Tryhackme: Threat Modelling

Daniel Schwarzentraub · Follow
7 min read · Sep 26, 2023

Task 1: **Introduction**

> *Amid an ever-evolving threat landscape, is your organisation prepared to mitigate potential risks? Do you proactively identify vulnerabilities, prioritise threats, and implement security measures to safeguard your critical assets? How does your approach to managing security risks contribute to maintaining customer trust?*
>
> These questions arise when you consider the importance of threat modelling in today's rapidly changing cyber security landscape. When confronted with a sophisticated threat actor, are you confident in your team's ability to neutralise it effectively, or will these actors succeed in achieving their goals?

> ### Learning Objectives
>
> In this room, we will learn to apply different threat modelling frameworks for reducing potential risks in an organisational landscape. In addition, we will tackle topics such as the following throughout the room:
>
> - Significance of threat modelling in building an organisation's resiliency from threats.
> - Fundamentals of modelling a significant threat applicable to your organisation for emulation purposes.
> - Learn different threat modelling frameworks like MITRE ATT&CK, DREAD, STRIDE and PASTA.
>
> ### Prerequisites
>
> It is suggested to clear the following rooms first before proceeding with this room:
>
> - Intro to Threat Emulation (coming soon!)
> - Principles of Security

Task 2: **Threat Modelling Overview**

As we dive into this topic, let's briefly define threat modelling to ensure a comprehensive understanding.

What is Threat Modelling?

Threat modelling is a systematic approach to **identifying, prioritising, and addressing potential security threats** across the organisation. By simulating possible attack scenarios and assessing the existing vulnerabilities of the organisation's interconnected systems and applications, threat modelling enables organisations to develop proactive security measures and make informed decisions about resource allocation.

Threat modelling aims to reduce an organisation's overall risk exposure by identifying vulnerabilities and potential attack vectors, allowing for adequate security controls and strategies. This process is essential for constructing a robust defence strategy against the ever-evolving cyber threat landscape.

Threat, Vulnerability and Risk

As mentioned above, the main goal of threat modelling is to reduce the organisation's risk exposure. So before we deep dive into its application, let's review first the definitions of **Threat, Vulnerability and Risk**.

Type	Definition
Threat	Refers to any potential occurrence, event, or actor that may exploit vulnerabilities to compromise information confidentiality, integrity, or availability. It may come in various forms, such as cyber attacks, human error, or natural disasters.
Vulnerability	A weakness or flaw in a system, application, or process that may be exploited by a threat to cause harm. It may arise from software bugs, misconfiguration, or design flaws.
Risk	The possibility of being compromised because of a threat taking advantage of a vulnerability. A way to think about how likely an attack might be successful and how much damage it could cause.

To simplify it, we can use an analogy of an organisation as a house and describe the potential threat, vulnerability and risk.

Type	Analogy
Threat	Occurrence of someone breaking inside your home and taking all your belongings.
Vulnerability	Weaknesses in your home security, such as broken locks or open windows.
Risk	Likelihood of being burglarised due to living in a neighbourhood with a high crime rate or a lack of an alarm system.

Understanding the differences between threat, vulnerability, and risk is essential for effective threat modeling. It enables the organisation to effectively identify and prioritise security issues, resulting in a faster way of reducing risk exposure.

High-Level Process of Threat Modelling

Before delving into different threat modelling frameworks, let's briefly run through a simplified, high-level process.

1. **Defining the scope**
   Identify the specific systems, applications, and networks in the threat modelling exercise.
2. **Asset Identification**
   Develop diagrams of the organisation's architecture and its dependencies. It is also essential to identify the importance of each asset based on the information it handles, such as customer data, intellectual property, and financial information.
3. **Identify Threats**
   Identify potential threats that may impact the identified assets, such as cyber attacks, physical attacks, social engineering, and insider threats.
4. **Analyse Vulnerabilities and Prioritise Risks**
   Analyse the vulnerabilities based on the potential impact of identified threats in conjunction with assessing the existing security controls. Given the list of vulnerabilities, risks should be prioritised based on their likelihood and impact.
5. **Develop and Implement Countermeasures**
   Design and implement security controls to address the identified risks, such as implementing access controls, applying system updates, and performing regular vulnerability assessments.
6. **Monitor and Evaluate**
   Continuously test and monitor the effectiveness of the implemented countermeasures and evaluate the success of the threat modelling exercise. An example of a simple measurement of success is tracking the identified risks that have been effectively mitigated or eliminated.

By following these steps, an organisation can conduct a comprehensive threat modelling exercise to identify and mitigate potential security risks and vulnerabilities in their systems and applications and develop a more effective security strategy.

Remember that the example above is a generic high-level process; threat modelling frameworks will be introduced in the following tasks.

Collaboration with Different Teams

The high-level process discussed above involves many tasks, so it is crucial to have multiple teams collaborate. Each unit offers valuable skills and expertise, helping improve the organisation's security posture. By collaborating, organisations can effectively address and align the security efforts needed to build a better defence.

In line with this, we will introduce the teams typically involved in a threat modelling Exercise.

Team	Role and Purpose
Security Team	The overarching team of red and blue teams. This team typically lead the threat modelling process, providing expertise on threats, vulnerabilities, and risk mitigation strategies. They also ensure security measures are implemented, validated, and continuously monitored.
Development Team	The development team is responsible for building secure systems and applications. Their involvement ensures that security is always incorporated throughout the development lifecycle.
IT and Operations Team	IT and Operations teams manage the organisation's infrastructure, including networks, servers, and other critical systems. Their knowledge of network infrastructure, system configurations and application integrations is essential for effective threat modelling.
Governance, Risk and Compliance Team	The GRC team is responsible for organisation-wide compliance assessments based on industry regulations and internal policies. They collaborate with the security team to align threat modelling with the organisation's risk management objectives.
Business Stakeholders	The business stakeholders provide valuable input on the organisation's critical assets, business processes, and risk tolerance. Their involvement ensures that the efforts align with the organisation's strategic goals.
End Users	As direct users of a system or application, end users can provide unique insights and perspectives that other teams may not have, enabling the identification of vulnerabilities and risks specific to user interactions and behaviours.

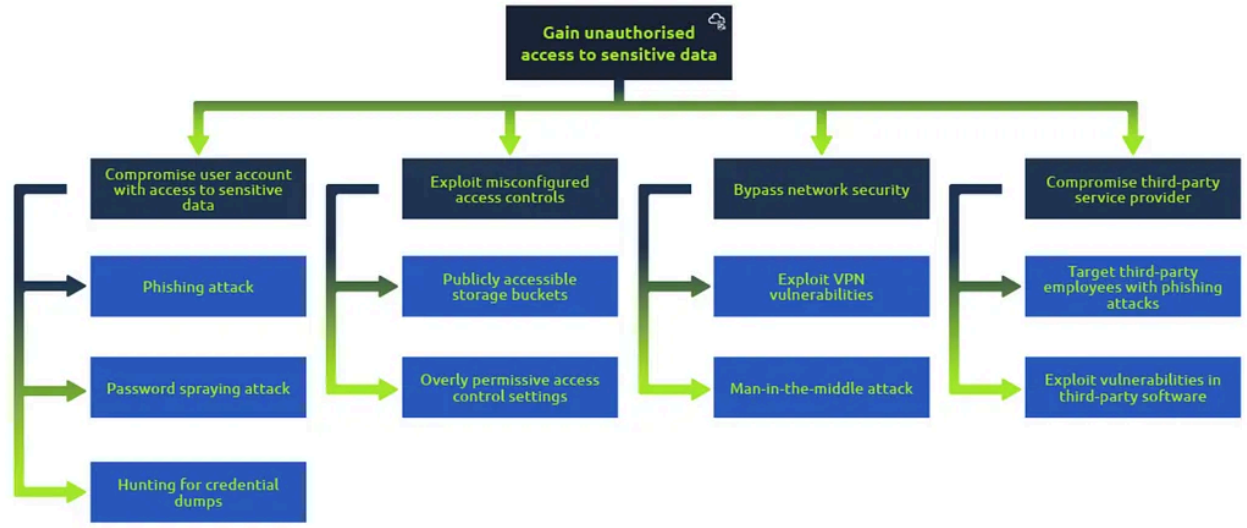
Note that the list is not limited to these teams and may vary depending on your organisational structure. Moreover, the collaboration of these teams is not limited to threat modelling exercises, as they also work hand in hand in securing the organisation through different initiatives.

Attack Trees

In addition to the high-level methodology discussed above, creating an attack tree is another good way to identify and map threats.

An attack tree is a graphical representation used in threat modelling to systematically describe and analyse potential threats against a system, application or infrastructure. It provides a structured, hierarchical approach to breaking down attack scenarios into smaller components. Each node in the tree represents a specific event or condition, with the root node representing the attacker's primary goal.

For a quick example, let's use the diagram below that represents a scenario of an attacker trying to gain unauthorised access to sensitive data stored in a cloud-based storage system.



In this diagram, the root node represents the attacker's primary goal: **gain unauthorised access to sensitive data**. The first level of child nodes represents different high-level strategies an attacker might do to achieve the goal. Each node further breaks down into specific steps, detailing the attacker's possible techniques and actions.

In addition to the traditional hierarchical structure, attack trees can be organised as attack paths, which depict the possible routes or sequences of vulnerabilities a threat actor can exploit to achieve their goal. Attack paths are essentially chains of vulnerabilities that are interconnected.

In an attack path representation, the initial starting node represents the attacker's entry point into the system or network. From there, the various branches or nodes represent the specific vulnerabilities, attack vectors, or steps the threat actor can follow to advance towards their objective.

What is a weakness or flaw in a system, application, or process that can be exploited by a threat?

Answer: **Vulnerability**

Based on the provided high-level methodology, what is the process of developing diagrams to visualise the organisation's architecture and dependencies?

Answer: **Asset Identification**

What diagram describes and analyses potential threats against a system or application?

Answer: **Attack Tree**

Task 3: **Modelling with MITRE ATT&CK**

What is the technique ID of "Exploit Public-Facing Application"?

Answer:

Under what tactic does this technique belong?

Answer:

Task 4: **Mapping with ATT&CK Navigator**

After having a good overview of threat modelling concepts, let's start with the first framework of this room - the MITRE ATT&CK Framework.

MITRE ATT&CK Framework

For a quick refresher, let's define MITRE ATT&CK again.

ATT&CK®

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a comprehensive, globally accessible knowledge base of cyber adversary behaviour and tactics. Developed by the MITRE Corporation, it is a valuable resource for organisations to understand the different stages of cyber attacks and develop effective defences.

The ATT&CK framework is organised into a matrix that covers various tactics (high-level objectives) and techniques (methods used to achieve goals). The framework includes descriptions, examples, and mitigations for each technique, providing a detailed overview of threat actors' methods and tools.

For a quick example, let's examine one of the techniques in the framework - Exploit Public-Facing Application.

