ShadowFox

LEARN • CREATE • LEAD

Cyber Security Internship Task List

Internship Pre-requisites before starting your tasks:

1.LinkedIn Profile Update: Ensure that your LinkedIn profile is updated to reflect your technical skills, and update your experience section to include **"ShadowFox Cyber Security Intern."**

2.LinkedIn Post: It's not mandatory to post the offer letter on LinkedIn, but if you wish to receive **extra swags** at the end of the internship, you can post your offer letter and **tag us** to receive assured swags.

3. Completion of Tasks: Complete the required tasks as specified in this Task List.

4. Proof of Work: At ShadowFox, we value **Proof of Work** (POW). You need to get validated from your mentor before you submit your respective tasks in the Task Submission Forms.

Note: Do not upload your Report in LinkedIn, this would allow others to copy your work. If the team finds out that you have posted your report in LinkedIn, your internship would be terminated.

After completing all the above steps, proceed with your task completion.Kindly note that all the details and reports you submit will be thoroughly verified before you receive the swags.

Task Level (Beginner):

1) Find all the ports that are open on the website http://testphp.vulnweb.com/
2) Brute force the website http://testphp.vulnweb.com/ and find the directories that are present in the website.
3) Make a login in the website http://testphp.vulnweb.com/ and intercept the network traffic using wireshark and find the credentials that were transferred through the network.

Task Level (Intermediate):

1) A file is encrypted using Veracrypt (A disk encryption tool). The password to access the file is encrypted in a hash format and provided to you in the drive with the name encoded.txt. Decode the password and enter in the vera crypt to unlock the file and find the secret code in it. The veracrypt setup file will be provided to you.

2) An executable file of veracrypt will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot.

3) Create a payload using Metasploit and make a reverse shell connection from a Windows 10 machine in your virtual machine setup.

4) Make a deauth attack in your own network and capture the handshake of the network connection between the device and the router and and crack the password for the wifi. To crack the password create a wordlist that can include the password of your network.

Task Level (Hard):
You Need to do 1 task out of 3

1) Using the Tryhackme platform, create a Panda room available in the king of the hills. Penetrate the machine and obtain the root access. Paste your name into the king.txt file and create a detailed report detailing the penetration test process and your plan to patch it.

(OR)

2) Using the Tryhackme platform, launch the Basic Pentesting room. Penetrate the room and answer all the questions that are given to you on the website and also create a detailed document of the process of penetration and how you did it.

(OR)

3) Create a detailed report including the information, planning and the attacks initiated and steps involved to analyze and initiate the attack in the website http://testphp.vulnweb.com/

Drive link for TASK 2 :-
https://drive.google.com/drive/folders/1hG7gOIms7Efnp8MtVmBTjzNqqHxEkY67