JOSHUA SMITH

Email: smithjk[at]infosecworx [.]com | LinkedIn: https://bit.ly/3aaP8YU
Twitter: @n0hats

ABOUT ME

A seasoned Information Security professional with over a decade of experience, I specialize in Cyber Forensics, Penetration Testing (both offensive and defensive), and Security Engineering. Currently honing my skills on platforms like Hack the Box and TryHackMe, I am dedicated to staying at the forefront of the evolving threat landscape.

SKILLS

KNOWN FRAMEWORKS AND TOOLS

Tcpdump / Splunk / DirBuster / frogger / Pacu / EtterCap / BetterCap / Nikto / Zap / Kali / WireShark / Nmap / MassScan / Recon-ng / SQLMap / GoBuster / NipperStudio / VMWare ESXi / VMware WS / BurpSuite Pro / Docker Containers / Active Directory / Metasploit Framework / PowerShell Empire / Cobalt Strike / TheHarvester / W3AF / CentOS / Penetration Testing and Execution Standard (PTES) / Information System Security Assessment Framework (ISSAF) / Open Source Security Testing Methodology Manual (OSSTMM) / Open Web Application Security Project (OWASP) / Smartphone Pentest Framework / HP ArcSight / ScoutSuite / Encryption Technologies / Unix and Windows / Ollydbg / IDAPro / Ghidra / Autopsy / gdb / ChatGPT/ PowerShell

LANGUAGES

Python / Bash / VBScript / Powershell / Ruby on Rails / .NET / Java / Perl

CLEARANCES

Top Secret with Poly – Expired

EXPERIENCE

SECURITY CONTENT ENGINEER
Sept 2020 – Present

DEVO Technology, Inc.

- Researched exploits, gathered logs, and identified signatures to generate alert content for the SIEM
- Developed a Flask-based Python application to streamline the detection creation process for the team, automating the input of relevant information and outputting the necessary files for ingestion into Devo
- Wrote PowerShell scripts to execute atomic tests individually or collectively, enhancing the team's capabilities
- Gathered requirements from stakeholders and prioritized tasks for the team, ensuring the timely delivery of critical security products
- Presented a talk at KubeCon 2022 on augmenting the analyst and sharing expertise in the security research field
- Crafted an extensive array of detections for various CVEs, showcasing a proficiency in identifying and mitigating vulnerabilities through strategic and effective security measures.

SENIOR SECURITY CONSULTANT
Dec 2019 – March 2020

Syntasa Corporation

- Improved overall security posture of the organization using tools like Wireshark, Nessus, BurpSuite, VMware and others
- Worked closely with team members to improve processes and procedures which, when implemented, improved productivity
- Translated very technical reports to non-technical management
- Provided guidance to external group on setting up their penetration testing team

CONTAINER SECURITY SPECIALIST
Sept 2019 – Dec 2019

Ingenium Consulting, LLC

- Launched an Enterprise wide container registry
- Deployed docker containers Enterprise wide
- Collaborated with external groups to understand and implement requirements
- Presented final solution to senior leadership and gained approval
- Mentored junior team members

SENIOR PENETRATION TESTER
March 2016 – Sept 2019

Pathoras / ProAptiv Corporation

- Performed penetration tests against the clients VoIP system
- Mentored junior employees by regularly training and providing career guidance
- Assessment of multiple cloud (AWS, GCP) and operating systems (Linux, Solaris, Unix or Unix-like operating systems, Windows, etc..) to perform full scope security assessments of information systems
- Experienced use of Kali Linux, Metasploit, NMAP, and other commonly used information security tools and finding undocumented functionality or exploitable vulnerabilities in all technology systems
- Provide systems security engineering advice & assistance to programs throughout the System Development Lifecycle (SDLC)

- Coordinating activities with other U.S. IC components & teams; briefing senior government officials regarding the results of formal requirements validation testing
- Operations with manual and automated exploit techniques and tools to include reverse engineering and disassemblers in a multi-vendor, high-energy joint team environment
- Testing of Cross-Domain or Multi-Level Security Solutions, Trusted Solaris and/or Trusted Extensions, Linux and SELinux, Windows, Cisco, Web Technology, Firewalls, Intrusion Detection Systems, Encryption, Network Security, PKI , Network and Systems Engineering, and Oracle
- Technical evaluations of information systems, to include comprehensive vulnerability assessments and/or penetration testing
- Ability to read or evaluate XML, Python, HTML, PERL, JAVA, and C++
- Web application assessments using Burp Suite, Web Inspect, OWASP top ten, ZAP

SENIOR CYBER DEFENSE SPECIALIST
Aug 2011 – Mar 2016

Mantech International

- Stood up the CIRT teams first computer forensics/malware reverse engineering lab
- Helped to improve technical capabilities of the CIRT team
- Transitioned a critical web application from Python to Ruby on Rails
- Selected to provide Mobile device imaging training to external organizations
- Assisted with mobile device exploitation
- Completed more than 100 highly sensitive network security penetrations on behalf of government organizations
- Performed Wireless attacks using the aircrack suite and the Metasploit Framework
- Completed both static and dynamic malware analysis using IDA and/or Virtual Machines
- Provided mentorship to team members to help improve teams capabilities
- Worked closely with Senior leadership to gain the confidence needed to complete sensitive projects
- Worked with multiple different groups and organizations to ensure project success

LEAD CYBER FORENSIC SPECIALIST
July 2009 – Aug 2011

BAE Systems Inc.

- Authored a large and complex EnCase EnScript that improved overall productivity by 80%
- Discovered an artifact during forensic evaluation that gained recognition throughout the team and was briefed to Senior Leadership

INFORMATION SYSTEMS SECURITY OFFICER
Nov 2005 – July 2009

Perot Systems Government Services Inc.

- Worked with different groups to help educate teams on the importance of designing and building a secure system
- Quickly gained recognition as a problem solver and moved to a more senior position

EDUCATION

GEORGE MASON UNIVERSITY
Jan 2003 – Jan 2008

Fairfax, VA
B.S. / Information Technology