Rahmat Wahyu Hadi

Kebon Kacang 41, Jakarta Pusat | hrahmatwahyu@gmail.com | 085205039835

Fast Response Telegram @rwahyu | linkedin.com/in/rahmat-wahyu-hadi-80a868103/ | github.com/wahyuhadi

About Me

I'm a software developer and application security specializing in advanced software development, with a strong proficiency in Linux-based environments. My programming experience spans over **7 years**, primarily in **Python**, **GoLang**, and **R**, with R being my go-to for statistical analysis. My driver development experience has mainly focused on Linux OS, and I'm actively expanding my skill set to keep pace with industry advancements. In addition to software development, I have a solid background in **cybersecurity**, particularly in **Security Engineering, Pentesting, Red Teaming, and DevSecOps**. With a proven track record in application and infrastructure security, my research focuses on security fuzzing techniques, including designing fuzzer payload patterns and occasionally building tools to integrate various security application.

Education

Telkom University, BS in Computer Engineering **Sept 2012 – May 2017**

- **GPA**: 3.1/4.0
- **Research Project:** *Software Architecture, Computer Architecture, Comparison of Learning Algorithms, Software Reverse Engineering, Cyber Security, OSINT, SIGINT*

Experience

Lead Cyber Security Engineer, Astro Quick Commerce - Work From Home **Aug 2022 – Now**

- Conduct thorough, daily penetration testing across company systems and applications to proactively identify vulnerabilities, mitigate potential threats, and strengthen security defenses.
- Continuously monitor system and network logs to identify, analyze, and respond to security incidents in real-time, ensuring rapid action on potential threats.
- Manage and mentor the cybersecurity team by providing guidance, setting goals, assigning tasks, and supporting professional growth, fostering a highly skilled and cohesive unit.
- Collaborate with various departments to help the company achieve and maintain ISO 27001 compliance, leading initiatives to develop, implement, and update robust security policies, procedures, and controls.
- Oversee and conduct comprehensive security awareness training programs for employees at all levels, ensuring they are knowledgeable about the latest security best practices, social engineering tactics, and phishing threats.
- Develop and enforce comprehensive security strategies and frameworks, aimed at protecting sensitive company data, assets, and infrastructure against internal and external threats.
- Coordinate closely with other departments, such as IT, Legal, and Compliance, to ensure all cybersecurity measures align with broader company goals and regulatory requirements.
- Conduct regular risk assessments and security audits to identify, evaluate, and address security risks, thereby maintaining a proactive security posture and ensuring ongoing compliance with regulatory standards.
- Lead and coordinate incident response efforts, providing swift, organized responses to security incidents, minimizing impact and restoring normal operations as efficiently as possible.
- Stay up-to-date with the latest trends, vulnerabilities, tools, and techniques in cybersecurity to ensure the adoption of proactive, cutting-edge security measures that address emerging threats effectively.
- Develop and maintain detailed documentation of all security policies, incident response plans, and cybersecurity procedures to ensure clear, accessible guidelines and continuity in security operations.

Senior Cyber Security Engineer, Finantier - **SG - Layoff 'Covid19 Black Swan'** **Mei 2022 – July 2022**

In 2022, my position was impacted by the economic downturn caused by the COVID-19 pandemic, a 'Black Swan' event that led to widespread disruption across the tech industry, with many startups facing severe challenges. While I had the opportunity to contribute to some key projects, resource constraints limited the scope of my responsibilities. Despite these challenges, I utilized this period to deepen my expertise in critical areas of cybersecurity and to stay agile in a shifting industry landscape.

- Conduct thorough, daily penetration testing across company systems and applications to proactively identify vulnerabilities, mitigate potential threats, and strengthen security defenses.
- Develop and enforce comprehensive security strategies and frameworks, aimed at protecting sensitive company data, assets, and infrastructure against internal and external threats.

Officer Offensive Security Engineer, Telkomsel - **Jakarta, ID** **Jan 2021 – March 2022**

- Lead DevSecOps implementation by integrating security practices within the development pipeline to ensure robust security throughout the software lifecycle.
- Conduct thorough penetration testing on applications and systems prior to release, identifying potential vulnerabilities to be addressed before deployment.
- Perform detailed code reviews, both manual and automated, using rule-based checks to ensure secure coding standards are met and vulnerabilities are minimized.
- Carry out Cyber Patrol and OSINT activities to proactively monitor the cyber landscape, identify potential threats, and gather intelligence to enhance security awareness.
- Manage third-party vendors and security tools, ensuring they comply with internal security standards and contribute effectively to the organization's cybersecurity posture.
- Investigate and respond to malicious activities within the internal infrastructure, analyzing incidents and implementing remediation steps to prevent future occurrences.
- Develop and maintain security playbooks and incident response plans to standardize procedures and enhance the organization's readiness for potential security events.

