Shubham Verma

https://github.com/smoo4h
https://www.linkedin.com/in/smoo4h

Rochester, New York
+1 585-290-2582
sv4168@rit.edu

Education

Rochester Institute Of Technology - RIT Aug. 2022 – May 2024
Master's in Cybersecurity *Rochester, NY*

Indian Institute of Technology - IIT Roorkee Aug. 2016 – July 2020
Bachelor of Technology in Electronics and Communication *Roorkee, India*

Skills

Interests: : Offensive Security | Data Security | Malware Analysis | Enterprise Security | Data Loss Prevention | Security Operations
Languages: : Python | Javascript | C++ | SQL | Java
Tools: : IDA Pro | PEBear | Cobalt Strike | Metasploit | PE Studio | Burp Suite | Wireshark | Cisco Packet Tracer | Snort | OWASP ZAP | Checkmarx | Veracode | SonarQube | Jenkins | Cuckoo Sandbox | Symantec DLP | Forcepoint | Security Onion | Aircrack-ng
Core Competencies: : Vulnerability Assessments | AWS | Exploitation frameworks | Web security testing | Secure Software Development
Certifications: :AWS Certified Solutions Architect - Associate | OSCP (pursuing) | TryHackMe | Hackthebox
Clubs: : RITSec | BSides Buffalo | Rochester Security Summit

Experience

Navy Federal Credit Union Feb. 2024 – Current
Application Security Engineer *Vienna, VA*

- Supported development teams with secure code reviews and other assessments to identify security weaknesses and vulnerabilities. Currently supporting 200+ development teams.
- Experience with various security tools in SAST, DAST, IAST, SCA.

Amgen May. 2023 – Aug 2023
Security Engineer GRAD Intern *Thousand Oaks, California*

- Developed Security Automations for controls on Gen AI-related tools for domain filtering and domain identification. Resulted in catching 50+ hidden domains in Gen AI apps.
- Implemented a robust Risk Management Framework to systematically measure, analyze, and mitigate risks arising from the integration of Gen AI tools with organization-owned data.

Societe Generale 2019 – 2022
Security Software Engineer - FullStack *Bengaluru, India*

- Conducted secure code reviews using tools such as Sonarqube, identifying and addressing an average of 15 potential vulnerabilities per code review.
- Demonstrated expertise in delivering software through DevOps practices, including CI/CD and automated testing, resulting in a 50% improvement in software deployment efficiency.
- Implemented alerting and monitoring systems, leading to a 80% reduction in system downtime and enhancing overall system reliability.
- Conducted penetration tests for an e-commerce platform, utilizing tools like Burp Suite and Checkmarx. Uncovered and successfully remediated a critical SQL injection vulnerability, resulting in a 30% improvement in overall system security assessments.
- Implemented and maintained robust security monitoring systems to detect and respond to potential security threats and vulnerabilities. Utilized SIEM (Security Information and Event Management) tools to analyze and correlate security events for proactive threat detection.
- Worked on project based on Event-Driven Architecture used for instant and safe transfer of encrypted JSON data. Worked on transfer from Event Producers to 5000+ Event Consumers through Event Router
- Programmed microservices for specific tasks like adapting data from UI(Angular) which involved streaming of messages in queue hence improving user experience, communication between the event router and Consumer/Producer which decreased the response time of application by 50%.
- Collaborated with cross-functional teams to develop and implement offensive security strategies, utilized offensive security tools, including Cobalt Strike and Empire, to assess and enhance the security posture of critical infrastructure.

Societe Generale May. 2019 – July 2019
Software Engineer - Intern *Bengaluru, India*

- Developed an onboarding web application for the DevOps platform which provided company-wide users to easily configure and access DevOps tools
- Reactjs and Spring framework was used for the development of the web application. MongoDB, a non-structured database was used as a database for the web application.

Projects

Meterpreter: Meterpreter from scratch using C++, python and flask using C2 (Command & Control) Infrastructure. Consists of three parts CLI, Server and Implant. Offers almost all the functionalities as meterpreter.
YARA-rule-generator: Tool that can generate YARA rules given a set of malware samples using machine learning methods. These generated rules could further be used to identify and successfully detect similar malware.
Advanced Keylogger: This keylogger is capable of recording all the keyboard and mouse input and mailing all the data recorded.By using an arbitrary keymap with human-friendly names, it translates the machine keys to something that the user can understand.
IoT enabled PSG machines: Using the Internet of things to get Polysomnography machine machines to transmit data wirelessly to internet servers and devices. Detecting and analyzing data to predict any anomalies.
Malware Sandbox: Malware analysis lab using REMnux, an open-source Linux toolkit for reverse engineering and malware analysis.
Deep Learning Applications in Railway Health Management: Railways Tracks were detected in images taken from the drone camera.Curves, coupling, detachment of broad gauge railway track was detected. Width was determined at several pixels in images. Resulting widths were then compared with the ideal width to check for defects.

Papers

Covert Channel using HTTP Headers : We have utilized "User-Agent" string to transmit our covert message with the help of the Cookie header, another HTTP header. The idea is to transmit covert messages character-wise by mapping the character value to a legitimate User Agent String and storing information regarding the covert channel inside the Cookie field.
Organizational Cybersecurity Evaluation : Evaluation of a real-time large enterprise. The evaluation included vulnerabilities found using Open Source Intelligence, Controls required to mitigate the vulnerabilities, and the total budget required to implement the controls.
Trusted computing in Mobile Network: aim to contribute a detailed survey about how trusted computing has evolved over the years and provide ways to implement trust and security in mobile communication networks starting from 3G, to 5G.