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

- Performed initial event triage and threat hunting to raise incidents for client corporations as part of POCs.
- Designed use cases to demonstrate anomalies such as beaconing, enumeration, insider threat, account misuse, credential sharing, fraud, etc., identify rogue insiders and detect advanced persistent threats.
- Accomplished activity correlation, data parsing, data enrichment with contextual information as TPI while ensuring privacy on user PII by integrating Snypr's (Securonix product) data masking & RBAC protocols.
- Collaborated with cross-functional teams to create end-to-end MITRE ATT&CK compliant threat models and policies, tuning it across complex environments to maintain quality and adhere to regulatory requirements.
- Scripted tools to help process data from standard log sources and automate daily tasks.

Threat Research and Development Intern May 2019 – Dec 2019

Webroot, An Open-text company Broomfield, CO

- Containerized dependencies to reproduce consistent and scalable builds, slashing human effort by 30%.
- Reverse engineered malware and assessed x86 windows binaries statically and dynamically in sandboxes.
- Developed modules to conduct YARA file scanning, PE file disassembly, and APK file decomplication.

PROJECTS

Web Application Security and Development: *Independent Study*, 2020

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.

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

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

Linux Systems Administration: Spring 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: Spring 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 efficiency by 8%.

Analysis of Web Trackers – Privacy and Compliance: Fall 2018

Case Study on web trackers – Analyzed web trackers and policies associated, their current practices, and studied anti-trackers. Assessed privacy exposures, data misuse and suggested mitigations.

EDUCATION

Master of Science, Cybersecurity: University of Colorado Boulder, CO GPA: 3.9 / 4 May 2020

Graduate Teaching Assistant – Penetration Testing Jan 2020 – May 2020

Graduate Teaching Assistant – Digital Forensics Aug 2019 – Dec 2019

AWARDS

William E. Rapp Fellowship Award for Cybersecurity Academic year: 2019-2020

KEY SKILLS

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

Application Security and Network Protocols:

Threat Modelling, STRIDE, OWASP Top 10, CWE Top 25, HTTP Headers, Same-origin Policy, Obfuscation, Penetration Testing, Web Application Firewall, TCP, IP, TLS, IPSec, DHCP, DNS, VPN, Wi-Fi, Fuzzing, Code Audit

Languages:

Python, PHP, C, C++, SQL, HTML, x86, Java, Bash/Shell Scripting, PowerShell, Go

Tools:

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

Domain Expertise and Coursework:

Reverse Engineering, Privacy Analysis, Policy, Digital Forensics, Differential Privacy, K-Anonymity, L-Diversity