Last Updated: 09/27/21

Sreyash Ratna Tripathi

sreyashtripathi.com

Education:

Carnegie Mellon University
December 2021 | Pittsburgh, PA
MS in Information Security
GPA: 3.86 / 4.0

NIIT University
July 2017 | Neemrana, India
B.Tech in Computer Science
GPA: 8.7 / 10.0

Coursework:

14810 – Network Security and Automation
14823 – Network Forensics
14740 – Fundamentals of Networks
14819 –Reverse Engineering
14761 – Applied Info Assurance
14760 – Information Security
14848 – Cloud Infrastructure
15746 – Storage Systems
15513 – Intro to Computer Systems
95-883 – Ethical Pen-Testing

Teaching Assistant:

14740 - Fundamentals of Networks
14761 – Applied Info Assurance

Skills:

Programming: Python, C, C#
Key Forte: Cyber Incident Response, Network Security, Network Forensics, Red/Purple Team
Platforms: Proxmark3, Crazy Radio, Raspberry Pi (three and Zero), USB Rubber Ducky, Cloud Servers

Leadership & Awards:

Vice President, Grad Organization @ INI, Carnegie Mellon University
In Charge, Cyber Security Lab Infrastructure Management, KPMG
Coordinator, Trainee induction and Mentoring program, KPMG
Ranked 12th, KPMG Global CTF with Immersive Labs
Accolades, Award for exceeding responsibility at KPMG

Professional Experience:

Activision | Information Security Intern
May – August 2021 | Los Angeles, CA
Developed a proprietary threat intelligence tool to be used by the Operation Security (OpSec) team.

KPMG | Associate Consultant
April 2019 – July 2020 | Gurgaon (NCR), India
Spearheaded Network Security and Cyber Incident Response engagements on 10 clients, both in the Indian subcontinent and overseas.
Led teams for Cyber Incident Response, Network Security, and Infrastructure Security at KPMG's biggest cyber transformation project in UIDAI – Aadhaar (the world's largest biometric-based identification system) in India.

KPMG | Analyst
July 2017 – March 2019 | Gurgaon (NCR), India
Conducted Network Security, Cyber Incident Response, and Cyber Red Team engagements for 12+ clients.
Performed IT Security Audits, Network Architecture Reviews, VAPT, and Threat Intelligence gathering for 20+ clients.

Projects:

15-746: Storage Systems | C++ *August 2021 – Present*
Implementing a Flash Translation Layer for SSD, responsible for Overprovisioning and Garbage Collection basis self-designed FTL policies.

14-848: Cloud Infrastructure | Docker, Kubernetes *August 2021 – Present*
Building a secure microservice that runs Hadoop, Spark, Jupyter Notebooks, and SonarQube in Docker containers deployed to a Kubernetes cluster.

14-761: Applied Information Assurance | Arkime *January – May 2021*
Created a CTF-style lab exploring Arkime and investigated exploitation of SMBv1 using EternalBlue and brute-force attacks on FTP server.

14-819: Reverse Engineering | x86, ARM, IDA, Ghidra *January – May 2021*
Conducted surface, runtime, and static analysis of an unknown malware to find its signatures and functionalities through tools such as IDA, Ghidra, OllyDbg, etc.

14-810: Network Security and Automation | Python, ML *January – May 2021*
Designed a reinforcement learning model for RUDY attack with a focus to elude parameter checks for data rate, packet size, content length, etc.

14-810: Network Security and Automation | Python *January – May 2021*
Programmed a software-based stateful F/W with VPN capabilities using AES-CBC symmetric encryption scheme supporting dynamic ACL policies.

14-760: Intro to Information Security | C, Assembly *August – December 2020*
Exploited buffer overflow vulnerability on randomized, non-executable, and canary-based stacks in x86_64 architecture.

REScure | MISP, GRR, Cuckoo *July 2018 – January 2019*
Co-created a threat intelligence platform that integrates, curates, and enriches threat feeds from 60+ resources integrated with GRR and Cuckoo functionalities.