**Threat model lab – personal computer security**

The objective of this lab is to enable students to develop a threat model for their personal computers. By identifying potential security risks, vulnerabilities, and attack vectors, students will gain a practical understanding of threat modeling principles and learn how to enhance the security of their own systems.

To achieve this objective, follow these steps:

1. **Introduction**: In this lab, you will create your own threat report. Begin by introducing the concept of threat modeling and its importance in computer security. Explain how threat modeling involves identifying potential threats, vulnerabilities, and possible mitigation strategies.

Threat modeling is a critical process in cybersecurity that involves identifying potential threats, vulnerabilities, and mitigation strategies to enhance the security of a system. By analyzing these factors, individuals can better protect their personal computers from cyber threats. In this report, I will develop a threat model for my personal computer by identifying assets, potential threat actors, attack vectors, risks, and mitigation strategies.

1. **Identify assets**: List valuable assets stored on your personal computer, such as personal documents, photos, passwords, financial information, and so on. Emphasize the importance of these assets and their potential attractiveness to attackers.

My personal computer contains several valuable assets, including:

* Personal documents (resumes, schoolwork, financial records)
* Stored passwords (saved in browsers or password managers)
* Photos and videos
* Email and social media accounts
* Stored credentials for banking and shopping websites
* Software and installed applications
* Network settings and Wi-Fi credentials

These assets are attractive to attackers because they can be used for identity theft, financial fraud, or unauthorized access to sensitive information.

1. **Identify threat actors**: Discuss various threat actors that could target personal computers, such as hackers, malware, insiders, and physical attackers. Research and list examples of attacks that each threat actor might launch against the system.

Several types of threat actors could target my personal computer:

* **Hackers**: Individuals or groups attempting to gain unauthorized access for financial gain or malicious intent.
* **Malware**: Automated threats such as viruses, ransomware, and spyware that can steal or damage data.
* **Insiders**: Individuals with authorized access, such as friends or family members, who might accidentally or intentionally compromise security.
* **Physical Attackers**: Thieves who gain physical access to my computer and attempt to extract sensitive data.

1. **Identify attack vectors**: Identify potential attack vectors that threat actors could exploit to compromise your computer’s security. These could include phishing emails, malicious websites, outdated software, unsecured Wi-Fi networks, and more.

Potential attack vectors that threat actors could exploit include:

* **Phishing emails**: Deceptive emails designed to trick users into revealing credentials.
* **Malicious websites**: Sites that deliver malware through drive-by downloads.
* **Outdated software**: Unpatched vulnerabilities in the operating system or installed applications.
* **Unsecured Wi-Fi networks**: Public or home networks with weak encryption.
* **USB devices**: Infected USB drives introducing malware.

1. **Risk assessment**: Assess the impact and likelihood of each identified threat. Use a simple risk matrix to categorize threats as high, medium, or low risk based on these factors.

Using a simple risk matrix, I categorize threats as follows:

* **High Risk**: Phishing attacks, outdated software vulnerabilities, and malware infections.
* **Medium Risk**: Unsecured Wi-Fi networks and unauthorized physical access.
* **Low Risk**: Accidental data deletion by an insider.

1. **Mitigation strategies**: Brainstorm and research mitigation strategies for each high- and medium-risk threat. These strategies could involve enabling **two-factor authentication (2FA)**, keeping software up to date, using strong and unique passwords, installing antivirus software, and being cautious about downloading attachments, for example.

To reduce risks, I will implement the following security measures:

* **Enable two-factor authentication (2FA)** for critical accounts.
* **Keep software up to date** by enabling automatic updates.
* **Use strong and unique passwords** for all accounts, stored securely in a password manager.
* **Install reputable antivirus software** to detect and prevent malware infections.
* **Be cautious with email attachments and links** to avoid phishing attacks.
* **Secure my Wi-Fi network** with a strong password and WPA3 encryption.

1. **Create a threat model**: Compile the findings into a comprehensive threat model for your personal computer. This should include a list of identified assets, threat actors, attack vectors, risk assessment, and associated mitigation strategies.

Based on the analysis, the final threat model for my personal computer includes:

* **Identified Assets**: Personal documents, stored credentials, and sensitive data.
* **Threat Actors**: Hackers, malware, insiders, and physical attackers.
* **Attack Vectors**: Phishing emails, malicious websites, outdated software, and unsecured networks.
* **Risk Assessment**: Categorized threats as high, medium, or low risk.
* **Mitigation Strategies**: Implementing security measures such as 2FA, software updates, antivirus protection, and safe browsing practices.

Through this hands-on lab, we develop a practical understanding of threat modeling by applying it to your personal environment. You will learn to think critically about potential security risks and devise effective strategies to mitigate those risks. This can then be applied to a larger environment ultimately contributing to better cybersecurity practices.