RISHAB KHARIDHI

Phone: 323-524-3506 / 720-569-5152 **Email:** rishab.kharidhi@gmail.com **LinkedIn:** linkedin.com/rishab-kharidhi **GitHub:** rishabkharidhi

WORK EXPERIENCE

Security Engineer Aug 2020 – Present
Securonix Jersey City, NJ

- Spearheaded high-pressure POCs that were responsible for about 20% increase in the team's revenue.
- Improved time efficiency by 50% in preparation and maintenance of POCs by automating and scripting tools.
- Collaborated with cross-functional teams to create end-to-end MITRE ATT&CK compliant threat models and policies, consulting client security teams to audit quality and maintain endpoint regulatory requirements.
- Strengthened privacy and compliance through data masking, implementing RBAC controls and integrating SAML on POCs for authentication and authorization services.
- Performed initial event triage and threat hunting by adopting STRIDE methodology to detect and document security incidents for client corporations on firewalls, corporate networks etc. to mitigate their security risks.
- Designed and set up 800+ use cases on average per POC to demonstrate anomalies such as beaconing, enumeration, insider threat, account misuse, credential sharing, endpoint malware, fraud, etc.

Threat Research and Development Intern May 2019 – Dec 2019
Webroot, An Open-text company Broomfield, CO

- Reverse engineered malware and analyzed x86 windows binaries statically and dynamically in sandboxes.
- Developed 3 modules for a threat engine for YARA file scanning, PE file disassembly and APK decompilation.
- Reduced human effort by 30% containerizing dependencies using Docker for a threat engine built by the team for a research project to reproduce consistent and scalable builds.

PROJECTS

Web Application Security and Development: *Independent Study*

- Performed threat analysis of a lab-based web application and executed cross-site scripting, SQL injection, request forgery, and DoS attacks. Built a small content management system in PHP, SQL.
- Have been involving in CTFs and hacking challenges weekly on websites such as tryhackme, ctftime etc.

Software Exploits, Anti-RE detection and Mitigation: Nov 2019

- Analyzed windows and Linux applications to evaluate vulnerabilities and constructed scripts to exploit functions in C to perform overflow attacks. Used IDA & IDA Python to detect and mitigate anti-re techniques.

Linux Systems Administration: Mar 2019 – April 2019

- Set up a small corporate network for 20 employees on Linux machines, configuring DHCP, DNS, and web servers with backups and implemented stateful firewalls incorporating defense in depth.

Forensic Data Carver Tool: Mar 2019

- Developed a Python tool to aid in forensic analysis to extract and recover files from within a filesystem hex dump. The tool implemented finite state machines and improved upon the efficiency of existing tools by 8%.

EDUCATION

Master of Science, Cybersecurity: University of Colorado Boulder, CO GPA: 3.9/4.0 May 2020
Graduate Teaching Assistant – Penetration Testing Jan 2020 – May 2020
Graduate Teaching Assistant – Digital Forensics Aug 2019 – Dec 2019
William E. Rapp Fellowship Award for Cybersecurity Aug 2019

TECHNICAL SKILLS

Cryptography: Symmetric and Asymmetric encryption, Digital Certificates, Hashing, PKI, Stream and Block Ciphers

Application Security: Threat Modelling, STRIDE, OWASP Top 10, NIST Framework, Mitre ATT&CK Framework

Network Protocols: TCP, IP, TLS, IPSec, DHCP, DNS, HTTPS, VPN, Firewalls

Programming/Scripting Expertise: Python, PHP, C, C++, SQL, HTML, x86, Java, Bash/Shell, PowerShell, Golang

Tools: IDA Pro, Burpsuite, Metasploit, Sleuthkit, Docker, NMAP, GDB, Wireshark, Splunk, Securonix SIEM & UEBA

Domain Expertise and Coursework: Malware Reverse Engineering, Privacy Analysis, Policy, Secure Code Audit