Activity: Identify the Attack Vectors of a USB Drive

Activity Overview

In this activity, I assessed the attack vectors of a USB drive by analyzing a scenario involving a found USB stick. The exercise focused on evaluating potential risks from both an attacker's and a target's perspective, highlighting the dangers of USB-baiting attacks.

Scenario

I was part of the security team at Rhetorical Hospital. One morning, I found a USB stick with the hospital's logo in the parking lot. Using virtualization software in a safe environment, I inspected the contents of the USB drive, which contained both personal and work-related files. This activity required analyzing the potential risks and crafting appropriate mitigations to prevent such attacks in the future.

Parking lot USB exercise

Contents	Some documents appear to contain personal information that Jorge wouldn't want made public. The work files also include other people's PII and information about the hospital's operations.
Attacker mindset	Timesheets can inadvertently provide an attacker with valuable intel about Jorge's colleagues. This information, whether work-related (like project deadlines or travel schedules) or personal (like hobbies or family members), could be exploited in social engineering attacks. For example, a malicious email could be crafted to appear as though it originates from a trusted coworker or family member, leveraging the information gleaned from timesheets to increase its credibility and deceive Jorge.

Risk analysis	Timesheet data poses a significant risk to Jorge and his colleagues. By revealing sensitive work and personal details, attackers can exploit this information for social engineering attacks. For instance, malicious emails can be crafted to appear legitimate by incorporating details gleaned from timesheets, increasing their credibility and deceiving recipients.

Conclusion

This exercise underscored the risks associated with USB drives and the importance of maintaining robust security protocols. By analyzing the attack vectors of the USB, I developed a comprehensive understanding of:

- The methods attackers use to exploit USB devices.
- Practical measures to mitigate USB baiting and related attacks.

This activity highlights my ability to assess risks, think like an attacker, and design effective security controls to protect an organization’s systems and data.