Nicholas Broussard

832-397-0710 NBroussard0710@gmail.com linkedin.com/in/nicholas-broussard github.com/P3akyB0y

Professional Summary

Aspiring cybersecurity professional with hands-on experience in security automation, threat detection, and endpoint hardening. Proven ability to script PowerShell-based solutions to enhance system integrity and streamline deployment. Experienced with MDR platforms and security monitoring tools such as Splunk. Strong academic foundation in cybersecurity, complemented by active pursuit of OSCP, and OSWP certifications. Committed to securing infrastructure and mentoring others in blue and red team operations.

Education and Certifications

Sam Houston State University **Sep 2019 – Dec 2024**
Bachelor of Science in Cybersecurity *Huntsville, TX*

CompTIA Security+ (Candidate ID: COMP001022756901) **Mar 28, 2025**
Verification Code: *R4X2HC0QRE4QQKK0* *Verify*

CompTIA Network+ (Candidate ID: COMP001022756901) **Aug 3, 2025**
Verification Code: *GS6ZW1MY71VQQDX2* *Verify*

Offensive Security Certified Professional (OSCP) **Est. Oct 2025**
Offensive Security PEN-200

Offensive Security Wireless Professional (OSWP) **Est. Oct 2025**
Offensive Security PEN-210

Relevant Coursework

- Cyber Warfare
- Information Security
- Malware
- Network Security and Cryptography
- Digital Forensics I
- Digital Forensics II
- Software Engineering
- Data Mining
- Computer Networks

Technical Skills

Security Tools: Metasploit, Burp Suite, Nmap, Wireshark, Blackpoint MDR, Splunk
Scripting & Programming Languages: Python, PowerShell, Ada, Java, SQL, YAML
Infrastructure/Monitoring: Docker, K3s, Helm, Prometheus, Grafana, Active Directory
Operating Systems: Kali Linux, Debian, Windows 10/11, macOS

Experience

Northrock Cybersecurity **Aug 2024 – Present**
IT Security Intern → Field Technician *Spring, TX*

- Developed PowerShell scripts to disable unnecessary services and harden Windows endpoints
- Automated deployment of Blackpoint Snap Defense agents across client infrastructure
- Built a PowerShell-based script to determine Windows 11 upgrade eligibility post-hours using PC Health Check API
- Transitioned client systems from Windows 10 to Windows 11 across multiple environments
- Installed and configured firewalls, switches, and secure APs for client infrastructure enhancement
- Maintained ISO 21007 compliance, customizing security frameworks for large car dealership networks
- Managed GPOs, domain policies, and access control via Active Directory

Online Training & Platforms

TryHackMe: https://tryhackme.com/p/nbroussard0710

Hack The Box: Student ID:HTB-02DE07775B

Projects and Organizations

Intruwatch Host-Based Intrusion Detection System

- Built a Python-based HIDS using Scapy and Pyshark to monitor files, processes, and traffic
- Integrated Matplotlib and NumPy for visual analytics of collected event logs
- Logged alerts and simulated triage scenarios for security incident response

Raspberry Pi Kubernetes Cluster

- Engineered a 3-node K3s cluster using Raspberry Pi to simulate secure microservice infrastructure
- Used Docker for containerization, Helm for app deployments, and Prometheus/Grafana for monitoring

Bearkat Association for Security and Hacking (BASH)

- Co-founded a mentorship program for Digital Forensics students
- Competed in CCDC Regionals with focus on Active Directory and ACL controls
- Participated in HiveStorm CTFs focused on forensic analysis of compromised systems