


Adi Narayana Reddy Chowdiredy Gari

Hindupuram, Andhra Pradesh | careddy5186@gmail.com | 7989323982 | | github.com/adi9032

 linkedin.com/in/adiredy-c-g

Summary

Motivated and detail-oriented Cybersecurity graduate with hands-on experience tracking threat actors, vulnerability discovery, and SOC workflow simulation. Skilled in Python/Bash scripting for investigation automation, and experienced in telemetry analysis using Wireshark, Nmap, Nessus, and OpenVAS. Developed threat intelligence reporting and agentic workflows during internships and job simulations. Familiar with adversary TTPs, cloud and infrastructure threats, and enthusiastic about applying investigative skills at scale.

Education

Bachelor of Technology (B.Tech), Computer Science Engineering June 2021 – July 2025
Viswa Bharatiya Vidhya Parishad (VBVP Institute), Andhra Pradesh, India

- GPA: 7.3 / 10
- **Coursework:** Data Structures & Algorithms, Operating Systems, Computer Networks, Cryptography, Cybersecurity, Quantum Computing

Senior Secondary (Class XII), M.P.C Stream April 2021
Haryana State Open Board of Schooling, India

- GPA: 7.2 / 10 (Based on 358 out of 500 marks)
- Subjects: Mathematics, Physics, Chemistry

Experience

Cybersecurity Intern – Elevate Labs (Best Performer) May 2025 – June 2025
Remote Internship Program, Ministry of MSME + Skill India

- Selected as Best Performer among participants for exceptional skills, professionalism, and analytical thinking.
- Worked on real-world cybersecurity challenges including vulnerability assessment, threat analysis, and incident response.
- Contributed to project deliverables such as threat intelligence summaries, scan reports, and remediation strategies.
- Tools Used: Nmap, Nessus, OpenVAS, Wireshark, GitHub, Markdown

Cybersecurity Analyst – Virtual Experience Projects May 2025 – June 2025
Mastercard, Deloitte, AIG, TCS, ANG (Forage Simulated Labs)

- Simulated SOC and cybersecurity analyst roles with real-world style incident response, threat hunting, and vulnerability assessments.
- Conducted CVE analysis, phishing detection, and documented full-stack attack scenarios including initial access, lateral movement, and data exfiltration.
- Analyzed network traffic using Wireshark, scanned assets with Nmap and Nessus, and created actionable security reports for fictional enterprise stakeholders.
- Followed SOC workflow including alert triage, investigation, incident documentation, and mitigation guidance based on MITRE ATT&CK techniques.
- Used GitHub for secure version control and documentation of investigation steps, tool outputs, and final reports.

Cybersecurity Defense Intern – Cyber Samurai Program March 2025
Remote, Hands-on Workshop

- Participated in advanced Red Team vs Blue Team defense simulations and real-time incident investigation challenges.
- Configured iptables firewall rules, traced threat actor activity through port scanning and packet capture, and documented findings.

- Improved network defense strategy by analyzing attack behavior patterns and proposing proactive detection rules.

Cybersecurity Trainee – Cyber Guru Program

February 2025

National Cybersecurity Awareness and Simulation Training

- Studied phishing, social engineering, and insider threats in enterprise settings and learned risk mitigation strategies.
- Performed simulated phishing campaign detection and contributed to awareness report generation using Markdown documentation.

Cybersecurity Trainee – ISRO Workshop on Cybersecurity & Geo-Location

January 2025

Indian Institute of Space Science and Research (IISR)

- Studied cybersecurity risks in satellite communication, space systems, and ground station networks.
- Conducted geolocation-based threat simulations and presented incident analysis to workshop leads.
- Received official certification from ISRO for completion of cybersecurity and geolocation training simulations.

Projects

Automated Threat Investigation Scanner

github.com/adi9032/webapp-vuln-scanner

- Built a Python-based scanner to identify common adversarial behaviors including XSS, SQLi, and CSRF patterns.
- Leveraged Requests, BeautifulSoup, and custom payload injection for behavioral analysis.
- Simulated attacker workflows and documented detection strategies aligned with MITRE ATT&CK.
- Tools Used: Python, Flask, Requests, BeautifulSoup, Markdown

Network Traffic Filtering & Threat Simulation

github.com/adi9032/personal-firewall

- Developed a custom personal firewall to simulate packet filtering and adversary control evasion techniques.
- Implemented live packet sniffing and rule management CLI for hands-on investigation.
- Tools Used: Python, Scapy, iptables, Linux

Malicious Extension Threat Intelligence Report

github.com/adi9032/Suspicious-browser-extensions-report

- Conducted analysis of browser extensions for signs of adversarial use cases including user tracking and data theft.
- Documented threats, mapped indicators, and provided mitigation strategies.
- Tools Used: Manual Analysis, Security Research, Markdown, GitHub

Cybersecurity: Vulnerability Assessment, Network Scanning, Penetration Testing (Basic), SOC Workflow Simulation, Threat Intelligence, CVE Analysis, Incident Reporting

Networking: OSI Model, TCP/IP, Firewall Rules, Port Scanning, Protocol Analysis

System Knowledge: Windows OS, Linux (Kali), Command Line Interfaces, Virtual Machines (VirtualBox)

Version Control: Git, GitHub CLI, Personal Access Token (PAT) Usage, Branching, Commit History Management

Documentation: Technical Report Writing, Markdown Formatting, GitHub Documentation, Cybersecurity Audit Reports.

Technologies

Languages: Python, Bash, HTML, Markdown, YAML

Technologies & Tools: Kali Linux, SIEM (simulated), Nmap, Nessus Essentials, OpenVAS, Burp Suite, Wireshark, Scapy, Git, GitHub CLI, Jupyter Notebooks, VirtualBox, Windows, Linux Terminal, MITRE ATT&CK Navigator

Skills

Threat Intelligence: Adversary Tracking, TTP Analysis, CVE Research, Threat Enrichment, Threat Modeling, Incident Triage, IOC Identification

Investigation: Log Analysis, Security Telemetry, SIEM-based Alert Investigation, Endpoint Behavior Analysis, Incident Reporting, Attack Surface Review

Cybersecurity: Vulnerability Scanning, Threat Detection, Red Team/Blue Team Simulation, Detection Engineering (Basic), Phishing Detection, SOC Workflow Simulation

Scripting & Automation: Python Automation, Bash Scripting, Data Parsing, CLI Workflows, Lightweight Tool Development

Documentation: Technical Reporting, Markdown/HTML, Investigation Logs, GitHub Wiki, Intel Sharing