Activity File: Domain-specific 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 3 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 3. 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: Network Security

▼ Click to expand.

Question 1: Faulty Firewall

"Suppose you have a firewall that's supposed to block SSH connections, but instead lets them through. How would you debug it?"

Make sure each section of your response answers the questions laid out below.

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 3, which machines were on the network?

- Which VMs were servers? Which protocol(s) did they serve?
- Which VMs were clients? Which servers did they communicate with?
- What network access policies were in place?

3. Explain the Solution Requirements
    - If one of your Project 3 VMs accepted SSH connections, what would you assume the source of the error is?
    - Which general configurations would you double-check?
    - What actions would you take to test that your new configurations are effective?
4. Explain the Solution Details
    - Which specific configurations within the faulty VM would you inspect to investigate the problem?
    - Which specific settings would you check?
    - How would you attempt to connect to your VMs to test that your fix is effective?
5. Identify Advantages and Disadvantages of the Solution
    - Does your solution guarantee that the Project 3 network is now "immune" to all unauthorized access?
    - What monitoring controls might you add to ensure that you identify any suspicious authentication attempts and/or failures?

Question 2: Unsecured Web Server

"Suppose you find a server running HTTP on port 80, despite compliance guidelines requiring encryption in motion. What do you do?"

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 3, did you have servers running HTTP on port 80? If so, why was it permissible to do so?
    - In a "real" deployment, which specific machine would you configure differently? How

and why?

3. Explain the Solution Requirements
    - Why is running HTTP on port 80 problem?
    - How would you reconfigure a server to serve HTTP traffic safely?
    - How does this solution fix the problem?
4. Explain the Solution Details
    - Which tools and technologies would you use to implement this solution in Project 3?
    - How would you specifically use these tools to harden your deployment?
5. Identify Advantages and Disadvantages of the Solution
    - Will your solution break clients that used to communicate with the server over port 80?
    - Do you have to do any work to keep this solution running long-term? Or can you simply "set it and forget it?"

Domain: Logging & Monitoring

▼ Click to expand.

Question 1: Setting Alerts in a New Monitoring System

"How do you determine which alerts to set in a new monitoring system?"

> Note: In Project 3, you configured a series of alerts based on your knowledge of the tactics used to infiltrate the target machine. This question provides an opportunity to explain how you reasoned through configuring their thresholds and metrics.

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - Describe the network provided for Project 3. Identify the VMs on the network and what they do.
    - Which VMs had public Internet access?

- Which VMs did not have public Internet access?
- Which VMs do you expect to receive traffic from the Internet, if any?
- Which VMs do you expect to receive traffic from the local network, if any?
- Which protocols did you observe on the Project 3 network?

3. Explain the Solution Requirements
    - Based on the likely origins, sources, and protocols identified above, which kinds of malicious traffic are most likely to appear on the network?
    - How would you baseline your network to validate your expectations?
    - For each type of malicious traffic:
        - Which metric would you set?
        - What threshold would you set?
        - Why?
4. Explain the Solution Details
    - Which tools in Project 3 did you use to set these alerts?
    - Which steps did you take to configure them?
5. Identify Advantages and Disadvantages of the Solution
    - Are there any malicious circumstances that the alert(s) discussed above do not address?

Question 2: Challenges of Collecting Large Amounts of Log Data

"What are the challenges of collecting huge amounts of log data, and how do security analysts deal with them?"

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 3, when did you deal with log data?

- What kind(s) of data did you investigate?
- How much data were you dealing with?
- What were you looking for?

3. Explain the Solution Requirements
    - What information did you need in order to find what you were looking for?
    - What tools and data does an analyst use to analyze large amounts of log and find this information?
    - In Project 3, which tools did you use to analyze log data?
4. Explain the Solution Details
    - How did you use these tools to find the log data? Which charts, graphs, or other tools were useful for parsing the logs?
5. Identify Advantages and Disadvantages of the Solution
    - What kinds of data did you not inspect during Project 3?
    - Would your process or conclusions change if you had access to this additional data? If so, how?

Question 3: Escalating Security Events

How do you determine if a given security event or alert is important enough for escalation?

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - What kinds of alerts did you set in Project 3?
    - Did these alerts fire as expected when tested?
    - Which specific test events did you use to generate alerts?
3. Explain the Solution Requirements
    - What kind of malicious activity does each alert suggest?

- How would you address each kind of malicious activity?
- Is this mitigation technique within the scope of a SOC Analyst, or should it be escalated or delegated?

4. Explain the Solution Details
    - How did you use Kibana to find this information?
5. Identify Advantages and Disadvantages of the Solution
    - In which circumstances would you not escalate an issue?
    - How would you respond if you learned that a team member "handled" an issue they should have escalated?

Domain: Offensive Security

▼ Click to expand.

Question 1: Planning an Engagement

"How do you plan and execute an effective offensive engagement?"

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 3, which VMs were on the network? What was the purpose of each?
    - Which of these VMs did you have to infiltrate?
    - What was your goal in infiltrating each VM?
    - Which tools did you use to perform the infiltration?
    - What kinds of security measures, if any, were enabled on the network?
3. Explain the Solution Requirements
    - How did you identify your targets?
    - How did you identify vulnerabilities in each target and which did you exploit?
    - What did you do after infiltrating?

