

# Jeremy MacRoberts

219-779-5807 • Fort Wayne, IN • [contact@jeremymacroberts.com](mailto:contact@jeremymacroberts.com) • <https://jeremymacroberts.com/>



## WORK EXPERIENCE

### Network and Security Engineering Intern

May 2023 - Present

CrowdStrike | Remote

- ❑ Implemented Ansible, Jinja2, and other automation technologies for device onboarding in datacenters.
- ❑ Completed a device configuration pipeline for onboarding and saving state of network devices.
- ❑ Implemented documentation and SOP for SOC2 compliance, as well as python automation for executing self-audits.
- ❑ Created scripts to automate NETENG tasks and intake firewall requests for execution on production environment.

### IT Intern

March 2023 – August 2023

Rea Magnet Wire | Fort Wayne, IN

- ❑ Headed research, proposal, and deployment of a network security monitoring solution.
- ❑ Leveraged PowerShell to automate device configuration backups and solve other department issues through automation.

## CERTIFICATIONS AND EDUCATION

INE | eLearnSecurity Junior Penetration Tester (eJPT)

2023 - 2026

Bachelor of Science in Cybersecurity | Indiana Institute of Technology

2021 - 2025

## ORGANIZATIONS

### Team Captain

2021 - Present

Indiana Tech Cyber Warriors | Indiana Institute of Technology

- ❑ Lead and managed team of approximately 20 members year over year.
- ❑ Trained for and competed in cybersecurity competitions including CyberForce, NCL, UBuff Lockdown, and CCDC.
- ❑ Contributed to the creation of documentation related to team strategy and specialty onboarding.
- ❑ Developed team training resources by implementing technologies such as GNS3 and Nomad.
- ❑ Managed team equipment including Student Datacenter, vSphere cluster, UPS backups, and all virtualized resources.

## TEAM PROJECTS AND ACTIVITIES

### Python Palo Alto Configuration Automation Utility

2022 - Present

- ❑ Python program that leverages Palo Alto's Rest API through the pan-os-python package to set and manage networking configuration with minimal user input.
- ❑ Creates firewall rules to secure underlying networks while still allowing required traffic without disrupting services.
- ❑ Automates the completion of tasks such as NAT configuration, logging to Splunk, password complexity rules, and login information.
- ❑ Allows for user input to configure extra services, NAT rules, and many others during runtime.

### Attack/Defense Exercises

2021 - Present

- ❑ Regularly (monthly/semi-monthly) participates in 6–8-hour long pentester vs sysadmin simulations, as the defense role.
- ❑ Manages administrative duties including building out 25-server network topologies with services and configuring scoring.
- ❑ Sysadmins (Blue Team) are tasked with maintaining 100% uptime while completing ~40 sysadmin task simulations.
- ❑ Pentesters (Red Team) try to maintain access to the machines undetected, using their access to intervene with uptime.

## EXPERIENCE

### Palo Alto

- ❑ Managed several Palo Alto devices for CCDC competition and learning purposes.
- ❑ Leveraged features such as IPsec tunnels, firewall rules, NAT rules, and logging to Splunk during competition.

### Cisco

- ❑ Completed networking classes at Indiana Institute of Technology designed around the CCNA and Cisco Equipment.
- ❑ Managed Cisco Firepower devices including configuration of next generation firewall capabilities.
- ❑ Established script and configuration templates which utilize routing, ACL's, SSH connectivity, and trunking.

### Windows

- ❑ Deployed Microsoft services such as Active Directory, DNS, Certificate Services, and DHCP in home environment.
- ❑ Updated and secured personal Windows servers and hosts while providing public services from personal lab.

## COMPETITIONS

- ❑ Collegiate Cyber Defense Competition– 2nd place (Regionals) 2022 - 2023
- ❑ Collegiate Penetration Testing Competition – 1st place (Regionals) 2023