Riva Imanudin

https://www.linkedin.com/in/rivaimanudin/

About Me

I have been working for 4 years in the IT field, covering areas such as Networking, AutoID/Mobile Computers, Barcode Printers & Scanners, and Cyber Security. I enjoy exploring new technologies and finding ways toapply themto solve problems

Contact

📞 *+62 878 0117 7413*

✉ *rifaimanudin@gmail.com*

📍 *Pasar Minggu, Jakarta Selatan 12510*

🐙 *https://github.com/rivaile96*

🌐 *https://riva-imanudin-portfolio.vercel.app/*

▶ *www.youtube.com/@textpl0it*

Skills

- Penetration Testing System
- Administration
- AIDC
- Network Topology
- Basic Web Programming
- Linux Fundamental
- Hardware/Software Installation
- Troubleshooting windows/Linux
- Python
- Laravel

Language

- Indonesian
- Englis

Education

(2023 - Present)

UNIVERSITAS TERBUKA

System Informasi Management

3.06

Experience

(2025 - Present)

Service & Warranty Coordinator

PT.Wahana Datarindo Sempurna

- Coordinated repair processes for customer Auto-ID units, from damage report to return delivery.
- Handled warranty validation, RMA processing (especially for Honeywell), and ticketing system input.
- Communicated with vendors (Zebra, Urovo, Idata, etc.) regarding repair quotes, PO approvals, and progress.
- Prepared delivery notes, work reports, and billing documents for customer and finance teams.
- Liaised across technical teams, sales, customers, and finance to ensure smooth after-sales workflow.

(2024 - 2025)

IT Support

PT.Wahana Datarindo Sempurna

- Diagnosed and resolved hardware issues across barcode scanners, printers, POS, RFID, and PDA devices.
- Installed and configured IT devices for client business operations.
- Provided product demos and technical explanations to clients and internal staff.

(2016 - 2018)

IT Helpdesk

Dinas Koperasi

- Configured network devices and ensured device connectivity.
- Assisted users with technical hardware, software, and network issues.
- Performed installation and configuration of company-required software, including antivirus programs, Microsoft Office suite, and internal business applications.

Personal Project

G-Track - Laravel - Full Stack Developer
GitHub: https://github.com/rivaile96/G-track

G-Track is a futuristic web-based application for real-time asset tracking and management, built with Laravel 12. It enables organizations to monitor moving assets such as vehicles and devices through an interactive map, geofencing system, and advanced reporting tools. In this project, I designed and implemented the system architecture, database schema, and UI/UX dashboard, integrating Leaflet.js for live map visualization and Laravel Reverb (WebSockets) for instant notifications.

