James Randall A. Magpantay

5 James St, Kingsville Executive Village, Mayamot, Antipolo City, 1871 | jamess.a.magpantay@gmail.com | 09915863298 | LinkedIn: james-randall-magpantay | github.com/jamesmagpantay

EDUCATION

Polytechnic University of the Philippines — **Manila, Philippines**
Bachelor of Science in Information Technology — *2028*

- **Relevant Coursework:** Cybersecurity Fundamentals, Network Administration, Operating Systems, Data Communications and Networking
- **Awards / Honors:** Gokongwei Brothers Foundation Scholar, President's Lister (AY 2024 - 2025)

EXPERIENCE

Department of Science and Technology (DOST) — **Manila, Philippines**
Software Developer Intern — *July 2026 – August 2026*

- Remediated a verification flaw in the authentication service that accepted forged tokens, restoring signature validation
- Blocked malicious file uploads by checking its contents against its claimed type, and rejecting files with embedded scripts
- Conducted security audits for vulnerabilities, documenting CWE findings and patching insecure upload and SVG handling

Cisco NetConnect PUP — **Manila, Philippines**
Vice Chief Technology Officer - CCNA Trained — *Feb 2026 – July 2026*

- Applied CCNA concepts including VLANs, trunking, network segmentating to strengthen infrastructure security
- Configured IPv4/IPv6 addressing, subnetting, DHCP, and DNS to maintain secure and reliable network operations
- Designed, analyzed, & troubleshot network topologies in Cisco Packet Tracer, incorporating security best practices

Google Developer Groups PUP — **Manila, Philippines**
Cybersecurity Compliance Analyst — *Feb 2026 – July 2026*

- Ensures the integrity of cybersecurity learning materials distributed to a cohort of 200+ Cybersecurity Cadets
- Co-facilitated cybersecurity workshops, showcasing security tools, best practices, and core cybersecurity concepts
- Designed a CTF challenge with a vulnerability, giving participants hands-on exploitation in a controlled environment

LEADERSHIP & ACTIVITIES

PUP OUS - SIEM and Ticketing System — **Manila, Philippines**
Independent Developer — *March 2026*

- Achieved 100% audit log tamper detection by implementing SHA-256 hash chaining on all database writes
- Reduced security alert noise by grouping 100% of concurrent events by source IP in a custom SIEM engine
- Mitigated 100% of brute-force login attempts using client-IP rate limits and account lockout logic

PUP OUS - Personnel Accomplishment Monitoring System — **Manila, Philippines**
Cybersecurity Lead & Project Manager — *March 2026*

- Implemented secure authentication by enforcing strong password requirements aligned with modern standards
- Established data handling policies to support the confidentiality, integirty, and availability of personnel information
- Implemented automated security scanning to detect vulnerabilities, insecure dependencies, and misconfigurations

CODEKADA - Hackathon — **Manila, Philippines**
Cybersecurity Lead (Project: Eely - AI Electricity Bill Scanner) — *May 2026*

- Formulated data privacy protocols for AI modeling, ensuring 100% compliance in securing sensitive utility data
- Implemented measures to preserve data confidentiality and integrity across AI-driven extraction workflows
- Conducted security reviews of application workflow to identify risks and strengthen data protection practices

AI Odyssey CTF - TryHackMe — **Virtual (International) | Manila, Philippines**
CTF Participant - AI Red Teamer — *April 2026*

- Bypassed LLM safety filters via prompt injection to capture flags and document vulnerabilities
- Leveraged Burp Suite to exploit machine learning vulnerabilities and intercept model traffic
- Analyzed AI/ML threats, focusing on model-specific weaknesses and adversarial machine learning risks

SKILLS & INTEREST

- **Security & Governance:** CIA Triad, AAA, Network Security Fundamentals, ISC2 CC standards
- **Networking:** IPv4/IPv6 Subnetting, VLANs, DHCP, Trunking, ACLs, EtherChannel, Routing, OSI Model, TCP/IP
- **Systems & Hardware:** Windows 10/11, Kali Linux, VirtualBox
- **AI Red Teaming:** Adversarial ML, Prompt Injection, Data Poisoning, Safety Filter Bypassing
- **Tools & Platforms:** Cisco Packet Tracer, PuTTY, CyberChef, Burp Suite, Nmap, Git, GitHub
- **Programming:** Python, Java, SQL, C
- **Leadership & Management:** Directed project lifecycles, managed teams, and aligned technical requirements