SUDHIR REDDY SURAM

Jersey City, NJ | Portfolio | 551-277-7006 | 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 CCNA and CCST, and PJPT (Active Directory). 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* | **Splunk**

SKILLS & INTEREST

Programming Languages: C, Python, Html, JavaScript, CSS, Bash, MySQL, PowerShell
Software Tools: Wireshark, Linux, Nmap, Burp Suite, Splunk, Metasploit, Bloodhound, IDA Pro, 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, AD, AWS Security
Cybersecurity Practice: Capture the Flag (CTF) challenges, HackTheBox, ethical hacking labs, security research
Languages: English, Italian, Telugu, Hindi, Tamil, Kannada.

EDUCATION

Saint Peter's University — **Jersey City, NJ**
MSc in Cybersecurity (GPA:4.0) — *Feb 2024-May 2025*

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

Presidency University — **Bangalore, IND**
BSc in Computer Science (GPA: 3.6) — *August 2018-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.

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.
- Implemented OpenCV-based recognition algorithms with optimized accuracy and performance for real-time detection.
- Enhanced device security by preventing unauthorized access in sensitive environments and maintaining audit-ready records.

Automated Active Directory Penetration Testing

- Automated Active Directory penetration testing using Nmap, CrackMapExec, SMB relay, and PsExec within the environment.
- Supported regular security assessments by ensuring consistent, repeatable testing and reducing manual effort.
- Utilized BloodHound to visualize attack paths and summarize results in actionable security reports
- 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.
- Integrated AES encryption for vote data and session tokens to ensure privacy and integrity across all transactions.
- Developed APIs tested with Docker and Postman for modular, reliable operation while preventing multiple votes from duplicate accounts.

PROFESSIONAL DEVELOPMENT AND INTERESTS

- Actively preparing for AWS certification and exploring cloud security tools (AWS, Azure).
- Building a repeatable AWS purple-team lab (Windows AD + Linux + containerized web app) that automates MITRE ATT&CK emulations, collects telemetry, and measures detection and response.
- Interested in SOC analysis, network security, and automation in cybersecurity environments.