

Nikhil Chaudhari

Security Researcher

9518948812

<https://dncrypter.github.io/Portfolio/>
[linkedin.com/in/nikhil--chaudhari/](https://www.linkedin.com/in/nikhil--chaudhari/)
nikhilchaudhari296@gmail.com
<https://nikhil-c.medium.com/>

Technical Skills

Languages : Python, JavaScript, PHP, C, SQL

Tools: EDR, Splunk SOAR, IDS, IPS, Jira, Wireshark, Firewall, Sandbox, Nessus, Metasploit, Nmap, Burp Suite

Scripting: Powershell, Python, shell scripting | **other tools:** Suricata, Snort, Yara

Operating systems: Linux : Ubuntu, CentOS, RHEL, Kali linux, Windows : Server 2022

Other Skills: log analysis, Digital forensics, VAPT, Computer Networking, Problem Solving, Coordination, OWASP 10

Projects

EDR - Fox : The Ultimate DFIR tool

August – November 2024

- Developed **PowerShell scripts** automating the collection of over 20 forensic artefacts, reducing manual effort by **50%**.
- Enhanced incident response with comprehensive data collection, including **local IP info, security events, and active processes**.
- Integrated scripts with **Microsoft Defender for Endpoint**, increasing productivity by **80%**.
- Facilitated remote data collection and report generation, supporting both standard and admin user executions, showcasing the project's **flexibility and scalability**.

Splunk SOAR : Virustotal Playbook

November – October 2024

- Designed a **playbook** which can search for malicious activity in events using the **integrated Gorman_Virustotal app**.
- This SOAR playbook helps in incidents such as sql injection, XSS, Phishing, 0-days, Malwares, etc.
- Created and inserted custom **hash scanning script** that takes selected logs, extract hashes and processes them using Virustotal api-key with **reducing manual work and efforts by 2 hours** and increasing workflow efficiency.
- Achieved a **70% increment in productivity** through maintaining a productive work culture.

PhishGuard : AI integrated Phishing Analysis

June – August 2024

- Accurately analysed uploaded emails, achieving a **90% accuracy** rate in threat detection.
- Delivered precise reports with artefacts and severity scores, maintaining a **95% success rate** in identifying critical threats.
- Achieved an **80% reduction in manual effort** for phishing email testing by implementing **automated** analysis.
- Integrated AI and ML** into a web application using Flask and React, achieving a **93% precision rate in phishing** detection by analysing content for LLM generation and typo errors.

Experience & Trainings

Spin the Hack Pvt. Ltd.

October 2022 – January 2023

VAPT intern

- Acquired hands-on experience with tools such as Nessus, Nmap, Metasploit, exploitDB, Wireshark, and BurpSuite.
- Completed a case study with a score of 94/100, demonstrating proficiency in handling practical scenarios and creating professional reports.

Awards & Achievements

- Tryhackme top 17, Web-Recon Pentesterlab certified, Hackthebox & BlueTeamLabs practitioner, VAPT case study.
- Successfully coordinated and managed college tech events, as Head-coordinator of TechnoUtsav-2024.
- Currently practising and preparing for CEH and RHEL certifications.

Education

Government College of Engineering, Chandrapur

Aug 2020 – June 2024

BE in Electronics & Telecomm. Engineering

Maharashtra, India