Praj Shete

Rochester, NY (OPEN FOR RELOCATION)

✉ prajshete17@gmail.com in linkedin.com/in/prajshete github.com/prajshete 🌐 prajshete17.medium.com

Summary

Passionate cybersecurity enthusiast with a Bachelor's in IT and experience as a Security Analyst. Currently pursuing MS in Cybersecurity. Looking for Full-time opportunities in Cyber Defense domains. **(IMMEDIATE JOINER)**

Education

Rochester Institute of Technology (RIT) - Rochester, NY **August 2022 – August 2024**
Masters of Science in Cybersecurity *GPA - 3.70*

Pune University - Pune, India **June 2016 – May 2020**
Bachelor of Engineering in Information technology *GPA - 3.30*

Experience

Algosmic Cybersecurity **May 2024 – August 2024**
Information Security Engineer Intern *Pune, India*

- Enhanced threat detection capabilities by expanding MITRE coverage through the creation of detection rules in ELK SIEM.
- Improved incident response efficiency by developing a Python-based automated tool that analyzed ELK SIEM logs and executed appropriate remediation actions.
- Optimized security infrastructure by securely setting up and migrating the ELK stack from the cloud to self-managed servers.

Tata Consultancy Services Ltd. – *Fulltime* **August 2020 – August 2021**
Assistant Systems Engineer-Cybersecurity Analyst(Project Role) *Pune, India*

- Proactively detecting and responding to threats in a 24x7 SOC for over 20,000 global endpoints.
- Mitigated phishing threats by analyzing over 30 phishing emails daily, enhancing email security and user trust.
- Monitoring and triaging security alerts using tools such as Proofpoint TAP, CrowdStrike EDR, and Splunk SIEM.
- Correlate SIEM logs for investigations from various source types like sysmon, proxy, firewalls, IDS/IPS.
- Conducted proactive threat-hunting operations, creating search queries from Sigma rules available through intelligence.
- Secured user accounts by monitoring and remediating suspicious sign-in attempts through Azure Active Directory.

Projects

Automate Incident Response | *Python, ELK SIEM, GitHub Link*

- Developed an automated incident response tool using Python and integrated with ELK SIEM APIs and VirusTotal API, reducing manual analysis by 50%.

The Invader - An Offensive Tool | *C++, Python, Malware, C2, GitHub Link*

- Built an offensive security tool with Python CLI and server for real-time command execution from a C++ payload, featuring post-exploitation techniques like process injection, privilege escalation, file transfer, screenshot capture, and password hash extraction using Mimikatz.

Attack and Defend Active Directory

- Emulate prominent attacks against the AD and derive detection strategies against them.

SOCker: A robust Incident Management and tracking application (Capstone Project. In Progress)| *GitHub Link*

- Developed an open-source web-based ticketing system for SOC analysts, streamlining incident response workflows, enhancing documentation, and providing real-time threat landscape insights through customized dashboards

Image EXIF based Covert Channel| *GitHub Link*

- Built an automated EXIF data based covert channel that hides information inside the images's metadata and sends over public channels.

Reversing Redline Stealer Malware| *GitHub Link*

- Performed static and dynamic malware analysis of redline stealer malware using various sysinternal and forensic tools.

Technical Skills

Security Domains: Incident Response, Malware Analysis, Threat Hunting, Email Security, Endpoint Security, Digital Forensics, Vulnerability Management, AWS Cloud Security.

Security Tools: Crowdstrike EDR, Splunk SIEM, ELK SIEM, Abnormal Security, Proofpoint, Active Directory, Sysinternals Suite, x64dbg, Wireshark, nmap, YARA, Sigma, Volatility, Autopsy, Snort, GitHub, IDS/IPS, Firewalls, Microsoft Office, Office 365

Code Analysis: Python(Development), C, Powershell, HTML, CSS, Javascript, .NET

Certifications

CompTIA CySA+(COMP001022374766), EC-Council Certified Incident Handler(ECC2013974856), ISC2 Certified in Cybersecurity(1229888), Chronicle Certified SOAR Analyst, Hack The Box CDSA(In Progress)

CTF Blue Team Challenge Labs

Solve various CTF labs related to Incident Analysis, Malware Analysis, Digital Forensics, Threat Hunting on platforms like Letsdefend, BTLO, CyberDefenders
Publish Write-ups/Blogs on **https://prajshete17.medium.com/**