Karter Barnes

Entry-level Cybersecurity Associate

(713) 555-0184 karter.barnes@example.com linkedin.com/example/karterbarnes Houston, TX 77002

STRENGTHS

Alert Analysis
During supervised SOC work, traced unusual logins across related events and gave instructors a clear investigative starting point.

Security Documentation
Created case templates and incident notes that made evidence, scope, disposition, and follow-up easier for peers to review.

Vulnerability Assessment
Used Nmap and Nessus Essentials in lab exercises, turning scan output into practical priorities and remediation guidance.

Clear Communication
Presented technical findings to instructors and classmates; concise explanations helped teams separate confirmed evidence from open questions.

Peer Support
Mentored fellow students during security exercises, sharing practical troubleshooting steps and becoming a dependable resource during reviews.

SKILLS

Analysis Skills | Career Development | Computer Security | Documentation | GCIH Certification | High School Diploma | Internet Security | Mentoring | Penetration Testing | Philosophy | Problem Solving Skills | Team Player | United States Citizen | Vulnerability Assessment | Security Monitoring

SUMMARY

Early-career cybersecurity professional prepared to support **security monitoring**, documentation, **vulnerability assessments**, and supervised **penetration testing**. Completed a Bachelor of Science in Cybersecurity in 2026, followed by hands-on work across SIEM analysis, network traffic review, endpoint triage, Linux administration, and internet security controls. Practical training includes Splunk, Microsoft Sentinel, Wireshark, Nmap, Nessus Essentials, Burp Suite, Metasploit, Kali Linux, Sysmon, and incident documentation. Built disciplined analysis habits through alert investigations, evidence capture, risk-based prioritization, remediation notes, and clear technical reporting. Completed **Google Cybersecurity Professional Certificate** and pursuing GCIH and OSCP pathways. Ready for in-person Dallas training, mentorship, continuous learning, and meaningful contributions across SOC analysis, incident response, GRC, and penetration testing.

EDUCATION

Bachelor's Degree in Cybersecurity

University of North Texas GPA: 3.7 2026 Denton, TX

Coursework: *Computer Security, Internet Security, Incident Response, Penetration Testing*

TECHNICAL SKILLS

- **SIEM Platforms:** Splunk, Microsoft Sentinel, SIEM alert triage
- **Network Analysis:** Wireshark, Nmap, network traffic analysis
- **Vulnerability Tools:** Nessus Essentials, Nmap, vulnerability scanning
- **Penetration Testing:** Burp Suite, Metasploit, Kali Linux
- **Operating Systems:** Linux, Windows, endpoint triage
- **Incident Response:** GCIH concepts, evidence preservation, incident timelines
- **Security Monitoring:** Firewall alerts, authentication logs, malware indicators
- **Web Security:** OWASP guidance, input validation, web application testing
- **Digital Evidence:** Sysmon, screenshots, request data, command output
- **Security Reporting:** Technical reporting, incident worksheets, remediation notes
- **Risk Analysis:** Risk-based prioritization, exploitability ranking, impact review
- **Security Documentation:** Case templates, escalation paths, disclosure records

EXPERIENCE

Cybersecurity Associate Training Practicum

Lone Star Cyber Defense Academy June 2026 - Present Dallas, TX

Supports supervised SOC training, security monitoring, **vulnerability assessment**, incident documentation, and authorized penetration testing across controlled lab environments. Converts technical observations into clear findings for instructors, mentors, and peers.

- Analyzed simulated firewall alerts in **Splunk**, documenting indicators and escalation paths for instructor review.
- Built **Microsoft Sentinel** searches for suspicious logins and malware indicators across controlled security datasets.
- Assessed lab systems with Nmap and **Nessus Essentials**, prioritizing findings through practical remediation notes.
- Preserved evidence and constructed incident timelines using GCIH pathway concepts during supervised investigations.
- Tested authorized web targets with **Burp Suite** and **Metasploit**, recording reproduction steps and mitigation guidance.
- Presented concise investigation summaries that helped peers distinguish confirmed findings from investigative leads.

Student Security Operations Analyst

University Security Operations Lab September 2025 - May 2026 Denton, TX

LANGUAGES

English — Native

Spanish — Intermediate

MY CAREER

- Cybersecurity Associate Training Practicum at Lone Star Cyber Defense Academy (3 Months)
- Student Security Operations Analyst at University Security Operations Lab (8 Months)
- Student Penetration Testing Analyst at North Texas Cybersecurity Capstone Project (7 Months)

Supported a classroom security operations environment spanning **Windows**, **Linux**, DNS, and authentication telemetry. Coordinated supervised response exercises, improved case documentation, and translated simulated incidents into actionable review materials.

- Triaged more than 400 simulated SIEM events by severity and source across Windows and Linux logs.
- Investigated phishing and credential misuse scenarios with **Wireshark**, **Sysmon**, and endpoint artifacts.
- Created repeatable alert-review procedures covering validation, enrichment, containment recommendations, and supervisor escalation.
- Mapped weekly vulnerability findings to affected services, risk considerations, and practical remediation steps.
- Coordinated four-person response exercises by assigning evidence tasks and maintaining an incident timeline.
- Standardized case templates capturing scope, indicators, analysis, disposition, and follow-up actions for lab review.

Student Penetration Testing Analyst

North Texas Cybersecurity Capstone Project — January 2025 - August 2025 — Denton, TX

Performed supervised penetration testing against an approved web application and segmented network prototype. Produced evidence-based reporting, validated remediation, and presented responsible disclosure practices to a faculty review panel.

- Assessed approved web targets with **Nmap**, Burp Suite, OWASP guidance, and **Kali Linux** tools.
- Ranked authentication and input-validation weaknesses by exploitability, affected component, and business consequence.
- Captured screenshots, request data, command output, and remediation evidence for controlled findings.
- Separated executive observations from technical reproduction steps in a concise **penetration testing** report.
- Retested proposed fixes through regression checks, confirming resolved issues and remaining development work.
- Presented scope, authorization, evidence handling, limitations, and disclosure practices to a faculty review panel.

PROJECTS

Supervised SOC Alert Investigation Lab — 2026

Built repeatable investigations across firewall, endpoint, authentication, and network telemetry. Used Splunk and Microsoft Sentinel to document indicators, preserve evidence, and recommend escalation paths.

Authorized Web Application Assessment — 2025

Tested an instructor-approved application with Burp Suite, Nmap, Kali Linux, and OWASP guidance. Reported findings, verified fixes, and communicated responsible disclosure practices.

LEADERSHIP & AWARDS

- Dean's List, University of North Texas — Fall 2025 and Spring 2026
- Cyber Defense Challenge Finalist — 2025
- Cybersecurity Capstone Presentation Award — 2025

CERTIFICATIONS

- Google Cybersecurity Professional Certificate — 2025
- GCIH - GIAC Certified Incident Handler Certification Pathway — 2026
- OSCP Preparation Track — 2026

PROFESSIONAL AFFILIATIONS

- Peer Mentor, University of North Texas Cybersecurity Student Association — 2025-2026
- Incident Response Study Group Coordinator, North Texas Cybersecurity Student Association — 2026

- Volunteer Lab Facilitator, Cybersecurity Awareness Workshop Series — 2025

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST