Akshit Singh

Reverse Engineer/Mobile Security Engineer

+91 9868520459 | akshitdavps@gmail.com | https://www.linkedin.com/in/akshit-singh-69ba5a192/
https://github.com/it4ch1-007 | https://it4ch1-007.github.io/ | https://x.com/akshit_it4ch1

ABOUT

Final year at IIT Roorkee. Aspiring low-level developer and cybersecurity enthusiast with experience in the fields of Android security, Reverse engineering, and Malware internals. Currently exploring Android Security and low-level Rust development

SKILLS

Soft Skills: Time Management, Communication, Problem-solving, Teamwork, Leadership, Software Design

Programming Languages: Java, Kotlin, C/C++, Python, Rust, Assembly, NodeJS, Shell scripting, Golang, Batch, Powershell, Visual Basic

Software Packages: Frida, Androiguard, ADB, Objection, Drozer, Apksigner, GDRA, IDA Pro, Ghidra, Cheat Engine, x64dbg, Tauri framework, RE automation, BurpSuite, Visual Studio, Eclipse debugger, Android Studio, Jadx, Apktool, AFLPlusPlus Fuzzer

DevOps: Linux, Docker, Git, Cloud security, Network security, Database security, AWS, GCP, Azure, Kubernetes

Cybersecurity: Car CAN Reverse Engineering, AI Security and Red Teaming, Android Internals, Android Debugging, Fuzzing, eBPF, Blockchain security, Kernel exploitation, Windows internals, Operating systems, Web pentesting, Malware internals, Windows kernel development, Database security, Linux kernel development, Game security, IoT/Hardware security

EXPERIENCE

Android/iOS Reverse Engineer | Talsec — Oct 2024 - Present

- Researched and developed new detection techniques for malicious Android and iOS practices like **Rooting, Emulating and Hooking.**
- Reverse engineered banking applications and security modules like **ICICI banking mobile app, Yono SBI App, BOSCHK, Lookout, Appdome and Lockin - for Shamiko Magisk, Zygisk hiders, Nox , Bluestacks emulator, Dopamine, Paleraine and Root detection.**
- Developed **Native C++** methods to detect hooking tools like **Frida and Objection in applications at runtime without root privileges.**
- Developed **Anti-root, Anti-hooking, Anti-multiinstancing and Anti-emulator methods** for **freeRASP**.
- **Skills: Android/iOS Studio debugging, Frida, adb debugging, C/C++, Java, Android/iOS OS internals, Android/iOS applications vulnerability research.**

Cloud Security Research Intern | CloudDefense.AI — July 2024 - Oct 2024

- Developed cloud monitoring tools for cloud platforms such as **Microsoft Azure, AWS and GCP and databases such as AlloyDB, AuroraDB, DynamoDB, MongoDB Atlas and MySQL.**
- Working on vulnerability scanning of Personal Identifiable data **inside databases, involving malwares and attack path scanning.**
- Working on cloud security tools deployment, **Cloud Software Development Kits for Gofiber using Golang** and the management of database systems inside the cloud platform accounts, alongwith privilege escalation techniques on cloud platforms and users' accounts.
- **Skills: Golang, Rust, C/C++, AWS, GCP, MongoDB Atlas, Java**

Android Security Research Intern | Forensics Cybertech Machines (Under Ministry of Home Affairs, India) — Mar 2024 - May 2024

- Conducted security research under the **Ministry of Home Affairs of India** on Android system exploits and proof of concepts of more than **100 vulnerabilities** in the Android kernel as well as **bugs in Android applications** giving us system privileges without authentication.
- **Reverse engineered** more than **50 N-day exploits** to reproduce exploit environments using tools like **IDA Pro, x64dbg and pwndbg**.
- Worked on development of exploits in Android devices and **debugging and emulation of N-day exploits** and bugs in the Android kernel.
- Worked on the **emulation of the exploits** in Android devices and gaining privileged information of the administrator using privilege escalation techniques and **C exploit development** in most common smartphone vendors in India, such as **Xiaomi, Apple and Samsung.**
- **Skills: IDA Pro, adb debugging, Frida, C/C++, Python, Android Studio, GDB debugging**

EDUCATION

Bachelors of Technology, IIT Roorkee {2022-26}
Majors: Electrical Engineering

Bachelors of Technology, NSUT Delhi {Dropout} {2021-22}
Majors: Computer Science Engineering

DAV Public School, New Delhi
Completed High School Education

CERTIFICATIONS

Awiros AppaThon , IIT Delhi
Developed a mobile application based on OpenCV for traffic monitoring.

3rd globally in PragyanCTF 2024, NIT Trichy

3rd globally in CodefestCTF2024, IIT BHU

4th globally in IncognitoCTF2024

ACHIEVEMENTS

- Presented on FRIDA internals at **Mobile Security Conference 2025 at Prague, Czech Republic**
- Qualified for **DCTF finals at DefCamp Conference in Romania**
- **Qualified for Awiros AppAThon finals at IIT Delhi**
- Finished **7th at EY DSCI CTF,2024**
- 1st in **CSAW'Quals 2025** (India region) organized by **New York University of Technology**
- 1st globally in **VishwaCTF 2024**
- 1st globally in **JerseyCTF 2024,** organized by the **New Jersey Institute of Technology**
- Qualified for the final round of TrustLabs CTF held at **IIT Bombay among more than 10 lakh national players.**
- 2nd position at Scythe CTF, held at **Cognizance IIT Roorkee**
- Qualified for **HackDay** CTF Finals 2024, **held at ESIEE, Paris**
- 6th globally in **b0il3rsCTF 2024**
- 9th globally in **BYUCTF 2024**
- 3rd globally in PragyanCTF 2024, **organized by NIT Trichy**
- 5th globally in **UMASSCTF 2024**
- 3rd globally in CodefestCTF 2024, **organized by IIT BHU**
- 9th globally in **HackDay Qualifications 2023**
- Won Times of India online **National English Debate Contest.**
- Got a book published by the **Children's Book Trust of India.**

