# SUDHIR REDDY SURAM

Jersey City, NJ | [Portfolio](https://sudhirreddy1312.github.io/Portfolio) | 551-277-7006 | [sudhirreddy1312@gmail.com](mailto:sudhirreddy1312@gmail.com)

## Summary

MSc Cybersecurity candidate (GPA 4.0) with hands-on experience in log analysis, penetration testing, and network operations. Certified in CompTIA Security+, Cisco CCST, and PJPT (Active Directory), with CCNA in progress. Skilled in Splunk, Active Directory, firewalls, and penetration testing tools including Nmap, Burp Suite, and Metasploit. Proven ability to learn and master new technologies quickly through labs, projects, and internships. Highly motivated to grow as a Security Analyst and contribute to enterprise security teams with dedication and results.

## CERtifications

**CompTIA** *Security*+ | **Cisco** *CCNA*  | **TCM Security** *PJPT* (Active Directory) | **Cisco** *CCST*

## education

**Saint Peter’s University Jersey City, NJ**

*MSc in Cybersecurity (GPA:4.0) May 2025*

* **Relevant Coursework**: Digital forensics, Ethical Hacking, Blockchain

**Presidency University Bangalore, IND**

*BSc in Computer Science (GPA: 3.6) Jun 2023*

* **Relevant Coursework**: DSA, Computer Programming Languages, Operating System

## work experience

**Saint Peter’s University Jersey City, NJ, USA**

*Cybersecurity Intern – Log Analysis with Splunk*

* Analysed DDoS attack logs from multiple IPs attempting various user credentials across different resources.
* Built Splunk filters for source IPs, compromised accounts, and credentials used in successful logins.
* Investigated e-commerce logs to track vendors, products, payments, and abandoned shopping carts.
* Created dashboards and reports summarizing anomalies, queries, and security insights for stakeholders.

**Flexsin Inc. Bangaluru, KA, IND**

*Jr. NOC Intern*

* Managed and maintained network hardware, software, and configurations to ensure smooth operations.
* Analysed network traffic in detail to identify potential issues, troubleshoot problems, and improve reliability.
* Performed capacity panning, optimized performance, and implemented security policies and procedures across network
* Participated in system upgrades, applied patch management, and responded to alerts from monitoring systems.

## projects

**TrustFace**

* Developed an offline face-recognition lock that secures devices by locking when an authorized user’s face is undetected.
* Designed the system to run fully on-device without internet, with support for multiple trusted users and local logging.
* Enhanced device security by preventing unauthorized access in sensitive environments and maintaining audit-ready records.

**Automated Active Directory Penetration Testing**

* Created automation scripts with BloodHound, CrackMapExec, and Mimikatz for penetration testing in Active Directory.
* Supported regular security assessments by ensuring consistent, repeatable testing and reducing manual effort.
* Automated credential spraying, privilege escalation, and other attack simulations to efficiently identify security weaknesses.

**Secure Voting App**

* Designed and implemented a secure voting app using Google OAuth for authentication and SQLite for vote storage.
* Delivered a secure, user-friendly platform suitable for small-scale elections or surveys.
* Developed APIs tested with Docker and Postman for modular, reliable operation while preventing multiple votes from duplicate accounts.

## skills & INTEREST

**Programming Languages**: C, Python, Html, JavaScript, CSS, Bash, MySQL, PowerShell

**Software Tools**: Wireshark, Linux, Nmap, Burp Suite, Splunk, Metasploit, Bloodhound, IDA Pro, SolarWinds, Ansible, AWS, n8n

**Networking**:TCP/IP, DNS, DHCP, VPNs (OpenVPN, IPsec), VLANs, Firewalls (Windows, Linux), Cisco Packet Tracer

**Operating Systems & Cloud**: Windows Server, Ubuntu Linux, Kali Linux, Microsoft Azure, AD, AWS Security

**Cybersecurity Practice**: Capture the Flag (CTF) challenges, HackTheBox, ethical hacking labs, security research

**Languages**: English, Italian