

Anand Pandey

anandpandey1982004@gmail.com | +91 7307451546 | <https://github.com/AnandPandey357> |
<https://www.linkedin.com/in/anand-pandey-898b1a235/>

EDUCATION

VIT Bhopal University	CGPA: 8.83
Bachelor of Technology, Computer Science and Engineering	October 2022 – onwards
UMA SHANKAR VIDYAPEETH	2021
12 TH Standard CBSE BOARD	97%
UMA SHANKAR VIDYAPEETH	2019
10 TH Standard CBSE BOARD	89%

SKILLS

- **Technical Skills:** Java, C++, Linux, Cyber Threat Intelligence, Network Security, Ethical Hacking, Incident Response
- **Tools:** Ghidra, Wireshark, Nmap, njRat, ADS Spy, Autopsy, BillCypher, GRECON, Burp Suite, Metasploit
- **Soft Skills:** Leadership, Event Management

PROJECT EXPERIENCE

1. Malware Analysis Using Method Identifiers

- **Analyzed WannaCry ransomware in a secure REMnux setup, identifying 12 key signs of infection (IoCs) to help detect threats quickly across enterprise networks without using third-party tools.**
 - **Used REMnux & FLARE VM to examine execution flow and simulate network traffic with INetSim.**
 - **Findings:** Identified key Indicators of Compromise (IoCs), C2 communication patterns, and obfuscation techniques.
 - **Impact:**
 - **Achieved 98% accuracy in malware classification.**
 - **Reduced manual analysis time by 35% through automated method tracing.**
 - **Enhanced detection efficiency by 40% using network simulation.**
 - **Technologies:** Kali Linux, Virtual Machine, REMnux, Flare VM, INetSim
 - **Project Link:** [Research Malware](#)
-

2. Malware Analysis by Reverse Engineering

- **Reverse-engineered WannaCry & Scareware malware using Ghidra to analyze function call patterns and detect vulnerabilities.**
- **Developed Python automation to detect exploitable functions & malware entry points.**
- **Findings: Identified three major attack vectors used for privilege escalation & remote execution.**
- **Impact:**
 - **Reduced malware analysis time by 40% via automated function identification.**
 - **Discovered 5 key vulnerabilities exploited for system compromise.**
 - **Improved accuracy of vulnerability detection by 30% using Python automation.**
- **Technologies: Kali Linux, Java, Python, Ghidra**
- **Demo Link:**
<https://github.com/AnandPandey357/MALWARE-ANALYSIS-USING-GHIDRA>

Relevant Courses: Ethical Hacking, Security Analyst, Cyber Physical Systems, Cybercrime and Laws, Advanced Cyber Security, Computer Network, Forensic Chemistry,

EXTRA-CURRICULARS AND ACHIEVEMENTS

- **Finalist** – Internal SIH, VIT Bhopal University (2024)
 - **Winner** – Project Expo (Cyber Physical Systems, Industrial Conclave)
 - **Winner** – National Mathematics Day (SERB)
 - **Hacker rank:** 3-Star in Java
 - **Google 2024** – Bits and Bytes of Computer Networking
 - **Cyber Physical Systems Certification** – Institute of Technology, Kharagpur
-
- **Hobbies:** Badminton, Singing.
 - **Languages:** English, Hindi.

CERTIFICATIONS

- **Certified Ethical Hacker (CEH)** – EC Council
- **Cyber Security Analyst** – IBM
- **GEN AI Using IBM Watsonx** - IBM
- **Foundations of Cyber Physical Systems** – NPTEL
- **Introduction to Cyber Security** – CISCO
- **Bits and Bytes of Computer Networking** – Coursera
- **Linux Training Course** – Udemy
- **Reverse Engineering: Ghidra** – Udemy