



Digisuraksha Parhari Foundation – Updated Ethical Hacking & Cybersecurity Course Schedule (Jul–Aug 2025)

Digisuraksha Parhari Foundation:

Introduction

Digisuraksha Parhari Foundation is a registered Section 8 non-profit organization in India focused on advancing cybersecurity, conducting impactful research, promoting information warfare awareness, providing hands-on internships, and running extensive awareness sessions throughout the country. The foundation is known for community service, industry participation, and collaboration with law enforcement and academic bodies.

Mission & Vision

- **Mission:**
To combat cyber threats, promote digital safety, and build cyber resilience through research, education, advocacy, and hands-on professional development.
- **Vision:**
To empower individuals and organizations to secure their digital lives and foster a secure, resilient digital ecosystem in India.

Research Work

- **Areas of Focus:**
 - Cyber threat landscapes, vulnerability management, and defense strategies.
 - Case studies on ransomware, hacking incidents, and digital forensics.
 - Development of open-source tools for deepfake detection, LFI scanning, and OSINT (Open-Source Intelligence).
 - Research contributions to law enforcement cybercrime investigations and threat actor profiling.
- **Information Warfare:**
 - Analyzing digital information threats including disinformation campaigns, social engineering tactics, and cyber psychological operations.

- Providing strategic insights to government stakeholders on cyber sovereignty, digital defense, and strategic communication.

Internship Programs

Cybersecurity & Ethical Hacking Internship

- **Format:**
100% online, accessible to students and professionals nationwide.
- **Duration:**
1 month (e.g., April–May 2025) or up to 2 months for specialized tracks.
- **Curriculum Highlights:**
 - Fundamentals of cybersecurity and ethical hacking
 - Cyber forensics and incident response
 - Car hacking and IoT security basics
 - Use of “Rubber Ducky” tools and social engineering
 - Malware analysis, incident investigation
 - Real-world case studies on cyberattacks and defense.
- **Outcomes:**
 - Hands-on projects and simulations
 - Live training from industry experts
 - Mentorship, certification, and career guidance
 - Contributions to foundation’s research and training materials.
- **Application:**
Open via the foundation’s website and platforms like Internshala, Unstop, and LinkedIn.

Awareness Sessions & Initiatives

- **Workshops & Educational Programs:**
 - Focus on vulnerability assessment, penetration testing (VAPT), data protection, secure browsing, and investigative forensics.
 - Regular sessions with schools, colleges, hospitals, and NGOs for digital awareness and cyber safety.
 - Collaborative awareness campaigns with law enforcement and community organizations.
- **Information Warfare Awareness:**
 - Seminars and webinars on combating digital misinformation and psychological manipulation in cyberspace.
 - Training in OSINT techniques, threat actor profiling, and detection of social media-based manipulation.
- **Community Engagement:**
 - National-level hackathons and competitions (e.g., as community partner for university cyber events).
 - Open sessions for the public on basic cyber hygiene and defense against everyday cybercrimes.

- Digisuraksha Parhari Foundation has been officially **verified and registered with Google for Nonprofits**, making it eligible to access and activate a suite of Google products for no cost, such as Google Ad Grants, Google Workspace for Nonprofits, YouTube Nonprofit Program, and Google Earth/Maps. As per current procedures, the verification was managed by Goodstack, a global partner facilitating nonprofit access to big technology company resources by validating the organization's legal and charitable status. Upon verification, Digisuraksha Parhari Foundation received guidance to activate the desired Google products and make full use of nonprofit management and outreach tools provided by Google.
- Additionally, the foundation has secured a **nonprofit discount and access to advanced AI tools through the ChatGPT nonprofit program**, positioning them to benefit from cutting-edge language assistance for research, project management, and outreach. Approval emails specifically mention eligibility for ChatGPT nonprofit discounts and reference broader recognition from other major tech partners, supporting Digisuraksha's operational and mission-driven needs.
- On **LinkedIn and other tech-sector networking platforms**, Digisuraksha Parhari Foundation's status as a verified and supported nonprofit is visible, helping it connect with stakeholders, partners, and volunteers for cybersecurity initiatives and digital safety campaigns.

