat.*

*The results of this research are expected to help improve cyber security, especially for organizations that use information technology in their daily activities. With a web-based cyber security monitoring system, users are expected to be safer and protected from cyber threats.*

**Keyword:** *Monitoring Systems, Cyber Security, Websites, Log Analysis, Machine Learning.*