Shoumit Karnik

skarnik@terpmail.umd.edu| (202) 386-0327 | College Park, Maryland | https://shoumitkarnik.github.io/resume/
https://www.linkedin.com/in/shoumitkarnik

EDUCATION

University of Maryland — **College Park, Maryland**
Master of Engineering, Cybersecurity, GPA: 3.5/4.0 — *Expected May 2021*

Savitribai Phule Pune University (formerly University of Pune) — **Pune, Maharashtra, India**
Bachelor of Engineering, Computer Science, GPA: 4.0/4.0 — *July 2012 - May 2016*

SKILLS & INTERESTS

Relevant Courses: Penetration Testing, Networks and Protocols, Applied Cryptography, Computer Forensics, Cloud Security, IoT
Cybersecurity: Malware Analysis, Risk Management, Penetration Testing, Threat Modelling, Vulnerability Assessment
Languages: C, C++, Java, Python 2.7,3, AngularJS, PHP and Android.
Platforms: Kali Linux, Linux Backtrack, Windows 8.1,10, Ubuntu, Fedora, Debian, TCP IP and Android Studio.
Databases: MongoDB, Oracle DB, SQL, MySQL, Cassandra and SQLite.
Tools: Nmap, Netcat, Hydra, Metasploit, Veil, RMF, Dirbuster, Wireshark, Burp Suite, OWASP ZAP, SIEM, Firewalls
Certificates: Network Security, Information Security, Software Security, Application Security, Hardware Security
Cloud Experience: Google Cloud Platform (GCP), Amazon Web Services (AWS), Microsoft Azure

RELEVANT WORK EXPERIENCE

Revolutionary Integration Group Inc. — **Connecticut, United States**
Artificial Intelligence (AI) Cyber Security Engineer Intern — *June 2020 - August 2020*

- Developed and modelled an end-to-end security product simulation, called the Dynamic Trust Framework, which included the placing of agents in a virtual environment and using reinforcement and deep learning for an authentication mechanism between the agents which helped them develop dynamic trust with each other.

ACADEMIC PROJECTS AND PATENTS

Master of Engineering Embedded Security Project

Return Oriented Programming on ARM — *May 2020*

- Demonstrated an ROP attack on BBB by designing a simple binary using C and testing it for buffer overflow vulnerabilities. Once the payload was executed, a persistent shell spawned on the BBB.

Master of Engineering Applied Cryptography Project

Building and Breaking various Cryptography Algorithms — *December 2019*

- Designed various existing Public and Private Key Cryptography as well as Hashing algorithms in Python and C (based on NIST compliance standards) such as the Diffie Hellman Key exchange, DES, AES, RSA, Elliptic Key Cryptography, SHA and H-MAC and developed exploits targeting these algorithms and successfully infiltrated these if they had certain vulnerabilities introduced in them.

Master of Engineering Binary Programming Project

Assembly Level Hacking, Return Oriented Programming and Unstable Code Optimization — *December 2019*

- Developed various exploits and scripts targeting vulnerable C programs and binaries which helped me deepen my understanding of reverse software engineering.

Master of Engineering Penetration Testing Project

Penetration Testing Engagement of a Complex Network — *December 2019*

- Implemented a project individually where the goal was to successfully infiltrate into a company's simulated network and gain access to their machines as well as data.
- Delivered a Penetration Testing Technical Report (PTR) that identified the high security risks, threats, and failures found during the mission and suggested risk mitigation strategies for the company.

Bachelor of Engineering Technical Patent and Project (*Patent Id – **201621016976***)

Secure Anomaly Based Real Time Intrusion Detection System — *May 2016*

- Created a system consisting of two types of IDS agents: Network and Host agent.
- Worked with a team of people to build a network agent system that employed machine learning to learn from the network and recognize unusual behaviour of network metrics with an accuracy rate of over 80%.
- Forecasted new types of attacks with the help of entropy calculation method using various parameters and assessed the risk that they pose based on their common vulnerability index.