Nivedita Waghmare

[niveditawaghmare2022@vitbhopal.ac.in](mailto:niveditawaghmare2022@vitbhopal.ac.in) - 9764097963

https://github.com/NW1306

Summary:

Detail-oriented and motivated fresher with a strong interest in digital forensics. Eager to leverage analytical skills and technical knowledge to investigate cyber incidents and support forensic investigations. Committed to continuous learning and contributing to team success in a dynamic digital environment.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Education:

St Helena’s High School

Bishop’s Junior College

BTech in Computer Science and Engineering in Cyber Security and Digital Forensics from VIT Bhopal - Current

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Skills:  
Programming Skills:

HTML CSS, Python

Technical Skills

Network Forensics, Malware Analysis

swap\_vert Analytical Skills

Critical Thinking, Problem Solving, Attention to Detail, Logical Reasoning

Software Proficiency

Wireshark

Digital Forensics

EC-Council Computer Hacking Forensic Investigator (CHFI) – In Progress

EC-Council | Hands-on Training in Digital Forensics, Incident Response & Cybercrime Investigation

Expected Completion: [June, 2025]

Computer Networks

Computer Networks

The Bits and Bytes of Computer Networking

Google via Coursera | Completed: [December, 2025]

Gained comprehensive knowledge of networking protocols, cloud computing, and network troubleshooting techniques.Domain Name System (DNS), Ipv4, Network model, Troubleshooting.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Academic Projects:

Current: Epics Project

Node.js, Built a profile data updation

Command & Control System for Ethical Hacking (Python)

Built a multi-client botnet-style command and control server to simulate post-exploitation techniques such as remote shell access, file transfer, screenshot capture, and session control.

[<https://github.com/NW1306/BOTNET/tree/main>] (https://github.com/NW1306)

Windows Keylogger for Digital Forensics (Python)

Created a keylogger that logs keystrokes for analysis in ethical forensics labs. Demonstrates how attackers monitor user input and reinforces the importance of endpoint protection.

[<https://github.com/NW1306/keylogger>] (https://github.com/NW1306)

Network Port Scanner (Python)

Developed a multi-threaded TCP port scanner that identifies open ports on a target system to detect network exposure and simulate attacker reconnaissance.

[[https://github.com/NW1306/portscanner](https://github.com/NW1306)](https://github.com/NW1306/portscanner%5D(https://github.com/NW1306))

Vulnerability Scanner (Python)

Engineered a basic scanner to identify common vulnerabilities (e.g., outdated services, open ports). Focused on practical security auditing in a controlled environment.

[<https://github.com/NW1306/vulscan>] (https://github.com/NW1306)

Intrusion Detection System (In Progress)

Designing an IDS using Python to detect suspicious traffic and anomalies in system logs for better network defense.