Activity Overview

Now that you've been introduced to attack surfaces and attack vectors, you can pause for a moment and think about what you are learning. In this self-reflection, you will think about how these factors can help identify threats and respond to brief questions.

You have learned many skills and concepts in this course. Completing this self-reflection will help you understand how you might use what you've learned for different tasks and roles in the security field. Answering and asking questions in this self-reflection will help to reinforce what you've learned, so it will be easier for you to remember it later.

Review the steps of applying an attacker mindset

Previously, you learned that applying an attacker mindset to any situation starts by asking yourself, "How would I exploit this vector?" This will require you to consider two elements: the attack surface and its attack vectors.

Remember, an **attack surface** includes all the potential vulnerabilities that a threat actor could exploit. An **attack vector** is the pathway that an attacker uses to penetrate security defenses of an attack surface.

After considering these elements, you can then go through a step-by-step process to apply an attacker mindset:

- Identify a target
- Determine how the target can be accessed
- Evaluate attack vectors that can be exploited
- Find the tools and methods of attack

For a refresher on the elements of an attacker mindset, you can review the video on attack vectors and the video on attack surfaces.

Reflection

Consider what you reviewed about applying an attacker mindset in relation to securing your home environment:

- What are the attack surfaces of a home? Are they physical or digital? What are their vulnerabilities? Are they currently exposed to risk?

1.

Question 1
Now, write 2-3 sentences (40-60 words) that describe important characteristics about the attack surfaces of your home. Type your response in the text box.

1 / 1 point

Attack surfaces in a home can be both physical and digital. Physical attack surfaces include vulnerabilities like lock picking doors, shattering windows, and crossing boundary walls or gates by hopping over them. Digital attack surfaces encompass wireless routers, fiber optic lines, and electric lines. Currently, these surfaces are secured and not exposed to risk.

Correct
Evaluating an attack surface is critical to understanding the operational environment you're in. By considering a system as a whole, you're better equipped to identify parts of the system that need to be reviewed more closely for security vulnerabilities.

Next, consider how an attacker might exploit the vulnerabilities of that surface.

- What are the attack vectors of this surface? Are there multiple entry points? How might the vulnerabilities be exploited? What defenses exist? Can new defenses be added?

2.

Question 2
Now, write 3-5 sentences (60-100 words) that explain what those attack vectors are and how you can apply the tools and/or strategies you've learned to protect your home. Type your response in the text box.

1 / 1 point
The attack vectors for these surfaces include sabotaging fiber optic cables or electric lines with sharp objects like knives, as well as attempting to lock pick or brute force entry through doors or hopping over boundary walls and main entry gates. Yes, there are multiple entry points, including a potential backdoor. Defenses such as barbed wire fencing are in place, and typically, electric lines and fiber optic lines are out of reach. Additionally, the locks are of high security with 7 levers. To enhance defenses, increasing the size of the main gates and making them pointed could be considered.

Correct
Great work strengthening your understanding of an attacker mindset with a thoughtful self-reflection! A good reflection on this topic would consider the wide range of attack vectors that can be used to exploit an attack surface and how the risk of an attack can be proactively reduced.

Applying an attacker mindset requires you to view the world differently. Most things are made with the assumption they'll be used as they were designed. As a security professional, it's important to always think about how things can be misused or abused. Doing so is key to reducing the likelihood of a security risk and having a solid plan.