Bhavik Shah

(781) 921-9780 | bhavikshah28699@gmail.com | LinkedIn | GitHub

EDUCATION

University of Maryland — **College Park, MD**
M.Eng., Cybersecurity. GPA 3.86 — *Aug 2022 - May 2024*

Vellore Institute of Technology (VIT - Campus Amaravati) — **Andhra Pradesh, India**
B.Tech., Computer Science with Specialization in Network and Security. CGPA 3.91 — *Aug 2017 - May 2021*

TECHNICAL SKILLS AND RELEVANT COURSEWORK

Certifications: eJPT, (ISC)2 Certified in Cybersecurity (CC), ICSI Certified Network Security Specialist (CNSS), CompTIA Security+ (In Progress)
Programming and Tools: Burp suite, Wireshark, Autopsy, Metasploit, Nmap, Nessus, MSFVenom, Hashcat, SQLmap, Hydra, Nikto, Gobuster, Microsoft Office Suite, John the Ripper, VMWare Workstation, Python, HTML, CSS, JavaScript, SQL
Other Skills and Relevant Coursework: OSINT, Linux, Firewalls, Network Security, NIST, AWS, SIEM, OWASP, Vulnerability Assessment, Git, Cloud Security, Information Assurance, Penetration Testing, Digital Forensics, Incident Response, Computer Networks

WORK HISTORY

ZS Associates, Business Operations Associate — **Pune, India**
Feb 2021 – Jul 2022

- Developed first draft of NIST-compliant training materials and presentations for a project, extensive study of NIST cybersecurity framework enabled creation of user-friendly content, driving a 30% increase in compliance levels.
- Incorporated data analysis and reporting skills to optimize goal-setting processes, resulting in a 40% increase in reps achieving target.
- Leveraged SQL proficiency to set up automated generation of goal-setting and sales reports for multiple products in the company's proprietary tool, decreasing time taken by 2 days.
- Produced comprehensive presentations for 4 product lines that presented in-depth sales data, growth insights, and market trends from the previous quarter; tailored content to ensure client-friendly format for easy understanding and decision-making.
- Mentored 3 new team members, identified process inefficiencies, and implemented solutions that led to a 15% improvement in operational efficiency.

RELEVANT EXPERIENCE (PROJECTS)

Digital Forensics Investigation Project

- Led a detailed investigation into a breached Windows virtual machine, leveraging disk imaging, memory analysis, and network packet capture techniques. Uncovered 4 key vulnerabilities and promptly applied patches to bolster cybersecurity measures and thwart potential threats.
- Executed a comprehensive analysis using Autopsy, FTK Imager, Wireshark, and CyberChef, leading to a detailed report for legal purposes, enhancing case understanding and enabling data-driven decisions.

Security Solutions Proposal Project

- Spearheaded a comprehensive assessment of security risks and assets based on the NIST Cybersecurity Framework and NIST SP 800-61 guidelines.
- Proposed 2 NIST-aligned security solutions, including on-premises and cloud-based options, to address identified vulnerabilities and ensure business continuity.

Vulnerability Assessment and Security Enhancement on AWS

- Performed a comprehensive vulnerability assessment on an AWS-based web application using Prowler, identifying 34 vulnerabilities across 6 broad areas like Data Security, EC2, Network Security and Logging.
- Proposed and implemented security controls, including S3 and EC2 security features, AWS GuardDuty, AWS WAF, AWS CloudTrail, CloudWatch and Amazon Macie resulting in a 70% reduction in potential security threats.

Capture the Flags

- Participated in Capture the Flag (CTF) competitions through ctftime.org and completed hands-on cybersecurity challenges on TryHackMe and HackTheBox, reaching top 1% on TryHackMe platform.
- Demonstrated proficiency in penetration testing, cryptography, OSINT, and steganography using advanced security tools, including Burp Suite, Nmap, Wireshark, Hydra, Shodan, exiftool, steghide, Metasploit, John the Ripper, and SQLmap.

ACTIVITIES AND AFFILIATIONS

Publication in Open Source for You (OSFY) Magazine, Apr 2020

- Wrote an article on introduction to Snort IDS and utilization of Snort in the world of cybersecurity.