Cybersecurity Interviews

Cybersecurity

Career Prep Day 2

Class Objectives

By the end of class, you will be able to:

- Prepare for initial phone interviews for IT and cybersecurity positions.
- Answer technical and behavioral interview questions.
- Participate in mock interviews.

Introduction to Cybersecurity Interviewing

Today, we will cover cybersecurity behavioral and technical interviewing.

This Week

Last class, we began preparing the resources and techniques needed to land an interview.

Once you get an interview, you'll need to consider the following:

01 How do I prepare for a successful interview?

02 What kind of questions will they ask during the behavioral interview?

03 What kind of questions will they ask during the technical interview?

04 What should I avoid when interviewing?

Stages of the Interview Process

There are three common interviews before receiving a job offer:

01

The Initial Interview
also known as the phone screener or preliminary interview

02

The Behavioral Interview

03

The Technical Interview

The Initial Interview

When your resume has been selected as a potential candidate, an HR staffer will usually conduct an initial interview.

This interview aims to:

- Narrow down the list of candidates for the final decision maker.
- Provide basic job description, location, and hourly expectations.
- Confirm the pay range is agreeable for both you and the employer.
- Confirm that this is a position you are interested in.

Behavioral Interviews

If you move on from the screener, you will have a behavioral interview, which aims to evaluate your future performance based on your communication and soft skills.

Often, the hiring manager is more concerned with how you answer the questions, than what you say in the answers.

Behavioral interview questions are often similar across companies.

Common Behavioral Question 1

Tell me about yourself.

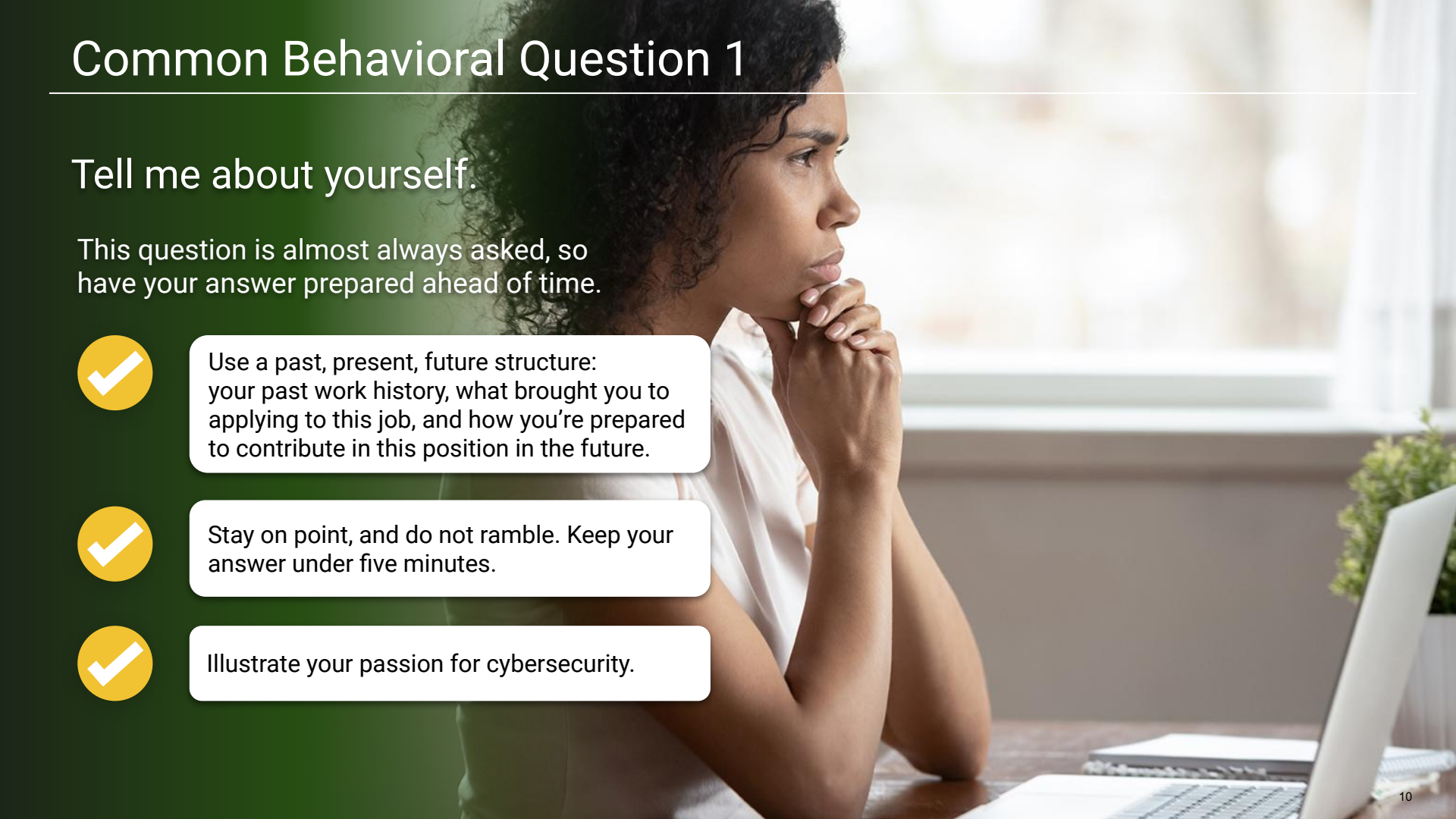
- Show your communication skills.
- Show off your skills and accomplishments.
- Pitch to why you are right for the job.
- Briefly explain your work history and how you came to apply for this position.