The features :
- Asset and driver management modules (CRUD),
- PDF export features,
- Advanced trip reporting system
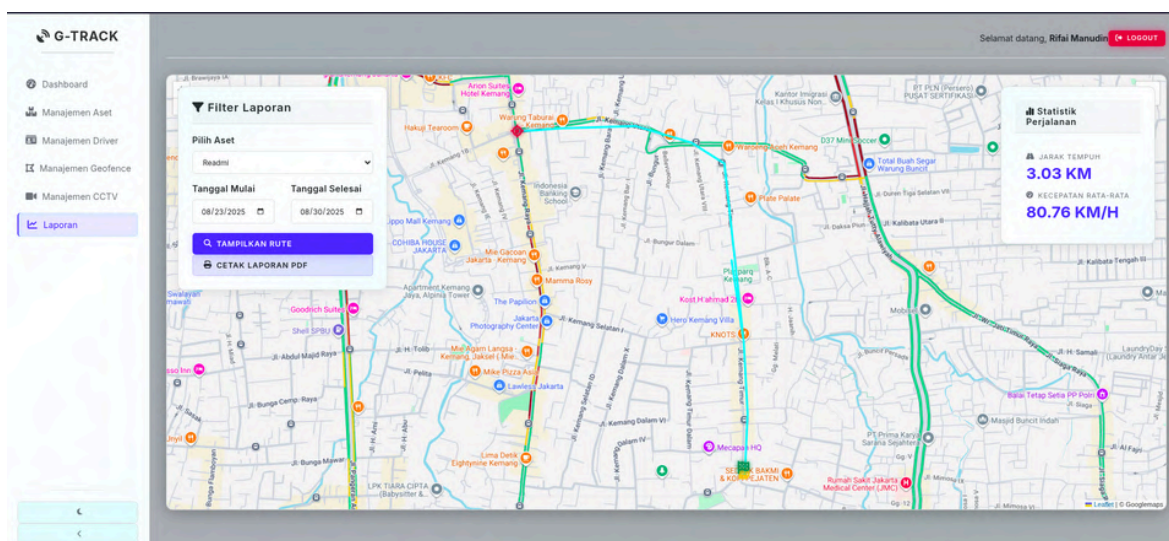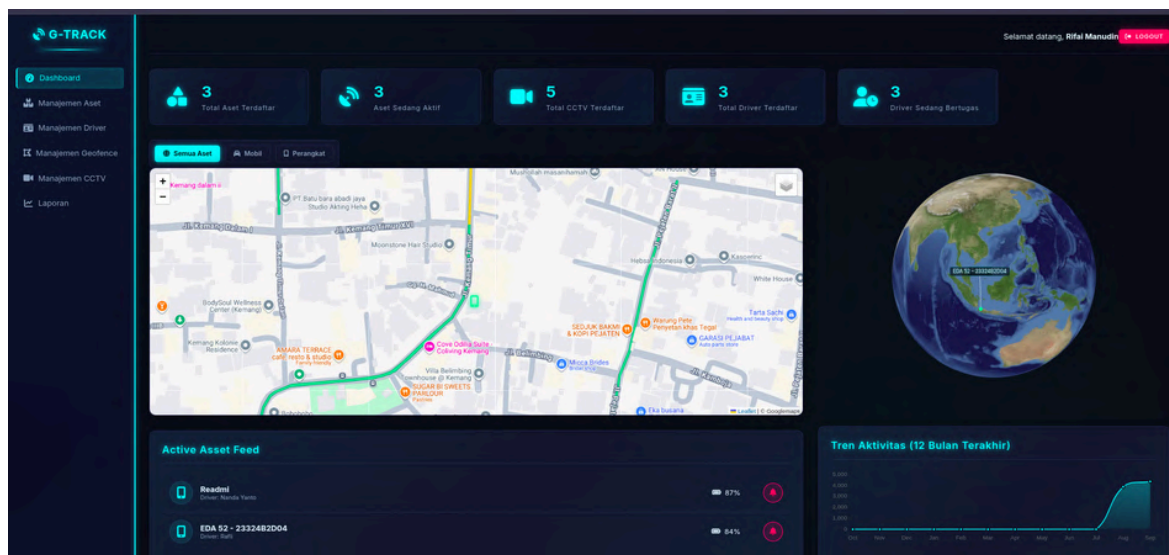
Personal Project

**Service Management System - Laravel - Full Stack Developer**
GitHub: https://github.com/rivaile96/data-service-ticketing

Service Management System is a comprehensive web-based application built with Laravel 10, designed to simplify and optimize end-to-end service workflow management. The system covers key processes such as service ticket registration, progress tracking, customer data management, reporting, and document generation.

In this project, I designed and implemented the system architecture, database schema, and interactive dashboard from the ground up. The dashboard provides dynamic data visualizations (Line, Doughnut, Bar charts) and key performance statistics to support better monitoring and decision-making.

The features:
- Advanced service management with full CRUD operations.
- Integrated customer management linked directly with service data.
- Advanced search & filtering by serial number, item name, customer, or date range.
- Report & export tools with Excel import/export support.
- Custom printable documents, such as service delivery notes.
- Dual theme (light/dark mode) for modern UI flexibility.
- Role-based authentication & authorization for admin/user access control.
- Custom popup & modal components for intuitive interaction.
- Customer distribution mapping powered by Leaflet.js for geographic visualization.
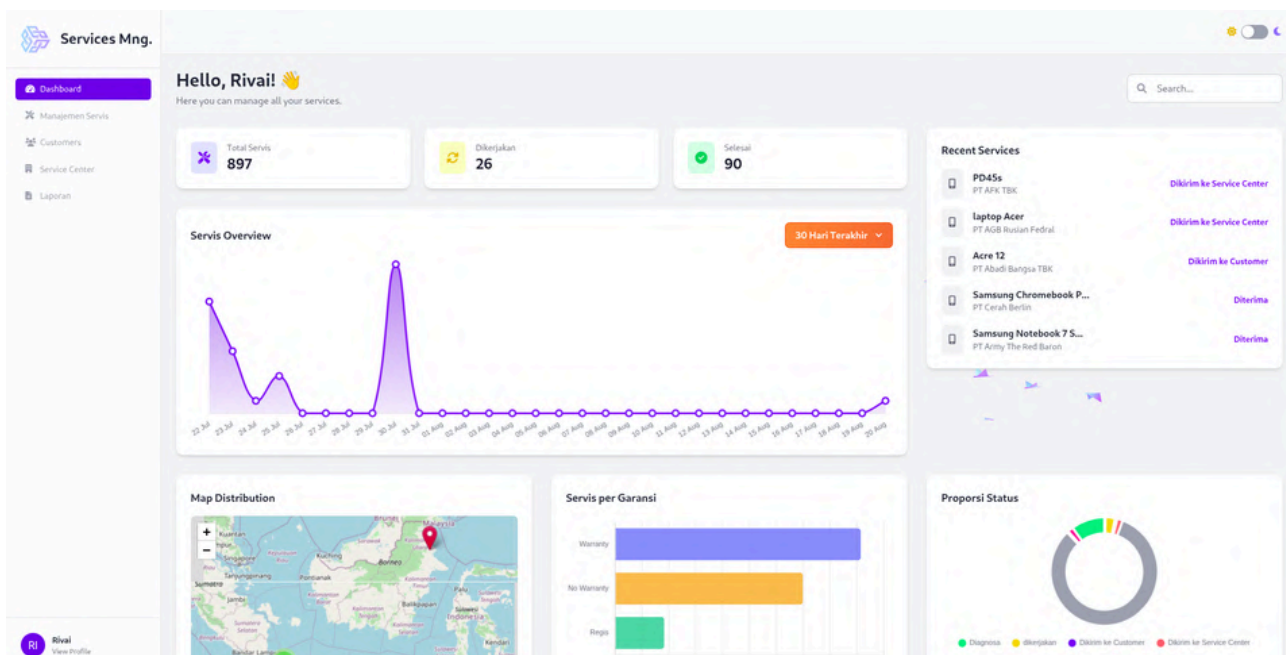
Personal Project