4. Explain the Solution Details
    - Which tools and commands did you use to identify your targets and their vulnerabilities?
    - Which exploits did you use against these vulnerabilities and how did you deliver them?
    - How did you achieve your goal after infiltration?
5. Identify Advantages and Disadvantages of the Solution
    - Were your methods covert or detectable by monitoring solutions?
    - How could you achieve your goal with greater stealth?

Question 2: Engagement Scope

"What is meant by 'engagement scope', and why is it important?"

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 3, which VMs were on the network? What was the purpose of each?
    - Which of these VMs did you intend to infiltrate?
    - By contrast, which of these VMs were out of scope?
3. Explain the Solution Requirements
    - Which VMs did you infiltrate during your engagement?
    - Which VMs did you avoid during your engagement?
    - What information could you have gathered by infiltrating the out-of-scope VMs?
4. Explain the Solution Details
    - Which tools did you use to identify your targets?
    - Did this tool affect machines other than your target(s)?
    - Which tools did you use to identify and exploit vulnerabilities?

- Did this tool affect machines other than your target(s)?
- Do any of your tools, tactics, or procedures have implications for other machines on the network? For example, clients accessing services that you may have modified?

5. Identify Advantages and Disadvantages of the Solution
    - Suppose you perform an engagement and only interact with machines that are in scope. Is it nevertheless possible to disrupt machines that are out of scope? If not, explain why not. If so, provide an example.

Question 3: Penetrating & Persisting in a Network

What steps would you take to penetrate a network, and what would you do once you've gained access?

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 3, which VMs were on the network? What was the purpose of each?
    - Which of these VMs were you intended to infiltrate?
    - What were your goals in infiltrating these VMs?
3. Explain the Solution Requirements
    - Which VMs did you infiltrate during your engagement?
    - How did you identify vulnerabilities in each target, and which did you exploit?
    - What did you do after infiltrating?
    - Once in, what steps did you take to find what you were looking for?
    - Did you employ stealth techniques? If so, which?
4. Explain the Solution Details
    - Which tools did you use to identify your targets?
    - Which tools did you use to identify and exploit vulnerabilities?
    - Which tools did you use post-exploitation to find your flags?

5. Identify Advantages and Disadvantages of the Solution
    - Suppose you disconnect from the target and learn that you missed a flag:
    - How would you reconnect to the target?
    - How can you create a way to reconnect without having to re-exploit the target?

      Note: This is called installing a backdoor.

Domain: Defensive Security

▼ Click to expand.

Question 1: Intrusion Detection Systems

"What does an intrusion detection system (IDS) do, and how does it do it?"

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 3, which logging and monitoring systems were in place?
    - Which kinds of data did these systems collect?
    - Which kinds of data did these systems not collect?
3. Explain the Solution Requirements
    - What did Kibana do while you performed your engagement on Day 1?
    - What did you use Kibana for on Day 2?
    - How did Kibana capture the data that it did?
    - Hint: Provide the names of the specific packages that collect data.
4. Explain the Solution Details
    - Did Kibana collect logs from all machines on the network? If not, which machines did not send logs to Kibana?
    - How could Kibana be configured to capture some of the data that it did not collect?

- Which tools did you use to analyze the data: search, queries, dashboards, etc.?

5. Identify Advantages and Disadvantages of the Solution
    - Should all machines on a network be subject to monitoring?
    - How do you decide which metrics to monitor?

Question 2: HIDS vs NIDS

"What is the difference between a HIDS and a NIDS? When would Blue Team operatives use one over the other?"

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 3, which logging and monitoring systems were in place?
    - Which kinds of data did these systems collect?
    - Which kinds of data did these systems not collect?
    - Do these sorts and sources of data make any of these systems a HIDS or NIDS?
3. Explain the Solution Requirements
    - What did Kibana do while you performed your engagement on Day 1?
    - What did you use Kibana for on Day 2?
    - Which VMs did Kibana collect data from?
4. Explain the Solution Details
    - How, specifically, do you know Kibana is a HIDS or NIDS?
    - How could Kibana be configured to capture some of the data that it did not collect?
    - Which tools did you use to analyze the data -- search, queries, dashboards, etc.?
5. Identify Advantages and Disadvantages of the Solution
    - Can a network have both HIDS and NIDS?

- Should a network have both HIDS and NIDS?
- When is it appropriate to use a HIDS?
- When is it appropriate to use a NIDS?

Question 3: Dashboards

Why are dashboards so important for log analysis?

1. Restate the Problem
2. Provide a Concrete Example Scenario
    - In Project 3, which logging and monitoring systems were in place?
    - Which kinds of data did these systems collect?
    - Which kinds of data did these systems not collect?
3. Explain the Solution Requirements
    - What did you use Kibana for on Day 2?
    - What kinds of data did you look for during your analysis?
    - Which tools did you use to analyze the data -- search, queries, dashboards, etc.?
    - Relative to the other tools, how much did you use dashboards and why?
4. Explain the Solution Details
    - Which dashboards did you use? Give at least three specific examples, including:
    - The name of the chart
    - The type of data on the plot axes (e.g., # of Requests vs Time)
    - What kind of activity it indicates
    - Recall the first "interesting" dashboard you examined. What stood out? Which dashboard did it lead you to next?
5. Identify Advantages/Disadvantages of the Solution

- Suppose you couldn't use dashboards. Which tools would you use instead?
- Which dashboards were most useful?
- Describe at least one dashboard you wish you had, but which does not exist.