Harsha V

v.harsha.sagar006@gmail.com | Denver, Colorado. | linkedin.com/in/harshasagar6

EDUCATION

Master of Science (MS), Information Systems *Jan 2023 – Present*
Indiana Wesleyan University

Master of Science (MS), Information Systems *Aug 2022 – Dec 2022*
University of Colorado Denver

PROJECTS

SOC Analyst Home Lab

- Created a personal Virtualized SOC home-lab using VirtualBox. Played the role of both a cyber security attacker and defender.
- Configured a C2 (command and control) server using Sliver and dropped a C2 payload on a victim machine (i.e. the Windows VM).
- Simulated attacks with Kali Linux against Windows environment and reviewed network traffic to generate alerts for attacks, harden environment, and write analysis of findings.
- Deployed Splunk to monitor a Windows environment including workstations and an Active Directory server.
- Analyzed telemetry and EDR (endpoint detection response) using Sysmon and Wazuh to detect (and defend) against Sliver.
- Perform analysis of potential phishing emails by investigating emails sent to my personal email address. Investigated email headers, sender domain and IP reputation, and attached links in a sandbox environment.
- Conducted malware traffic analysis using Wireshark, identifying malicious network activity, and enhancing threat detection capabilities.
- Engaged in coursework and participated in Capture the Flag (CTF) challenges on TryHackMe platform, developing practical cyber security skills and enhancing knowledge in offensive and defensive techniques.
- Skilled in identifying and understanding cyber adversary tactics, techniques, and procedures (TTPs). Proficient in researching and writing reports on cyber actors and their ecosystems.

EXPERIENCE

Risk Investigator, **Amazon Development Center, India Pvt. Ltd** *Aug 2019 – July 2022*

- Collaborated with incident response teams, demonstrating goal-driven and curious attitude, leading to a 15% reduction in incident resolution time.
- Conducted thorough threat detection, monitored, and analyzed security incidents, showcasing a self-starter approach to contribute to proactive cybersecurity practices. Provides analysis during investigations, identifying adversarial activity and methods for future detection and prevention.
- Applied cybersecurity analytics for monitoring, identifying patterns, and providing insights into potential risks, emphasizing a flexible approach in a dynamic environment, resulting in a 25% improvement in incident detection.
- Collected and analyzed diverse IOCs using innovative methods, showcasing a unique perspective in information gathering.
- Ensured protocol compliance and stayed updated on industry best practices, showcasing a detail oriented and analytical mindset for a more secure complex environment.

Security Engineer, Intern, UrbanRaptors *July 2018 – May 2019*

- Implemented a range of security products including firewalls, URL filtering, information security, and virus protection, fortifying organizational defenses against criminal cyber threats.
- Employed hands-on experience with Web Application Firewalls and attack mitigation techniques, mitigating potential security risks and ensuring robust defense mechanisms.
- Conducted vendor risk assessments, understanding the threat landscape related to vendors, and ensuring security standards were met throughout the supply chain.
- Created and ran routine reports and data analytics in Excel and Tableau, auditing and validating data/reports to inform decision-making and drive security improvements.
- Played a key role in threat modeling, secure code review, risk analysis, design/architecture reviews, penetration testing, and SOC maintenance, ensuring the security of systems and applications throughout the development lifecycle.

University Network Admin, Intern, Vignana Bharathi Institute of Technology *Jan 2018 – May 2018*

- Accomplished the installation, configuration, and maintenance of the organization's LAN/WAN infrastructure and workstations, showcasing proactive problem-solving and collaborative prowess in a dynamic team environment.
- Mastered core network and security components, including routers, switches, and firewalls. Implemented advanced IP address management techniques for optimized network performance.
- Successfully deployed internal network services, streamlining operations. Developed foundational understanding of IPSec and SSL VPN technologies, supplemented by practical Python programming skills for automation.
- Accomplished installation, maintenance, and administration of storage area network servers within a VMware environment, optimizing data storage and retrieval capabilities to meet organizational needs.

Technical Skills

- **Programming Languages**: C, Python, Perl, PowerShell.
- **Scripting Languages**: AngularJS, HTML, JavaScript, XML, jQuery.
- **Other Skills**: Threat Analysis, Network Security, Penetration Testing, Tableau, Rest, NodeJS, CSS, Git.
- **Frameworks**: MITRE ATT&CK, Cyber Kill Chain Frameworks, OSNIT framework and OWASP.