Ismael **Penacho**

Capabilities

Proactive problem solver and team player with leadership experience. Self-starter with a continuous learning mindset. Experienced in cloud security, detection engineering, and software development, with a strong understanding of attacker techniques gained through ethical hacking and penetration testing.

Skills

- Security Engineering & Detection: Vulnerability assessment, misconfiguration detection, incident response, monitoring, attacker techniques
- Cloud Security & Compliance: AWS, Azure, GCP, Kubernetes, Docker, CSPM, CNAPP, policy-as-code (OPA/Rego)
- Pentesting / Offensive Security: Web & infrastructure pentesting, OSINT, network protocols, exploitation, service enumeration & data gathering
- Tools & Frameworks: Nmap, Burp Suite, Kali Linux, Airodump-ng, OWASP, MITRE ATT&CK, CIS, NIST
- C, C++, Java, Python, Go, Bash, SQL

Certifications

- eJPT
- eWPT

Contact information

@ p3n4x0@protonmail.com
in LinkedIn
GitHub
WebSite
EN: Fluent
ES: Native

About Me

Cybersecurity Professional with a strong background in **offensive security** and a current focus on **cloud security engineering, detection, and automation**. Experienced in **AWS, Azure, GCP**, designing and implementing security architecture and controls across workloads, hosts, and containerized environments.

Skilled in **Go and Python** for automation, detection logic, and developing security tools, allowing me to approach challenges from **defensive, offensive, and engineering perspectives**.

Previously specialized in **ethical hacking and penetration testing**, leveraging that mindset to build **defensive strategies**. Passionate about continuous learning and active in security research and community challenges.

Experience

Cloud Security Engineer (Promoted from Cloud Security Analyst) at *Sysdig*

Jan 2024–Currently

◇ Designed and automated security policies to ensure 360º protection across workloads, hosts, Kubernetes/Docker clusters, and multi-cloud infrastructures (AWS, Azure, GCP).

◇ Led the detection of publicly exposed resources and misconfigurations, strengthening overall cloud security posture.

◇ Developed in Go and Python for automation, detection logic, and service components powering security products such as CSPM, CNAPP, and other cloud-native protection modules.

◇ Implemented policy-as-code and compliance mapping (CIS, NIST, ISO, MITRE) to achieve best-in-class coverage and reduce misconfiguration risks.

◇ Built and managed cloud environments using IaC (Terraform, CloudFormation), achieving secure, compliant, and scalable deployments.

Red Team Lead (Promoted from Operator) at *DigitalHM*

Jun 2023–Jan 2024

◇ Led red team operations, including vulnerability assessment, OSINT, and advanced adversary simulations.

◇ Automated offensive workflows through custom scripting to improve efficiency and reproducibility.

◇ Designed and executed simulated phishing and malware campaigns to assess organizational resilience.

◇ Directed team coordination and knowledge sharing as Red Team Lead.

Cyber Security Engineer Intern at *NoLogin*. **Jul 2022–Sept 2022**

◇ Monitored servers and services in both on-premise and cloud environments (AWS, Azure, GCP), ensuring operational continuity and security compliance.

◇ Maintained and developed scripts and automation tools to streamline workflows and enhance security controls.

◇ Supported incident diagnosis and response activities, applying security best practices and detection techniques.

Education

Master in Cybersecurity. *IMF Smart Education / University of Avila*.

2023–2024

◇ Thesis: Pentesting of a Content Management System

◇ *Average Grade:* 8.7/10

Computer Science. *University of Zaragoza*. **2019–2023**

◇ Thesis: WiFiGhost, Offensive WiFi audit tool.

◇ *Average Grade:* 7.0/10