Summary of Tech Partner Support:

- **Google for Nonprofits:** Full access to Google's suite of nonprofit resources, including productivity tools and Ad Grants for outreach.
- **OpenAI (ChatGPT):** Eligibility for nonprofit-specific discounts and enhanced access for AI-powered content creation and support.
- **LinkedIn:** Featured as a verified organization, facilitating broad community and professional engagement.
- **Other big tech partners:** The foundation is positioned to gain support and software from additional companies (e.g., Perplexity, Microsoft, etc.) as part of its verified nonprofit status, though specific integrations may depend on partner policies and registrations.
- Digisuraksha Parhari Foundation leverages this backing from global technology leaders to further its **cybersecurity education, awareness sessions, research, and project support activities** across India, as reflected in its public-facing communications and web presence.

Core Services & Solutions

Area	Description
Cybersecurity Research	Case studies, incident response research, OSINT, tool development
Training & Internships	Ethical hacking, forensics, malware analysis, hands-on projects
Awareness Programs	Digital safety workshops, seminars, social media campaigns
Consultancy	Free cybersecurity consulting for organizations, incident investigation
Community Engagement	Events, hackathons, partnerships with academic and law enforcement bodies

Additional Activities

- **Development of In-House Tools:**
Tools for cyber threat detection, deepfake identification, vulnerability analysis, and behavioral monitoring.
- **Support for Law Enforcement:**
Contributions to digital evidence collection, cyber forensic investigation, and advisory support in cybercrime cases.
- **Public Resources:**
Educational content, downloadable guides, social media updates, and participation in major cybersecurity conferences and events.

Recognition & Outreach

- Registered under the Ministry of Electronics & IT and NITI Aayog (NGO Darpan).
- High public trust with recognition for innovative cyber safety solutions and professional consulting.
- Frequent speaker and partner at major industry events and university hackathons.

Contact & Social Media

- **Website:** digisuraksha.org
- **Email:** support@digisuraksha.org

- Instagram: @digisurakshafoundation
- LinkedIn: Digisuraksha Parhari Foundation

By merging research, real-world information warfare intelligence, internships, and nationwide awareness programs, Digisuraksha Parhari Foundation stands as a leader in empowering India's digital future and combating emerging cyber threats.

UGC Internship Guidelines – Bullet Summary

Objective of the Internship

- Bridge academic learning with real-world workplace experiences.
- Develop job-ready, research-oriented, and ethically grounded graduates.
- Encourage active learning, creativity, and problem-solving.
- Enhance exposure to technologies, governance, and industry practices.
- Promote social responsibility and collaborative mindset.

Types of Internships

- **1. Employability-Focused Internship:**
 - Boosts confidence, teamwork, leadership, ethical values, and workplace readiness.
- **2. Research Aptitude Internship:**
 - Focus on ideation, data collection, simulation, analysis, academic writing, and ethics.

Key Skills & Competencies Developed

- Research methodology and analytical tools.
- Critical thinking and innovation.
- Communication of technical/research findings.
- Adaptability, collaboration, and ethical conduct.

Duration & Academic Credit Structure

- **60–120 hours = 2 to 4 credits** (after 4th semester).
- Mapped with UGC's **120 credit scheme** for 3-year UG and **160/164 for 4-year UG** programs.
- For Honours with Research: **12 credits**, with 360 hours in the 8th semester for dissertation/research work.

Internship Hosting Structure

- **HEIs must:**
 - Appoint a **Nodal Officer** to coordinate internships.
 - Set up an **R&D Cell** and digital internship portal.
 - Facilitate MoUs with industries, government bodies, NGOs, research labs.
 - Promote cluster-based, group, or individual internship opportunities.
 - Ensure evaluation, mentor assignment, and skill mapping.

Roles and Responsibilities

- **Internship Providing Organisation (IPO):**
 - Facilitate research/work environment, ID cards, access, etc.
- **Nodal Officer (from HEI):**
 - Organizes internship framework, outreach, MoUs, and intern welfare.
- **Internship Supervisor:**
 - Monitors attendance, project progress, and final report.
- **Mentor:**
 - Guides the intern academically/professionally; validates and certifies internship.

Evaluation & Monitoring

- **Components:**
 - Weekly logs, project report, presentation, attendance, and viva-voce.
- **Criteria:**
 - Innovativeness, research quality, ethics, skill acquisition, and impact.

