GRANT SMITH

Boston, MA 01810 | 978-973-0262 | grantsmith@vt.edu | Linkedin.com/in/grant-smith-129240199/

Security Engineer | Penetration Tester

Highly collaborative and goal-oriented IT professional with over 6 years of experience optimizing hardware and software design, installation, administration, configuration, and penetration testing to strengthen business impact. Thorough understanding of network protocols, data on the wire, and system security vulnerabilities. Proven analytical and problem-solving skills with a keen ability to assess needs, define requirements, and develop value-added solutions. Utilize modern tools to meet the needs of a dynamic and continuously changing enterprise environment.

CORE COMPETENCIES

Binary Exploitation | System Design | System Security | Reverse Engineering | Open-source intelligence (OSINT) | Web exploitation/API Hacking | Networking | Python Scripting | Program Management | Reconnaissance | Administrative Task | Record Management | Leadership & Collaboration | Coaching | Excellent Communication Skills

PROFESSIONAL EXPERIENCE

ASSOCIATE SECURITY ENGINEER INTERN – RED TEAM | The Walt Disney Company, Burbank, CA | May 2022 – August 2022
- Assisted with anti-virus evasion, active directory exploitation, open-source intelligence (OSINT), web exploitation, red teaming, command and control (C2) penetration testing, application programming interface (API) hacking, etc.
- Identify, troubleshoot, and resolve issues with the systems, servers, hardware, applications, and software.
- Assist with attacking all aspects of the company's network and computer security, including local area networks, wide area networks, virtual private networks, routers, firewalls, and other related network equipment.

ASSISTANT MONTEREY PHOENIX THREAT MODELING COACH | Naval Postgraduate School, Virtual | Jul 2020 – Aug 2020
- Scheduled and oversaw practice sessions, kept training modules up-to-date, and organized team activities.
- Supported the lead professor and handled administrative tasks.
- Provided training instruction, inspiration, and advice to students to prepare them for real world threat modeling.

INTERN | National Security Agency & Naval Postgraduate School, Virtual | Jun 2020 - Jul 2020
- Contributed to creating and rolling out a comprehensive strategy to safeguard the communication chain between drones, operators, and weapon systems.
- Presented findings to senior leadership that created impact on the way the DOD handles autonomous drones and weapon systems.
- Identified, explored, and assessed potential software and service solutions for internal usage; offered a good matrix, if feasible, listing the features of each application or service.

INTERN | US Army Cyber Command, Virtual | Jun 2020
- Contributed to creating custom exploits for embedded systems.
- Conducted security testing to identify vulnerabilities; kept up with shifting best practices and potential dangers in information technology security.
- Learned about the internal structure of Cyber Command and how teams integrate with one another.

TECHNICAL SUPPORT SPECIALIST | American Graphics Institute, Woburn, MA | May 2016 - August 2020
- Served as the company's first point of contact with employees, documenting their concerns, identifying their causes, and keeping them apprised of developments.
- Contributed to the quality assurance testing of newly designed and implemented procedures and upgrades inside, ensuring client satisfaction by listening carefully to personal needs and developing bespoke solutions.
- Completed the setup, maintenance, and upgrading of over 80 systems in three office locations.

EDUCATION

BACHELORS IN CYBERSECURITY MANAGEMENT | Virginia Tech | Blacksburg, VA | Ongoing

CERTIFICATIONS

Web Application Penetration Tester (EWPT) | eLearnSecurity, August 2022
Certified Ethical Hacker | Practical (CEH), EC-Council, April 2022
Junior Penetration Tester (EJPT) | eLearnSecurity, December 2021

TECHNICAL SKILLS

Microsoft Office (Word, Excel, PowerPoint, Outlook), Nmap, Metasploit, impacket, Active Directory, Phishing, Red teaming, Penetration testing, Web exploitation, API hacking, Python, Bash, Linux, Windows, MacOS, Networking, Defense evasion, Physical security testing