Senior Offensive Security Engineer, Tiket.com - **Jakarta, ID** **Sept 2019 – Dec 2021**

- Perform comprehensive security code reviews to identify potential vulnerabilities and ensure adherence to secure coding practices.
- Oversee the development and change management lifecycle for information systems, implementing security best practices at each stage to maintain a robust security posture.
- Monitor information systems continuously to detect, investigate, and respond to security incidents and vulnerabilities, maintaining a proactive stance against emerging threats.
- Maintain and operate security controls and countermeasures within information systems, ensuring they function effectively to protect sensitive data and infrastructure.
- Conduct regular penetration testing to evaluate system resilience, and provide actionable guidelines and best practices for mitigation based on findings.
- Coordinate with relevant development teams to track and address security bugs, facilitating timely fixes and enhancing overall system security.
- Develop and manage a User Access Matrix (UAM) for monitoring access rights and credentials, ensuring strict control over user permissions and data access.
- Participate in comprehensive security assessments and compliance activities, including PCI DSS, ISO 27001, and OWASP, to ensure organizational standards meet industry and regulatory requirements.
- Deliver security awareness training to new employees, particularly in compliance areas relevant to their roles, fostering a culture of security mindfulness across the team.
- Develop and implement GitHub monitoring (GitMon) to prevent accidental code and credential leaks in public repositories, safeguarding organizational data and intellectual property.

Software Engineer and Devops, Gits Indonesia- Bandung ID **Aug 2016 – Feb 2019**

- Develop a new Node.js framework tailored for developers, focusing on scalability, performance, and ease of use to enhance development efficiency.
- Gather and analyze specifications and requirements in close collaboration with clients to ensure the final product aligns with their business needs and objectives.
- Design and build applications based on client requirements, adhering to best practices in coding and ensuring functionality aligns with specifications.
- Perform comprehensive testing, including unit, integration, and user acceptance testing, to ensure the system meets quality standards and is ready for release.
- Implement CI/CD pipelines to automate deployment processes, streamline updates, and ensure consistent integration and delivery of new code.
- Conduct ongoing research into emerging software technologies and industry trends, evaluating their potential application to enhance current projects and innovate within the development team.
- Built an app to compute the similarity of all methods in a codebase, reducing the time from $\mathcal{O}(n^2)$ to $\mathcal{O}(n \log n)$
- Assist with DevOps deployment processes, ensuring seamless integration between development and operations teams for efficient, reliable, and scalable application releases.

Certifications

BSSN **1 June 2024**

Auditor Keamanan Informasi Badan Siber Dan Sandi Negara

ISO/IEC 27001:2022 **26 Feb 2024**

Lead Implementer Training Course

CEH **27 Aug 2021**

Certified Ethical Hacker

OSCP **5 Sept 2019**

Offensive Security Certification Professional

Projects

Nuclei Fuzzing Template

- Develop automatic for nuclei template to fuzzing by intercept requests
- Repo: github.com/wahyuhadi/nuc-fuzzing-template
- Tools Used: Go, Yaml

Nakula - Shellcode enc

- Shellcode encryption and hiding to bypass Windows Defender
- Repo: github.com/wahyuhadi/nakula
- Tools Used: python, go, msfvenom

Kurawa - Droper for Implant Execution

- Dropper shellcode for execution
- Repo: github.com/wahyuhadi/kurawa
- Tools Used: python, Go, msfvenom

Revershell Detection by Proccess

- Built a UNIX-style process to catch rever shell from interact sh, bash, zsh or shell default
- Repo: github.com/wahyuhadi/linux-soc
- Tools Used: Go

Offensive Security Project

Surabaya Industrial Estate Rungkut
- Helping SIER conduct penetration testing on nine internal applications, hardening internal on-premise systems, and providing secure code training for new internal engineering staff.

PT Digital Berkah Mandiri

- Assisting PT DBM in conducting penetration testing on the Itwasum Polri application to identify security vulnerabilities and strengthen the application's defenses against potential cyber threats.

PT Tiga Pilar Maju Mandiri

- Assisting PT Tiga Pilar in performing penetration testing on the Logistik Polri application and in creating secure code and infrastructure design

Pusdatin Kemenkes

- Assisting Kemenkes in conducting penetration testing on the Covid Antigen application, implementing secure development practices in the SILACAK application, and tuning and hardening DHIS2 to enhance security.

PT Sentra Vidya Utama

- Assisting Sevima in conducting penetration testing on the Sevima Pay application, Sevima Siakad application, and Sevima Edlink application.

kata.ai

- Assisting Kata.ai in conducting penetration testing on the cx.kata.ai application and two internal applications, as well as designing a Secure Software Development Life Cycle (SDLC) for enhanced security throughout the development process.

paper.id

- Assisting Paper.id in conducting penetration testing on the Paper.id application and providing secure code training for new internal engineering staff to enhance application security and coding practices.

PT Pelindo Marine Service

- Assisting Pelindo in conducting penetration testing on two internal applications and providing security awareness training for 25 employees to strengthen both application security and staff knowledge on cybersecurity practices.

PT Gits Indonesia

- Assisting GITS in conducting penetration testing on the Merchant Pertamina application, providing secure code training for backend engineers, and delivering mobile penetration testing training for mobile development engineers.

** **Certain projects are confidential and cannot be disclosed due to NDA agreements** **

Technologies

Languages: Go, Python, C++, Java, R

Technologies: BurpSuite, Zap, Ghidra, Frida