Domains of Internship

Students may intern in diverse sectors such as:

- Cybersecurity and IT
- Education, Public Policy, Governance
- Environment, Agriculture, Art, and Design
- Health, Finance, Law, Communication, and more

Special Provisions

- Internship doesn't affect core academics if conducted during summer/winter breaks.
- Digital or remote internships are acceptable alternatives if physical mode is not feasible.
- Mentors may include retired scientists, local experts, professionals, or international collaborators.

For Digisuraksha Parhari Foundation

Based on this framework, the foundation's internship:

- Complies with the **UGC 120-Hour Credit Model**.
- Covers both **employability** (VAPT, Linux, GitHub) and **research** (threat intelligence, OSINT, etc.).
- Includes **community involvement**, **law enforcement engagement**, and **open-source research**.
- Supports **offensive/defensive cybersecurity**, aligning with NEP 2020's focus on digital skills.

Total Duration:

- **120 Hours**
 - **Live Sessions (Weekends): 34 hours**
 - **Practical Work (Weekdays): 86 hours**

Live Technical Sessions (2 hrs per session)

Cybersecurity Internship Program Schedule

#	Date	Day	Topic	Category
1	15 Jul	Tue	Orientation & Course Walkthrough	Program Kick-off
3	19 Jul	Sat	Introduction to Cybercrime & Ethical Hacking	Fundamentals
4	20 Jul	Sun	Malware Analysis – Static & Dynamic	Malware Analysis
5	25 Jul	Fri	◆ Session	To Be Declared
6	26 Jul	Sat	Cyber Threat Intelligence	Threat Intelligence
7	27 Jul	Sun	Cloud Security Testing	Cloud Security
8	1 Aug	Fri	◆ Session	To Be Declared
9	2 Aug	Sat	Digital Forensics – Tools & Evidence Handling	Digital Forensics
10	3 Aug	Sun	OSINT (Open Source Intelligence) Techniques	OSINT
11	8 Aug	Fri	◆ Session	To Be Declared
12	9 Aug	Sat	AI in Penetration Testing	Recon
13	10 Aug	Sun	PCI-DSS	Compliance + AI PT
14	15 Aug	Fri	◆ Session <i>(Independence Day)</i>	To Be Declared

15	16 Aug	Sat	ISO 27005 + Vulnerability Rating + Risk Mgmt	InfoSec Governance
16	17 Aug	Sun	Passwordless Auth & Identity Attacks	Exploitation
17	22 Aug	Fri	◆ Session	To Be Declared
18	23 Aug	Sat	Social Engineering & Psychological Tactics	Social Engineering
19	24 Aug	Sun	Car Hacking – Intro to Automotive Security	IoT/Automotive
20	29 Aug	Fri	◆ Session	To Be Declared
21	30 Aug	Sat	Rubber Ducky & HID Payloads	Hardware Hacking
22	31 Aug	Sun	Lock Picking & Device Access Exploits	Physical Security
23	5 Sep	Fri	◆ Session (<i>Teacher's Day</i>)	To Be Declared
24	6 Sep	Sat	Incident Response & Threat Hunting	IR & Threat Hunting
25	7 Sep	Sun	● Project Presentation + 🗡️ CTF Final + Closing	Final Exam & Project
26	12 Sep	Fri	◆ Session	To Be Declared
27	15 Sep	Mon	🎓 Certificate Distribution Ceremony	Completion & Recognition

Practical Work Plan (86 Hours)

Weekdays (Mon–Fri), flexible 2–3 hrs/day. Tasks to be submitted via GitHub or email.

Week	Focus Topics	Tools / Platform	Hours
1	MITRE Mapping, TTP Analysis	TryHackMe, Custom Labs, YARA, MISP	14
2	✅ Malware Report Writing, IOC Feed Analysis, Threat TTP Mapping & Real-life Case Studies (APT28)	MalwareBazaar, Hybrid Analysis, MISP	12
3	Linux & Command Practice (OverTheWire: Bandit), Local Priv Escalation	OverTheWire, THM	10
4	OSINT Lab Work (Email, Metadata, Image, IP Tracking), Passive & Active Recon	HackTheSite, THM (OHSint, Shodan)	10
5	Web Exploits (XSS, SQLi, CSRF, Auth Bypass, SSRF)	PortSwigger, THM	12
6	Vulnerable VM Exploitation (Mr. Robot, Basic Pentesting, DC-1)	VulnHub	12
7	Log Analysis, Event Timeline Reconstruction, Threat Hunt Drill	THM IR Labs, Graylog, ELK	8
8	Final Lab Cleanup, GitHub Push, Report Review & Peer Check	GitHub, PDF Docs	8