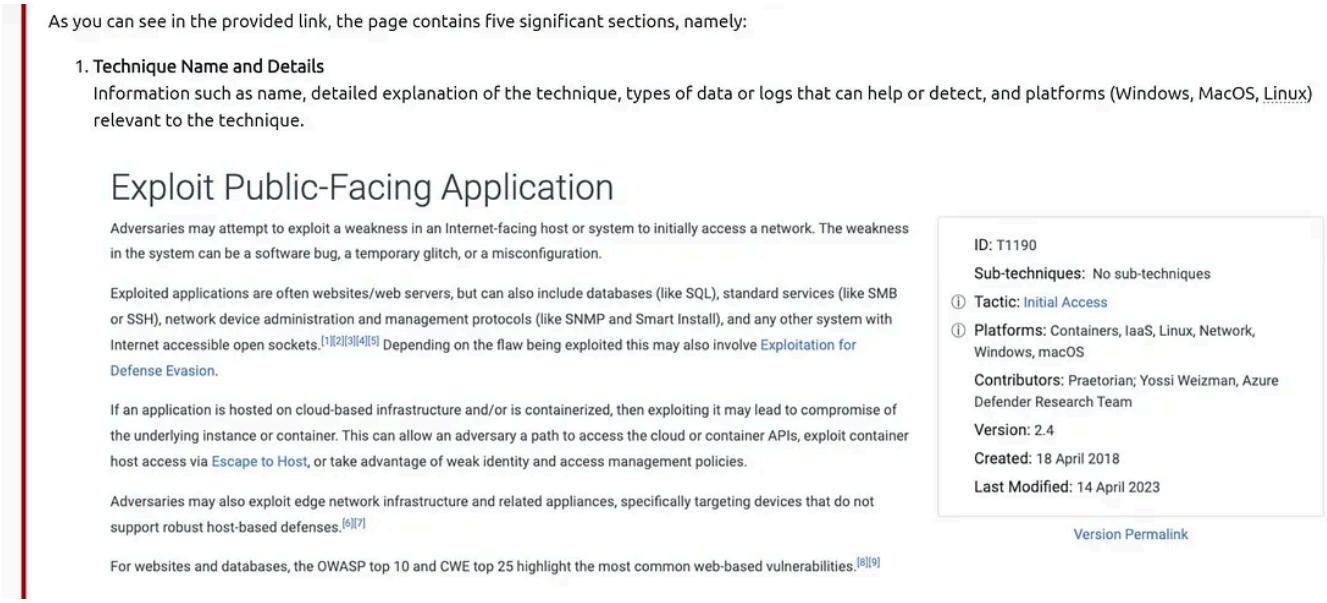
Exploit Public-Facing Application

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The...

attack.mitre.org

As you can see in the provided link, the page contains five significant sections, namely:

1. **Technique Name and Details**
   Information such as name, detailed explanation of the technique, types of data or logs that can help or detect, and platforms (Windows, MacOS, Linux) relevant to the technique.



Exploit Public-Facing Application

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.

Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.[1][2][3][4][5] Depending on the flaw being exploited this may also involve Exploitation for Defense Evasion.

If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via Escape to Host, or take advantage of weak identity and access management policies.

Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.[6][7]

For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.[8][9]

ID: T1190
Sub-techniques: No sub-techniques
Tactic: Initial Access
Platforms: Containers, IaaS, Linux, Network, Windows, macOS
Contributors: Praetorian; Yossi Weizman, Azure Defender Research Team
Version: 2.4
Created: 18 April 2018
Last Modified: 14 April 2023

Version Permalink

2. **Procedure Examples**
   Real-world examples of how threat actors have employed the technique in their adversarial operations.

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has used a variety of public exploits, including CVE 2020-0688 and CVE 2020-17144, to gain execution on vulnerable Microsoft Exchange; they have also conducted SQL injection attacks against external websites.[10][11]
G0016	APT29	APT29 has exploited CVE-2019-19781 for Citrix, CVE-2019-11510 for Pulse Secure VPNs, CVE-2018-13379 for FortiGate VPNs, and CVE-2019-9670 in Zimbra software to gain access.[12][13]
G0087	APT39	APT39 has used SQL injection for initial compromise.[14]
G0096	APT41	APT41 exploited CVE-2020-10189 against Zoho ManageEngine Desktop Central, and CVE-2019-19781 to compromise Citrix Application Delivery Controllers (ADC) and gateway devices.[15]
G0001	Axiom	Axiom has been observed using SQL injection to gain access to systems.[16][17]

3. **Mitigations**
   Recommended security measures and best practices to protect against the technique.

Mitigations

ID	Mitigation	Description
M1048	Application Isolation and Sandboxing	Application isolation will limit what other processes and system features the exploited target can access.
M1050	Exploit Protection	Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application.
M1030	Network Segmentation	Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.
M1026	Privileged Account Management	Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system.
M1051	Update Software	Update software regularly by employing patch management for externally exposed applications.
M1016	Vulnerability Scanning	Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.[8]

4. **Detections**
   Strategies and indicators that can help identify the technique, as well as potential challenges in detecting the technique.

Detection

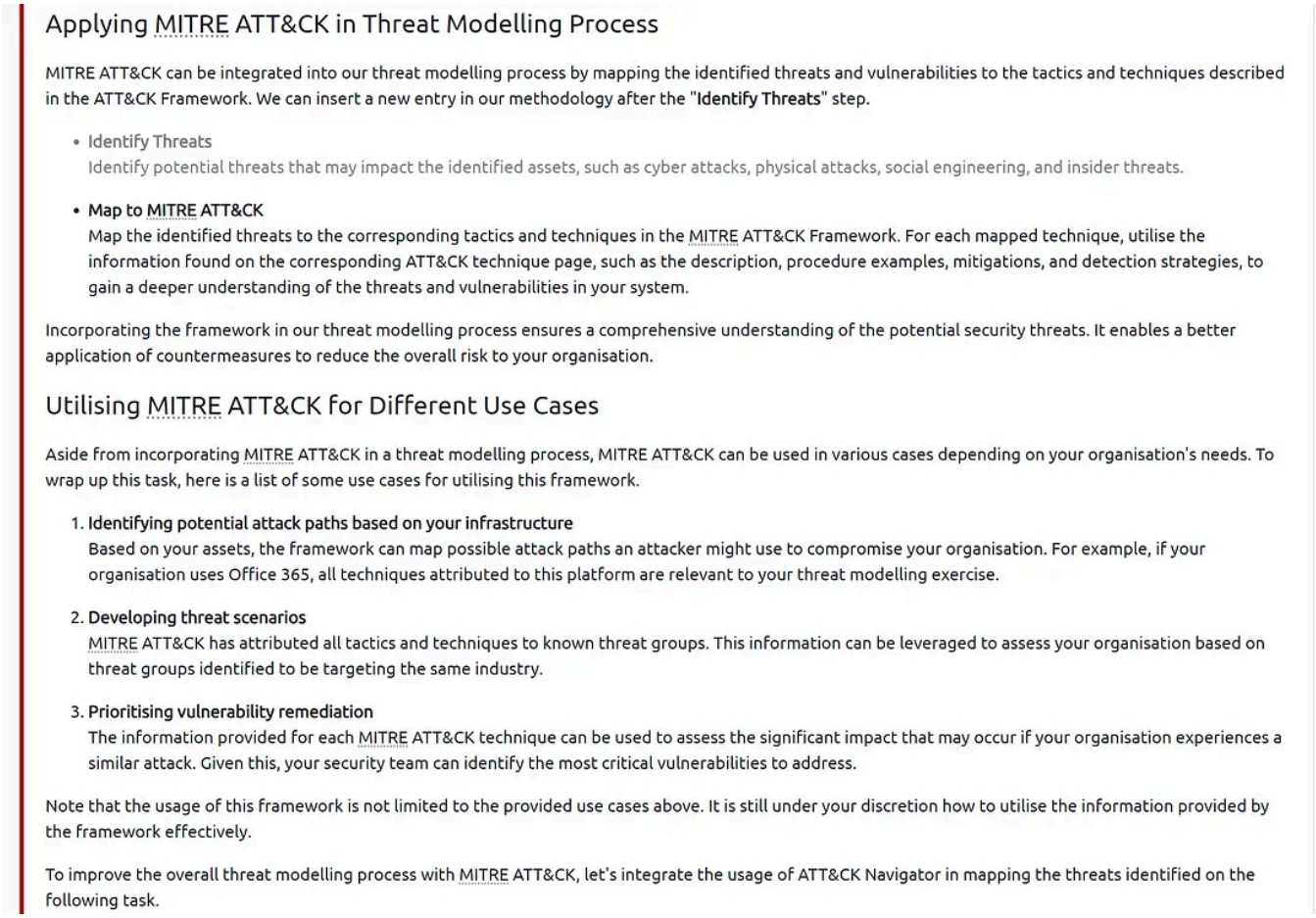
ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Web Application Firewalls may detect improper inputs attempting exploitation.
DS0029	Network Traffic	Network Traffic Content	Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings or known payloads.

5. **References**
   External sources, reports, and articles that provide additional information, context, or examples related to the technique.

References

1. National Vulnerability Database. (2017, February 2). CVE-2016-6662 Detail. Retrieved April 3, 2018.
2. CIS. (2017, May 15). Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution. Retrieved April 3, 2018.
3. US-CERT. (2018, April 20). Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices. Retrieved October 19, 2020.
4. Omar Santos. (2020, October 19). Attackers Continue to Target Legacy Devices. Retrieved October 20, 2020.
5. National Vulnerability Database. (2017, September 24). CVE-2014-7169 Detail. Retrieved April 3, 2018.
31. MSTIC. (2019, December 12). GALLIUM: Targeting global telecom. Retrieved January 13, 2021.
32. Counter Threat Unit Research Team. (2019, September 24). REvil/Sodinokibi Ransomware. Retrieved August 4, 2020.
33. MSTIC. (2021, March 2). HAFNIUM targeting Exchange Servers with 0-day exploits. Retrieved March 3, 2021.
34. Gruzweig, J. et al. (2021, March 2). Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities. Retrieved March 3, 2021.
35. Bromiley, M. et al. (2021, March 4). Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities. Retrieved March 9, 2021.

By exploring the contents of a MITRE ATT&CK technique page, you may gain valuable insights into the specific methods employed by an adversary and enhance your organisation's overall security posture by implementing the suggested mitigations and detection strategies.



Applying MITRE ATT&CK in Threat Modelling Process

MITRE ATT&CK can be integrated into our threat modelling process by mapping the identified threats and vulnerabilities to the tactics and techniques described in the ATT&CK Framework. We can insert a new entry in our methodology after the "**Identify Threats**" step.

- Identify Threats
  Identify potential threats that may impact the identified assets, such as cyber attacks, physical attacks, social engineering, and insider threats.
- **Map to MITRE ATT&CK**
  Map the identified threats to the corresponding tactics and techniques in the MITRE ATT&CK Framework. For each mapped technique, utilise the information found on the corresponding ATT&CK technique page, such as the description, procedure examples, mitigations, and detection strategies, to gain a deeper understanding of the threats and vulnerabilities in your system.

Incorporating the framework in our threat modelling process ensures a comprehensive understanding of the potential security threats. It enables a better application of countermeasures to reduce the overall risk to your organisation.

Utilising MITRE ATT&CK for Different Use Cases

Aside from incorporating MITRE ATT&CK in a threat modelling process, MITRE ATT&CK can be used in various cases depending on your organisation's needs. To wrap up this task, here is a list of some use cases for utilising this framework.

1. **Identifying potential attack paths based on your infrastructure**
   Based on your assets, the framework can map possible attack paths an attacker might use to compromise your organisation. For example, if your organisation uses Office 365, all techniques attributed to this platform are relevant to your threat modelling exercise.
2. **Developing threat scenarios**
   MITRE ATT&CK has attributed all tactics and techniques to known threat groups. This information can be leveraged to assess your organisation based on threat groups identified to be targeting the same industry.
3. **Prioritising vulnerability remediation**
   The information provided for each MITRE ATT&CK technique can be used to assess the significant impact that may occur if your organisation experiences a similar attack. Given this, your security team can identify the most critical vulnerabilities to address.

Note that the usage of this framework is not limited to the provided use cases above. It is still under your discretion how to utilise the information provided by the framework effectively.

To improve the overall threat modelling process with MITRE ATT&CK, let's integrate the usage of ATT&CK Navigator in mapping the threats identified on the following task.

What is the technique ID of “Exploit Public-Facing Application”?

Answer: **T1190**

Under what tactic does this technique belong?

