Jacob Hammargren

Tampa, FL • jacobh.io • github.com/Jacob-Ham • jake@jacobh.io

EDUCATION & CERTIFICATIONS

University of South Florida, **B.S. in Cybersecurity**	May 2025
Offensive Security Certified Professional **(OSCP**)	In Progress
Certified Red Team Operator **(CRTO)**	2024
TCM Practical Junior Web Tester **(PJWT)**	2024
Offensive AWS Security Professional **(OAWSP)**	2024
HackTheBox Certified Defensive Security Analyst **(CDSA)**	2024
HackTheBox Pro-Lab (**Genesis)**	2023
TCM Practical Network Penetration Tester **(PNPT)**	2023
TCM Practical Junior Penetration Tester **(PJPT)**	2023
CompTIA **Security+**	2023

PROFESSIONAL EXPERIENCE

FanDuel, Atlanta GA — June 2023 – August 2024

Security Analyst & SecOps Engineer (internship)

- **Triaged security incidents** using enterprise **SIEM** technologies in a cloud-native environment (DataDog, AWS)
- **Performed a vulnerability assessment** on a corporate **Active Directory** network consisting of thousands of domain joined servers & computers uncovering several critical findings and exposing multiple attack paths that could lead to full domain compromise.
- **Lead email security automation efforts** utilizing the **Sublime** security platform. Lead bi-weekly meetings with the vendor and security operations team, wrote detection & remediation rules resulting in a **96%** auto-remediation rate for phishing emails - roughly **86,000 emails** per month.
- **Created a fully automated** incident response workflow in the **Tines SOAR** tool aimed at mitigating credential stuffing & Signup Path attacks against our edge login endpoint, resulting in ~ **100,000 blocked** attempts within its first month in production.
- **Collaborated with security researchers** on our **HackerOne Bug Bounty** program, validating reports of web application vulnerabilities from **XSS** to **exposed secrets** and beyond.
- **Collaborated** with teams across the security department to deploy various WAF rules aimed at mitigating credential stuffing attempts - successfully **blocking millions of requests** per month

ACTIVITIES & PROJECTS

USF CyberHerd, *Co-Captain & Founding Member*

- Co-Captain of **USF's official collegiate cyber team**, engaging in weekly meetings to advance red/blue teaming skills to prepare for **state**, **regional,** and **nation-wide** cybersecurity competitions.
- Managed **Virtual Machine** infrastructure for the team utilizing **Proxmox Hypervisor** to rapidly deploy practice VMs accessible via a **Tailscale VPN** tailnet with subnet routing.

Notable Competition Placements:

- **1st - NCAE VIVID** Nationals 2024
- **1st - Raymond James** CTF 2024
- **1st** - **NCAE Cyber Games** Regionals 2024
- **1st** - **HackSpaceCon** 2024 Badge CTF
- **1st** - **BSides Tampa** 2024 Badge CTF
- **2nd - SECPTC** 2024
- **2nd** - **SECCDC** 2024
- **3rd** - **National CCDC** WildCard Tournament
- **3rd** - **SECCDC** Qualifiers 2024
- **4th** - **DOE National CyberForce** 2023

Other Competitions

- CSAW Quals 2024
- CPTC 2023
- CSAW Quals 2023
- CakeCTF 2023
- BucketCTF 2023
- UMDCTF 2023
- vsCTF 2023
- PicoCTF 2022, 2023, 2024
- DiceCTF 2022

Whitehatters Computer Security Club, *Member, Vice-President (former), President (former)*

- **Taught** a club of **600+ members** linux fundamentals, active defense, penetration testing, digital forensics, kali linux, virtual machines, active directory exploitation.
- **Organized** industry and student guest lecturers to teach subjects involving AWS, Incident Response, Binary Exploitation, OWASP Top 10, etc..
- **Created** a one-stop-shop website **wcsc.info** to consolidate knowledge, scheduling, and communications to ensure consistent semester to semester transitions.

Offensive Security Proving Grounds, *Learning Platform*

- **Exploited 82 vulnerable hosts,** capturing **142 user and root** hashes.
- **Wrote** 40 exploitation **writeups** for jacobh.io/writeups to cement attacker TTPs and practice key reporting skills. Password protected for OffSec IP: **writeuppass**

HackTheBox, *Learning Platform*

- **App:** Exploited **25 hosts**, capturing 25 initial access flags and 25 privilege escalation flags
- **Academy:** Exploited **239 targets** including the **CDSA** path & certification**, top 1%** of academy users
- **Enterprise:** Exploited **31 machines**, 10 Windows, 21 Linux including the **Genesis Pro-Lab**

PicoGym, *Learning Platform*

- **Trained** for CTF competitions in categories: **Web, Forensics, Crypto, General, Reversing, and Pwn**.
- **15,149 points** earned: **55** Easy, **77** Medium **3** hard challenges completed.

TryHackMe, *Learning Platform*

- **Top 1%** THM user with 81 practice rooms completed

Gbins, *Project*

https://github.com/Jacob-Ham/gbins

- **Python** script that fetches binary **GTFOBins** reference and displays the entry directly in your **terminal.**
- **Reduces** time required to exploit key binaries and consolidates required information

SADScriptCTF, *Project*

https://github.com/Jacob-Ham/SADScriptCTF

- Developed a **Bash script** designed to automate the setup, configuration, and deployment of various security vulnerabilities and user scenarios within a controlled environment, facilitating **hands-on cybersecurity training**.

SKILLS

Blue Team Skills

- **SOC Processes**
- **SIEM Operations**
- **Log Analysis**
- Threat Hunting
- Malware Analysis
- Digital Forensics
- Incident Response
- Network Traffic Analysis IDS/IPS
- Active Directory Attack Analysis

Red Team Skills

- **Penetration Testing**
- **Vulnerability Assessment**
- **Risk Assessment**
- Post-exploitation enumeration
- Windows & Linux Privilege escalation
- Vuln/Risk reporting
- Web application pentesting
- Active Directory pentesting
- OSINT
- OWASP 10

Technologies/Environments

- **Metasploit**
- **Impacket**
- **BurpSuite**
- **NetExec, CrackMapExec**
- **Mimikatz**
- **Kali Linux**
- Splunk - Elastic
- AWS
- CrowdStrike EDR
- Sleuthkit
- DataDog CloudSiem
- Sublime Security
- Impart Security

Programming/Scripting

- **Bash**
- **Python**
- **Powershell**
- SQL
