Project

USB Drive Security Assessment

As a member of the security team at Rhetorical Hospital, I will conduct a comprehensive security assessment of a USB drive found in the hospital parking lot. This project aims to evaluate potential attack vectors associated with the discovered USB drive and analyze the risks from both an attacker's and a target's perspective.

Key objectives include:

1. Safely examining the USB drive's contents using virtualization software
2. Identifying potential malware or security threats
3. Assessing the types of sensitive information that could be compromised
4. Analyzing how this information could be exploited by threat actors
5. Developing recommendations for improving organizational security against USB-based threats

This assessment will provide valuable insights into our current security vulnerabilities and help strengthen our defenses against potential USB baiting attacks and other related security risks.

Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. *Some documents appear to contain sensitive information that should not be made public. These documents include personal details about Jorge and employees. Work documents also reveal confidential information about the hospital's internal operations and strategic details. Careful handling and strict confidentiality protocols are essential to safeguard this sensitive information.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. *The timesheets reveal details about Jorge's professional network and work patterns, which could be weaponized by attackers for social engineering. A malicious actor could craft convincing emails appearing to be from a coworker or relative, using insider information to increase the credibility of their deception. These targeted communications could trick Jorge into revealing sensitive information or taking potentially harmful actions.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: *A USB drive found in a parking lot could contain dangerous malware like viruses, trojans, or keyloggers from a malicious actor pretending to be the USB drive owner. If inserted into a company computer, it could rapidly spread infection across the network. The sensitive information a threat actor might discover includes personal financial records, passwords, and confidential work documents. Such data could enable identity theft, financial fraud, or corporate espionage.* *Cybercriminals could leverage these details to blackmail individuals, compromise organizational*

	security, or sell information to competitors, demonstrating the significant risks of an unattended USB drive.