JARRED M. CARTER

jarredmcarter.com

EDUCATION

M.S., Cybersecurity, New York University, May 2025, GPA 3.8/4.0

- Coursework: Information Security and Privacy, Network Security, Pentesting and Vulnerability Analysis, Application Security, Computer Networking, Digital Forensics, Reverse Engineering, Web Application Exploitation
- Certifications: CompTIA Security+, OSCP+ (in progress)
- CyberCorps Scholarship for Service Scholar, awarded to top 1% of the class for two years in a row.

B.S., Computer Science & B.S., Cybersecurity, Marshall University, Dec. 2022, GPA 3.7/4.0

RELEVANT EXPERIENCE

Security Analyst 06/2024 — 09/2024

Open Law Library, Washington, D.C.

- Developed documentation and reporting workflows to improve adoption of security tooling and remediation processes by engineering and operations teams.
- Supported 40k+ users by maintaining operational security tooling to ensure continuous verification of code commits, preventing malicious activity on public law hosting infrastructure.
- Supported the vulnerability management program by validating findings, tracking remediation progress, and ensuring adherence to internal triage and remediation SLAs.
- Aggregated and analyzed vulnerability and system data to support risk assessment, reporting, and prioritization across application and infrastructure environments.

Penetration Testing Engineer 08/2022 — 12/2022

City National Bank, Cross Lanes, WV

- Conducted adversarial testing and vulnerability assessments across enterprise infrastructure, validating findings and translating technical results into risk-based remediation recommendations for technical and executive stakeholders.
- Maintained and operated vulnerability scanning, detection, and monitoring systems supporting continuous identification of security risks.
- Collaborated with SOC analysts, infrastructure, and IT operations teams to prioritize vulnerabilities based on risk, exploitability, and asset criticality, serving as technical liaison between security and business units.
- Performed incident response and threat analysis including malware payload analysis, email investigation, and network traffic analysis using Wireshark and security tooling to identify anomalous activity and TTPs aligned with MITRE ATT&CK framework.

Information Systems Specialist I 05/2018 — 08/2023

WorkForce West Virginia, Charleston, WV

- Increased cross-functional visibility by 70% across 18 centers statewide through design, implementation, and maintenance of live dashboards and KPIs for IT asset inventory, system usage, and lifecycle tracking.
- Cut ~$150k in costs by designing and deploying in-house systems that streamline software licensing and hardware usage tracking across 18 career centers, improving IT asset visibility, and reducing waste.
- Managed end-to-end IT asset lifecycle workflows (provisioning, de-provisioning, replacements, end-of-life), ensuring alignment with security and compliance standards.
- Served as primary technical point of contact for 18 regional centers, translating complex technical requirements into actionable solutions for diverse stakeholder groups.
- Aggregated data from asset inventory, identity systems, and software licensing platforms to support risk, compliance, and remediation decision-making.

SKILLS

Languages: English (native), Spanish (reading, writing, speaking), Python, SQL, HTML, CSS, Flask, C#, .NET.
Communication: Communication for technical and non-technical stakeholders, collaboration, conflict resolution, training, attention to detail, client outreach.
SIEM & Monitoring: Performed incident response and threat analysis including malware payload analysis, email investigation, and network traffic analysis using Wireshark and security tooling to identify anomalous activity and TTPs aligned with MITRE ATT&CK framework.
GRC & Compliance: Risk assessment methodologies, control implementation and testing, audit evidence collection, access control frameworks (least privilege, SoD, privileged access management), compliance documentation.
Pentesting & Vulnerability Assessment: Metasploit, Nmap, Recon-ng, AMASS, Maltego, Shodan, FOCA, Nessus, Scalpel, FTK Imager, Autopsy, GDB, Binary Ninja/Ghidra, Burp Suite, IDA Pro, Django Security, Container Security, Mobile App Security.
Vulnerability Management & AppSec: Triage and remediation tracking, application security testing, false-positive reduction.

AWARDS & PUBLICATIONS

- J.M. Carter, Y. Makula, D. Sheshappa, S.P. Virigineni, Lightweight Threat Model for Emissary Ingress, Cloud Native Computing Foundation (2026).
- J.M. Carter, C.E. Morris, M.J. Oliver, Addition of Stahl Heater to the Propulsion System Laboratory Simulator's 450lb Airline, NASA Internal Paper (2021).