PROJECTS

SilentPulse {SeLinux Bypass, Magisk's libSu, SandHook implementation }
https://github.com/it4ch1-007/audioRecorder

- An Android application that gains root inside the victim's device using **Magisk's libSu API** and uses background service to inject malicious hooking library into the processes' memory and **modify those process' memory** without any notification on the victim's screen.
- It **bypasses the SELinux** policies using **supolicy** tool and **custom Sandhook mechanism** to be able to hook into the audioserver process of the device,detect when a call is made by or to the device, and collect the **PCM data packets** of VoIP calls made through the device.
- It **bypasses any notification prompts** to the user to execute all its functionalities stealthily in the background of the device.
- It uses **priority queues for real-time storage and reordering** of outgoing and incoming packets in files inside external storage without explicit permissions using **FFT algorithm** to determine amplitude of PCM packets in real-time.
- Uses **ADB Bridge, AIDL interface, C/C++, Java, Kotlin, SuPolicy, SandHook, x86_64 assembly**

Overlay Hacker {Shizuku, ADB Bridge, Android native programming, AIDL interfacing }
https://github.com/it4ch1-007/AttackerAppJava |

- An Android **pentesting** application that uses **Shizuku-API** and **IShizuku** service to elevate privileges **without jailbreaking** the device.
- Uses **Overlay attacks, Multithreading and API calls** to simulate an environment that **steals the users' credentials** without any permission prompt and sends it to the attacker's system as well as store them inside privileged environment.
- Able to execute any ADB commands remotely using Wi-Fi debugging bridge of the device and elevating privileges to ADB permissions.
- Uses **ADB Bridge, AIDL interface, C/C++, Java, Kotlin**

Cobra {Rust, Windows Internals, Malware Analysis, Powershell, Batch, AV Evasion}
https://github.com/it4ch1-007/Cobra

- A **Rust based C2** software that evades more than 25 Windows security mechanisms to take control of the system using AV evasion.
- Developed not to trigger any AV checks and exploit the basic mechanisms of the **Windows subsystem with modern persistence techniques, Credential stealing techniques, Lateral Movement techniques and unauthorized signature forging techniques.**
- Uses **Powershell and Batch scripting to bypass UAC checks** and implement new AV evasion techniques like **Custom crypto algorithms**, **PEB traversal** debug checks, **WLAN Parsing**, APC Queue injection, Code injection, DLL injection, API hashing and more.

Buzz {Rust, Tokio-rs, RataTui-rs}
https://github.com/it4ch1-007/Buzz.git

- Developed a **concurrent peer-to-peer chat application in Rust** using the **Tokio-rs** runtime for **efficient asynchronous I/O and concurrency.**
- Designed and implemented client and server channels for efficient communication and sharing of resources using **Mutex locks** and **ReadWrite locks** with **Atomic reference** counters to ensure that the clients are able to communicate in groups using chat rooms and names.
- Negligible monitoring of the clients to ensure **anonymity** and **privacy** of the clients using the application.
- Fast rendering and response user interface rendered by the RataTui-rs crate in Rust, made exclusively for terminal application development.
- Utilizes Rust crates like **Tokio-rs, RatatTui-rs, Futures, Mutex locks, ReadWrite locks, Asynchronous buffers** and **Reference counters**.

EXTRACURRICULAR

Reverse Engineer, InfoSecIITR
https://infoseciitr.in/

- InfoSecIITR is a team of cybersecurity enthusiasts at IIT Roorkee, and is one of the **top 10 CTF teams globally**, and stands **second** in the national CTF ranking . The whole society works towards promotion of cybersecurity throughout the campus through lectures and at international level through CTFs.
- Participation in **global CTFs** and security hackathons at the national level as a core team member and player in the category **Reverse Engineering**.
- Conducting CTFs and lectures to promote Information Security like **Backdoor CTF** and **n00bCTF** as challenge author and platform auditor.

Organizer, BackdoorCTF (2024,2025)
https://ctftime.org/ctf/49/

- BackdoorCTF is one of the most presitigious cybersecurity rumble organized by any Indian CTF team, gathering more than 500 CTF teams and people all over the globe to compete in a jeopardy style hacking competition.
- Audited the CTF platform using **CTFd** on **Google Cloud Platform** and designed challenge problems for the CTF contest in the **Reverse Engineering** category.

Organizer, ScytheCTF'24
https://www.cognizance.org.in/events/centerstage/27/61

- ScytheCTF is a major cybersecurity competition organized by **Cognizance**, **the technical fest team of IIT Roorkee,** gathering more than 100 participants all over India.
- Audited the CTF platform using **CTFd** and designed challenge problems for the CTF contest in the **Reverse Engineering** category.
- Acted as the **first person of contact** for the offline participants during Cognizance IIT Roorkee.

PUBLICATIONS

- *Android Malware Analysis*
- *Shizuku Article*
- *Android Signature Model and APKSignatureKiller*
- *Frida Internal Working*
- *IDA Pro Internals*