

Cyber Leelawat – Cyber Security Internship Program

Organized By: Cyber Leelawat

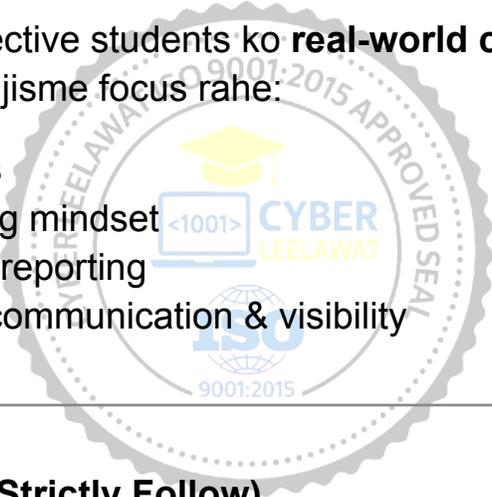
Duration: 1 Month (4 Weeks)

Mode: Online | Hands-on Labs

Language: Hinglish (English + Hindi)

Program Objective

Is internship ka objective students ko **real-world cybersecurity exposure** dena hai jisme focus rahe:

- Practical skills
 - Ethical hacking mindset
 - Industry-style reporting
 - Professional communication & visibility
- 
-

Mandatory Rules (Strictly Follow)

- Har task **7 din ke andar submit karna compulsory**
 - **Live / recorded presentation mandatory**
 - **Non-submission OR presentation miss = Disqualification**
 - Sirf **legal & authorized platforms** par testing allowed
 - Har task submit karne ke baad **LinkedIn par sharing mandatory** (details below)
-

LinkedIn Visibility Requirement (Mandatory)

Har task ke successful submission ke baad:

1. Apni **LinkedIn profile par ek post share karni hogi**
 2. Post me:
 - Task ka short overview
 - Tools / labs used
 - Learning outcome
 3. **Tag karna compulsory hai:**
 - [Cyber Leelawat](#) (Company Page)
 - Hiring Manager ([Virendra Kumar](#))
-

Internship Structure & Weekly Tasks

Week 1 – Information Gathering & Networking Fundamentals

Focus: Passive Recon + Networking Basics

What You'll Learn

- Public information gathering
- DNS, IP, subdomains basics
- Networking fundamentals (beginner-friendly)

Mandatory Lab (TryHackMe)

Room: Information Gathering

1. Passive Reconnaissance

👉 <https://tryhackme.com/room/passiverecon>

2. Active Reconnaissance

👉 <https://tryhackme.com/room/activerecon>

Room: Intro to Networking

👉 <https://tryhackme.com/room/introtonetworking>

- **Slow Walkthrough:**
 - Concepts explanation
 - Manual understanding of networking basics
- **Medium Walkthrough:**
 - Lab completion with screenshots
 - Commands & outputs explanation

Practice Targets (Recon – Public Info Only)

- <https://www.cyberleelawat.in>
- <https://tryhackme.com>

Suggested Tools

- Shodan
- crt.sh
- Hunter.io
- Whois
- Subfinder
- Amass
- Httpx



Deliverables

- [findings.pdf](#)
- TryHackMe completion proof

Note: No exploitation. Sirf publicly available information.

Week 2 – Port Scanning & Service Enumeration

Focus: Nmap mastery + Enumeration

🔧 Mandatory Lab (TryHackMe)

Room: Further Nmap

👉 <https://tryhackme.com/room/furthernmap>

- **Slow Walkthrough:**
 - Step-by-step Nmap flags explanation
 - TCP / UDP / Version scan concepts
- **Medium Walkthrough:**
 - Full lab completion
 - Output analysis & screenshots

🔧 Tools

- Nmap
- Searchsploit
- msfconsole

🧠 Extra Requirement (Metasploitable VM)

Download Metasploit link:

<https://sourceforge.net/projects/metasploitable/>

- Exploit **any 3 vulnerable services**
- Medium-level walkthrough required
- Risk + mitigation explanation

📦 Deliverables

- [ports-report.html](#)
- Scan & exploit screenshots
- TryHackMe proof

Week 3 – Web Application Bug Hunting

Practice Platforms

Website :-

1. testphp.vulnweb.com
2. testfire.net
3. <https://tryhackme.com>
4. <https://www.cyberleelawat.in>

Platform :-

1. TryHackMe
2. PortSwigger Web Security Academy

Vulnerabilities to Cover

- XSS (Reflected & Stored)
- Information Disclosure
- HTML Injection

Extra: PortSwigger Labs

XSS labs (2) — slow + medium walkthroughs

1. Reflected XSS — find reflected param, manual payload
2. Stored XSS — inject in comment/profile, show persistent execution.

Information Disclosure (2) — slow + medium walkthroughs

1. Information disclosure via error messages
2. Source code disclosure via backup files / old backups

Extra: TryHackMe Labs

Xss Lab — slow + medium walkthroughs

<https://tryhackme.com/room/axss>

Deliverables (Per Vulnerability)

- PoC Screenshot

- Vulnerability Report (PDF)
 - Mitigation Section
-

Week 4 – Social Proof + Mini Project

Part A – Social Media Proof

Submit timestamped screenshots after following:

- **YouTube :-** <https://www.youtube.com/@CyberLeelawat>
 - **LinkedIn Company Page :-**
<https://www.linkedin.com/company/cyberleelawat>
 - **Instagram (both handles) :-**
https://www.instagram.com/cyber_leelawat,
<https://www.instagram.com/cyberleelawat>
 - **Hiring Manager LinkedIn Profile :-**
<https://www.linkedin.com/in/mrleelawat/>
-

Part B – Mini Project (Choose Any ONE)

1. **Password Strength Checker :- (Python)**
2. **Website Information Tool (Recon-lite) :- (Python)**
3. **Port & Service Scanner + HTML Report :- (Python)**
4. **Keylogger Detector :- (Python)**

Project Deliverables

- GitHub Repository
 - README
 - Demo Video
 - Final Project Report
-

Mandatory Internship Video Review

Duration: 30–60 seconds

Cover:

1. Kya seekha
2. Kya benefit mila
3. Best part
4. Improvements
5. Trainer review

 **Contact & Submission**

 cyberleelawat@gmail.com

Prepared By: Program Coordinator – **Cyber Leelawat**

