Solution Guide: Threat Modeling: Steps 1 - 4

In this activity, you applied the first four steps of the threat modeling process to a business scenario.

- **Step 1**: Determine Assessment Scope
    - We completed Step 1 by reading the provided information and familiarized ourselves with the assessment scope.
- **Step 2:** List three threat agents relevant to the intranet.
    - Script kiddies
    - Organized cybercriminals
    - Insider threats
- **Step 3:** List three potential attacks against the intranet.
    - **Phishing**: An attacker might try to gain access to the private intranet by phishing employees.
    - **Malware**: Attackers might use malware to infect the intranet. For example, they may infect it with ransomware.
    - **Physical attacks**: Attackers might be able to gain physical access to the building.
- **Step 4:** Identify three possible vulnerabilities in the intranet, and rank them in order of severity. Explain how each one could be exploited.
    - **No content filter**: Employees can download files from any site they want. This makes it much easier for attackers to introduce malware.
    - **Poor access control policies**: Every employee in a department should not have access to all of that department's data.
    - **Older workstations**: Windows 7/8 machines are more vulnerable than newer versions.

Bonus: Web Application Infrastructure

- List three threat agents relevant to the web application:
    - **Script kiddies** are a risk to any website. They are unsophisticated and don't have a lot of money, so they're fairly harmless, unless there are easily exploitable vulnerabilities in the client-side web application.
    - **Organized cybercriminals** might specifically target GeldCorp because they manage money and equity transfers. These attackers are well-motivated and skilled enough to identify and exploit subtle security holes.
    - **Insider threats** are worth considering. Recall that all employees in a given department can access all of that department's data. This means that an engineer on the front-end web team would be able to read the code behind the automated trading algorithms, which the company considers top secret. This is a problem, because that engineer can now leak those secrets, even though he didn't need access to them in the first place.
- List three attacks that threat agents might attempt against the web application. Explain what the attacker gains from the attack.
    - **DDoS**: The trading platform must respond to the market in real time. Taking down the web application through a DDoS attack would have serious impact on the business's reputation. This is most likely to come from script kiddies.
    - **Dumping the database**: Attackers might attempt to use SQL injection to dump the database to steal social security numbers. Script kiddies and more sophisticated attackers might both try this attack.
    - **Cross-site scripting (XSS)**: With cross site scripting, an attacker can execute malicious code into a vulnerable web page. Depending on the code, attackers can execute a number of attacks, including the transmission of sensitive data such as cookies and session information, redirecting the victim to malicious web content, or compromising the victim’s machine.
- Identify three possible vulnerabilities in the web application infrastructure, and rank them in order of severity. Explain how each one could be exploited.
    - The **app server** is probably vulnerable to XSS vulnerabilities. These can be used to steal user cookies and hijack their sessions.
    - The **database** is probably vulnerable to SQL injection. This could be exploited to dump

confidential PII.

- GeldCorp did not state that the database was encrypted. If attackers dump the database, they'll immediately have access to confidential PII in plaintext.