Zachary D. Henard

(423) 293-2364 - Zachary@Henard.tech
https://henard.tech - https://GitHub.com/zdhenard42
Clearance: Active DOD Sponsored Secret Clearance

EXPERIENCE

Tennessee Valley Authority Nashville, TN
Technology & Innovation Intern January 2023 - Present

-Created Ansible Playbooks to automate IOS upgrades for 523 Cisco devices and reducing upgrade time by 95%.
  -Deployed the playbooks to Ansible Automation Platform to leverage RBAC and management capabilities.
  -Integrated verification tasks ensuring that failed upgrades would result in minimal network downtime.
  -Added 11 distinct roles enabling simultaneous upgrades across multiple Cisco models.
-Leveraged PowerShell to create over 300 rooms into Exchange, eliminating a $167,000/year contract.
  -Employed Graph API functions for in-depth analytics on resources, aiding in data-driven decision-making.
  -Partnered with department heads and directors to design a service model for a smooth enterprise-wide transition.
-Conduct routine audits on Cisco gear, ensuring adherence to STIG guidelines and DISA standards.
  -Utilize these assessments to highlight Cat-1 vulnerabilities found on devices supporting critical infrastructure.

Conquest Cyber Nashville, TN
SOC Analyst Intern September 2022 – January 2023

-Designed "SOC Multitool", a browser extension that aggregates 23 security tools for efficient investigations.
  -Reached #22 on GitHub Trending and averages 3,000+ monthly users on Chrome Web Store.
  -Received positive reviews from multiple security blogs and shared by industry leaders on social media.
  -Utilized a combination of JavaScript, HTML, and ManifestV3 to create a seamless and effective user experience.
-Constructed a Windows batch tool that reduced documentation/analysis of evidence time by 50%.
-Addressed 20+ daily security incidents using XSoar, Microsoft Azure/Sentinel, and QRadar.
-Developed 13 complex KQL queries increasing efficiency of evidence collection by 30%.

Intuitive Research & Technology Huntsville, AL
System Administrator Intern May 2022 – August 2022

-Developed "Thick2Thin Converter", utilizing Batch, PowerShell, and WinPE to automate desktop migration
  -Deployed a login script that automated 14 tasks for user environment migration from thick to thin clients.
  -Reduced user interruption by an average of 30 minutes per user for over 400 employees.
  -Created a custom boot drive that automated re-imaging and conversion of desktops with WinPE and Wyse.
-Served as the primary contact for Virtual Desktop Infrastructure issues for over 500 employees.

Army National Guard Knoxville, TN
Track Vehicle Mechanic April 2021 - Present

-Graduated as top of class from Advanced Individual Training, showing exceptional technical and leadership skills.
-Responsible for maintaining high-value military equipment ensuring they are in combat ready status.
-Trained in operational security and information security, applying these practices to secure communications and data.
-Collaborate in teams to solve complex technical problems, enhancing effectiveness in high-pressure situations.
-Participate in regular drills and exercises that emphasize strategic thinking and quick decision-making.

TECHNICAL EXPERTISE & CERTIFICATIONS

-**Certifications:** CompTIA Security+, Microsoft SC-200: Security Operations Analyst, DOD Secret Clearance
-**Programming Languages:** C/C++, Python, JavaScript, SQL/KQL, YAML.
-**Unix Tools:** bash, Wireshark, Nmap, Metasploit, DirBuster, Ghidra, exploitdb, Kali, RHEL, and Ansible Tower.
-**Windows Tools:** PowerShell, Batch, Windows Subsystem for Linux, WinPE, Firewall, and Registry.
-**Cloud Technologies:** Kubernetes, K3s, Rancher, Longhorn, MetalLB, Azure Apps, Entra ID, and Exchange Online.

PROJECTS

Home Lab

-Designed and managed a sophisticated home lab with ESXi 6.5/8 for virtual machines and containers.
-Implemented OPNsense as a firewall, DHCP server, and router for network security and integrity.
-Integrated Rancher to deploy a self-hosted Kubernetes cluster running RKE2 to replicate a federal environment.
-Deployed VMware VCenter allowing for cluster autoscaling via Rancher and the VCenter API.
-Utilized MetalLB to manage the network load balancing of my bare-metal K8s cluster.
-Integrated NGINX Ingress controller with Let's Encrypt to automatically obtain SSL certificates for my applications.
-Installed Longhorn allowing for orchestration of persistent volumes and backups across multiple nodes.
-Applied STIGs to align the ESXi environment with DoD security standards.
-Leveraged EVE-NG to replicate the configuration of intricate enterprise Cisco environments (IOS/IOS-XE).
-Utilized the simulated Cisco environments for robust testing of Ansible automation playbooks.
-Deployed Pi-hole as a DNS server, providing ad-blocking and privacy protection.
-Administer Windows Server 2020 domain controller for managing multiple Windows VMs.
-Employed Kali Linux (Original/Purple) for penetration testing and cybersecurity analysis.
-Configured a managed switch for VLAN traffic segregation and network organization.

Advanced QR-Code Analysis

-Designed and implemented a web-based tool to decode and extract detailed information from QR codes.
-Leveraged JavaScript, Fetch API, and Cloudflare Workers for seamless integration and data presentation.
-Integrated 6 threat analysis platforms, offering insight into QR content such as URL reputation and network data.

LinkedIn Connector

-Developed a Python script leveraging Selenium for automated LinkedIn connection requests.
-Utilized 'undetected Chrome driver', random intervals, and user-agent spoofing for bot detection evasion.
-Achieved up to 1,000 weekly connection requests without triggering security measures.
-Employed XPaths for personalized connection messages based on the target's job title.
-Maintained consistent 100 daily connections without disruptions to account functionality.
-Implemented automatic removal of outdated pending connection requests for streamlined management.

Anti Anti-VM

-Created a Batch script to bypass VM detection methods employed by software to identify OS environments.
-Modified Registry to eliminate instances of strings commonly targeted during VM detection.
-Spoofed hardware MAC addresses, mimicking legitimate vendor OUIs for user environment authenticity.
-Enabled passthrough of prerecorded video and audio as live content through a webcam.

Currency Converter

-Developed a Chromium browser extension to convert web page prices to user's preferred currency.
-Utilized a REST API for live exchange rates and JavaScript for currency identification.
-Supports **270** currencies including cryptocurrencies for simplified global currency conversions.

EDUCATION

Tennessee Technological University Cookeville, TN
B.S Computer Science, concentration in cybersecurity, 3.8 GPA May 2024
-Affiliations: Honor's Society, CyberEagles, Offensive/Defensive Cyber, and Student Veterans Organization.

Northeast State Community College Blountville, TN
Associate of Science, Computer Science, 3.8 GPA August 2019 - May 2021