NgOCR-in — Creator & Lead Developer
GitHub: github.com/rivaile96/NgOCR-in

NgOCR-in is a command-line OCR toolkit designed for Linux and WSL environments, with support for batch image processing, auto language detection, and optional multi-language translation.

In this project, I designed the full system architecture, including its flowchart, user interaction logic, and modular codebase. I developed the OCR core using Python, Tesseract, and OpenCV, and implemented a colorized ASCII-based UI for better terminal interaction. I built custom preprocessing filters to improve text recognition accuracy, created the logic for optional translation flows, and designed export functions for .txt and .docx formats.

Additionally, I optimized the script for performance and cross-platform compatibility, planned future integration with GUI and AI-based auto-answer features, and documented the entire development process for open-source collaboration.

PHISPYRATE_FaceVerification — Creator & Lead Developer
GitHub: github.com/rivaile96/PHISPYRATE_FaceVerification

PHISPYRATE_FaceVerification is a web-based facial authentication simulation tool designed for OSINT, penetration testing, and cybersecurity training. It replicates the Android face unlock interface to collect and auto-upload recorded facial videos for ethical phishing simulations and user behavior studies.

In this project, I led the full-stack development process, designing the system architecture, interaction flow, and frontend that mimics a realistic Android authentication UI. I built the backend using Flask and implemented continuous video recording using the MediaRecorder API with automated 10-second intervals and silent background uploads to a server.

I also integrated tunneling support via Ngrok and LocalXpose for real-time external access and designed the project to be lightweight, Linux-friendly (especially for Kali/WSL), and easily deployable for educational and testing purposes. The project emphasizes ethical use in cybersecurity and OSINT labs, and includes documentation to support collaborative development.

My Certificate & Transcript

FORTINET Training Institute

This acknowledges that

Riva Imanudin

successfully completed the course

The Evolution of Cybersecurity

Rob Rashotte
Vice President, Global Training &
Technical Field Enablement at Fortinet

Date: June 10, 2023

FORTINET — NSE Certification Program

This certifies that

Riva Imanudin
has achieved
NSE 1 Network Security Associate

Date of achievement: June 10, 2023
Valid until: June 10, 2025
Certification Validation number: wquk5schYs

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology
Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

FORTINET — NSE Certification Program

This certifies that

Riva Imanudin
has achieved
NSE 2 Network Security Associate

Date of achievement: June 10, 2023
Valid until: June 10, 2025
Certification Validation number: yD0CrD0SBY

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology
Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

FORTINET — NSE Certification Program

This certifies that

Riva Imanudin
has achieved
NSE 3 Network Security Associate

Date of achievement: June 17, 2023
Valid until: June 17, 2025
Certification Validation number: 64U8p2jnzq

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology
Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

SEKOLAHMU

Certificate no. #1020074

dengan bangga mempersembahkan
proudly presents

SERTIFIKAT KEPESERTAAN
the certificate of completion

kepada
to

rifa imanudin

atas keberhasilan menyelesaikan program
for the successful completion of the program

Web Desain

Lembaga Pendidikan Dian Nusantara

Jakarta, 05-05-2020

Najelaa Shihab
Head of Sekolah.mu

Honeywell | THE FUTURE IS WHAT WE MAKE IT

TECHNICAL ACCREDITATION TRAINING CERTIFICATE

Presented to

RIVA IMANUDIN
(PT. Wahana Data Teknologi)
Partner ID: 1929755

Has successfully completed the
Honeywell Performance Partner Technical Accreditation Program
for Mobility, Scanning and Printing

Shawn Yeo
Senior Solution Architect - Indonesia
Honeywell Productivity Solutions and Services

Valid Until December 31, 2026

Claudio Bratovic
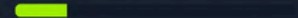Senior Director – APACI
Honeywell Productivity Solutions and Services

File Inclusion

11 Sections Medium Offensive

File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.