Deliverables by Students

- GitHub Repo with Documentation
- Mitre Attack framework ttps all solving
- IOC + YARA Rule Submissions
- Threat Report (.doc/.pdf)
- Final Project Walkthrough
- CTF Score Sheet

Lab Platforms Used

- [TryHackMe.com](https://tryhackme.com)
- [OverTheWire.org](https://overthewire.org)
- [HackThisSite.org](https://hackthissite.org)
- [VulnHub.com](https://vulnhub.com)
- [PortSwigger Web Academy](https://portswigger.com/webacademy)
- [MISP Project](https://misp-project.org)
- [MalwareBazaar](https://malwarebazaar.com)
- [Hybrid Analysis](https://hybrid-analysis.com)

Repo Name: Cybersecurity-Internship-Program-2025

GitHub Repository Folder Structure (Tree Format)

plaintext

CopyEdit

Cybersecurity-Internship-Program-2025/

├── README.md

├── Week-1_MITRE-TTP-Mapping/

| ├── MITRE-Map.md

| ├── YARA-Rules/

| | └── apt28_custom.yar

| ├── MISP-Export/


| └── Screenshots/

- └── Week-2_Malware-IOC-APT28/
 - └── Malware-Reports/
 - └── APT28-CaseStudy.pdf
 - └── IOC-Feeds/
 - └── MISP-Exports/
 - └── HybridAnalysis-Summary.md
- └── Week-3_Linux-Privesc/
 - └── Bandit-Writeup.md
 - └── Local-Privesc-CheatSheet.md
 - └── Screenshots/
- └── Week-4_OSINT-Recon/
 - └── Email-Metadata-Report.pdf
 - └── Image-Tracking-Tools.md
 - └── Passive-Recon.md
 - └── OHsint-Notes.md
- └── Week-5_Web-Exploits/
 - └── XSS-Report.md
 - └── SQLi-Logs.md
 - └── SSRF-Test-Scripts/
 - └── PortSwigger-Links.md
- └── Week-6_VulnVMs/
 - └── MrRobot-Writeup.md
 - └── DC-1-Root.md
 - └── Screenshots/
- └── Week-7_Log-IR/
 - └── Graylog-Queries.md

```
| |—— Timeline-Reconstruction.xlsx
| |—— Threat-Hunting-Checklist.md
|—— Week-8_Finalization/
| |—— Final-Reports/
| | |—— Internship-Report_YourName.pdf
| |—— GitHub-Upload-Guide.md
| |—— Peer-Review-Summary.md
|—— LICENSE
```

Access Instructions

To **grant access to support@parharifoundation.org**:

1. Go to the repository on GitHub.
2. Click on  Settings → Collaborators & teams.
3. Click **Add people** → Enter the email support@digisuraksha.org or GitHub username (if known).
4. Assign role: Write (for uploads) or Admin (if they need full control).
5. Click **Invite**.

Optional Enhancements

- Add GitHub Actions to auto-check markdown/PRs.
- Use .gitignore for .DS_Store, *.log, etc.
- Use Issues to track submission status and review deadlines.

Let me know if you'd like:

- A **ZIP of this folder template**
- A **custom README.md**
- Help setting up this repo directly via GitHub CLI or GitHub Classroom integration for interns.

Attendance System Using Flags & GitHub

Attendance Folder Structure (in GitHub)

Cybersecurity-Internship-Program-2025/

- └── Attendance/
 - └── Week-1/
 - └── ShivamMittal_Flag1_Enter.jpg
 - └── ShivamMittal_Flag2_BlurMode.jpg
 - └── ShivamMittal_Flag3_LinkedInPost.jpg
 - └── Week-2/
 - └── ...
- └── README.md

► Flag System for Attendance



Flag No.	Name	Description
	Enter Flag	Simply join the session (Zoom/Meet etc.) – take a screenshot of your screen
	Blur Mode	Use your camera in blur mode during session – screenshot it
	LinkedIn Post	Post about the internship session with hashtags (e.g., #digisuraksha)
	Social Flag	Share a story, reel, or tweet on any social media platform

📺 What Interns Must Do

1. **Attend session** and complete at least 1 flag during or after the session.
2. **Take a screenshot** as proof of the flag.
3. **Upload the screenshot** to:

1. CopyEdit
2. /Attendance/Week-X/YourName_FlagX_Description.jpg
3. **Optional:** Add a short README.md in each week folder with a description:
4. markdown

Week 1 Attendance - Shivam Mittal

- Flag 1: Entered session on Zoom 
- Flag 2: Camera Blur Mode active 
- Flag 3: LinkedIn Post: [Link to Post](https://linkedin.com/...)

