



Kunal Walavalkar

✉ kunalw2002@gmail.com ☎ +91 9326745256 🔗 Personal Website  LinkedIn  Github

EDUCATION

2020 – 2024	Bachelors of Engineering in Computer Science <i>Vidyalankar Institute of Technology</i>	Mumbai, India
2022 – 2024	Minor degree in Cybersecurity <i>Vidyalankar Institute of Technology</i>	Mumbai, India

PROFESSIONAL EXPERIENCE

Digital Forensics Intern (Cyber Secured India)

March 2023 - July 2023

- Learnt networking fundamentals.
- Performed web application penetration tests using Burpsuite.
- Used Autopsy for data recovery, analysis of evidence and reporting.

PROJECTS

O.S.S.O.C 🔗

Proof of Concept for an open-source Security Operations Centre which has automation capabilities.

- Set up an endpoint on a Windows using Wazuh host to detect incidents and respond to them.
- Leveraged TheHive's case management to store IOC and classify incident.
- Used Cortex analyzers to query relevant threat intelligence feeds with the stored IOC.
- Created an automation workflow within Shuffle that performs all of these steps without the need of human intervention.

D|Cipher 🔗

Cryptography toolkit that allows users to encode and decode their text using an algorithm of their choice.

- Includes five different cryptography algorithms.

Hexplorer 🔗

Command-Line hexdump utility written in C.

- Allows developers and engineers to examine the raw bytes of a file or data stream.

Write-ups 🔗

Collection of CTF write-ups.

- Includes writeups for: Binary Exploitation, Reverse Engineering, Web Exploitation, Network Forensics, System Forensics

RiSkore 🔗

Calculator to calculate the risk faced by organizations

Risk is calculated based on the following factors suggested by OWASP:

- Threat agent: Skill level, Motive, Opportunity, Size of threat actor group.
- Vulnerability: Ease of discovery, Ease of exploit, Awareness, Intrusion Detection.
- Technical impact: Loss of Confidentiality, Loss of Integrity, Loss of Availability, Loss of Availability.
- Business impact: Financial Damage, Reputation Damage, Non-Compliance, Non-Compliance.

CERTIFICATIONS

- eJPTv2 🔗
- INE Certified Cloud Associate 🔗
- Fortinet NSE 1 🔗

SKILLS

Reverse Engineering

GNU Debugger, Cutter, Ghidra, Flare VM, REMnux

Penetration Testing

Burpsuite, Nmap, Metasploit, Nessus, OpenVAS, Windows, Linux

Secure Code Review

Semgrep, Manual Secure code review, SAST, DAST.

Programming

Python, Assembly, C

Digital Forensics

Autopsy, FTK Imager, Wireshark