# CFSS Internship

Welcome to CFSS - Your Cybersecurity Internship Journey Begins!

**Dear Intern**,

We're thrilled to have you on board for this exciting cybersecurity internship program at CFSS! Here are some important details about your project:

Project Confidentiality: Please remember that the project provided is confidential. Do not share it with anyone outside of CFSS.

Evaluation Process: Your answers won't be marked by a specific scale. Our task checker will assess your explanations comprehensively.

Letter of Recommendation: The top 50 interns will receive a coveted Experience Certificate. This endorsement can significantly bolster your prospects in the security field.

Project Submission: Ensure your personally curated project reaches us by April 22th in PDF format. The submission form will open on April 23th.

Scoring System: A total of 100 points are available. To achieve certification, strive for a minimum of 65 points. Aim for excellence and attempt as many questions as possible to secure a spot in the top 50.

CTF Accounts: If your project includes CTF challenges, kindly create accounts on the specified websites.

Screenshots: Enhance the clarity of your project by including screenshots.

Presentation Matters: Make your project clean, clear, and visually appealing. A well-presented project facilitates a thorough evaluation.

ISO with IAF & MSME Verified Certificate: Our certificates hold ISO (with IAF) and MSME verification by the Indian Government, ensuring global recognition and guaranteeing the quality and authenticity of our programs. Your completion certificates will hold substantial value in the cybersecurity industry worldwide.

We're confident that this internship will be an enriching experience for you, and we're excited to see the incredible projects you'll create!

# CFSS CyberSecurity & Ethical Hacking Project

Please ensure that you have Kali Linux or Parrot Linux installed on your machine, as well as the Metasploitable virtual machine.

Q1. Vulnerabilities scanning:

1. Install Nessus on your system.

2. Perform a vulnerability scan on the Metasploitable machine using Nessus.

Take screenshots of the identified vulnerabilities.

Provide a detailed description of the scanning process, including any configurations or settings used. Submit the screenshots along with the description.

Q2. Utilize various tools such as Sublist3r and Maltego, along with the search engine Netcraft, to discover subdomains of the target 'bbc.com'. Additionally, please capture screenshots of your findings.

Q3. Explain what the Wayback Machine is and how it functions. Describe the process of retrieving sensitive data from the Wayback Machine. Provide a screenshot of how the website 'bbc.com' appeared in 2010, obtained from the Wayback Machine.

Q4. Establish a connection to a local area network (LAN) via Wi-Fi. Utilize the NMAP tool to determine the number of devices currently connected to the LAN. Please include the specific command you used for this task and provide a screenshot of your terminal showing the results.

Q5. Perform privilege escalation on the Metasploitable machine and provide a detailed description of the process you used to achieve this. Explain how you gained elevated privileges.

# CFSS Internship

Q6.Employ a password cracking tool such as John the Ripper or Hydra to illustrate how a weak password can be compromised. Provide a detailed explanation of the step-by-step process you followed to achieve this.

Q7. Conduct a simulated phishing attack in a wide area network (WAN) environment using any suitable tool to demonstrate potential risks, specifically focusing on accessing webcams. Provide a detailed account of the steps you took during the simulation.

Additionally, explain effective strategies for educating and raising awareness among employees about safeguarding against such types of phishing attacks.

Q8. Scenario:

You work for a medium-sized e-commerce company that handles a large volume of customer data, including personal information and payment details. The company's website and backend systems are crucial for operations.

One morning, an employee notices unusual activity on the company's internal network monitoring system. After further investigation, it becomes evident that an unauthorized user has gained access to the company's customer database. The security team suspects a potential data breach.

Task:

As an intern in the cybersecurity and ethical hacking domain, your task is to develop an incident response plan to address this situation. The plan should outline the steps to take in case of this security incident.

# CFSS Internship

Q9. Provide an in-depth explanation of the distinctions between WEP, WPA, WPA2, and WPA3 in the context of wireless networking. Additionally, please share your recommendation for the most secure option among them and elucidate the reasons behind your choice.

Q10. Can you provide insight into the methods for accessing a CCTV camera without authorization? If so, kindly describe the process. If not, please elucidate the challenges and difficulties you encounter in attempting to gain unauthorized access.