Example README.md for Attendance Folder

markdown

Attendance System - Instructions

To mark attendance:

1. Participate in the session.
2. Complete at least 1 flag (more = better visibility).
3. Take a screenshot.
4. Upload here in the format: `YourName_FlagX_Desc.jpg`

Flags:

- Flag 1: Session Entry
- Flag 2: Blur Mode On (with Camera)
- Flag 3: LinkedIn Post (with relevant hashtags)
- Flag 4: Social Story/Post (Instagram, Twitter, etc.)

Let me know if you want:

- A **pre-made Attendance folder template in ZIP**
- A **GitHub Actions workflow** to auto-check uploaded attendance

- A **weekly leaderboard system** based on flags earned

1. Individual Projects

- Each team member will work on a **separate project** that results in a **single research paper** or **report**.
- Focus areas: OSINT, Malware Analysis, VAPT, Mobile Security, Cloud Security, API Pentesting, etc.

1. Tool-Based Focus (2-Week Cycles)

- Every 2 weeks, teams will deep-dive into **2 cybersecurity tools** (e.g., Burp Suite, Volatility, Wireshark, MobSF, etc.).
- Each tool-based sprint includes:
 - Hands-on tasks
 - Research & documentation
 - Mini-project / PoC (Proof of Concept)
 - Final presentation and GitHub submission

1. Centralized Project Repository

- All work is documented in a **central GitHub repository** with proper folder hierarchy:

Task 1: Learn GitHub

Understand the basics of version control using Git and GitHub:

- Explore repositories, commits, branches, pull requests.
- Recommended: [GitHub for Beginners - YouTube](#)

Task 2: Learn Linux Administration

Gain foundational skills in Linux:

- Basic commands, file handling, permissions, services, users.
- Recommended: [Linux for Beginners - Free Course](#)

Task 3: Create Your GitHub Account

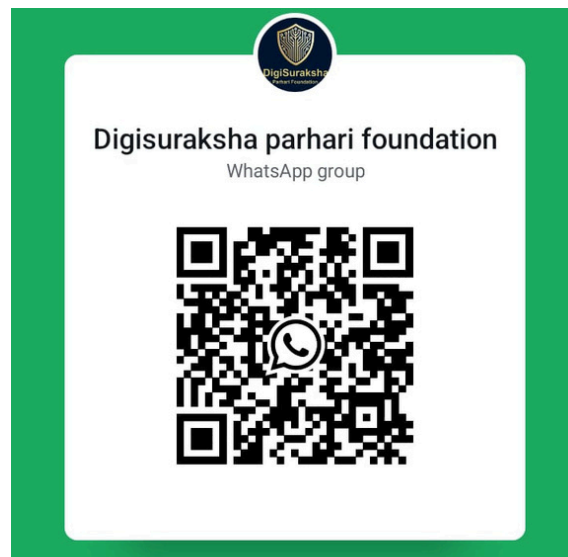
- Sign up: <https://github.com>
- Use your real name for professional credibility.

Task 4: Create a New Repository

- Name it something like cybersecurity-internship-digisuraksha.
- Divide the repo into **two folders**, one for each month (e.g., /Month1 and /Month2).
- Update your progress weekly by pushing documentation, assignments, and screenshots.

📱 Task 5: Join & Pin the WhatsApp Group

- Join the official WhatsApp group here:



- Pin the group for important updates and communication.

📱 Task 6: Follow Us on Social Media

Stay updated and support the foundation by following us:

- [🔗 LinkedIn](#)
- [📷 Instagram](#)

✅ **Deadline to Complete Tasks:** [Insert Deadline, e.g., July 18, 2025]

Once completed, update your GitHub repository and share the link in the WhatsApp group.

Let's build your cybersecurity journey together! 💻🛡️

For support, reach out on WhatsApp or contact@digisuraksha.org