Common Behavioral Question 1

Tell me about yourself.

This question is almost always asked, so have your answer prepared ahead of time.

- Use a past, present, future structure: your past work history, what brought you to applying to this job, and how you're prepared to contribute in this position in the future.
- Stay on point, and do not ramble. Keep your answer under five minutes.
- Illustrate your passion for cybersecurity.



Common Behavioral Question 2

Why are you interested in cybersecurity and this position?

Discuss what led you to this boot camp, and what parts of the boot camp were the most exciting.

If the question is focused on the exact position, be prepared to describe what in the job description you are passionate about.

For example, *if the position uses Burp Suite, explain how you enjoy finding web application vulnerabilities and note that it was your favorite part of the course.*

Common Behavioral Question 3

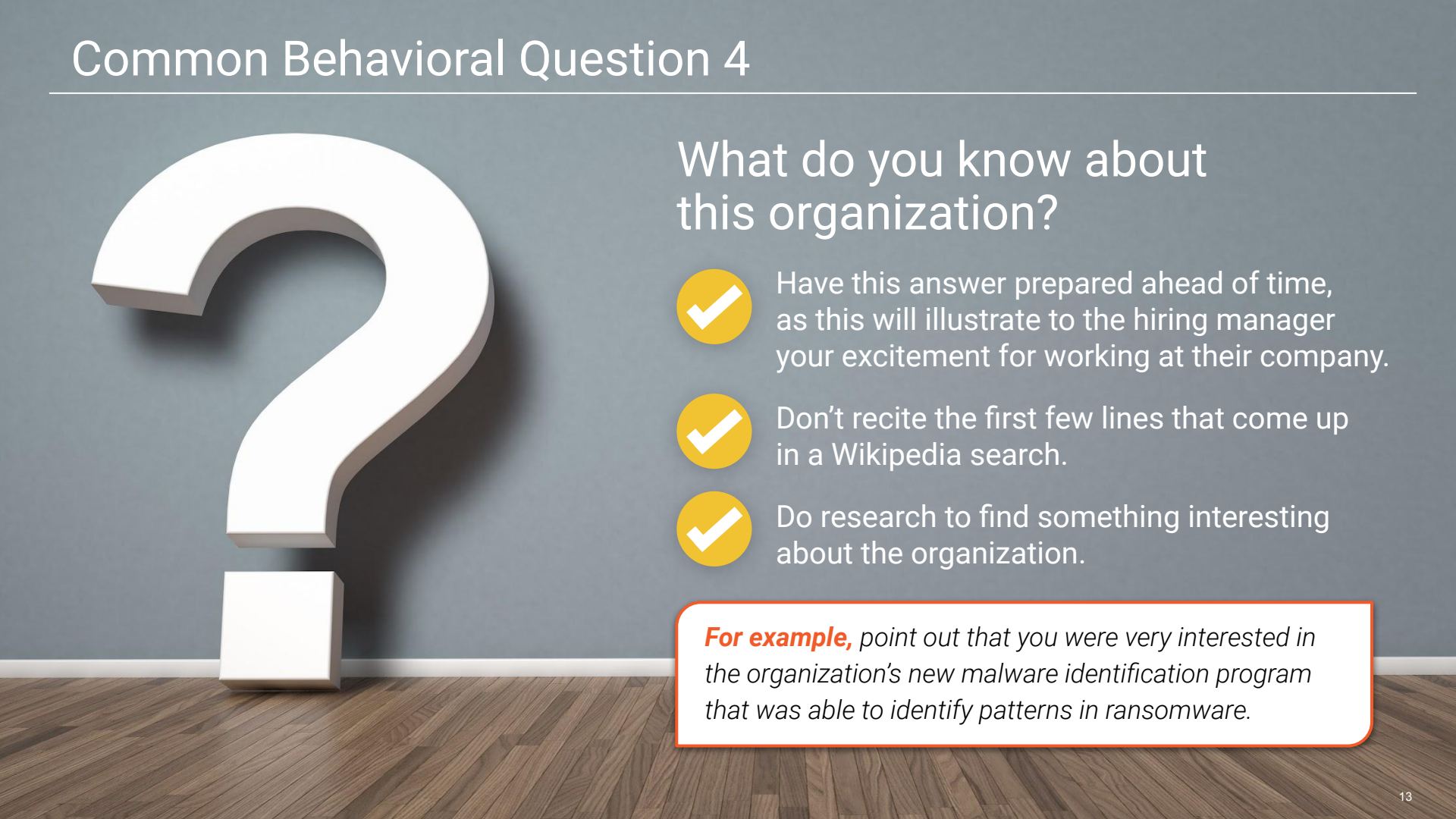
Why did you leave your last position? Why are you looking for a new position?

Be careful with how you answer this question. Under no circumstances should you say negative things about your past employer.

Your answer should stay focused on your passion for cybersecurity and why the position you are applying for aligns with this passion.

For example, *I left (am leaving) my last position because I have a passion for cybersecurity and this position better aligns with my future goals.*

Common Behavioral Question 4



What do you know about this organization?

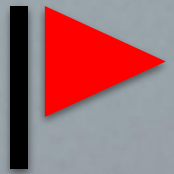
- Have this answer prepared ahead of time, as this will illustrate to the hiring manager your excitement for working at their company.
- Don't recite the first few lines that come up in a Wikipedia search.
- Do research to find something interesting about the organization.

For example, *point out that you were very interested in the organization's new malware identification program that was able to identify patterns in ransomware.*

Common Behavioral Question 5

What questions do you have for us?

This question will usually come at the end of interviews.



