Cybersecurity Internship Program – A Practical Approach to Ethical Hacking & Digital Defense

# Organization Overview

Digisuraksha Parhari Foundation is a registered non-profit (Section 8) in India focusing on:  
- Cybersecurity awareness  
- Information warfare research  
- Digital safety training  
- Internships and outreach programs  
- Strategic collaboration with law enforcement and academia

# Project Objective

To provide students and professionals a hands-on learning experience in ethical hacking, digital forensics, malware analysis, and cybersecurity tools via:  
- Practical labs  
- Real-world simulations  
- Research activities  
- Final project + CTF (Capture the Flag) event

# Course Curriculum

## Live Weekend Sessions (34 hours)

- Orientation & Cybercrime Basics  
- Malware Analysis  
- Cloud Security  
- Cyber Threat Intelligence  
- Digital Forensics  
- OSINT Techniques  
- AI in Penetration Testing  
- ISO 27005 & Risk Management  
- Car Hacking  
- Social Engineering  
- Rubber Ducky Payloads  
- Incident Response  
- CTF Final Exam & Project

## Practical Weekday Tasks (86 hours)

- MITRE ATT&CK Mapping & YARA Rules  
- IOC Feeds & APT28 Malware Case Study  
- Linux Privilege Escalation Labs  
- Web Exploits: XSS, SQLi, CSRF, SSRF  
- Vulnerable VMs (Mr. Robot, DC-1)  
- OSINT and Recon (Email, Metadata, IP)  
- Threat Hunting & Log Analysis  
- GitHub Submissions, Peer Reviews, Final Reports

# Deliverables

- GitHub repository with weekly folders  
- Malware reports (APT28, IOC)  
- OSINT Reports  
- XSS/SQLi Exploit Logs  
- YARA rules  
- Final Project Report  
- CTF Participation Sheet  
- Attendance via “Flag System”

# Tools & Platforms Used

- TryHackMe, HackThisSite, OverTheWire, VulnHub, MISP, PortSwigger, Hybrid Analysis  
- YARA, Wireshark, Burp Suite, Volatility, MobSF, ELK, Graylog

# Research Focus Areas

- Malware Reverse Engineering  
- OSINT Reconnaissance  
- VAPT  
- IoT/Automotive Security  
- API & Cloud Security Testing  
- Social Engineering  
- Compliance (ISO, PCI-DSS)

# Project Team Structure

- Mentor: Guides learning and research  
- Supervisor: Monitors performance  
- Nodal Officer: Coordinates internships in academic settings

# UGC Internship Alignment

- Duration: 120 Hours = 2–4 Academic Credits  
- Aligned with NEP 2020  
- Evaluated through logs, reports, presentations, attendance, and viva

# Sample Individual Project Topics

1. OSINT Techniques for Criminal Profiling  
2. Static & Dynamic Malware Analysis  
3. Web Application Security Testing  
4. IoT Security  
5. Detecting Deepfakes  
6. Social Engineering Simulations  
7. Digital Forensics Case Simulation

# Final Report Structure

1. Title Page  
2. Abstract  
3. Introduction  
4. Objective & Scope  
5. Tools Used  
6. Methodology  
7. Results  
8. Conclusion  
9. References  
10. GitHub Link

# Completion Benefits

- Government Certificate  
- Final Presentation  
- LinkedIn Endorsement  
- Resume-boosting GitHub Repo  
- OpenAI AI Tools Access