Nitav Shah

Philadelphia, PA 19104
443-947-0663 shahnitav@gmail.com linkedin.com/in/nitavshah github.com/shahnitav nitav.me

Education

University of Maryland **Aug 2021 – May 2023**
Master of Engineering in Cybersecurity, GPA: 3.93 *College Park, MD*

Navrachana University **Aug 2016 – June 2020**
Bachelor of Technology in Computer Science and Engineering, CGPA: 8.67 *India*

Certificates

- CompTIA Security+ SY0-601 - CompTIA
- Investigation Theory - Applied Network Defense

Experience

Susquehanna International Group **Jul 2023 – Present**
Security Engineer *Bala Cynwd, PA*

- Responding to security incidents monitored using SIEM/EDR, coordinating a cohesive response for escalated incidents involving in-depth analysis, containment, and remediation.
- Write new detections in the SIEM for the rapidly changing threat landscape by following current security trends, advisories, publications, and research.
- Deployed and manage log integration to QRadar SIEM using WEC, Sysmon, WinCollect from thousands of workstations and servers across more than 4 global sites.
- Architectured scanning and vulnerability management using Tenable.sc & NMap to reduce the external attack surface.
- Developed a custom SOAR web application that performs queries, gathers intel, gets relevant information from the security stack, and provides custom workflows after an incident to help analysts investigate.
- Monitor for sensitive data leaving the environment using Forcepoint DLP while fine tuning it to reduce false positives.
- Automate, store, and maintain Threat Intelligence feeds and use them for threat hunting across the environment.

University of Maryland **Jun 2022 – May 2023**
Graduate IT Assistant *College Park, MD*

- Triage incoming tickets and provide technical support by resolving the incidents.
- Developed PowerShell scripts to automate system administration tasks reducing the ticket response time by 100%.

University of Maryland **Jan 2022 – May 2022**
Teaching Assistant *College Park, MD*

- Partnered with Prof. Nirupam Roy to implement suitable lessons for CMSC417-Computer Networks for 70 students.

Syncron **Jul 2020 – Jul 2021**
Software Engineer *Bangalore, India*

- Incorporated scripts using Python and Golang to automate QA Testing and perform Functionality and Load Testing.
- Utilized AWS Codepipeline & Codebuild to provide a CI/CD solution that runs builds and generates reports.
- Lead the development of a cross-platform Chatbot using Golang and Python Boto3 library to carry out DevOps task on AWS Infrastructure from Microsoft Teams Bot Framework.

Projects

Homelab | *VMWare, pfsense, Kali Linux, Windows Server, Splunk, VLAN* | Project Link **June 2022**

- Built and maintain a lab to test, upskill, and maintain an enterprise-grade environment.The lab uses a Hypervisor, Pfsense, Security Onion, Splunk, Windows Server, Metasploitable machines, Kali Linux Attacker and more.

Go Port Scanner | *Go, Network Scanning* | Project Link **April 2022**

- Developed a Port Scanner that uses multi-threading to scan multiple ports/hosts simultaneously using goroutines.

Advanced Exploitation Techniques for x86 Architecture | *GDB, Assembly* | Project Link **December 2021**

- Used problem solving and reverse engineering to find the exploits for 10 binaries with ASLR turned on by exploiting vulnerabilities using Heap Buffer Overflows and Return Oriented Programming.
- Created shellcode & deduced the NOP Slide required to overwrite the return address to point to the heap or bss regions.

Penetration Test | *Privilege Escalation, Threat Hunting, Vulnerability Analysis* | Project Link **December 2021**

- Discovered exposed cloud credentials, configuration flaws and unpatched systems exploitable with critical CVE.
- Adapted a security posture improvement response strategy with guidelines to deploy security controls & policies.

Technical Skills

Languages: Python, Go, C, HTML/CSS, JavaScript, SQL, C#, Bash, PowerShell
Scanning: Nmap, Wireshark, Nessus Tenable, GDB, QRadar, Splunk, SOAR, Firewall Configuration, RBAC
Exploitation: Burpsuite, Metasploit, MITRE ATT&CK, Penetration Testing, Detection Engineering
Technologies: AWS, Linux, Docker, Git, OAuth, LDAP, Azure, Cloud Infrastructure, TCP/IP, DNS, Active Directory
Security: Incident Response, Forensic Analysis, Vulnerability Management, DLP, NIST CsF, ISO 27000, Security Controls