Shaunak Peri

(980) 425-8722 | speri0915@gmail.com | https://www.linkedin.com/in/shaunak-peri/ | https://github.com/shaunakperi

EDUCATION

University Of North Carolina at Charlotte — Charlotte, NC
M.S. Computer Science, Cybersecurity — Expected: May 2027
B.S. Computer Science, Cybersecurity — Expected: Dec 2026

TECHNICAL SKILLS & CERTIFICATIONS

Languages
Python, Java, C, JavaScript, Assembly, HTML, CSS, SQL, C++, Bash, PowerShell

Cybersecurity & Networking
Wireshark, Threat Detection, Incident Response, Risk Assessment, Security Analysis, Kali Linux, Ubuntu, Splunk, Metasploit, Nmap, John the Ripper, Event Viewer, Volatility3

Tools & Platforms
VS Code, GitHub, Microsoft Defender, Burp Suite, Word, PowerPoint, Excel, Docker, OpenStreetMap, PostgreSQL, Bash, Kiwix, TileServer GL, Navidrome, tilemaker, Raspberry Pi 5

Operating Systems
Windows 10/11, Linux, Virtual Machines(VirtualBox)

Certifications
Google Cybersecurity Professional, Cisco Introduction to Cybersecurity, TryHackMe Cybersecurity 101, Microsoft Excel

PROJECTS

Offline Cyberdeck
Portable Survival Computing Platform — March 2026

- Architected a containerized service stack using Docker on ARM64 (Raspberry Pi OS), deploying and troubleshooting multiple services, including Kiwix, TileServer GL, and Navidrome in isolated environments
- Demonstrated systems hardening principles by disabling unnecessary services (MySQL, MariaDB) to eliminate port conflicts and reduce attack surface on the host OS
- Diagnosed and resolved container networking failures, port binding conflicts, database corruption from unclean shutdowns, and ARM64/amd64 platform incompatibilities.
- Applied CIA triad principles by ensuring critical reference data remained available (availability), unmodified (integrity), and locally controlled (confidentiality) without reliance on external infrastructure
- Demonstrated incident response skills by recovering from a corrupted PostgreSQL database caused by a power interruption during a live data import

CAPTURE THE FLAGS

Hack The Box | North Carolina National Guard | UNC Charlotte On-Campus CTF
UNC Charlotte – 49th Security Division, Team "49th Cyber Syndicate" — October 2025

- Placed 2nd out of 23 collegiate teams in an on-site Hack The Box CTF hosted by the North Carolina National Guard.
- Collaborated with a 5-member team as part of UNC Charlotte's 49th Security Division.
- Captured 10+ forensic-based flags across multiple domains, including OSINT, reverse engineering, and digital forensics.
- Solved challenges in forensics, AI exploitation, reverse engineering, and web exploitation under strict time constraints.
- Demonstrated strong technical analysis, efficient triage strategy, and SOC-style teamwork in a competitive, time-sensitive environment.

Hack The Box | Holmes CTF 2025 |Blue Team CTF
UNC Charlotte – 49th Security Division, Team "Sherlock's Homies" — September 2025

- Solved 50+ SOC, threat intelligence, and malware forensics challenges in a time-boxed incident response environment.
- Performed log analysis, memory and disk forensics, and malware triage to identify attack paths and root causes.
- Investigated forensic artifacts and network traffic to uncover indicators of compromise (IOCs).
- Applied structured investigative methodology to simulate real-world blue team operations.
- Coordinated with a 5-member blue team to prioritize cases, triage alerts, and maintain high investigative thoughtput under competition constraints.

CAMPUS INVOLVEMENT

49th Security Division | Cybersecurity Club | UNCC College of Computing and Informatics — Feb 2025 - Present
Member

- Completed hands-on labs and technical workshops focused on cloud security, Linux administration, Nmap scanning, reconnaissance techniques, social engineering tactics, and defensive cybersecurity methodologies.
- Participated in cybersecurity competitions, applying practical technical skills in live scenarios while enhancing collaboration, critical thinking, and problem-solving abilities.