PRAJ SANJAY SHETE

380 John St, Rochester, NY, 14623 | **Phone:** (585)-537-8489 | **Email**: prajshete17@gmail.com
LinkedIn: linkedin.com/in/prajshete | **GitHub:** https://github.com/prajshete

SUMMARY

Passionate cybersecurity enthusiast with a Bachelor's in Information Technology and experience as a Security Analyst. Currently pursuing Master's in Cybersecurity. My technical skills encompass Incident Response, Malware Analysis and Email & Endpoint Security.

EDUCATION

Rochester Institute of Technology (RIT) – Rochester, NY
Master of Science in Cybersecurity **GPA: 3.70/4.0** ***Aug 2022 - May 2024***

Pune University - Pune, India
Bachelor of Engineering in Information Technology **GPA: 7.55/10** ***June 2016 - May 2020***

WORK EXPERIENCE

Tata Consultancy Services Ltd.
Cybersecurity Analyst ***Aug 2020 – Aug 2021***

- Co-ordinated in a 24x7 Security Operation Centre (SOC) to proactively detect and respond to threats
- Conducted in-depth analysis and triage of phishing email alerts, enhancing email security.
- Prioritized and managed alerts generated by Proofpoint TAP, ensuring timely response to potential threats.
- Enhanced continuous monitoring of endpoints effectively using Crowdstrike and Splunk SIEM.
- Perform static and dynamic malware analysis of samples that generated alerts, improved detection capabilities.
- Mitigated suspicious user sign-in attempts using Azure AD, minimizing unauthorized access.
- Resolved email gateway-related issues through fine-tuning of the email gateway configuration within Proofpoint.
- Proactively hunted IOCs across threat intelligence sites, executing checks and blocks.
- Developed & updated SOPs related to alerts and cybersecurity tools, promoting efficient incident handling.

PROJECTS

SOC Home Lab

- Built an attack defend lab infrastructure consisting of Windows server with ADDS.
- Linux Server with web, FTP and SSH server and one client windows machine.
- A detection lab with ELK running as the SIEM, the lab also contains malware analysis capabilities.
- Emulate attacks/scans using a Kali machine and detect these attacks using local machine and SIEM logs.
- Schedule alerts based on the logs observed for future detections.

Reversing Redline Stealer Malware – *Malware Reverse Engineering – Summer 2023*

- Performed Basic Static, Basic Dynamic, Advanced Static analysis on Redline Stealer malware
- Used tools such as strings, TCPView, Wireshark, Procmon, Regshot, Process Explorer, IDAPro, x32dbg
- Reported all the findings and inner workings of the malware sample.

Host IDS -- *Summer 2023 (Personal Project)*

- Developed a Host IDS which will execute at regular intervals to check for modifications made in any directory.
- Provides an alert if any modifications are found with file path of the modified file.

Covert Channel using Image Exif Data – *Covert Communications – Fall 2023*

- Built and tested a novel covert communication channel using Image Meta-data.
- Used Exif tool to modify the contents of the exif data with ASCII encoding
- Dynamically encode messages into image meta data and send it through a transmission channel.

ACTIVITIES

RITSEC – RIT Cybersecurity club

- Active participation in interest groups like VAPT, CTFs, Reversing.
- Volunteered as a student at Rochester Security Summit. Attended various talks
- Competed in clubs Attack-Defend competition called IRSec.

Online Learning Platform

- **Cyber Defenders | Blue Team Labs:** Complete CTF challenges related to Reverse Engineering, DFIR, Threat Hunting.
- **Try Hack Me | TCM Security**: Complete relevant courses/rooms in Cyber Defense areas.

CERTIFICATIONS

- CompTia CySA+
- EC-Council Certified Incident Handler
- ISC2 Certified in Cybersecurity
- SOC Level 1 (Try Hack Me)
- Cyber Defense (Try Hack Me)

SKILLS

Tools: Crowdstrike EDR, Splunk SIEM, Abnormal Security, Proofpoint, Active Directory, Sysinternals Suite, IDAPro, x32Dbg, Wireshark, Autopsy, Velociraptor, Zeek, OSquery, nmap, GitHub, IDS/IPS
Domains: Incident Response, Malware Analysis, Threat Hunting, Email Security, Endpoint Security, Vulnerability Management
Programming: Python, C, C++, Assembly