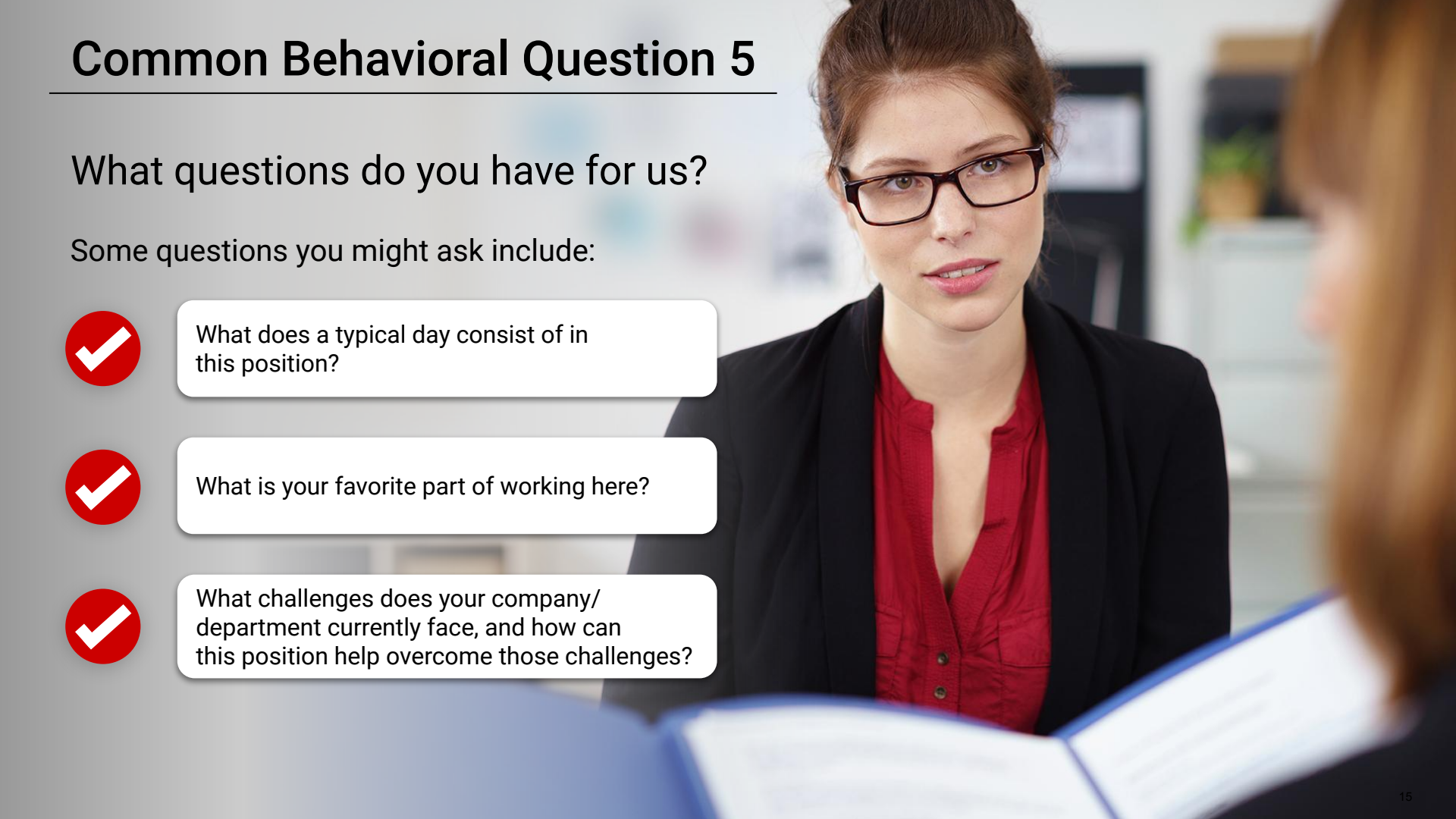
Not asking any questions can be a red flag for the employer. It can signal that you lack interest in the job or company.

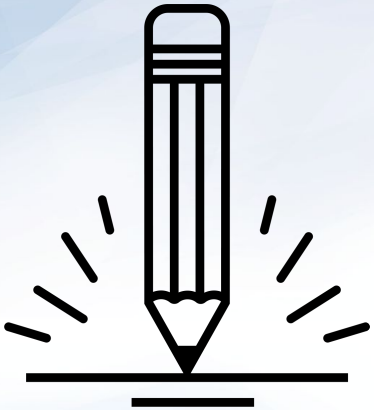
Common Behavioral Question 5

What questions do you have for us?

