

Zachary D. Henard

(423) 293-2364 - Zachary@Henard.tech

<https://henard.tech> - <https://GitHub.com/zdhenard42>

Clearance: DOD Sponsored Secret Clearance (Active)

CAREER SUMMARY: Passionate Computer Science student specializing in cybersecurity, showcasing a strong background in system administration and cybersecurity solutions. Demonstrated expertise in various programming languages and tools, with a portfolio of impactful projects. Committed to optimizing security operations through innovative approaches and creative problem-solving. Proud holder of CompTIA Security+ and Microsoft SC-200 certifications, reflecting dedication to ongoing professional development.

EDUCATION

Tennessee Technological University

Cookeville, TN

B.S Computer Science, concentration in cybersecurity, 3.9 GPA

Projected May 2024

-Organizations: Honor's Society, CyberEagles, Offensive/Defensive Interest Groups, Student Veterans Organization

Northeast State Community College

Blountville, TN

A.S. Computer Science, 3.8 GPA

May 2021

-Graduated with *Magna Cum Laude*.

-Placed on "President's List" all semesters attended.

EXPERIENCE

Tennessee Valley Authority

Nashville, TN

Technology & Innovation Intern

January 2023 - Present

-Significantly reducing verification time for **384** endpoints connectivity by **80%** utilizing PowerShell scripts and SSH.

-Maintaining IOS, ROMMON, and CPLD updates for **63 Cisco switches** and **3 Cisco Routers**.

-Developing and maintaining a script that automates verification and accuracy of ownership for 320 AD group owners.

Conquest Cyber

Nashville, TN

SOC Analyst Intern

September 2022 – January 2023

-Developed **13 complex KQL queries** increasing efficiency of evidence collection by **30%**.

-Created CLI tool and browser extension to decrease documentation/analysis of evidence by **50%**.

-Resolved **20 cases/day** gathering evidence from XSoar, Microsoft Azure/Sentinel, and QRadar.

Intuitive Research & Technology

Huntsville, AL

System Administrator Intern

May 2022 – August 2022

-Automated Thin Client migration (**14 tasks**) for **300+ employees** reducing disruption time by **100%**.

-Acted as primary point of contact for Virtual Desktop Infrastructure issues for **500+ employees**.

-Automated Re-imaging and conversion from Thick Client OS to Dell Wyse Thin Client OS for **80 workstations**.

Army National Guard

Knoxville, TN

Track Vehicle Mechanic

April 2021 - Present

-Graduated Advanced Individual Training as the valedictorian of my class.

-Stepped up to act in an E6 position to ensure that the unit's motor pool was in a combat ready status.

-Experienced in handling confidential information and following strict security protocols.

CERTIFICATIONS

-CompTIA Security+ acquired August 2022

-Microsoft SC-200: Security Operations Analyst acquired January 2023

-DOD Sponsored Secret Security clearance acquired March 2021

COMPUTER LANGUAGES AND TOOLS

-Languages: C/C++, Python, JavaScript, SQL/KQL

-Unix: bash, Wireshark, Nmap, Metasploit, DirBuster, Ghidra, exploitdb, Kali, RHEL

-Windows: PowerShell, Batch, Windows Subsystem for Linux, WinPE, Firewall, and Registry

-Virtualization: VMware(Workstation/Horizon/ESXi), Docker, and Google Compute Engine

PROJECTS

SOC Multi-tool

- Developed an open-source Chrome extension that aggregates over **20** security investigation tools.
- Reached **#22 on GitHub Trending** and has garnered over **500** active users from the 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.

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.
- 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.
- Applied STIGs to align the ESXi environment with DoD security standards.
- Configured managed switch for VLAN traffic segregation and network organization.
- Integrated Suricata as an Intrusion Prevention System (IPS) to monitor and protect against network threats.

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 XPath 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.

Thick Client Migrator

- Customized PowerShell script automating **14 tasks** for user environment migration from thick to thin clients.
- Embedded in user login script for seamless experience without manual intervention.

Thick2Thin Converter

- Automated re-imaging and conversion of thick clients to thin clients.
- Utilized bootable flash drive with WinPE and Wyse converter.
- Communicated with a central directory using NAS for management and control.

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.

ADDITIONAL

- Awards: Army Achievement Medal, President's List, Dean's List
- Competitions: Top 5% (329/6483) in HTB "CYBER APOCALYPSE 2023" CTF
- Soft Skills: Communication, teamwork, problem-solving, and time management.