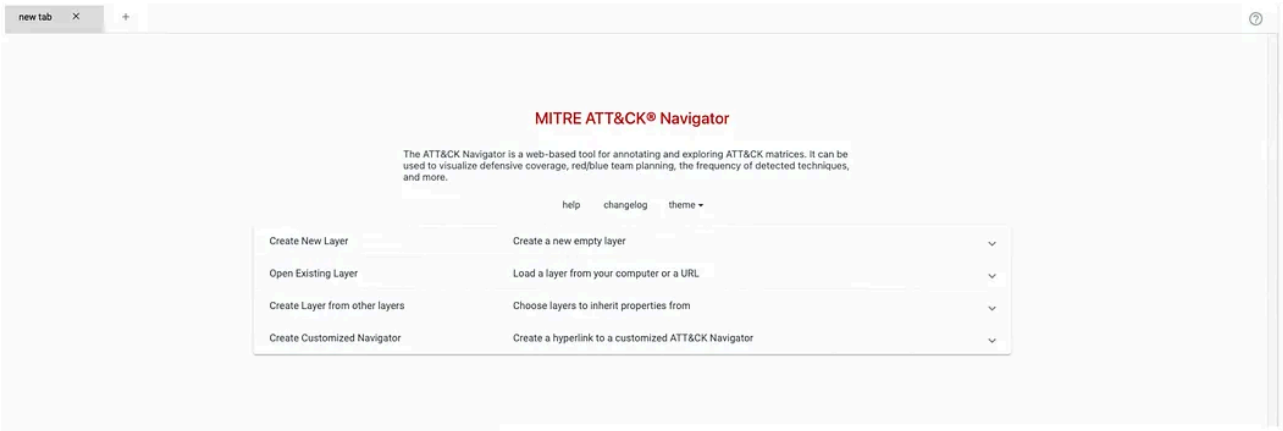
Answer: **Initial Access**

Task 4: **Mapping with ATT&CK Navigator**

ATT&CK Navigator

Start Machine

Before discussing the ATT&CK Navigator, you may start the machine attached to this room by clicking the **Start Machine** button. Once the machine is up, access the ATT&CK Navigator webpage via the **AttackBox** or **VPN** using this link - http://MACHINE_IP. You will see this landing page once you access the provided link.



Note: This open-source application is also accessible via this link. However, we will use the provided VM to have consistency in the ATT&CK Navigator version used in this task.

Now that the web application is running, let's discuss the MITRE ATT&CK Navigator!

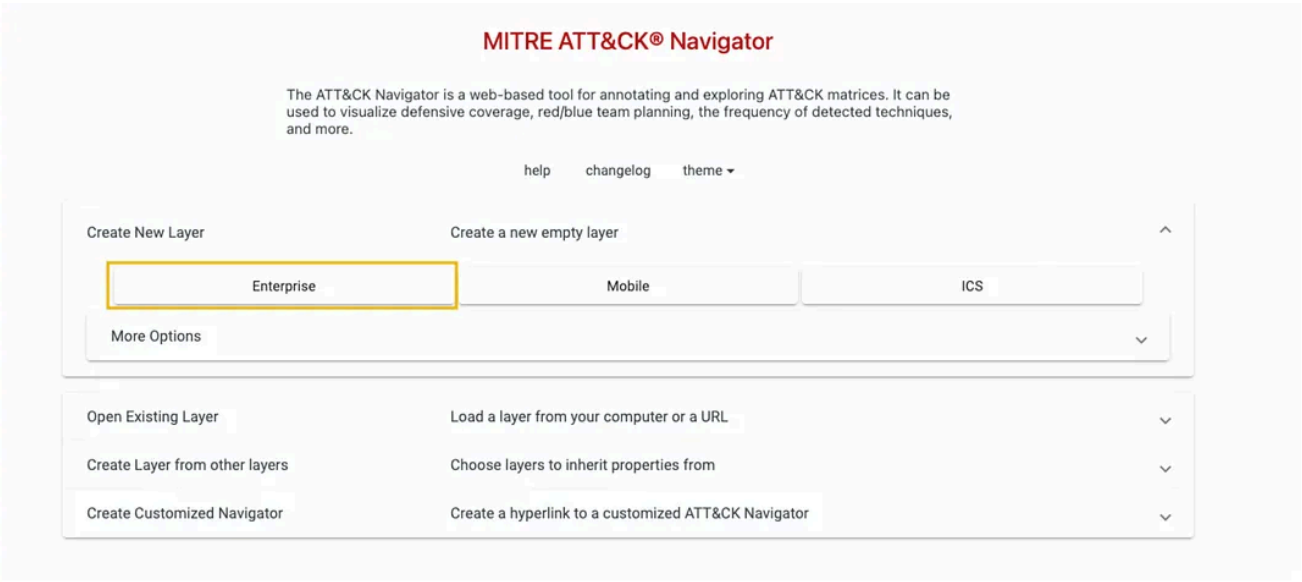
The MITRE ATT&CK Navigator is an open-source, web-based tool that helps visualise and navigate the complex landscape of the MITRE ATT&CK Framework. It allows security teams to create custom matrices by selecting relevant tactics and techniques that apply to their specific environment or threat scenario.

This task will have a walkthrough on creating a layer and mapping the relevant techniques for your threat modelling exercise. Here is a brief overview of the steps and features we will utilise.

1. Creation of a new layer.
2. Searching and selecting techniques.
3. Viewing, sorting and filtering layers.
4. Annotating techniques with fills, scores and comments.

Creating a New Layer

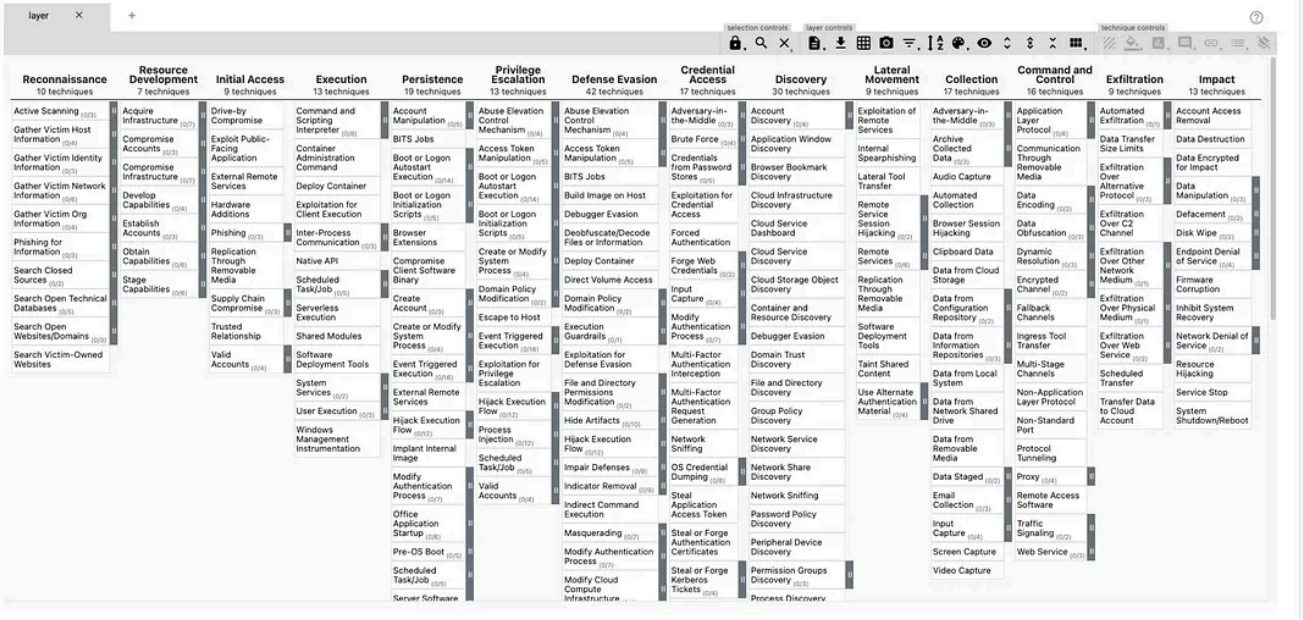
To start with, let's create a new layer and choose enterprise.



You may have observed that there are three options for creating a new layer. These layers pertain to the three MITRE ATT&CK matrices, namely:

- **Enterprise** - The Enterprise Matrix focuses on threats and techniques commonly used against enterprise networks.
- **Mobile** - The Mobile Matrix focuses on threats and techniques against mobile devices, such as smartphones and tablets.
- **ICS** - The ICS Matrix focuses on threats and techniques against industrial control systems, which control critical infrastructure, such as power plants, water treatment facilities, and transportation systems.

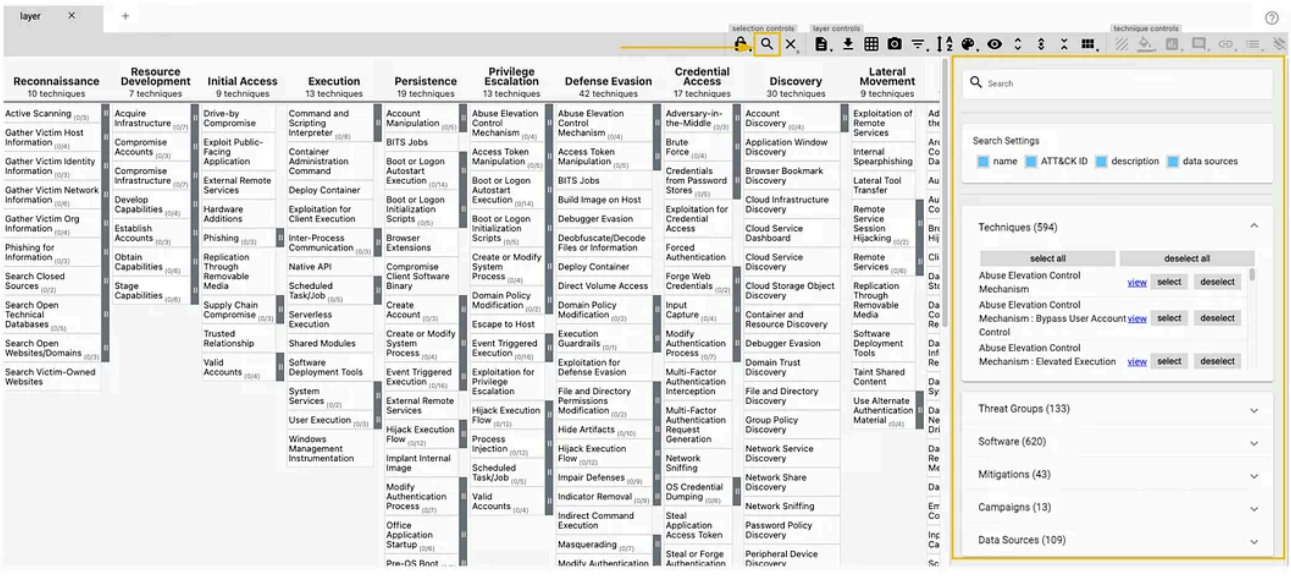
We have chosen the Enterprise Matrix to cover threat actors' typical techniques when targeting an organisation. After creating a new layer, you will have this view once the web page has loaded.



