Kevin Smythe

Wilmington, NC
phone: 619-712-1343
ks.logged@gmail.com
github | LinkedIn

Cybersecurity enthusiast with extensive hands-on experience gained through academic labs, projects, and home environments. Skilled in SOC fundamentals, threat detection, log analysis, incident response simulations, vulnerability assessment, Windows administration, and virtualization. Demonstrated ability to investigate simulated security incidents, recover digital evidence, and configure secure networks in controlled lab settings. Committed to preventing unauthorized access and supporting enterprise cyber defense operations.

EDUCATION & CERTIFICATIONS

A.A.S, Computer Networking Systems, Houston Community College

Security+ (exam date: [02/26])

TECHNICAL SKILLS

Security & SOC: SIEM basics, log analysis, incident triage, firewall setup, vulnerability assessment, malware/attack analysis, penetration testing fundamentals
Forensics: Data recovery, imaging & hashing, mobile/email/cloud analysis, VM forensic investigation, reporting
Networking & Systems: TCP/IP, OSI model, switches/routers, wireless security, Windows OS installation/configuration, Active Directory, user/device management
Virtualization: VM deployment & management, virtual NIC configuration, secure testing & incident replication
Programming & Automation: Python, scripting, structured algorithms
Tools: Splunk, Wireshark, Nmap, VirtualBox/VMware, Windows Admin Tools, PowerShell basics, kali linux

ACADEMIC TRAINING & HANDS-ON LABS 2023-2025

- **SOC Simulation Lab –** Configured a virtual SOC environment; monitored simulated logs for anomalies, triaged alerts, and documented incident findings.
- **Windows Enterprise Lab –** Installed and configured multiple Windows clients; implemented user permissions, group policies, updates, and system monitoring.
- **Digital Forensics Lab** – Recovered deleted/hidden files, analyzed email artifacts, validated data integrity, and generated forensic reports.
- **Networking & Packet Analysis Lab** – Scanned and enumerated virtual networks, analyzed packet captures, and identified potential security issues in controlled environments.
- **Virtualization Lab** – Built virtualized test environments to simulate secure network segments, deploy vulnerable systems safely, and practice incident response workflows.

PROFESSIONAL DEVELOPMENT

- Attended webinars, such as ***"Ransomware Actors: A closer look at the Criminals behind the Attacks"*** by [**Bitdefender**] and ***"Understanding Attack Surface Management"*** [**CyCognito/Gigamon**]
- Continuously practicing network and security tool usage (**Wireshark, Burp Suite, Nmap, OpenVAS, etc**.)
- Avid listener of cybersecurity podcasts like ***Darknet Diaries*** and ***CyberWire Daily***
- Improving command line proficiency in Windows and Linux operating systems
- Completing structured learning paths on platforms such as **TryHackMe, Cybrary, INE, Coursera, or Pluralsight**
- Actively studies threat intelligence reports (**CISA, Verizon DBIR, Mandiant**)
- Follow the **NICE Framework** to structure ongoing learning and career progression