Jasjyot Singh Saini

+91 8424063696 | definitelynot.jas@gmail.com

www.linkedin.com/in/jasjyotsaini/

EDUCATION

SHAH AND ANCHOR KUTCHHI ENGINEERING COLLEGE
Bachelor of Engineering in Cyber Security, Jun 2025
CGPA: 9.05 (as of semester V)

EXPERIENCE

Cyber Security Defense Center (SOC) Intern | John Deere India: Jan 2024 – Jun 2024

- Learnt email phishing analysis and used Cofense to analyze 700+ suspicious emails to provide verdicts.
- Developed a Microsoft Teams notification system to notify phishing analysts of emails that have not been evaluated for more than 4 hours.
- Performed log analysis and Splunk searches to respond to various cyber security incidents.
- Acquired knowledge of AWS cloud services such as Lambda, API Gateways, and CloudWatch for project implementation. With the assistance of the team, we deployed all cloud resources via Terraform and GitHub Actions (GHA).
- Developed a Full Stack Application to analyze user-reported emails, including URLs and attachments, and reorganize them based on potential maliciousness.

Capture The Flag (CTF) Developer | SAKEC Center Of Excellence (COE): Jan 2023 – Apr 2023

- Lead the development process of all the challenges under the sub domain of Digital Forensics.
- Used Volatility Framework to create challenges involving extraction of digital artifacts from volatile memory (RAM) samples. These samples were created using VMware in a specific manner to hide Flags in them.
- Learned about the concept of Magic Bytes and implemented it in a manner to create a CTF challenge, where a file identified as a .pdf but when run as a .png file it reveals the flag.
- Learned about Time & Project management.

PUBLICATION

“The Art of Crafting CTF Challenges: Insights and Lessons Learned” - Research Paper

- The Research Paper talks about how me and my team developed several CTF challenges, difficulties we faced, The tools we used and discussed the do’s and dont’s in the development phase of the CTF challenge incase the reader wants to make their own CTF Challenges.
- This Paper is Published in Journal of Emerging Technologies and Innovative Research Volume 10 Issue 5 May-2023 eISSN: 2349-5162
- PDF URL: https://www.jetir.org/papers/JETIR2305C81.pdf

“MiTM using custom packet sniffer” - Report

- In this report I discuss about how me and my team created our very own packet sniffer and port scanner using a python library called scapy, an then demonstrated a Man in the Middle attack on a HTTP session. we then copyrighted this work from the copyright office in Delhi
- ROC No : L-124636/2023
- Diary No. : 26343/2022-CO/L

Projects

- **Phishing Notification System**: Using AWS SNS, Microsoft Teams API, and Cofense APIs, I created a system that displayed all emails that had not been analyzed by the analyst in more than 4 hours.

- **Email Queue Generator and Analyzer**: Using ReactJS for the UI and Python for the backend, we created an application that can scan URLs and attachments using the VirusTotal and IPQualityScore APIs, and then reorganize emails based on suspected maliciousness.

- **Discord Bot**: I built a discord bot in JAVA using the JDA library, This discord bot used to remember dates by saving them in a text file and would remind the user about how many days are left for that saved date. Using this people who would forget important dates like birthdays or anniversaries would get a daily reminder.

Skills

- Languages: C, Java, Python, HTML, CSS, JavaScript, ReactJS
- Technologies: Ubuntu, Git, Bash, Volatility, Splunk, Cofense