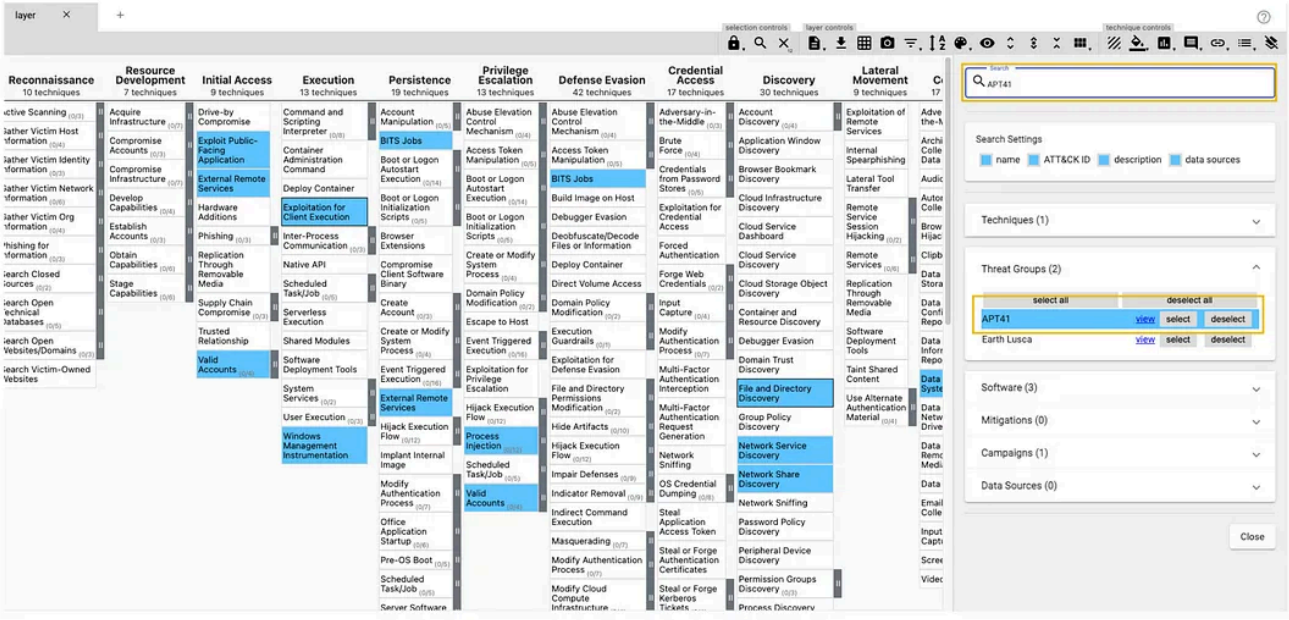
Searching and Selecting Techniques

The first important feature we want to utilise in this application is the search functionality under the **Selection Controls** panel. This feature allows us to search and multi-select techniques you want to highlight or mark.

You may press the magnifier button to access the right sidebar, search using any keywords, or choose any selection under **Techniques, Threat Groups, Software, Mitigations, Campaigns, or Data Sources**.

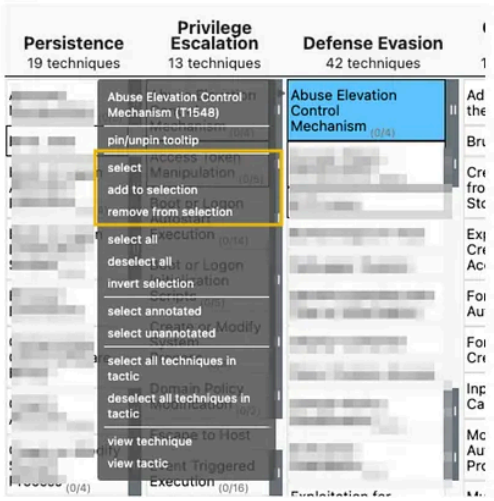


For a quick example, search for **APT41** and hover its entry on the **Threat Groups** section. You may observe that it will highlight all techniques attributed to this threat group. Once you click the select button, the highlighted techniques will be selected as a group and can be annotated with a score or a background fill, which will be discussed in the following instructions.



After selecting the threat group, you may also observe that the deselect button now has a numerical value. This indicates the current number of chosen techniques. You may press this button to remove all your current technique selections.

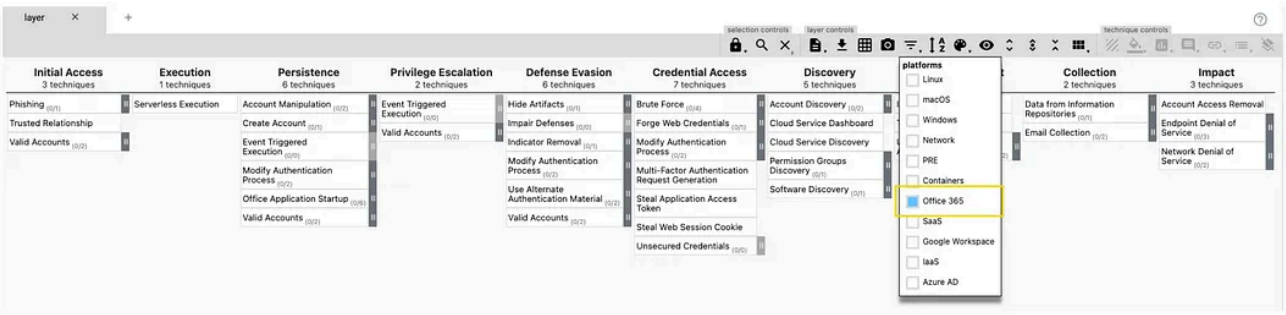
Lastly, you may right-click any technique if you prefer to do an action on a single technique (e.g. select, add to selection, remove from selection).



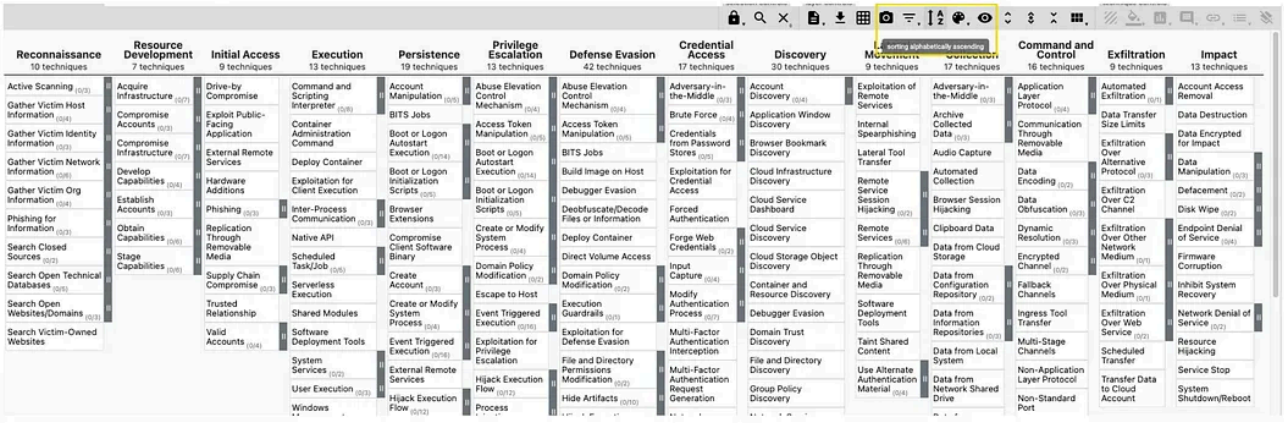
Viewing, Sorting and Filtering Layers

We will tackle the next set of features under the **Layer Controls** panel. However, we will only focus on the following:

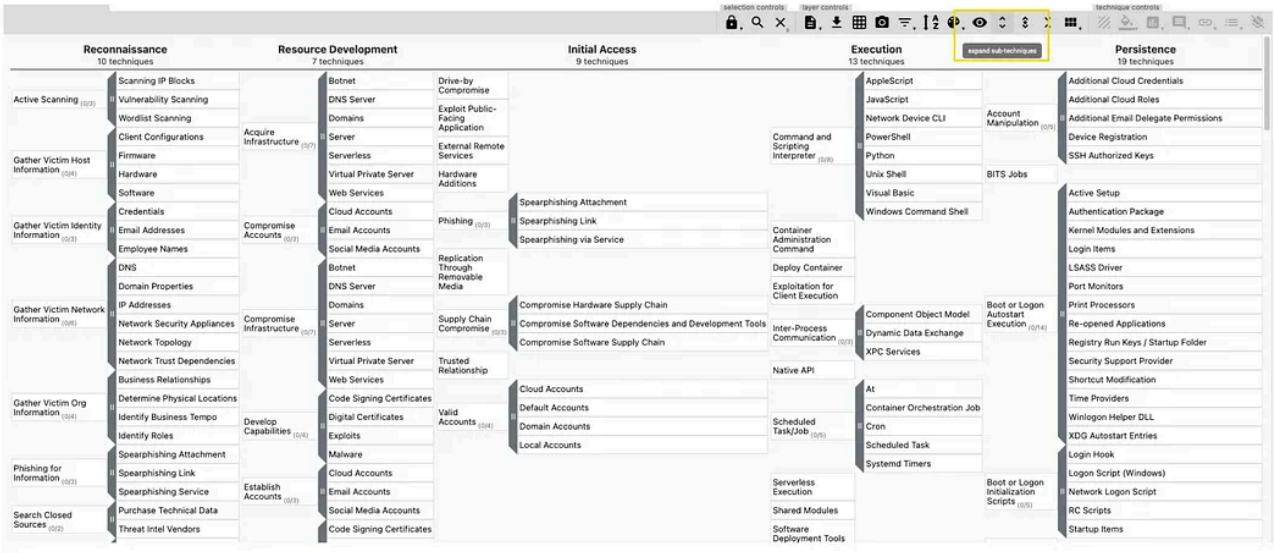
- Exporting features (download as JSON, Excel, SVG) - This allows you to dump the selected techniques, including all annotations. The data exported can be ingested again in the ATT&CK Navigator for future use.
- Filters - Allows you to filter techniques based on relevant platforms, such as operating systems or applications. For a quick example, the image below shows all techniques that are attributed to Office365.



- Sorting - This allows you to sort the techniques by their alphabetical arrangement or numerical scores. The image below shows that all techniques are arranged alphabetically.



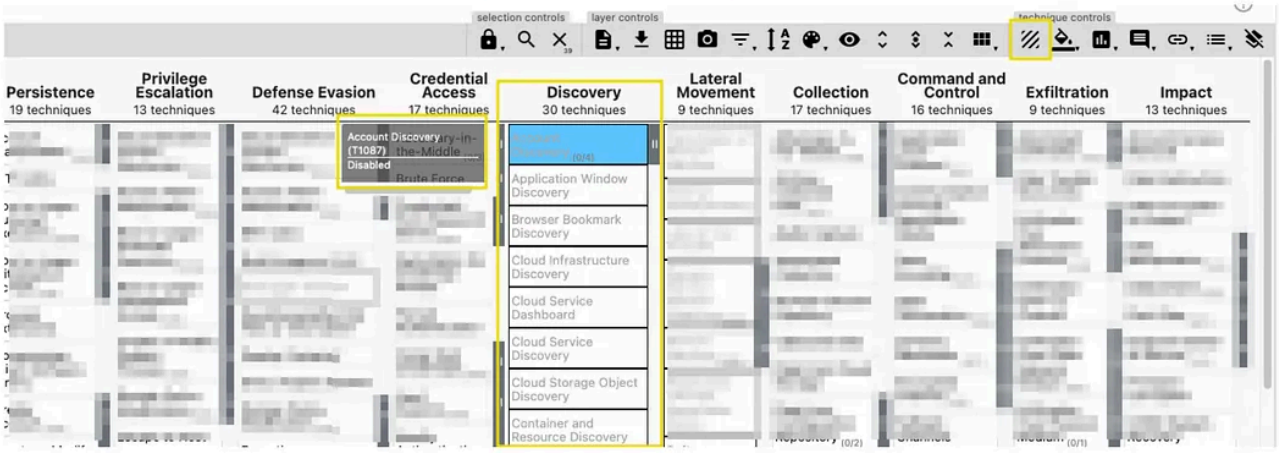
- Expand sub-techniques - View all underlying sub-techniques under each technique, expanding the view for all techniques. You will have a similar view with the image below once you have expanded the sub-techniques.



