CFSS Internship

(Rules & Regulations)

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: If you're one of the top 50 interns, you'll have the opportunity to get a coveted 'Letter of Recommendation' (LOR). To help us with collaborations, there's a small charge for the LOR, which is not a significant amount.

Why do we do this? It's all about creating connections with other companies that can boost your chances of landing a job quickly!

Project Submission: Ensure your personally curated project reaches us by November **25th** in PDF format. The submission form will open on Last Week of November.

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 and small video.

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

Government Approved Certificate: Upon successful submission and passing the evaluation, you will receive a government-approved certificate.

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 Penetration Testing Project

Practical Challenges:- (Perform any 8)

1. https://ctflearn.com/challenge/114
2. https://ctflearn.com/challenge/109
3. https://defendtheweb.net/playground/where-am-i
4. https://www.vulnhub.com/entry/hacklab-vulnix,48/
5. https://play.picoctf.org/practice/challenge/262
6. https://www.vulnhub.com/entry/fristileaks-13,133/
7. https://play.picoctf.org/practice/challenge/109
8. https://play.picoctf.org/practice/challenge/4
9. https://www.vulnhub.com/entry/kioptrix-level-12-3,24/
10. https://www.vulnhub.com/entry/escalate-my-privileges-1,448/

Theory Questions: Attempt All

1. Explain the difference between vulnerability assessment and penetration testing.

2. Describe the role of social engineering in a penetration test and how it can be mitigated.

3. What is privilege escalation, and how is it achieved during a penetration test?

4. Discuss the significance of a honeypot in a cybersecurity environment.

5. How does a Denial of Service (DoS) attack differ from a Distributed Denial of Service (DDoS) attack, and what measures can mitigate their impact?

6. Explain the concept of "pivoting" in a penetration test and its significance in lateral movement within a network.

7. Describe the concept of "zero-day" vulnerabilities and propose strategies to mitigate their impact in cybersecurity.