JARRED M. CARTER

jarredmcarter.com

PROJECTS

Threat Intelligence Investigation: Automated Bot Traffic & Ad Fraud Analysis Spring 2026

- Identified 25.51% automated bot traffic across 126,959 e-commerce sessions by analyzing behavioral signals including interaction timing, ASN infrastructure sources, and device fingerprint reuse.
- Correlated multiple detection signals including datacenter ASNs, headless browser indicators, timezone mismatches, and inhuman interaction speeds to distinguish automated attacks from legitimate user activity.
- Detected bot-driven attacks targeting checkout, login, and product endpoints, revealing patterns consistent with inventory hoarding and credential stuffing campaigns impacting revenue-generating workflows.
- Estimated $3,362–$13,448 in wasted advertising spend by analyzing paid Google and Bing search traffic consumed by automated sessions interacting with marketing campaigns.
- Developed a prioritized mitigation strategy including ASN blocking, device fingerprint detection, checkout rate limiting, credential-stuffing protections, and MFA enforcement to reduce automated abuse and protect customer accounts.

Pentesting and Vulnerability Analysis Project Fall 2024

- Conducted comprehensive penetration testing for NBN Corporation, identifying critical vulnerabilities including Cross-Site Scripting (XSS), SQL Injection, Local File Inclusion, and unauthorized server access, leading to root access on all systems.
- Assessed and scored vulnerabilities using NIST's CVSS Version 3, with an average criticality score of 8.86, highlighting the high risk and immediate need for mitigation.
- Recommended immediate security fixes and mitigations, including sanitization of user input, system updates, enhanced password policies, and implementing microservice architecture to isolate network assets.

Offensive Security CTF Challenges Fall 2024

- Analyzed malicious artifacts and reverse engineered 20+ malware samples using Ghidra and Binary Ninja to identify threat actor TTPs and attack chains.
- Conducted root cause analysis of 20+ security vulnerabilities across memory corruption and application security issues, transforming technical findings into actionable remediation strategies using reverse engineering methodologies and enterprise-grade analysis tools.
- Assessed business impact of web application vulnerabilities through comprehensive security testing, documented detailed analysis and remediation recommendations, and presented findings in formats suitable for both technical teams and senior leadership.

Digital Forensics Final Project Spring 2024

- Analyzed malicious email attachments and reverse engineered 20+ malware samples using Ghidra and Binary Ninja to identify threat actor TTPs and email-based attack chains.
- Investigated phishing and BEC attack vectors, analyzing email headers, attachments, and links to determine maliciousness and attack patterns.
- Conducted threat intelligence analysis by reassembling deleted evidence from 8 system images and correlating findings to identify attack patterns and TTPs.
- Reassembled deleted and obfuscated evidence from 8 system images using Scalpel and FTK Imager for recovery of hashes, user accounts, logs, documents, and metadata to deepen digital evidence recovery insights.
- Identified 80+ functions, libraries, and security vulnerabilities by reverse engineering unknown executables, creating and inspecting forensic images/file systems with Procmon and PeStudio.

Application Security Engineering Projects Spring 2024

- **AI-Ready Security Assessment:** Identified and remediated 4 critical vulnerabilities (XSS, CSRF, SQL Injection, command injection) in Django web application; implemented automated detection rules and established security controls applicable to AI/ML API environments.
- **Mobile App Security:** Conducted security audit of Android gift card application, fixing Intent vulnerabilities, implementing HTTPS encryption for REST API communications, and removing privacy-invasive monitoring code.
- **Container Security for ML Environments:** Secured containerized applications using Kubernetes, implementing automated monitoring with Prometheus and establishing security controls directly applicable to AI/ML model serving environments.
- **Binary Security & Fuzzing:** Identified and fixed 6 buffer overflow and memory corruption vulnerabilities, achieving an 85% + code coverage through systematic case development by performing a vulnerability assessment on legacy C application using AFL++ fuzzer and coverage analysis.
- **API Security & Monitoring:** Implemented comprehensive API security controls and monitoring solutions, establishing foundation for securing AI model APIs and detecting anomalous usage patterns.