

Activity overview

In this activity, you will assess the attack vectors of a USB drive. You will consider a scenario of finding a USB drive in a parking lot from both the perspective of an attacker and a target.

USBs, or flash drives, are commonly used for storing and transporting data. However, some characteristics of these small, convenient devices can also introduce security risks. Threat actors frequently use USBs to deliver malicious software, damage other hardware, or even take control of devices. **USB baiting** is an attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network. It relies on curious people to plug in an unfamiliar flash drive that they find.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You are part of the security team at Rhetorical Hospital and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. There's no one else around who might have dropped it, so you decide to pick it up out of curiosity.

You bring the USB drive back to your office where the team has virtualization software installed on a workstation. Virtualization software can be used for this very purpose because it's one of the only ways to safely investigate an unfamiliar USB stick. The software works by running a simulated instance of the computer on the same workstation. This simulation isn't connected to other files or networks, so the USB drive can't affect other systems if it happens to be infected with malicious software.

The flash drive appears to contain a mixture of personal and work-related files. Consider how an attacker might use this information if they obtained it. Also, consider whether this whole event was staged.

For example, an attacker could have placed these files on the USB drive as a distraction. They might have targeted Jorge or someone he knows, hoping they would find the device and plug it into their workstation. In doing so, the attacker could establish a backdoor into the company's systems while the unsuspecting target browsed through the files.

In the **Attacker mindset** row of the activity template, write **2-3 sentences** (40-60 words) about how this information could be used against Jorge or the hospital.

Pro tip: The Cybersecurity and Infrastructure Security Agency (CISA) provides some [security tips on using caution with USB drives](#), including keeping personal and business drives separate.

You have *not* opened any of the files on the device, which is best practice.

Attackers sometimes conduct USB baiting attacks to deliver malicious code that they've crafted.

However, this USB drive was still a security risk even though it did not contain malicious code. It could have easily been found by an attacker who might have used its contents to plan a variety of attacks.

Consider some of the risks associated with USB baiting attacks:

- What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?
- What sensitive information could a threat actor find on a device like this?
- How might that information be used against an individual or an organization?

In the **Risk analysis** row of the activity template, write **3 or 4 sentences** (60-80 words) describing any technical, operational, or managerial controls that could mitigate USB baiting attacks.

Be sure to address the following criteria in your completed activity:

- 2-3 sentences about the types of information stored on the USB drive
- 2-3 sentences about how the information could be used against the owner and/or organization
- 3-4 sentences analyzing the risks of USB baiting attacks