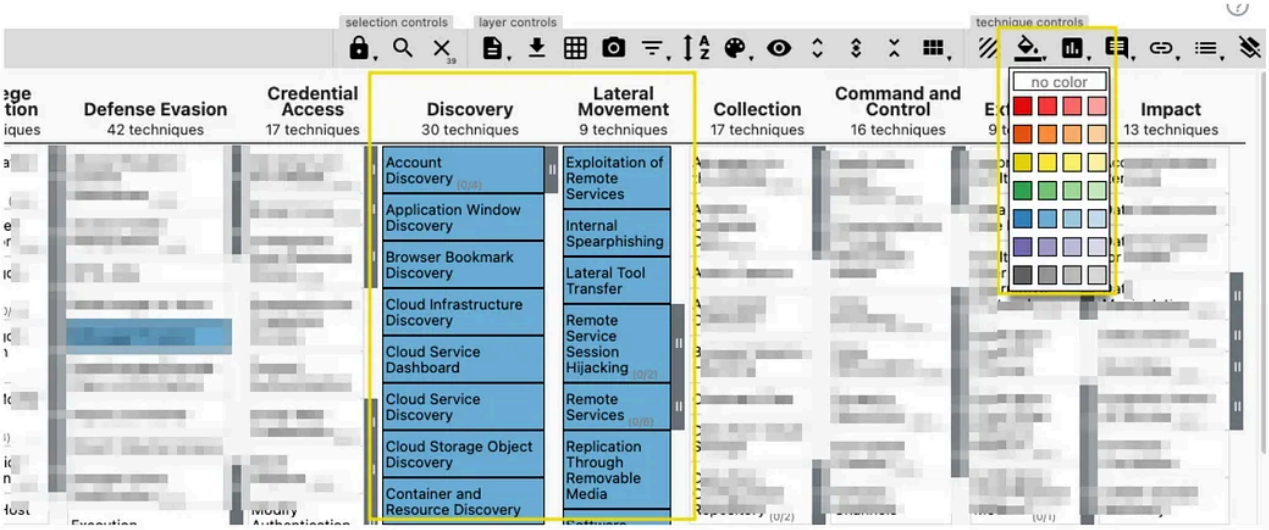
Annotating Techniques

Now, the last set of features is under the **Technique Controls** panel. These buttons allow you to annotate details on selected techniques. For a quick run-through, here are the features under the panel mentioned (from left to right):

- Toggle state - This feature allows you to disable the selected techniques, making their view greyed-out.

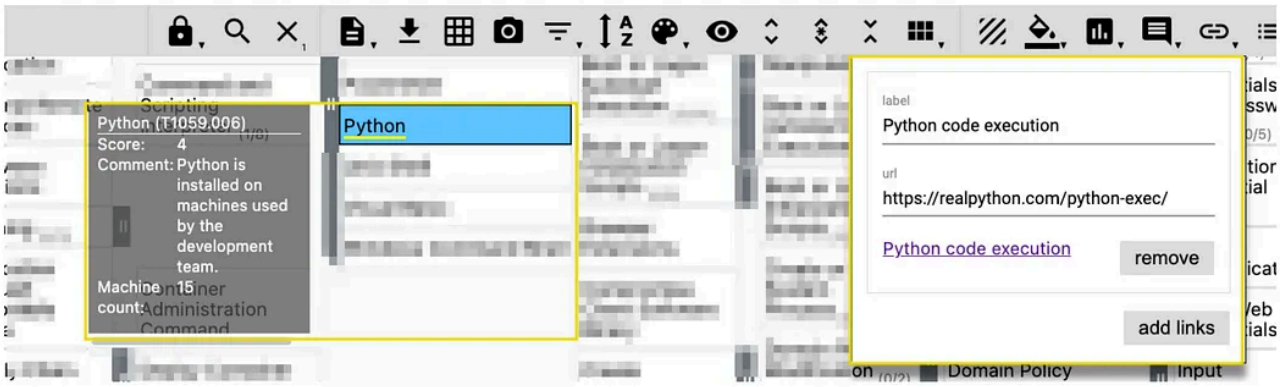


- Background color - This allows you to change the background color of the selected technique, for highlighting and grouping purposes.



- Scoring - Allows you to rate each technique or set of techniques based on criteria depending on your needs, such as the impact of a technique.
- Comment - Allows you to add notes and observations to a technique.
- Link - Allows you to add external links, such as additional references related to the technique.
- Metadata - Allows you to add custom tags and labels to a particular technique.
- Clear annotations on selected - Remove all annotations on selected techniques.

The image below is an example of using Scoring, Comment, Link and Metadata features.



Utilising ATT&CK Navigator

To put the concepts of this framework into practice, let's use the following scenario below.

You are tasked to utilise the MITRE ATT&CK framework for your threat modelling exercise. The organisation you're currently working with is in the financial services industry. Given that, some known threat groups targeting this industry are:

- APT28 (Fancy Bear)
- APT29 (Cozy Bear)
- Carbanak
- FIN7 (Carbanak/Fancy Bear)
- Lazarus Group

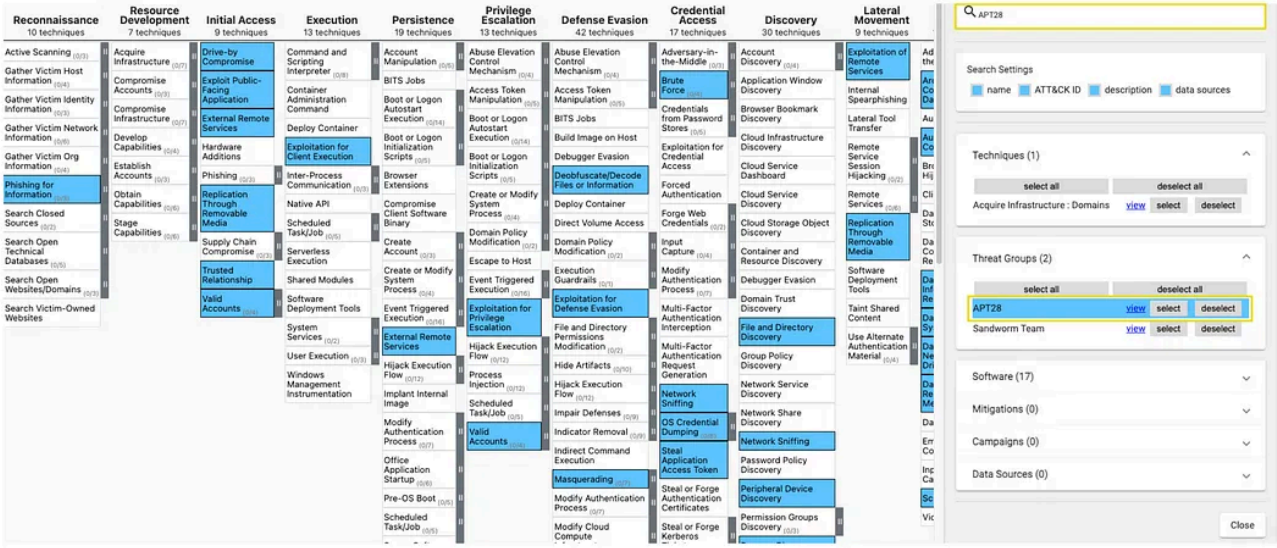
In addition, your organisation uses the following technologies:

- Google Cloud Platform (GCP) for cloud infrastructure
- Online banking platform developed by internal developers
- A Customer Relationship Management (CRM) platform

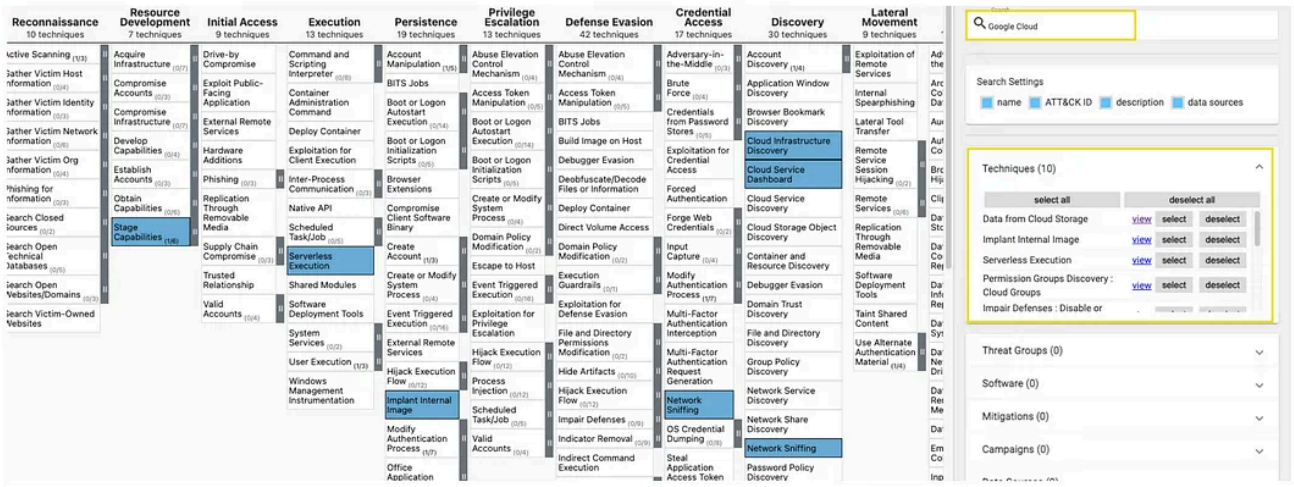
Lastly, the critical assets that you handle based on your business stakeholders are the following:

- Customer financial data
- Transaction records
- Personally identifiable information (PII)

Given this scenario, you can use the MITRE ATT&CK framework and ATT&CK Navigator to map and understand the significant techniques attributed to the provided threat groups and those affecting GCP and web applications.



Techniques used by APT28



Techniques related to Google Cloud

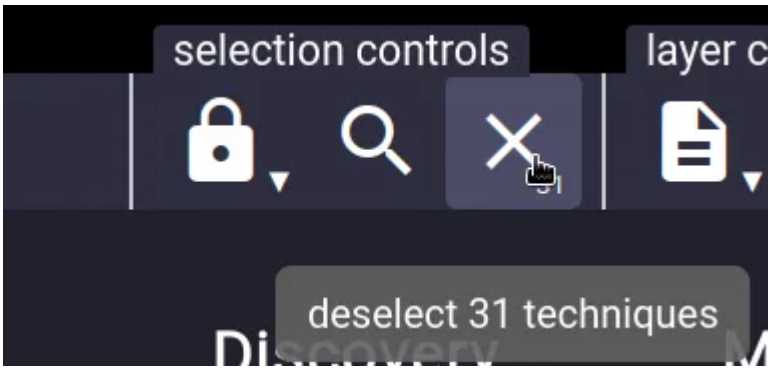
Once these techniques are identified, you should prioritise the potential vulnerabilities that may affect the systems that handle your critical assets (financial data, transaction records, and PII). Some of the techniques that you may consider prioritising are the following:

- **Exploit Public-Facing Application (T1190)** - Securing the public-facing application is crucial to prevent unauthorised access attempts.
- **Exploitation for Privilege Escalation (T1068)** - The prevention of escalating attackers' privileges reduces the chances of obtaining critical data only accessible to administrators.
- **Data from Cloud Storage (T1530)** - Since the cloud instance contains critical data, safeguarding the confidentiality and integrity of the data stored is crucial.
- **Network Denial of Service (T1498)** - The technique may not directly target the critical data within the cloud instance. Still, it can lead to service disruptions and potential impacts on the availability and accessibility of the data.

Now that we have identified these, the next step for the threat modelling exercise is to remediate and apply appropriate security controls to reduce the potential attack surface of our organisation.

