George D. Smith III

Entry-Level IT/Cybersecurity Candidate | Security Plus Certified

Norfolk, VA • georged.smith4@gmail.com • (757) 839-3592 • LinkedIn[1] • GitHub[2] • ePortfolio[3]

EDUCATION

Old Dominion University — Norfolk, VA
Bachelor of Science in Cybersecurity, GPA: 3.47

CERTIFICATIONS

• CompTIA Security+ (SY0-701) — *f35f2fe77b4f401ab826b641bafc0b8b*
• Offensive Security Certified Professional (OSCP) — *In Progress (July 2026)*
• CompTIA CySA+ — *In Progress (December 2026)*

Work Experience

Information Security - Intern

Chartway Credit Union — Virginia Beach, VA

May 18, 2026 – July 27, 2026

• Utilized Security tools such as Microsoft Sentinel and Qualys for threat hunting, vulnerability scanning, and reporting to other departments
• Integrated connectors to ServiceNow Ticketing service to highlight vulnerable machines that need investigation or remediation.
• Worked with my team members to create documents and policies to define when vulnerabilities need to be escalated into tickets for investigations
• Researched new and upcoming vulnerabilities to stay updated on new threats in the wild.

TECHNICAL SKILLS

Programming: Python, Bash, PowerShell, C++ (foundational)

Operating Systems: Windows 7–11, Windows Server 2025, Kali Linux, Kali Purple, Ubuntu Linux, Metasploitable

Security Tools:
Nmap, Metasploit, Wireshark, Burp Suite, Aircrack-ng, SEToolKit, Gophish, RouterSploit, Wazuh, Security Onion, Fail2ban

Networking:
TCP/IP, Subnetting, VLANs, NAT, Firewall Configuration, Network Segmentation

---

[1] http://www.linkedin.com/in/george-smith-1b62b6295
[2] https://github.com/tsgds05
[3] https://sites.wp.odu.edu/georgesmith/

SECURITY CONCEPTS

• Penetration Testing Methodology (MITRE ATT&CK)
• Incident Response Fundamentals
• Log Analysis & SIEM Monitoring
• Red Team vs Blue Team Operations

CYBERSECURITY PROJECTS

Home Lab Architect & Operator *(2024–Present)*
Designed and maintained a multi-subnet virtual cybersecurity lab simulating real-world red and blue team operations.
• Built segmented networks using OPNSense with firewall rules, NAT, and traffic isolation
• Deployed Windows Server (Active Directory) to test privilege escalation and misconfigurations
• Integrated Wazuh SIEM for log monitoring and detection analysis across endpoints
• Used Security Onion for network-based monitoring and traffic analysis on isolated subnets
• Simulated attacks using Kali Linux and analyzed detection visibility from the defender's perspective

---

Penetration Testing & Offensive Security Practice
Performed controlled penetration testing in lab environments using industry tools.
• Conducted enumeration and exploitation using Nmap and Metasploit
• Practiced privilege escalation and post-exploitation techniques
• Used RouterSploit for embedded device testing
• Simulated phishing campaigns using Gophish and SEToolKit

Penetration Testing Documentation & Analysis (In Progress)
Developed structured documentation of penetration testing activities within a controlled lab environment.
• Recorded reconnaissance, enumeration, and exploitation attempts across multiple target systems
• Analyzed scan results, service behavior, and vulnerabilities identified during testing
• Organized findings into a structured format aligned with penetration testing methodologies
• Built reports that translate technical findings into clear security insights

---

ACTIVITIES

• ODU CyberOps CTF Participant (2024–2026)
• Mid-Atlantic Collegiate Cyber Defense Competition Participant (2026)
• VMI CyberFusion CTF 6th Place Team (2026)
• CNU CyberForge Participant (2026)
• UMGC's MACCDC HTB CTF 3rd Place Team (2026)
• Regent University PLC + Cyber Defense CTF Participant (2026)
• Cyber Skyline National Cyber League Top 30% Individual CTF (2026)
• Cyber Skyline National Cyber League Top 22% Team CTF (2026)