Ava S. Hughes

Red Team Operator

📍 Augusta, GA
✉ ava@skyfault.com
☎ +1 (270) 401-8948
@Skyfa117

PROJECTS

Bit-Bandits

https://bit-bandits.com

Contributor to Bit-Bandits, a Github Pages hosted wiki dedicated to providing detailed writeups on different CVE's and attacker techniques.

EDUCATION

Army 17C MOS Training

Over 1500+ academic hours of training that teaches the knowledge and skills required for offensive and defensive cyber operations. Graduated as the class' distinguished honor graduate as the student with the highest grade and performance

EXPERIENCE

Active Security Clearance:
TS/SCI w/ CI Polygraph

Cyber Operations Specialist (17C)

U.S. Army Cyber Protection Brigade

Cyber Threat Emulator | October 2023 - Present

Senior Operator in the unit's Cyber Threat Emulation (CTE) cell, additionally responsible for critical red team infrastructure and networking.

Planned and conducted custom red and purple team exercises against the unit's blue teams, researching vulnerabilities and exploits, coordinating and executing complex attack paths, and emulating Advanced Persistent Threats (APTs).

Developed, deployed and maintained infrastructure and networking critical to conducting operations, and produced scripts and tools to automate and manage these resources.

Generated data analytics by virtualizing, deploying and executing CVEs and TTPs, customizing exploits to meet mission goals and client requirements.

Crafted documentation and training as well as mentored junior operators on tools, infrastructure, and exploitation techniques.

- Red Team
- C2 Frameworks
- Active Directory
- AV Evasion
- Web Exploitation
- SQL
- DevOps
- Proxmox
- Networking

Network Analyst | February 2021 - October 2023

Senior Network Analyst on a U.S. JFHQ Department of Defense Information Network (JFHQ-DODIN) based Cyber Protection Team (CPT).

Engaged in a variety of missions including incident response, network hardening, and threat hunting on diverse Enterprise, ICS and Cloud networks.

Analyzed data gathered from various on-site and team-deployed tools to detect vulnerabilities, misconfigurations and indicators of compromise, providing clients with detailed reporting and actionable remediations.

Mentored junior analysts on exploitation techniques, defense evasion, and attacker methodologies and how to use this knowledge to detect and protect against adversary activities.

- Security Onion
- Elastic Stack
- Endgame
- Splunk
- Sysmon
- MITRE ATT&CK

SKILLS

- DevOps
- Networking
- CI/CD
- Proxmox
- Automation
- Scripting
- SIEM
- Dashboards
- Data Analytics
- Digital Forensics
- Security Onion
- Elastic Stack
- Endgame
- Splunk
- Microsoft Sentinel
- Sysmon
- Linux

- Metasploit
- Nessus
- Cobalt Strike
- Burp Suite
- Pentesting
- Active Directory
- AV Evasion
- Persistence
- PrivEsc
- Exfiltration
- Web Exploitation
- SQL
- Reverse Shells
- Python
- Bash
- PowerShell
- Windows

CERTIFICATIONS

Global Industrial Cyber Security Professional (GICSP)

March 2023 | SANS Institute

Offensive Security Certified Professional (OSCP)

September 2024 | OffSec

Red Team Apprentice Certified

January 2024 | k>fivefour

Red Team Journeyman Certified

March 2025 | k>fivefour

ACHIEVEMENTS

Defense Cyber Marvel 4 (DCM4)

February 2025

Participated in the red team component in a multi-national cyber exercise involving teams and personnel from 27 nations. Conducted advanced exploitation techniques across a large multi-domain network with diverse Enterprise and ICS systems to meet red team goals and cause effects on network. Along with these responsibilities, produced both detailed attack reports and provided daily mentorship and feedback to participating blue teams.

CISA Presidents Cup VI

January 2025

A nationwide cybersecurity competition hosted by CISA that challenged members of the federal workforce to defend networks, analyze threats, and uncover vulnerabilities. **Scored in the top 8% of competing teams (16/191) in Round 1 and qualified for Round 2. Proceeded to then score in the top third of teams (21/63) that moved on to Round 2.**

Hack the Railroad 2023

October 2023

A hybrid cybersecurity event powered by US Cyber Command, Cylus, TAC (formerly MISI), and Amtrack focused on cybersecurity in the context of railway and ICS systems. During the event, **competed and placed 1st out of 18 teams** in a two-day CTF featuring challenges based on real world attacks and vulnerabilities - including hacking in-use ICS systems, reverse engineering and exploiting ticketing systems, and abusing railroad signals.

Cyber Apocalypse CTF 2023 (Hack the Box)

March 2023

Participated in a global 5-day CTF featuring 74 challenges ranging across diverse topics, including web exploitation, digital forensics, reverse engineering, vulnerability analysis and exploitation, and various others. **Team placed in the top 3% of competing teams (245/6483).**