Julfri Caguiat

Springfield, VA | julfri.caguiat@gmail.com | (571) 395-3016 LinkedIn | GitHub | Cybersecurity Blog

Summary

Aspiring Cybersecurity Analyst with hands-on experience in virtual lab environments, network configuration, and threat monitoring. Holds CompTIA Security+ (SY0-701, 2025) and TryHackMe SOC Level 1 certifications. Practical exposure to SIEM tools, intrusion detection, VLAN segmentation, and network fundamentals through home lab projects, TryHackMe exercises, and CCNA study.

Certifications

- CompTIA Security+ (SY0-701) | 2025 [Verification Link]
- SOC Level 1 Learning Path | TryHackMe | 2025 [Verification Link]

Education

- Graduate Diploma in Computer Science | University of the Philippines OU (GPA 1.6/1.0) | 2023
- B.S. in MIS/Decision Science | George Mason University (GPA 3.45/4.0) | 2001

Skills

Cybersecurity & Risk Management:

NIST RMF (SP 800-37) – categorization, control selection, implementation, assessment, continuous monitoring, system hardening, access control, and vulnerability assessment

Networking & Security Tools:

TCP/IP, subnetting, VLANs, routing & switching (CCNA prep); Linux, SIEM, IDS/IPS, DFIR, Wireshark, and other Cybersecurity Toolkits (TryHackMe); virtualization, pfSense firewall, Wazuh SIEM, network design, implementation, integration, segmentation, system hardening, and monitoring (home lab projects)

Scripting; Database Management: Software & Web Development [GitHub]

Python & Bash scripting (basic); SQL; JavaScript, CSS, HTML, JavaScript, MarkDown; Java core

AI Tools: ChatGPT, DeepSeek, Google Gemini

Hands-On Projects & Labs [Projects Blog Site Link]

Cybersecurity Virtual/Physical Home Lab & Blog | Ongoing

- Applied NIST RMF lifecycle to design, implement, and monitor a fully segmented lab environment (Kali Linux & Windows VMs on VirtualBox hypervisor, VLANs implemented on Cisco 2960 switch, pfSense virtual firewall appliance, Wazuh SIEM on Ubuntu headless server)
- Asset Assessment / Categorization: Identified and classified virtual and physical devices (laptops, VMs, endpoints, firewall) by role and criticality
- Control Selection: Designed and implemented firewall rules, VLAN segmentation, and SIEM monitoring
- Implementation: Installed and configured VMs and different devices based on the network topology design and architecture
- Assessment / Testing: Tested network connectivity and segmentation, confirmed VM isolation, reviewed firewall rule enforcement, and validated logging and vulnerability detection.
- Continuous monitoring: via Wazuh alerts with Sysmon integration
- Published guides: VirtualBox lab setup, pfSense integration, essential Linux commands
- Current project: Integrating physical and virtual devices with VLAN segmentation

Networking & Security Labs | TryHackMe / CCNA Prep | Ongoing

- Completed SOC Level 1 and continues practice with pentesting on TryHackMe lab environment.
- Designed and implemented virtual and physical network integration with security controls
- Applied NIST SP 800-37 RMF steps 4–6: assessing, authorizing, and monitoring security controls
- Continuously practicing network configurations in Cisco Packet Tracer, including VLANs, routing, and subnetting (CCNA prep).