18.18% Completed

Introduction to Networking

21 Sections Fundamental General

As an information security professional, a firm grasp of networking fundamentals and the required components is necessary. Without a strong foundation in networking, it will be tough to progress in any area of information security. Understanding how a network is structured and how the communication between the individual hosts and servers takes place using the various protocols allows us to understand the entire network structure and its network traffic in detail and how different communication standards are handled. This knowledge is essential to create our tools and to interact with the protocols.

100% Completed
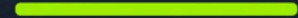
Using the Metasploit Framework

15 Sections Easy Offensive

The Metasploit Framework is an open-source set of tools used for network enumeration, attacks, testing security vulnerabilities, evading detection, performing privilege escalation attacks, and performing post-exploitation.

100% Completed

Windows Fundamentals

14 Sections Fundamental General

This module covers the fundamentals required to work comfortably with the Windows operating system.

100% Completed

Attacking Web Applications with Ffuf

13 Sections Easy Offensive

This module covers the fundamental enumeration skills of web fuzzing and directory brute forcing using the Ffuf tool. The techniques learned in this module will help us in locating hidden pages, directories, and parameters when targeting web applications.

100% Completed

Introduction to Active Directory

16 Sections Fundamental General

Active Directory (AD) is present in the majority of corporate environments. Due to its many features and complexity, it presents a vast attack surface. To be successful as penetration testers and information security professionals, we must have a firm understanding of Active Directory fundamentals, AD structures, functionality, common AD flaws, misconfigurations, and defensive measures.

100% Completed

Introduction to Web Applications

17 Sections Fundamental General

In the Introduction to Web Applications module, you will learn all of the basics of how web applications work and begin to look at them from an information security perspective.
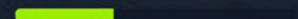
100% Completed

Getting Started

23 Sections Fundamental Offensive

This module covers the fundamentals of penetration testing and an introduction to Hack The Box.

34.78% Completed

Paths completed: 1
Targets compromised: 48
Ranking: Top 5%

PATHS COMPLETED | PROGRESS

Operating System Fundamentals
3 Modules Easy

To succeed in information security, we must have a deep understanding of the Windows and Linux operating systems and be comfortable navigating the command line on both as a "power user." Much of our time in any role, but especially penetration testing, is spent in a Linux shell, Windows cmd or PowerShell console, so we must have the skills to navigate both types of operating systems with ease, manage system services, install applications, manage permissions, and harden the systems we work from in accordance with security best practices.

100% Completed

MODULE | PROGRESS

Intro to Academy
8 Sections Fundamental General

Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.

100% Completed

Learning Process
20 Sections Fundamental General

The learning process is one of the essential and most important components that is often overlooked. This module does not teach you techniques to learn but describes the process of learning adapted to the field of information security. You will learn to understand how and when we learn best and increase and improve your learning efficiency greatly.

100% Completed

Linux Fundamentals
30 Sections Fundamental General

This module covers the fundamentals required to work comfortably with the Linux operating system and shell.

100% Completed

Introduction to Bash Scripting
10 Sections Easy General

This module covers the basics needed for working with Bash scripts to automate tasks on Linux systems. A strong grasp of Bash is a fundamental skill for anyone working in a technical information security role. Through the power of automation, we can unlock the Linux operating system's full potential and efficiently perform habitual tasks.

100% Completed

Web Requests
8 Sections Fundamental General

This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.

100% Completed

Intro to Network Traffic Analysis

15 Sections Medium General

Network traffic analysis is used by security teams to monitor network activity and look for anomalies that could indicate security and operational issues. Offensive security practitioners can use network traffic analysis to search for sensitive data such as credentials, hidden applications, reachable network segments, or other potentially sensitive information "on the wire." Network traffic analysis has many uses for attackers and defenders alike.

100% Completed
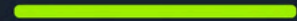
Setting Up

9 Sections Fundamental General

This module covers topics that will help us be better prepared before conducting penetration tests. Preparations before a penetration test can often take a lot of time and effort, and this module shows how to prepare efficiently.

100% Completed

Stack-Based Buffer Overflows on Windows x86

11 Sections Medium Offensive

This module is your first step into Windows Binary Exploitation, and it will teach you how to exploit local and remote buffer overflow vulnerabilities on Windows machines.

9.09% Completed