Charles Lewis

Cybersecurity Analyst | Security Administrator | Vulnerability Management

PROFESSIONAL SUMMARY

Security-focused systems administrator and cybersecurity professional with 5+ years of experience supporting identity, endpoint security, patching, system hardening, access controls, log review, and vulnerability remediation across healthcare and enterprise environments. Skilled with Active Directory, Entra ID, Microsoft 365, Intune, Microsoft Defender for Endpoint, PowerShell automation, and security operations. Hands-on offensive security lab experience with authorized enumeration, web application testing, privilege escalation, and remediation reporting.

CORE SECURITY SKILLS

Security Operations: log review, incident support, vulnerability remediation, risk-based hardening, HIPAA support, audit support
Identity & Access: Active Directory, Entra ID/Azure AD, Microsoft 365, MFA, Conditional Access, RBAC, Group Policy, Okta, JML
Endpoint & Cloud: Intune, Microsoft Defender for Endpoint (MDE), Azure, Windows, Linux/Kali, VMware, patch management
Testing & Analysis: Nmap, Burp Suite, Gobuster, Wireshark, Hashcat, John the Ripper, Metasploit in authorized labs
Automation: PowerShell, Bash, Python, SQL, JSON reporting, administrative scripting

PROFESSIONAL EXPERIENCE

SECURITY PROJECTS & LABS

- MGS – Mini Group Strike: Developed a Python-based authorized lab enumeration/reporting tool with subnet discovery, service inventory, and structured JSON output; maintaining a public-safe GitHub version with sample output and responsible usage documentation.
- PowerShell Administration & Security Toolkit: Created scripts for Active Directory support, endpoint maintenance, BitLocker/LAPS workflows, software inventory/removal, reporting, and auditing.
- GhostDefense Home: Built defensive validation tooling for Windows/WSL lab environments to identify configuration and vulnerability signals and support system hardening.
- Offensive Security Labs: Conducted authorized lab assessments covering reconnaissance, enumeration, web testing, exploitation, privilege escalation, evidence collection, and remediation reporting.

CYBERSECURITY COMPETITIONS

- National Cyber League: Top 2% Individual / Top 1% Team; solved challenges in cryptography, web exploitation, traffic analysis, password cracking, log analysis, and OSINT.

CERTIFICATIONS

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | Google Cybersecurity Certificate | MTA: Server Administration | eJPT (In Progress)

EDUCATION

Bachelor of Science, Information Technology & Networking (Cyber Security)
Associate of Applied Science
Associate of Applied Science, Computer Engineering