

# GOUTHAM

Pondicherry | goutham.cyber@proton.me | 8072408520 | [linkedin.com/in/GOUTHAM](https://www.linkedin.com/in/GOUTHAM)

## Professional Summary

Enthusiastic cybersecurity professional with a strong foundation in ethical hacking, penetration testing, and incident response. Seeking a role in cyber Offense and Defense to apply my skills in threat analysis, vulnerability assessment, and security operations.

## Technical Skills

- **Programming Language:** Bash, Python
- **Offensive Security:** Penetration Testing, Vulnerability Assessment, Exploitation Techniques, Command and Control
- **Defensive Security:** SIEM, Log Analysis, Incident Response, Threat Hunting
- **Tools:** Burp Suite, Metasploit, Wireshark, Nmap, Hydra, John the Ripper, Nessus, Nikto, SQLmap, Gobuster
- **Frameworks and Compliance:** OWASP, ISO 27001, MITRE ATTCK, CVSS
- **System and Network Security:** Privilege Escalation Techniques, Network and Vulnerability Scanners, Web Application Security, Active Directory
- **Operating Systems:** Windows, Linux (Kali, Debian, Fedora)

## Education and Certification

<b>Certified Ethical Hacking- (V13)</b>	complete
• EC-Council	
<b>Advanced Diploma in Cyber Defense -(ADCD)v3</b>	2024 - 2025
• RedTeam Hacker Academy	
<b>Sri Manakula Vinayagar Engineering College - (BSC-CS)</b>	2021 - 2024
• Bachelor in Computer Science	

## Experience (Projects)

<b>Security Engineer @(Swipe to Future Technologies) - present[2025]</b>	<b>Work Experience (Offensive Security)</b>
<ul style="list-style-type: none"><li>• Performed Vulnerability Assessment and Penetration Testing on web applications and internal systems.</li><li>• Identified security weaknesses such as broken authentication, insecure session handling, and access control flaws.</li><li>• Used offensive tools including Burp Suite, Nmap, SQLmap, and manual testing techniques to exploit vulnerabilities.</li><li>• Documented findings with severity ratings (CVSS), attack methodology, and proof-of-concept screenshots.</li><li>• Provided remediation recommendations to improve overall application security posture</li></ul>	

## Projects (Practical Experience)

- Performed VAPT on VELS University Student Portal and identified major vulnerabilities.
- Discovered OTP brute-force vulnerability on Joboy.in and recommended security fixes.
- Completed SIEM deployment and threat monitoring using Wazuh and Splunk.
- Configured and secured Active Directory with Group Policies and RBAC

## Achievements (Certifications)

- Completed networking fundamentals training from Cisco Networking Academy.
- Completed Cyber Security 101 learning path on TryHackMe.
- Completed SIEM training with hands-on log analysis on LetsDefend
- Solved CTF challenges that improved teamwork, problem-solving, and security skills.

## Soft Skills

Communication, Critical Thinking, Risk Assessment, Time Management, Collaborative Skills.

**Languages:** Tamil | English