Rashi Sharma

rashi18@gmail.com | Phone: +1 (240) 927 7077 | USA | LinkedIn | Project Portfolio: https://rashisharma18.github.io/

PROFESSIONAL SUMMARY

Committed Cyber Security graduate student with professional experience in Threat Intelligence and Threat Hunting, backed by a strong foundation in Software Engineering. Proficient in thoroughly analyzing, communicating, and remediating security threats and conducting comprehensive penetration tests. Seeking an opportunity to contribute my skills and knowledge to dynamic and innovative teams.

EDUCATION

University of Maryland — **College Park, Maryland**
Master of Engineering (M.Eng.) in Cybersecurity *(GPA: 3.94/4.0)* — August 2022 - May 2024
Coursework: Hacking with C and Unix Binaries, Networks and Protocols, Cloud Security, Secure Software Coding and Tools, Network Security, Security Tools for Information Security, Penetration Testing, Digital Forensics and Incident Response, Reverse Engineering**,** Information Assurance

PES University — **Bengaluru, India**
Bachelor of Technology (B.Tech.) in Electronics and Communication Engineering (Major) — August 2016 - May 2020
Computer Science Engineering (Minor)
Coursework: DSA, Computer Networks, Database Management Systems, Computer Architecture and Design, Operating Systems, Internet of Things

WORK EXPERIENCE

First American Title Insurance Company — **Remote, Maryland**
Graduate Intern, Information Security: Cyber Threat Intelligence and Threat Hunting — June 2023 – Present

- Mitigated and remediated security threats using Rapid7 IntSights at an average of 20 threats per day.
- Improved threat detection accuracy by re-evaluating and reconfiguring the threat monitoring tool across 6 distinct categories.
- Completed over 10 threat-hunting projects, conducting log and code analysis using Splunk, Microsoft Defender, Qualys, ServiceNow and Tanium.
- Reported weakly threat-hunt findings, presented them to relevant stakeholders, and assisted them with first-response remediation efforts.
- Researched, curated, and communicated Security Advisories and corresponding risk assessments to over 25 non-connected business units.
- Implemented an upgraded communications strategy to tabulate and monitor active vulnerabilities across the organization efficiently.

Hewlett Packard Enterprise, Software Operations, India — **Bengaluru, India**
Systems/Software Engineer, Networking — August 2020 – August 2022

- Developed, executed, and debugged test scripts for validated environments reducing manual test effort by 60%.
- Increased efficiency and accuracy of existing automation scripts from 40% to 90-98%.
- Qualified the team for primary Regression Testing, by overseeing reporting, analysis, and technical documentation of test results and automation scripting bugs.
- Troubleshot, and maintained the sanity of the 4 testing environments, including periodical triage, patching, hardware updates, network configuration, and TCP/IP traffic flow analysis using Wireshark.
- Supervised comprehensive source code reviews for automation scripts, providing critical insights and feedback based on thorough analytics to enhance performance and ensure the seamless operation of 9 test systems.

PROJECTS

Penetration Testing of Windows Information System — **University of Maryland**

- Exploited a system of 4 vulnerable Windows machines, Ubuntu Servers, and AWS Cloud resources using Metasploit, Brute Forcing Tools, and Privilege Escalation techniques.
- Outlined 10+ specific vulnerabilities with severity classification and proposed strategic security solutions in a comprehensive technical report.

Complete Forensic and Malware Analysis of Windows Image — **University of Maryland**

- Leveraged Autopsy and Wireshark to analyze memory images, obfuscated malicious code, and traffic to conduct vulnerability assessments and create reports detailing the cyber-attack.
- Utilized encryption software VeraCrypt to decrypt the extracted malware and proposed 5 recommendations to increase security posture.

Offensive and Defensive Analysis of Lockheed Martin Kill Chain — **University of Maryland**

- Deployed a vulnerable network infrastructure of 3 servers using AWS Virtual Private Cloud and performed extensive Threat Modelling of the Network by a new Microsoft Threat Modelling Tool Template to integrate AWS and Client-Server Threats, using the STRIDE Framework.
- Analyzed the offensive and defensive techniques of the 7 steps of Lockheed Martin Kill Chain on the System.

Penetration Testing and Vulnerability Scanning of Web Application on Linux Systems — **University of Maryland**

- Performed end-to-end Vulnerability Scanning and Penetration Testing of an Apache Web Application Server.
- Exploited SQL Injection, Command Injection, and File Upload Vulnerabilities and found 6 concrete security vulnerabilities.

Cloud Migration of on-premises Web Server using AWS — **University of Maryland**

- Outlined a migration plan and web-server architecture using Amazon Web Services to combat 5 high-priority security issues such as DoS.
- Deployed a Proof of Concept for the proposed solution by porting the code to 8 AWS resources and reinforcing security requirements.

SKILLS

Programming Languages: C/C++/C#, Python, Perl, Bash, Java, JSON, HTML, PowerShell, PHP, JavaScript, CSS, IoT
Tools/Frameworks: Git, GitHub, Jenkins, Robot Framework, PyTest, Wireshark, Docker, MySQL, PostgreSQL, REST API, Firewalls, ISO Framework, BurpSuite, IDA Pro, Ghidra, Kali, VMWare, Splunk, Jira, ServiceNow, MITRE ATT&CK Framework, VeraCode, NMAP, NIST, Nessus.
Security Knowledge: Ethical Hacking, Risk Management, Access Control, Secure Development/Testing, OWASP Top 10, Penetration Testing, Vulnerability Scanning, Forensic Analysis, Reverse Engineering, Firewalls, Intrusion Detection/Prevention Systems, Proxies, Web Applications.
Public Cloud Platforms: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)
Operating Systems: Linux, Windows, macOS, Command Line Interface.
General Technical Knowledge: Data Structures and Algorithms, Application Testing, Agile Software Development Lifecycle (SDLC), TCP, IP, OSI.