Activity Overview

In this activity, you will practice using the Process of Attack Simulation and Threat Analysis (PASTA) threat model framework. You will determine whether a new shopping app is safe to launch.

Threat modeling is an important part of secure software development. Security teams typically perform threat models to identify vulnerabilities before malicious actors do. PASTA is a commonly used framework for assessing the risk profile of new applications.

Scenario

You're part of the growing security team at a company for sneaker enthusiasts and collectors. The business is preparing to launch a mobile app that makes it easy for their customers to buy and sell shoes.

You are performing a threat model of the application using the PASTA framework. You will go through each of the seven stages of the framework to identify security requirements for the new sneaker company app.

Part 2 - Complete the PASTA stages

The main goal of Stage I of the PASTA framework is to understand why the application was developed and what it is expected to do.

Note: *Stage I typically requires gathering input from many individuals at a business.*

First, review the following description of why the sneaker company decided to develop this new app:

Description: Our application should seamlessly connect sellers and shoppers. It should be easy for users to sign-up, log in, and manage their accounts. Data privacy is a big concern for us. We want users to feel confident that we're being responsible with their information.

Buyers should be able to directly message sellers with questions. They should also have the ability to rate sellers to encourage good service. Sales should be clear and quick to process. Users should have several payment options for a smooth checkout process. Proper payment handling is really important because we want to avoid legal issues.

In the **Stage 1** row of the **PASTA worksheet,** make **2-3 notes** of business objectives that you've identified from the description.

In Stage II, the technological scope of the project is defined. Normally, the application development team is involved in this stage because they have the most knowledge about the code base and application logic. Your responsibility as a security professional would be to evaluate the application's architecture for security risks.

For example, the app will be exchanging and storing a lot of user data. These are some of the technologies that it uses:

- **Application programming interface (API):** An API is a set of rules that define how software components interact with each other. In application development, third-party APIs are commonly used to add functionality without having to program it from scratch.
- **Public key infrastructure (PKI):** PKI is an encryption framework that secures the exchange of online information. The mobile app uses a combination of symmetric and asymmetric encryption algorithms: AES and RSA. AES encryption is used to encrypt sensitive data, such as credit card information. RSA encryption is used to exchange keys between the app and a user's device.
- **SHA-256:** SHA-256 is a commonly used hash function that takes an input of any length and produces a digest of 256 bits. The sneaker app will use SHA-256 to protect sensitive user data, like passwords and credit card numbers.
- **Structured query language (SQL):** SQL is a programming language used to create, interact with, and request information from a database. For example, the mobile app uses SQL to store information about the sneakers that are for sale, as well as the sellers who are selling them. It also uses SQL to access that data during a purchase.

Consider what you've learned about these technologies:

- *Which of these technologies would you evaluate first? How might they present risks from a security perspective?*

In the **Stage II** row of the **PASTA worksheet**, write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others.

During Stage III of PASTA, the objective is to analyze how the application is handling information. Here, each process is broken down.

For example, one of the app's processes might be to allow buyers to search the database for shoes that are for sale.

Open the **PASTA data flow diagram** resource. Review the diagram and consider how the technologies you evaluated relate to protecting user data in this process.

Note: *Software developers usually have detailed data flow diagrams available for security teams to use and verify that information is being processed securely.*

Stage IV is about identifying potential threats to the application. This includes threats to the technologies you listed in Stage II. It also concerns the processes of your data flow diagram from Stage III.

For example, the apps authentication system could be attacked with a virus. Authentication could also be attacked if a threat actor social engineers an employee.

In the **Stage IV** row of the PASTA worksheet, list **2 types** of threats that are risks to the information being handled by the sneaker company's app.

Pro tip: *Internal system logs that you will use as a security analyst are good sources of threat intel*

Stage V of PASTA is the vulnerability analysis. Here, you need to consider the attack surface of the technologies listed in Stage II.

For example, the app will use a payment system. The form used to collect credit card information might be vulnerable if it fails to encrypt data.

In **Stage V** of the **PASTA worksheet**, list **2 types** of vulnerabilities that could be exploited.

Pro tip: *Resources like the CVE® list and OWASP are useful for finding common software vulnerabilities.*

In Stage VI of PASTA, the information gathered in the previous two steps are used to build an attack tree.

Open the **PASTA attack tree** resource. Review the diagram and consider how threat actors can potentially exploit these attack vectors.

Note: Applications like this normally have large, complex attack trees with many branches.

PASTA threat modeling is commonly used to reduce the likelihood of security risks. In Stage VII, the final goal is to implement defenses and safeguards that mitigate threats.

In **Stage VII** of the **PASTA worksheet**, list **4 security controls** that you have learned about that can reduce the chances of a security incident, like a data breach.

What to Include in Your Response

Be sure to address the following elements in your completed activity:

- **2-3** business objectives
- **2-3** technology requirements
- **2** potential threats
- **2** system vulnerabilities
- **4** defenses that limit risk