

# Aditya Singh

+919451110293 | aroo25may@gmail.com | [LinkedIn](#) | [GitHub](#)

## EDUCATION

<b>Thapar Institute of Engineering and Technology</b> <i>Bachelor of Engineering in Computer Engineering— CGPA: 8.08</i>	Patiala, India <i>October 2021 – June 2025</i>
<b>Guru Nanak Public School</b> <i>Passed 12th standard with 91.8 percentage</i>	Chandigarh, India <i>April 2019 – May 2021</i>
<b>Manav Mangal Smart School</b> <i>Passed 10th standard with 89.8 percentage</i>	Mohali, India <i>April 2017 – May 2019</i>

## TECHNICAL SKILLS

<b>Languages:</b> C, C++, Python(3.10), SQL
<b>Cybersecurity:</b> Packet Analysis, MITM Attacks, Environment Variable Exploitation, Buffer Overflow Vulnerabilities, SQL Injection, Attack Mitigation
<b>Security Tools/Framework:</b> Wireshark, Metasploit, Cisco Packet Tracer, Burp Suite, PuTTY, OllyDBG, XVI32, LordPE
<b>Developer Tools:</b> Git, VS Code, Kali Linux
<b>Soft Skills:</b> Problem-Solving, Leadership, Teamwork, Time Management, Adaptability

## EXPERIENCE

<b>NAS Systems Engineering Intern</b> <i>STPI (Software Technology Park of India)</i>	June 2024 - July 2024 <i>Mohali, India</i>
<ul style="list-style-type: none"><li>Designed and implemented a schema to connect systems to Network Attached Storage (NAS), improving data access efficiency by 30%.</li><li>Developed a robust backup solution supporting daily backups, which enhanced data security and integrity, reducing data loss incidents by 40%.</li><li>Collaborated with the IT team to analyze system requirements and ensure seamless integration with NAS</li></ul>	

## PROJECTS

<b>Advanced KeyLogger</b> <i>Python(3.10), Pynput, Cryptography, and Pillow</i>	March 2024 - April 2024
<ul style="list-style-type: none"><li>Developed an advanced Python keylogger capturing keystrokes, system data, clipboard contents, audio, and screenshots.</li><li>Integrated encryption and email functionality to securely send captured data to a specified email address, ensuring data privacy and automated file cleanup post-transmission.</li></ul>	
<b>RevShell Injection</b> <i>LordPE, XVI32, OllyDBG, Metasploit, Ubuntu 12.04, WindowsXP</i>	January 2024 - February 2024
<ul style="list-style-type: none"><li>Engineered a project that utilized LordPE, XVI32, and OllyDBG to modify an application, successfully embedding a payload to create a reverse shell.</li><li>Employed the Metasploit framework to facilitate the payload injection, allowing for remote access.</li></ul>	
<b>Wireshark Manipulation</b> <i>Wireshark, NANO, Linux Shell</i>	March 2023 - April 2023
<ul style="list-style-type: none"><li>Developed a project that utilized Wireshark to capture network packets, enabling the analysis of communication between two endpoints.</li><li>Modified captured packets to alter their content and executed a replay attack by repeatedly sending the modified packets to the target user, showcasing vulnerabilities in unsecured network communication.</li></ul>	

## PATENTS AND PUBLICATIONS

<ul style="list-style-type: none"><li>* <b>Indian Patent, Application No.</b> 202411065970, "PRIVACY-PRESERVING MULTIMODAL FIRE DETECTION SYSTEM," Filed Aug 31, 2024, Published Sep 20, 2024. Inventor(s): Aditya Singh</li><li>* <b>Indian Patent, Application No.</b> 202411065971, "FEDERATED LEARNING-ENHANCED MULTIMODAL GAS DETECTION SYSTEM," Filed Aug 31, 2024, Published Sep 20, 2024. Inventor(s): Aditya Singh</li></ul>	
---	--