## **Parking lot USB exercise**

Lab work project 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:**

**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.**

|  |  |
| --- | --- |
| **Contents** | Write **2-3 sentences** about the types of information found on this device.   * *Are there files that can contain PII?* * *Are there sensitive work files?* * *Is it safe to store personal files with work files?*   *What I found in this file was that it contained information that was mostly work related to display company based files of what “jorge” was going to work on. There were some PII files that showed his personal life of him wanting to get married and go on vacation for certain planned trips. In conclusion, I would say these files Jorge has are not safe to be mixed with his personal files being together with work files. This can lead to certain issues where criminals will use certain information they will find in their attempt to harm anyone with the exposed information they’ll use for future planned attacks.* |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.   * *Could the information be used against other employees?* * *Could the information be used against relatives?* * *Could the information provide access to the business?*   *The information that Jorge contains can easily be compromised with criminals utilizing files such as his business files to be altered and someone can impersonate his identity to make up lies on what he’s edited into the created files. Also, his PII files can easily be used for hunting tactics criminals may use for future attacks to strike his identity and track every move he does to be a hunted victim. This plays a massive role in criminality in principle for Jorge to be heavily tracked without knowing someone is watching him with bad intentions.* |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of 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?*   *Some outcomes that would have resulted if Jorge's USB was compromised would be lots of malware infections or spyware to track everything he does to be attacked in cybercriminal hacking methods. Other malicious software could include Trojan viruses, rootkits, SQL injection virus and many more in the realm of thinking. The PII sensitive information can easily be exposed to many other criminals to work in mass numbers to gain more information to attack a company and ruin their expenses for future attacks. The information on the USB will be very valuable for criminals to use whatever methods they may plan for gaining criminal intent gain for their attempt to make a big heist for depriving resources against the target business. To prevent measures for this happening again jorge needs to encrypt his USB drive and make sure it’s not accessible for criminals to use for their bad intentions. That way it can be harder for criminals to not gain information on a company’s details to gain access to plan any future attacks.* |