Some questions you might ask include:

- What does a typical day consist of in this position?
- What is your favorite part of working here?
- What challenges does your company/ department currently face, and how can this position help overcome those challenges?





Activity: Behavioral Interviews

In this activity, you will answer a behavioral question and practice it with a partner.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Technical Interviews

Technical Interviews

In the technical interview, you will be asked technical and problem-solving questions. These will cover:

- Basic technical knowledge
- Background technical experience
- Situational technical decision making

Technical Interview

When answering technical questions, use the following tips:

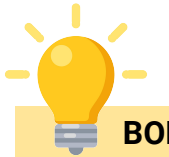
Answer the question and provide additional details if you are able.

We'll cover the difference between basic and detailed responses next.

It is acceptable and recommended to recite back the question before answering.

If you do not know the answer, be truthful and say you do not know.

Explain how you would research the answer to this question.



BONUS

After the interview, send the interviewer the answer to the question you didn't know.

Basic Technical Sample Question

What is the difference between TCP and UDP?

Basic Answer

TCP is connection-oriented and UDP is connectionless.

Detailed Answer

TCP works well for applications that require high reliability, UDP works well for applications that don't require reliability but prefer speed, such as games or videos.

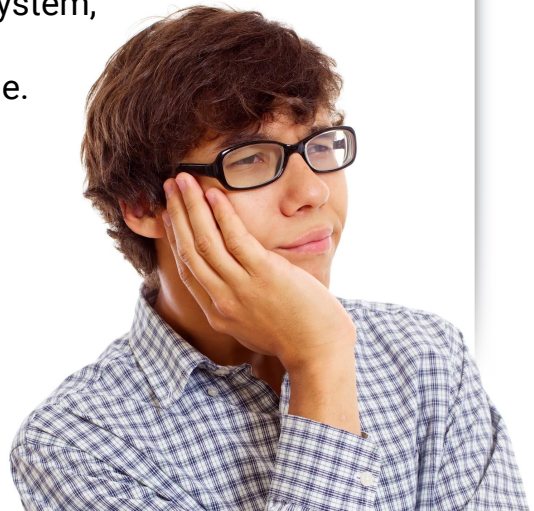
Basic Technical Sample Question

What is the difference between data in motion and data at rest in terms of security?

Basic Answer

Data in motion is data that is “live on the wire,” e.g., being transferred on the network between machines.

Data at rest is data that is being stored on a static file system, such as a hard drive or database.



Detailed Answer

Encrypting data in motion typically requires faster algorithms than encrypting data at rest. This is because, when data is being transferred between machines, slow algorithms manifest as high latency (i.e., large transfer times). Reducing latency requires using faster algorithms.

For this reason, protocols like SSL/TLS use symmetric encryption for the main data transfer, and not slower asymmetric methods.

Basic Technical Sample Question

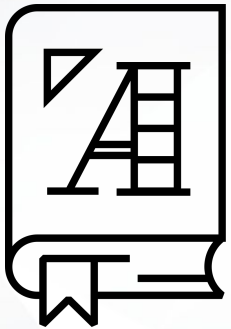
How many keys does asymmetric encryption use?

Basic Answer

Two.

Detailed Answer

Asymmetric encryption uses a public and private key. Each individual is required to have this two-key pair.



Background technical questions

gauge your experience and exposure to real-world scenarios and foundational ideas.

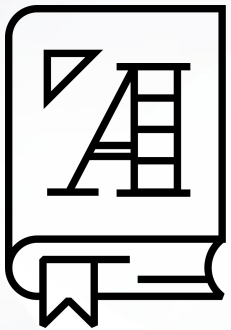
Background Technical Experience Questions

Describe a breach or security vulnerability you contained.

If you do have an example of a breach or security vulnerability you worked on professionally, be sure to explain your step-by-step process for identifying and containing the breach or vulnerability.

