Activity File: Interview Questions

Instructions

The work you did on this project cuts across a wide range of topics: network security logging and monitoring, offensive and defensive security.

When networking and talking to potential employers, you should know how to discuss the work you did on your project to address specific interview questions or to show your skills within a specific domain. This section will teach you how to do this.

First, you will choose a domain that you are interested in pursuing as a career. For this project, you will choose from among the following domains:

- **Network Security**
- **Logging & Monitoring**
- **Offensive Security**
- **Defensive Security: Incident Response Phases I & II**

If you are unsure of which domain you would like to focus on, that's ok! You can either choose the one that you are the most comfortable discussing, or you can also complete the tasks in two or three domains.

For each domain, you will be provided a set of interview questions. For each question, you will be prompted to think about specific aspects or tasks you completed in Project 2 that you can use to answer the question.

In this section, you will:

- **Select one domain and one question.**
- **Write a one-page response that answers the question using specific examples from your work on Project . Your response should flow and read like a presentation while still keeping the general structure of the**

technical question response guidelines.

A good response includes the following:

- **Restate the Problem**
- **Provide a Concrete Example Scenario**
- **Explain the Solution Requirements**
- **Explain the Solution Details**
- **Identify Advantages/Disadvantages of the Solution**

Including each of these components will ensure you provide the interviewer with proof of competency of subject matter and critical thinking.

Submission Guidelines: You will submit your one-page response. At the end of the project, you will have the opportunity to present your answer if you desire

---

Common Interview Questions

Below you will find a list of questions, grouped by specific domains. Select one question to answer.

For each question, feel free to use the provided prompts to structure each section of your response.

Domain: Offensive Security

Question 1: Planning an Engagement

How do you plan and execute an effective offensive engagement?

- In order to execute an effective offensive engagement:
    - I make sure I have clear objective in mind.
    - Avoid Bad Operational Security
- Provide a Concrete Example Scenario
    - In this Project there are 3VMs on the network
        - Kali Machine - used to attack the target machine
        - Capstone Machine - the target Machine
        - HyperV Azure Host Machine - used for blue teaming
    - The Kali Machine is used for infiltration.
    - My goal in infiltrating the VM is to get a hold of the secret folder and webDAV folder.
    - I used the following tools to infiltrate the VM:
        - Hydra - for Brute force
        - Nmap to do a port scan and look for open ports
        - Crackstation.com to crack the hashed password.
        - Reverse shell to access the webDAV
- Explain the Solution Requirements
    - I Identified my target by finding the ip address using “curl ifconfig.me”
    - I then did a port scan to identify which ports are open using nmap.
    - Once I knew the open ports were open I opened a browser and tried which one of them is accessible and then began the infiltration.
- Identify Advantages and Disadvantages of the Solution
    - For this project the methods used were detectable by monitoring solutions as we are also required to record and analyze the attack.
    - In order to be more stealthy I recommend doing slower scans.