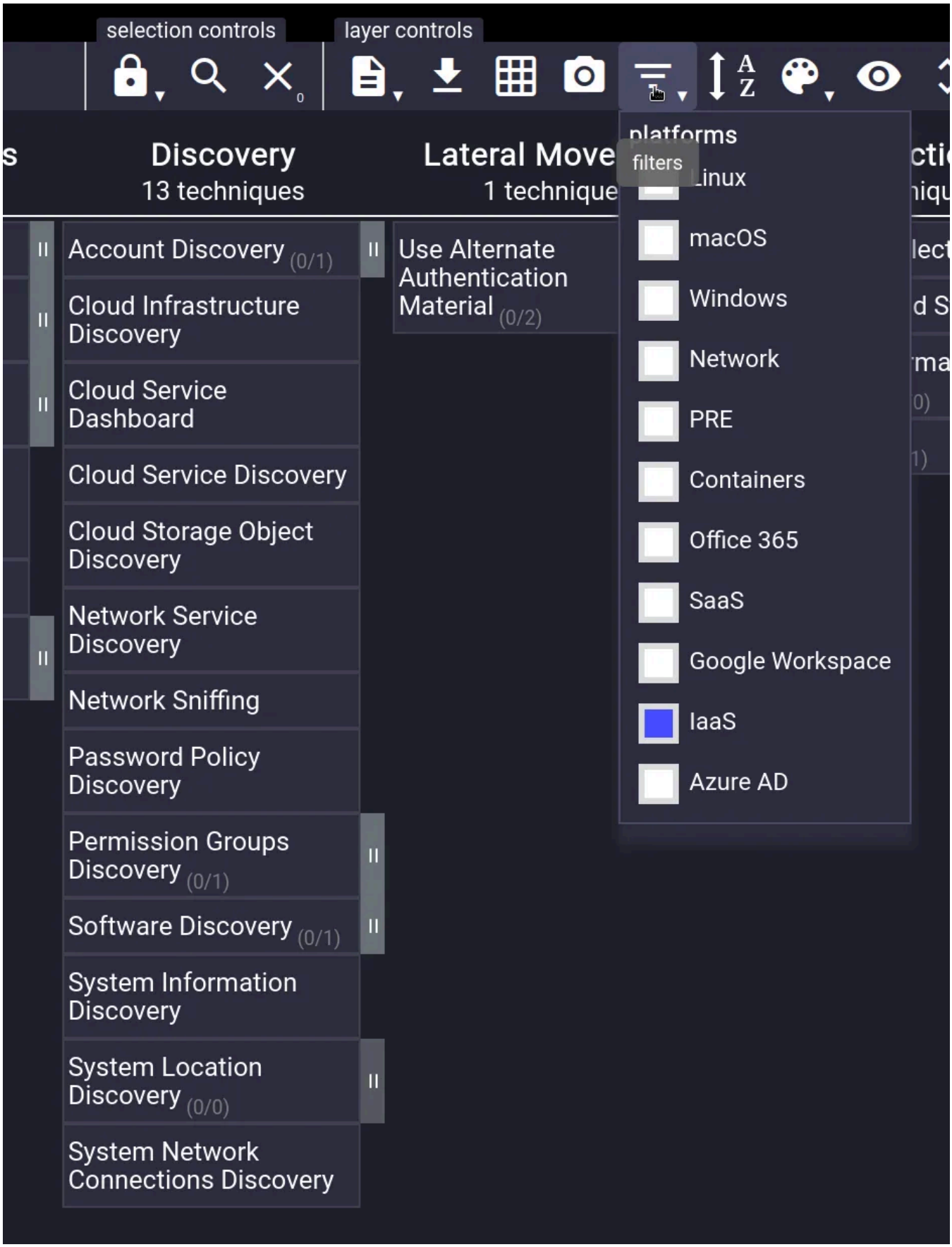
https://mitre-attack.github.io/attack-navigator/

How many MITRE ATT&CK techniques are attributed to APT33?



Answer: **31**

Upon applying the IaaS platform filter, how many techniques are under the Discovery tactic?



Answer: **13**

Task 5: **DREAD Framework**

What is the DREAD Framework?

The DREAD framework is a risk assessment model developed by Microsoft to evaluate and prioritise security threats and vulnerabilities. It is an acronym that stands for:

DREAD	Definition
Damage	The potential harm that could result from the successful exploitation of a vulnerability. This includes data loss, system downtime, or reputational damage.
Reproducibility	The ease with which an attacker can successfully recreate the exploitation of a vulnerability. A higher reproducibility score suggests that the vulnerability is straightforward to abuse, posing a greater risk.
Exploitability	The difficulty level involved in exploiting the vulnerability considering factors such as technical skills required, availability of tools or exploits, and the amount of time it would take to exploit the vulnerability successfully.
Affected Users	The number or portion of users impacted once the vulnerability has been exploited.
Discoverability	The ease with which an attacker can find and identify the vulnerability considering whether it is publicly known or how difficult it is to discover based on the exposure of the assets (publicly reachable or in a regulated environment).

The categories are commonly phrased with the following questions to ingest the definitions provided above quickly:

- **Damage** - How bad would an attack be?
- **Reproducibility** - How easy is it to reproduce the attack?
- **Exploitability** - How much work is it to launch the attack?
- **Affected Users** - How many people will be impacted?
- **Discoverability** - How easy is it to discover the vulnerability?

Using the questions above assists in understanding each category and applying it in a risk-assessment context.

DREAD Framework Guidelines

As mentioned above, the DREAD framework is an opinion-based model that heavily relies on an analyst's interpretation and assessment. However, the reliability of this framework can still be improved by following some guidelines:

1. Establish a standardised set of guidelines and definitions for each DREAD category that provides a consistent understanding of how to rate vulnerabilities. This can be supported by providing examples and scenarios to illustrate how scores should be assigned under various circumstances.
2. Encourage collaboration and discussion among multiple teams. Constructive feedback from different members aids in justifying the assigned scores, which can lead to a more accurate assessment.
3. Use the DREAD framework with other risk-assessment methodologies and regularly review and update the chosen methods and techniques to ensure they remain relevant and aligned with the organisation's needs.

By ensuring that these guidelines are strictly followed, organisations can reduce the subjective nature of the framework and improve the accuracy and reliability of their risk assessments.

Qualitative Analysis Using DREAD Framework

The DREAD Framework is typically used for Qualitative Risk Analysis, rating each category from one to ten based on a subjective assessment and interpretation of the questions above. Moreover, the average score of all criteria will calculate the overall DREAD risk rating.

To understand how the scoring works, let's put the concepts into practice by using a good scenario.

A software company has developed a new website and needs to assess the risk associated with various security threats. Your team has created a guideline for scoring each component of the DREAD framework, as shown below:

DREAD Score	2.5	5	7.5	10
Damage	Minimal infrastructure information disclosure	Minimal information disclosure related to client data	Limited PII leak	Complete data leak
Reproducibility	Multiple attack vectors requiring technical expertise	Minor customisation for public exploits needed	Little prerequisite technical skills needed to run the exploit	Users with public exploits can successfully reproduce the exploit
Exploitability	Almost no public exploits are available and need customisation of scripts	Complicated exploit scripts available in the wild	Minimal technical skills are required to execute public exploits	Reliable Metasploit module exists
Affected Users	Almost none to a small subset	Around 10% of users	More than half of the user base	All users
Discoverability	The significant effort needed to discover the vulnerability chains for the exploit to work	Requires a manual way of verifying the vulnerability	Public scanning scripts not embedded in scanning tools exist	Almost all known scanning tools can find the vulnerability

Given this guideline, we can assess some known vulnerabilities in the application. Below is an example of scoring provided for each vulnerability.

1. **Unauthenticated Remote Code Execution (Score: 8)**
   - Damage (D): **10**
   - Reproducibility (R): **7.5**
   - Exploitability (E): **10**
   - Affected Users (A): **10**
   - Discoverability (D): **2.5**
2. **Insecure Direct Object References (IDOR) in User Profiles (Score: 6.5)**
   - Damage (D): **2.5**
   - Reproducibility (R): **7.5**
   - Exploitability (E): **7.5**
   - Affected Users (A): **10**
   - Discoverability (D): **5**
3. **Server Misconfiguration Leading to Information Disclosure (Score: 5)**
   - Damage (D): **0**
   - Reproducibility (R): **10**
   - Exploitability (E): **10**
   - Affected Users (A): **0**
   - Discoverability (D): **5**

Now what's left is to prioritise the vulnerabilities based on their score and apply mitigations to secure the application.

What DREAD component assesses the potential harm from successfully exploiting a vulnerability?

Answer: **Damage**

What DREAD component evaluates how others can easily find and identify the vulnerability?

Answer: **Discoverability**

Which DREAD component considers the number of impacted users when a vulnerability is exploited?

Answer: **Affected Users**

Task 6: **STRIDE Framework**

What is the STRIDE Framework?

View Site

The STRIDE framework is a threat modelling methodology also developed by Microsoft, which helps identify and categorise potential security threats in software development and system design. The acronym STRIDE is based on six categories of threats, namely:

Category	Definition	Policy Violated
Spoofing	Unauthorised access or impersonation of a user or system.	Authentication
Tampering	Unauthorised modification or manipulation of data or code.	Integrity
Repudiation	Ability to deny having acted, typically due to insufficient auditing or logging.	Non-repudiation
Information Disclosure	Unauthorised access to sensitive information, such as personal or financial data.	Confidentiality
Denial of Service	Disruption of the system's availability, preventing legitimate users from accessing it.	Availability
Elevation of Privilege	Unauthorised elevation of access privileges, allowing threat actors to perform unintended actions.	Authorisation

As you can see, the table above also provides what component of the CIA triad is violated. The STRIDE framework is built upon this foundational information security concept.

By systematically analysing these six categories of threats, organisations can proactively identify and address potential vulnerabilities in their systems, applications, or infrastructure, enhancing their overall security posture.

To understand the framework better, let's deep-dive into each category and discuss some examples.

- **Spoofing**
  - Sending an email as another user.
  - Creating a phishing website mimicking a legitimate one to harvest user credentials.
- **Tampering**
  - Updating the password of another user.
  - Installing system-wide backdoors using an elevated access.
- **Repudiation**
  - Denying unauthorised money-transfer transactions, wherein the system lacks auditing.
  - Denying sending an offensive message to another person, wherein the person lacks proof of receiving one.
- **Information Disclosure**
  - Unauthenticated access to a misconfigured database that contains sensitive customer information.
  - Accessing public cloud storage that handles sensitive documents.
- **Denial of Service**
  - Flooding a web server with many requests, overwhelming its resources, and making it unavailable to legitimate users.
  - Deploying a ransomware that encrypts all system data that prevents other systems from accessing the resources the compromised server needs.
- **Elevation of Privilege**
  - Creating a regular user but being able to access the administrator console.
  - Gaining local administrator privileges on a machine by abusing unpatched systems.

The examples above illustrate various scenarios in which the categories can occur, emphasising the importance of implementing robust security measures to protect against these threats.

A typical representation of results after using the STRIDE framework is via a checklist table, wherein each use case is marked based on what STRIDE component affects it. In addition, some scenarios may cover multiple STRIDE components.

