





# Anirvinya Sharma

---

 [cyber.anirvinya@gmail.com](mailto:cyber.anirvinya@gmail.com)  +91 9374569125  Vapi, Gujarat  [anirvinya-sharma](https://www.linkedin.com/in/anirvinya-sharma)

---

## CYBER THREAT INTELLIGENCE ANALYST

---

Enthusiastic individual with a focus on securing critical information, malware detection, endpoint security and SOC operations. Possesses a foundation in Cyber Security and hands-on experience in Malware analysis and log analysis. Demonstrated ability to quickly grasp new concepts and apply them in practical scenarios. Keen interest in SOC management and threat intelligence and response, with a commitment to continuous learning and contributing to organizational success and securing the digital infrastructure.

## EDUCATION

---

### Masters in Cyber Security (M.Sc.)

National Forensic Sciences University, Gandhinagar  
CGPA: 8.01

Gujarat (2022 - 2024)

### Bachelor's of Computer Application (Hons)

Lovely Professional University, Jalandhar  
CGPA: 8.46

Punjab (2019 - 2022)

## EXPERIENCE

---

### COE (CS) Cyber Defence Centre, NFSU

(January 2024 - August 2024)

Student (Intern)

As a Student Intern at the COE (CS) Cyber Defence Centre, NFSU, contributed to cybersecurity research by working on various projects focused on real-world scenario, assisted development of various security tools and approaches to tackle or improve the current drawbacks.

### CyberXplore

Remote (March 2023 - April 2024)

Security Researcher (Intern)

- Focused on vulnerability research, identifying and analyzing software and network weaknesses, and developing security tools.
- Assisted in the development and enhancement of security tools and automation scripts. Contributed to detailed documentation and reporting on threats and vulnerabilities.

## PROJECTS

---

### *EVTX.py*

- Developed an efficient Windows Event Log parsing tool designed to extract actionable insights from system and security logs.
- Implemented using Python, subprocess and xml.dom.minidom
- The tool helps in the identification of security incidents, timestamps, troubleshooting of system issues, and aid in monitoring and pointing out potential threats.

### *Automated Malware Analysis and Sandboxing*

- Built a python based tool aiding in bulk analysis of purposed malicious files and help in better static and automated malware analysis in an isolated environment deployment.
- Utilized tools like VirtualBox, Oracle Snapshot Utility and VMware for creating nested sandboxed VMs.
- Established connections between nested VMs using WinSCP, for secured transfer of malicious files into the target machine for analysis.
- Leveraged Sysinternals and pefiles modules for aiding in the automated static analysis of the file.

## ONGOING PROJECTS

---

### **Dark Web OSINT (2024 - Present)**

- Currently in the development phase of a Dark Web OSINT tool, intended to facilitate the extraction and analysis of intelligence from hidden online sources.
- Refining capabilities for capturing and scrapping of information and illicit content from the websites.
- Uncovering and extracting information using regex for aiding in the investigation process.

### **Simplifying Threat Intelligence with ORCA2 (2024 - Present)**

- Developing a Python-based tool to translate complex Threat Intelligence (TTPs), from various sources like windows event files into easily understandable information.
- Mapping the TTPs with the MITRE framework to categorize cyber threats, techniques, tactics, and procedures (TTPs).
- Using the ORCA2 reasoning model by Microsoft to provide clear, actionable insights into various threats, enabling better comprehension and informed decision-making.
- Aiming to bridge the gap between technical data and practical understanding therefore enhancing awareness and response capabilities.

## ACHIEVEMENTS

---

### **2'nd Runner-up**

**Secured 2nd** place out of 10 teams in the Capture The Flag (CTF) competition organized by **Toyota Tsusho Systems, India (TTS)** at National Forensic Sciences University (NFSU), Gujarat Campus in 2024.

### **1'st Prize**

**Won first place in the Capture The Flag (CTF)** competition held by the School of Cyber Security and Digital Forensics for National Forensic Sciences University Students (NFSU) in the year 2023.

### **2'nd Runner-up**

**Secured second place in the AHAMROOT Capture The Flag (CTF)** competition held by the School of Cyber Security and Digital Forensics for National Forensic Sciences University Students (NFSU) in the year 2022

## CO-CURRICULAR ACTIVITIES

---

### **Discord Server Moderation (2020-2023)**

- Moderated and managed the Discord Server for Jinkou, a Solana-based NFT project, ensuring adherence to guidelines, providing technical support. partnerships, supported secure operations.

### **BSides Ahmedabad Security Conference (2024)**

- Part of the team assisted in organizing and managing event logistics while ensuring smooth execution of speaker sessions.
- Gained hands-on experience in cybersecurity community engagement and networking with industry professionals.

## SECURITY TOOLS

---

- |            |             |              |              |             |          |
|------------|-------------|--------------|--------------|-------------|----------|
| • Wazuh    | • ZenMap    | • SQLMap     | • ELK        | • BurpSuite | • ClamAV |
| • Suricata | • Nessus    | • FTK Imager | • Metasploit | • OWASP Zap | • Snort  |
| • Splunk   | • Wireshark | • Maltego    | • MISP       | • Postman   |          |

## TECHNICAL SKILLS

---

Threat Analysis and Response

OSINT

SOC & IRM

Malware Analysis

SIEM

VAPT

Network Penetration Testing

Blockchain Forensics

Digital Forensics

## SOFT SKILLS

---

Adaptability

Collaboration

Communication

Multitasking

## OS & PROGRAMMING

---

Windows

Linux

Python

Bash