TRI WIBOWO CAHYO

L2 Support Engineer & Cyber Security Enthusiast | Red Team Specialist

"Self-driven red team specialist ranking Top 3 in Indonesia on TryHackMe with 750+ days of practical cybersecurity training. Proven track record through 25+ detailed exploitation writeups and enterprise-grade projects spanning AD penetration testing to advanced threat simulation. Backed by 2 years of technical problem-solving experience in high-pressure enterprise environments."

Malang, East Java, Indonesia ☎ 0823 2800 2098 twibowo288@gmail.com Tri Wibowo Cahyo

WORK EXPERIENCES

April 2025 - May 2025
India (Remote)

Red Team Intern - Hack Secure

- **Executed comprehensive penetration testing operations** using industry-standard tools (Nmap, Burpsuite, SQLMap) to identify critical vulnerabilities across web applications and network infrastructure
- **Performed advanced adversary simulation exercises** utilizing Metasploit, Empire, and Starkiller C2 frameworks to simulate real-world attack scenarios and test organizational security posture
- **Conducted web application security assessments** including SQL injection, XSS exploitation, and directory enumeration attacks, successfully identifying and documenting security weaknesses
- **Delivered actionable security reports** documenting vulnerabilities, attack vectors, and remediation strategies based on comprehensive red team assessments and CTF challenge completions

April 2023 - April 2025
Yogyakarta
(2 years)

L2 Support Engineer - PT Solusi247

- **Delivered critical L2 technical support for AI/ML platforms** by diagnosing complex backend infrastructure issues and implementing automated solutions using SQL, Bash, and Python scripting
- **Performed systematic root cause analysis and incident triage** to identify underlying system issues and implement preventive measures, developing analytical thinking essential for security assessments
- **Managed high-pressure incident escalations** within SLA requirements, developing operational resilience and real-world incident response capabilities essential for cybersecurity operations
- **Automated system troubleshooting workflows** using Python and Bash scripting, improving operational efficiency and reducing manual intervention in critical security infrastructure

CYBERSECURITY PROJECTS

Red Team Operations & Adversary Simulation

- **Astaroth-Style Red Team Campaign | Advanced Threat Simulation**
  Executed sophisticated fileless attack simulation using LOLBins (mshta.exe) mimicking real-world APT tactics
  Techniques: *LOLBins, Red Team, Fileless Attack, Defender Evasion*
- **GhostStager | Advanced C# Fileless Binary Loader**
  Built a fileless malware staging framework with reflective PE loading, AMSI/ETW evasion, and Sliver C2 integration for advanced red team operations.
  Techniques: *C#, Malware Development, Memory Execution, Evasion*

Offensive Security Development

- **Red Teaming 101: VBA Exploitation with Microsoft Word | Malware Development**
  Developed macro-based attack vector for initial access, demonstrating social engineering and payload delivery methods
  Techniques: *VBA, Microsoft Word, Reverse Shell, Exploitation*

Penetration Testing Methodology & Research

- **Internal Pentest: Active Directory Exploitation | Enterprise Security Assessment**
  Comprehensive penetration testing of AD environment demonstrating privilege escalation and lateral movement techniques
  Techniques: *Active Directory, Windows Server, Kerberoasting, Privilege Escalation*
- **25+ Hackrace-ranges CTF Machine Writeups | Practical Skills Documentation Detailed**
  technical writeups demonstrating exploitation techniques across diverse attack vectors and operating systems
  Platform: *Hacktrace-ranges*

🔔 ***Portfolio:*** *cybersecurity compiled projects*

TECHNICAL SKILLS

Cybersecurity & Red Team

- **Offensive Security Tools:** Burp Suite, SQLMap, Metasploit, Hydra, Gobuster, Nikto
- **Enumeration & Privilege Escalation:** LinPEAS, WinPEAS, pspy, BloodHound, mimikatz
- **Red Team Techniques:** VBA Macro Exploitation, Payload Crafting, Reverse Shell, Post-Exploitation, LOLBins
- **Vulnerability Assessment:** OWASP Top 10, SSRF, LFI, XSS, SQL Injection
- **Network Security:** Wireshark, DNSRecon, Nmap, Packet Analysis
- **Security Tools:** JohnTheRipper, pwncat, Impacket, CrackMapExec

Infrastructure & Platform Support

- **Cloud & Orchestration:** AWS (EC2, S3), Kubernetes, Apache Airflow DAG Management
- **Data Analytics Platforms:** Grafana, Apache Superset, MLCore, Dremio
- **Big Data Technologies:** Apache NiFi, Cloudera Flow Management, Hadoop Ecosystem
- **Database Operations:** Spark-SQL, Dependency Tracing, Data Pipeline Troubleshooting
- **Programming & Automation:** Python, Bash, SQL - Log Analysis, Sanity Testing, Whitelist Management

CERTIFICATIONS & RANKS

- **Certified API Security Practitioner** – APISEC University
- **Red Team Internship Certification** – HackSecure
- **Practical Ethical Hacking** – TCM Security
- **Practical Web Application and Testing** – TCM Security
- **Practical Web Hacking** – TCM Security
- **IT Support** - Google

- 🥉 **TryHackMe Top 3 – Indonesia** (750+ day streak)
- 🔐 **Hacktrace Ranges Top 20**

EDUCATIONS & CONTINUOUS LEARNING

2025 - 2025
(4 Months)

AWS re/Start Program | ***Batch 12 (In Progress)***

- Building foundational AWS cloud knowledge including core services, security fundamentals, and basic architecture principles
- Preparing for AWS Certified Cloud Practitioner certification through hands-on labs and practical cloud computing exercises

2012 - 2015

SMK Diponegoro Tumpang
Teknik Komputer Jaringan (TKJ)

- IT Division Head at OSIS (Student Council) for 2 years: Led the IT division, overseeing school-wide tech initiatives, managing IT infrastructure, and collaborating with other departments to enhance digital experiences for students and staff
- Internship at ITN Malang (Institut Teknologi Negeri Malang) as an IT Support Technician for 6 months: Provided technical support, troubleshooting, and maintenance for campus networks and systems, contributing to smooth operations and system enhancements