Scenario	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Sending a spoofed email, wherein the mail gateway lacks email security and logging configuration.	✓		✓			
Flooding a web server with many requests that lack load-balancing capabilities.					✓	
Abusing an SQL injection vulnerability.		✓		✓		
Accessing public cloud storage (such as AWS S3 bucket or Azure blob) that handles customer data.				✓		
Exploiting a local privilege escalation vulnerability due to the lack of system updates and modifying system configuration for a persistent backdoor.		✓				✓

Threat Modelling With STRIDE

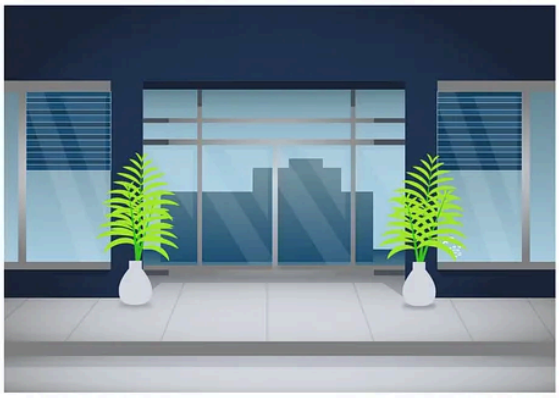
To implement the STRIDE framework in threat modelling, it is essential to integrate the six threat categories into a systematic process that effectively identifies, assesses, and mitigates security risks. Here is a high-level approach to incorporating STRIDE in the threat modelling methodologies we discussed.

1. **System Decomposition**
   Break down all accounted systems into components, such as applications, networks, and data flows. Understand the architecture, trust boundaries, and potential attack surfaces.
2. **Apply STRIDE Categories**
   For each component, analyse its exposure to the six STRIDE threat categories. Identify potential threats and vulnerabilities related to each category.
3. **Threat Assessment**
   Evaluate the impact and likelihood of each identified threat. Consider the potential consequences and the ease of exploitation and prioritise threats based on their overall risk level.
4. **Develop Countermeasures**
   Design and implement security controls to address the identified threats tailored to each STRIDE category. For example, to enhance email security and mitigate spoofing threats, implement DMARC, DKIM, and SPF, which are email authentication and validation mechanisms that help prevent email spoofing, phishing, and spamming.
5. **Validation and Verification**
   Test the effectiveness of the implemented countermeasures to ensure they effectively mitigate the identified threats. If possible, conduct penetration testing, code reviews, or security audits.
6. **Continuous Improvement**
   Regularly review and update the threat model as the system evolves and new threats emerge. Monitor the effective countermeasures and update them as needed.

By following this approach, you can effectively incorporate the STRIDE framework into your threat modelling process, ensuring a comprehensive analysis of potential security threats.

Application of STRIDE Framework

To apply the concepts discussed in this task, let's simulate a scenario wherein we can use the STRIDE framework.



Scenario: Your e-commerce company is in the process of designing a new payment processing system. To ensure its security and minimise the risk of compromise, you are tasked to conduct a threat modelling exercise using the STRIDE framework. All your assets are stored in a secure cloud infrastructure developed by your system architects.

As the leader of this initiative, you will be working with different teams to create a thorough threat modelling plan. Together, you aim to identify potential security threats and protect your payment processing system, ensuring the safety of your customers' information.

As a guide, here are the roles and responsibilities of the teams joining the initiative:

Team	Roles and Responsibilities
Development Team	Responsible for building systems and applications used by the organisation.
System Architecture Team	Responsible for designing the overall architecture of the cloud services used by the organisation.
Security Team	Provide expertise on threats, vulnerabilities, and risk mitigation strategies.
Business Stakeholder Team	Provides valuable input on critical assets and business processes, and ensures alignment between the initiative and the organisation's strategic goals.
Network Infrastructure Team	Manages the organisation's network infrastructure, including servers and critical systems.

To start working, click on the green **View Site** button in this task to open the static site lab and start working on your preparation for the threat modelling exercise by following the provided instructions.

What foundational information security concept does the STRIDE framework build upon?

Answer: **CIA Triad**

What policy does Information Disclosure violate?

Answer: **Confidentiality**

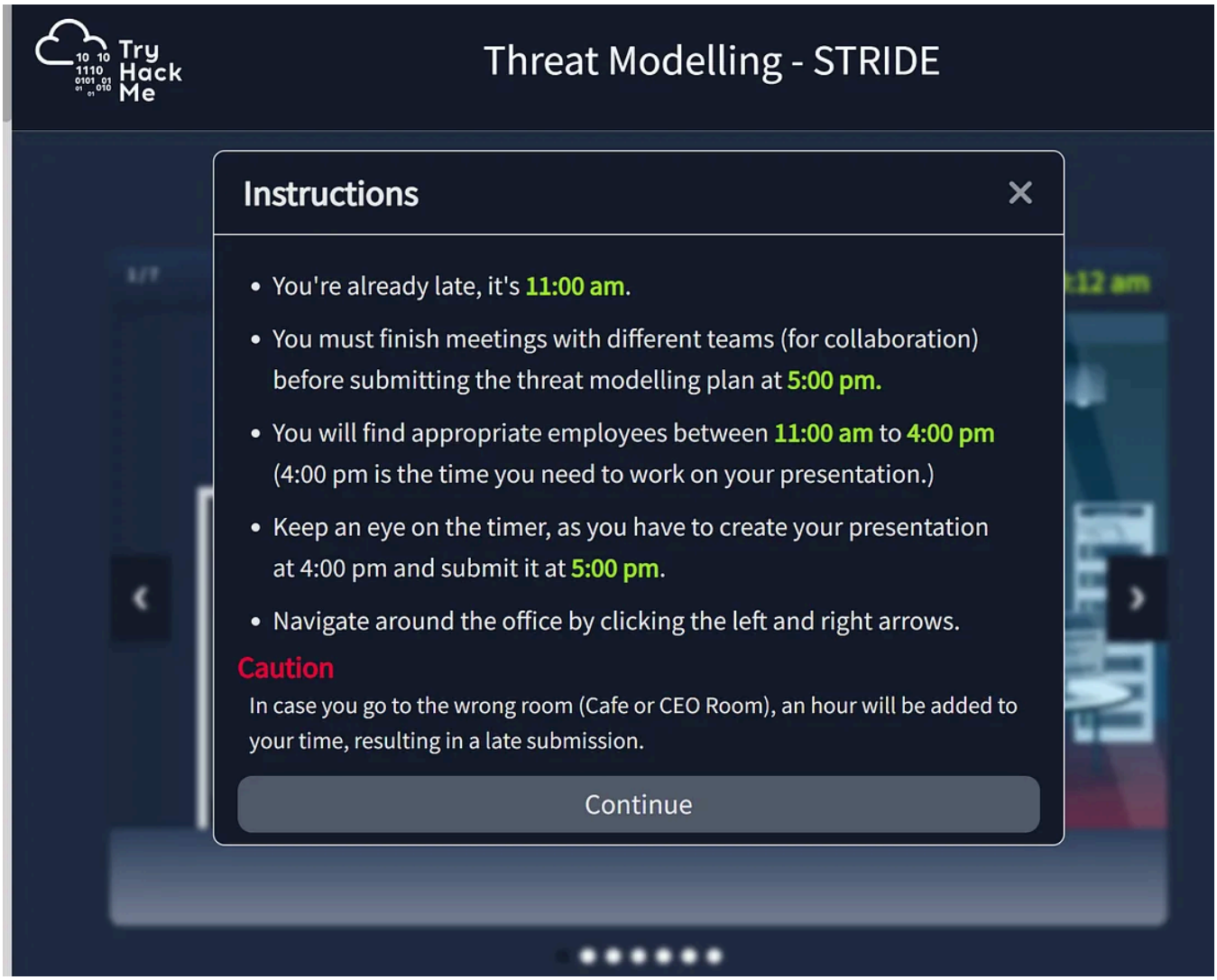
Which STRIDE component involves unauthorised modification or manipulation of data?

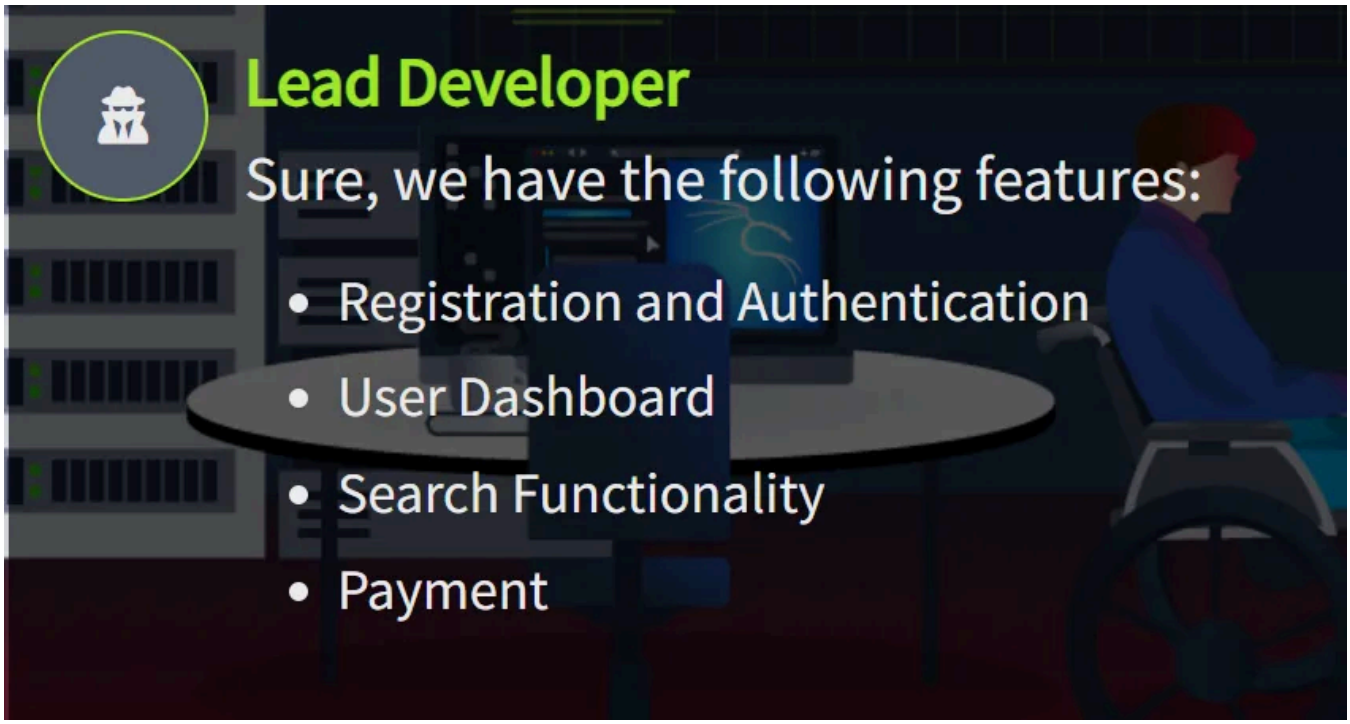
Answer: **Tampering**

Which STRIDE component refers to the disruption of the system's availability?