If you don't have that professional experience, pick a breach or vulnerability from the news and explain how you would contain it.

For example: "For the Apache Struts vulnerability, since this affected organizations that didn't patch their apache servers, I would ensure our organization had a detailed process that guaranteed that all systems were patched appropriately and in a timely manner."



Situational technical questions gauge your decision-making ability when presented with a problem.

Situational Technical Questions

Suppose you've implemented a firewall policy on an HTTP server.

How would you test it?

NOTE:

These questions are meant to gauge how you think more than what you know.

Situational Technical Questions

Suppose you've implemented a firewall policy on an HTTP server.
How would you test it?

First

Restate the question:

"So, in this situation, I've got a host running an HTTP server, and I've set some firewall rules to allow access only to specific ports and block attackers from all others."

Next

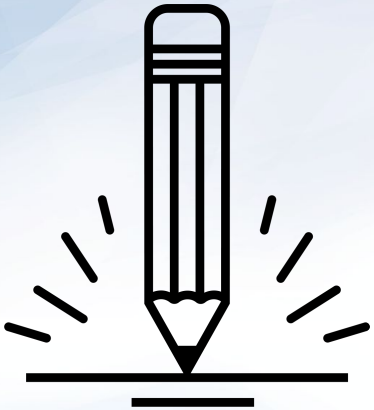
Elaborate and provide a conceptual solution:

"Since this is an HTTP server, I guess you only want to allow access to/from port 80 and 443. If the firewall is working properly, I should be able to send an HTTP or HTTPS request to the server from a foreign host, and get a response back. I should not be able to get a response from any other port."

Last

Explain the specific steps you'd take to implement your solution sketch:

"To test that I'm getting HTTP and HTTPS requests/responses, I'd use curl to hit the firewalled server from a foreign host. I'd expect to get a response. To test that all the other ports were closed, I'd use Nmap to run a port scan."



Activity: Technical Interviews

In this activity, you will practice situational interview questions with your partner.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.


Break

Mock Interview

The best way to prepare for these interviews is to practice them.

Mock Interview

In the following activity, we will work in groups to conduct, answer, and observe mock interviews.

You will be provided a script of behavioral and technical questions to ask a classmate.

Mock Interview Set Up

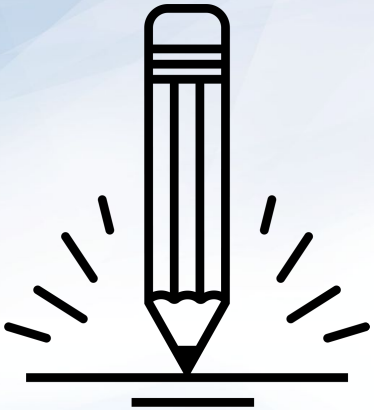
In groups of 4 or 5, each student will have an opportunity to ask and answer questions.

- Each student will be assigned a letter between A and E.
- Each student will be assigned a script of questions to ask another student.
- Three students will observe the interview and provide feedback about responses and communication skills.

Mock Interview Setup

Use the following table to coordinate interview rotation:

Student	Interview 1	Interview 2	Interview 3	Interview 4	Interview 5
A	Conduct	Observe	Observe	Observe	Answer
B	Answer	Conduct	Observe	Observe	Observe
C	Observe	Answer	Conduct	Observe	Observe
D	Observe	Observe	Answer	Conduct	Observe
E	Observe	Observe	Observe	Answer	Conduct



Activity: Mock Interviews

Open the interview script corresponding to your letter. Use these questions to conduct the interview.

Suggested Time:
1:00

Time’s Up! Let’s Review.

Demo Day!

You will have an opportunity to discuss the projects you have built in this class and network with employers and with other cybersecurity professionals during an event called **Demo Day**.

This event is organized by Career Services. If you have any further questions about the format, structure, or dates of the Demo Day, you should reach out to their Career Services Director.

- What is the Cybersecurity Demo Day?


The End