Suraj Yadav

suraj372y@gmail.com | linkedin.com/in/k4n3ki/ 0xk4n3ki.github.io

About

Dedicated Security Researcher specializing in reverse engineering and malware analysis, seeking to leverage advanced academic research opportunities to pioneer innovative approaches in binary analysis, exploit development, and vulnerability research.

Education

Indian Institute of Technology Roorkee 2020-2024
Bachelor of Technology ***GPA: 7.013/10***
Chemical Engineering

Experience

Cyble Inc. June 2024 - Sep 2024

Security Research Intern *Malware Analysis, Threat-hunting*

- Perform daily threat hunting and analyze new malware samples, and have published blogs revealing the **OpenAI Sora** and **Zoom phishing** campaigns, which delivered Stealers and Remote Access Software.
- Prepared weekly intel reports on CVEs, Linux malware, and brute force attacks, managing T-POT honeypots to gather IoCs for threat analysis.
- Identify and track newly registered domains—including those mimicking legitimate brands—to detect phishing sites, designed to distribute malware to unsuspecting users.
- Publish daily advisory reports on emerging security threats and data breaches, providing timely insights to enhance organizational security posture.

Cloud Security Club May 2024 - June 2024

Cloud Security Research Intern *AWS*

- Proficient in AWS cloud services, including EC2, S3, IAM, and Lambda as well as the misconfigurations within them that attackers could exploit in real-world scenarios.
- Authored Step-by-Step guides on **flaws.cloud**, **flaws2.cloud** and Cloudgoat educating the community on AWS misconfigurations and best practices.

Cyber Cohesion May 2023 - June 2023

Cyber Security Intern R&D *Python, C++, Malware Analysis*

- Worked on automation tools and scripts in Python to streamline malware analysis processes
- Performed reverse engineering on malware samples to extract valuable information such as command and control (C2) servers, encryption methods, and evasion techniques

Projects

Blog Site Jan 2023 - Ongoing

Technical Blogs realated to Malware Analysis & Digital Forensic

- Developed this Blog Site to publish blogs related to Malware Analysis and Reverse Engineering, Binary Analysis, Vulnerability Research, Digital Foresnsics, CTF Writeups.
- Has analysed many Real-world Malware samples like Luckbit Ransomware, Agentb Trojan, Dridex Stealer.
- "**Solving flare-on challenge using DBI**": Used a binary analysis technique i.e. instruction count, to solve the crackme
- "**Malwy(Shellcode Execution)**": showed a shellcode execution technique which stores shellcode in form of UUID string
- "**Heaven's Gate Technique**": Explained about the Heaven's gate technique used by APTs as anti-analysis technique

Shellcode Injector Jan 2024

Shellcode injector bypassing defender, triggering a message box *C++*

- Developed a C++ proof-of-concept tool that employs dynamic API resolution through hashing techniques to obscure system calls and modify a remote process in a controlled test environment.
- Validated the approach by enumerating running processes and modifying the memory of a standard application (Notepad) to display a test message, demonstrating a method for assessing system defenses..

PEparser Dec 2022

PE file header parser *C++*

- Developed this project in C++ to parse PE (Portable Executable) file structures, including headers, sections, imports, and exports, providing detailed insights into binary files
- Demonstrated expertise in reverse engineering and understanding the internal workings of 32-bit binaries

Twitter Sentiment Analysis | IIT Roorkee March 2023 - May 2023

- Developed a model to perform sentiment classification of tweets, ensuring data integrity. Performed data cleaning, stopping word removal, and tokenization as a part of data preprocessing.
- Analyzed using Vader and trained models like SVC and logistic regression, demonstrating a strong grasp of data analytics and machine learning techniques. Evaluated models in metrics like precision, recall, and f1 score.

Leadership Roles

InfoSecIITR Sep 2021 - March 2023

CTF Player *Python, C++, IDA Pro, x64dbg, gdb*

- InfosecIITR promotes the culture of cyber security on campus through various workshops and Organizes BackDoor CTF, Noob CTF every year.
- Along with Malware Analysis and Reverse Engineering, I also learned about Exploit Development, Digital Forensics, Steganography and OSINT.
- Secured 1st position in CSAW CTF finals in India.
- Secured 3rd position in JadeCTF 2022.
- InfoSecIITR is ranked 2nd in India on the CTFtime leaderboard.

Community Involvement Feb 2022 - May 2024

- Video Editor at onRec, the official podcasting and storytelling group of IIT Roorkee. Edited videos, including a podcast for the Class of 2022, and managed tasks for junior members to ensure smooth workflow.
- Joint Secretary of the Himalayan Explorer Club, led treks, mountaineering, adventure sports, and environmental drives while demonstrating leadership and teamwork skills.

Skills

Languages: Python, C, C++

Tools: IDA, x64dbg, DiE, GDB, Ollydbg, angr, Wireshark, Procmon, AWS, Burpsuite, Maltego, FTK, Autopsy, AWS

Certifications:

- C Programming for Everybody Specialization
- Data Structures and Algorithms Specialization
- Cryptography I
- Google Cybersecurity Certificate
- Malware Analysis and Introduction to Assembly Language by IBM