My F. Name (Clearances: Secret & Public Trust)

username@email.com – linkedin.com/in/theprofile – github.com/leet-hacker

Certifications: CompTIA- PenTest+, Security+, & Linux+

PROFESSIONAL SUMMARY

Vulnerability management specialist focused on reducing cyber risk through automation, scalable detection, and cross-functional collaboration. Trusted to lead high-impact initiatives that streamline triage, integrate threat intelligence, and improve remediation outcomes across diverse enterprise environments. Experienced in designing repeatable workflows and tools that empower both technical and non-technical teams to manage vulnerabilities with confidence and clarity.

EXPERIENCE

Large Consulting Firm (January 2022 – Present)

Vulnerability Analyst
Contract supporting CISA (April 2023 – Present)

- Automated vulnerability investigation workflows with Python, reducing data collection time by over 50% and streamlining false positive triage across federal compliance reporting.
- Built user-friendly GUI tools, enabling non-technical staff to independently query databases, manage configurations, and export reporting for over 10,000 stakeholders.
- Engineered Shodan scanning scripts with modular signature design, enabling scalable detection of known exploited vulnerabilities and doubling notifications to critical infrastructure entities.
- Flagged high-risk exposures in critical infrastructure sectors, including Food & Agriculture and Water & Wastewater, leading to targeted CISA interventions.
- Integrated ransomware threat intelligence into CISA's Known Exploited Vulnerabilities (KEV) database, improving prioritization for stakeholder resilience strategies.

Network Engineer
Contract supporting US Coast Guard (January 2022 – March 2023)

- Designed repeatable mitigation workflows for US Coast Guard (USCG) continuous monitoring servers, standardizing the cycle of vulnerability analysis, triage, testing, and production deployment.
- Strengthened artifacts collected for DISA STIG documentation (a federal system hardening framework), cutting audit prep time by 50% and improving evidence quality.
- Mapped Standard Operating Procedures to NIST SP 800-53 controls (a cybersecurity framework) to demonstrate how continuous network monitoring improved USCG's compliance posture.

ADDITIONAL EXPERIENCE

Security Analyst
Small MSSP (April 2025 – Present)

- Prepared forensic evidence for courtroom use, enabling legal teams and juries to clearly understand technical findings and strengthen case arguments.
- Performed comprehensive wireless assessment using protocol analysis tools to detect misconfigurations, rogue access points, and insecure encryption settings in an enterprise-grade environment.

Adjunct Instructor (Linux+ Certification Prep)
Local Community College (October 2023 – December 2023)

- Provided supplementary instruction to students, answering advanced questions during lectures, reinforcing Linux server administration concepts, and guiding exam preparation strategies.

Cybersecurity Intern
Small Consulting Firm (May 2021 – September 2021)

- Authored 3–5 threat intelligence briefings weekly for their community platform, using OSInt research to analyze recent cyberattacks, identify threat actors, and recommend defense strategies.
- Built foundational skills in vulnerability management and incident response through hands-on exposure to cybersecurity platforms and compliance frameworks.

TECHNICAL PROJECTS

See GitHub page (URL at top right) for tutorials and walkthroughs to support cybersecurity community learning.