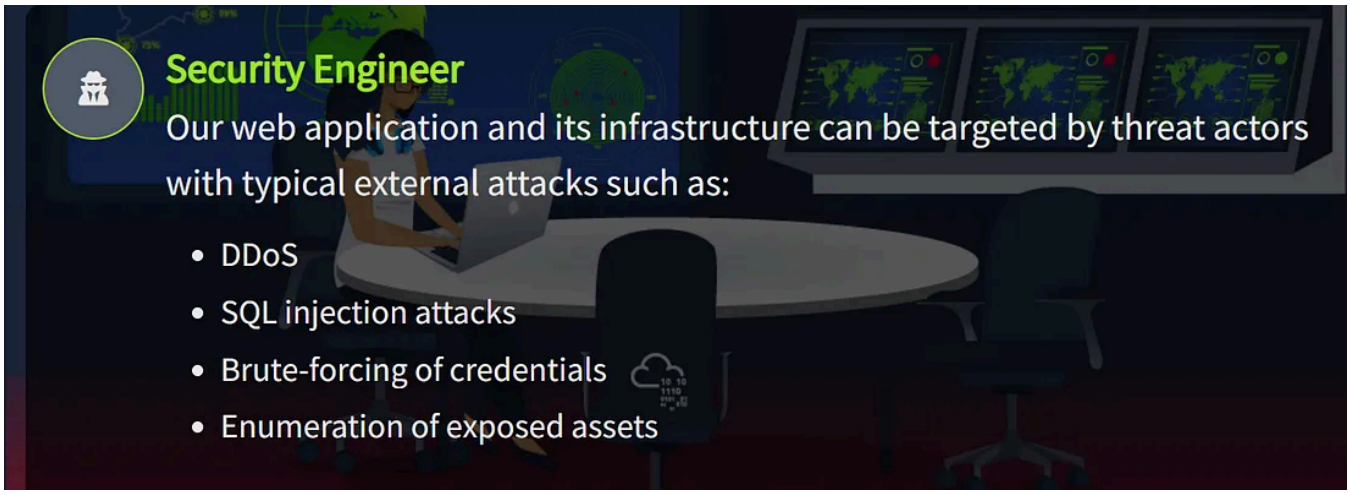
Answer: **Denial of Service**

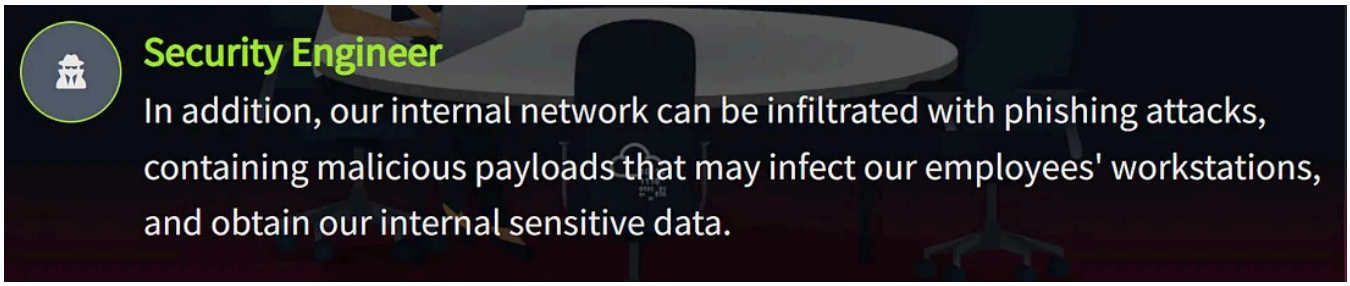
Provide the flag for the simulated threat modelling exercise.

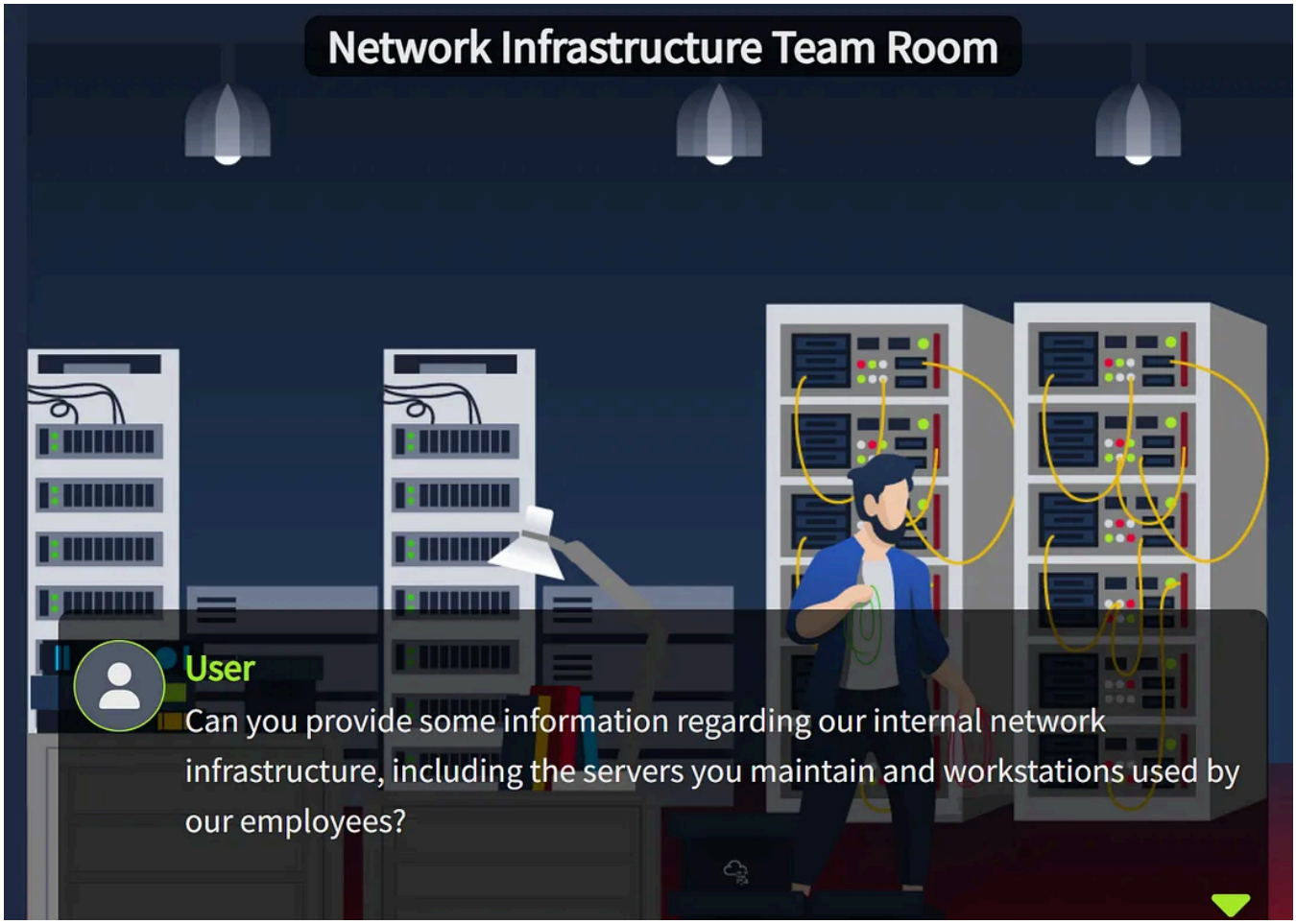


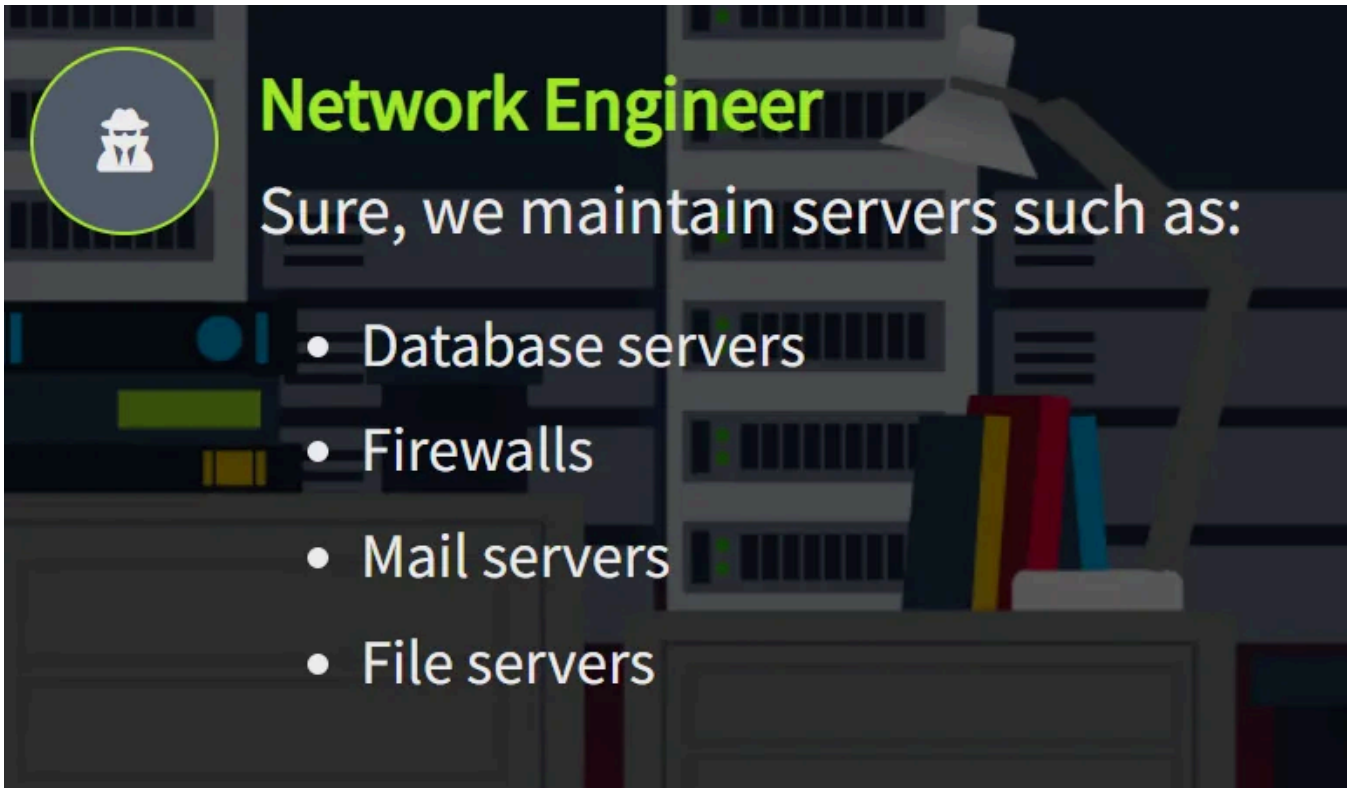

Lead Developer
Sure, we have the following features:
• Registration and Authentication
• User Dashboard
• Search Functionality
• Payment

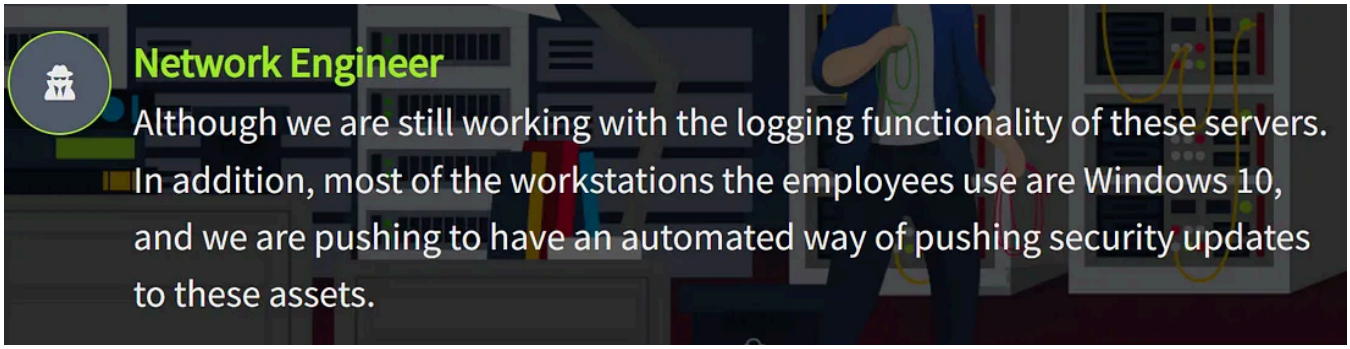

Security Team Room
User
Hi! Can you help me identify potential threats and vulnerabilities to our organization, including all of its infrastructure and our internal infrastructure?


Security Engineer
Our web application and its infrastructure can be targeted by threat actors with typical external attacks such as:
DDoS
SQL injection attacks
Brute-forcing of credentials
Enumeration of exposed assets

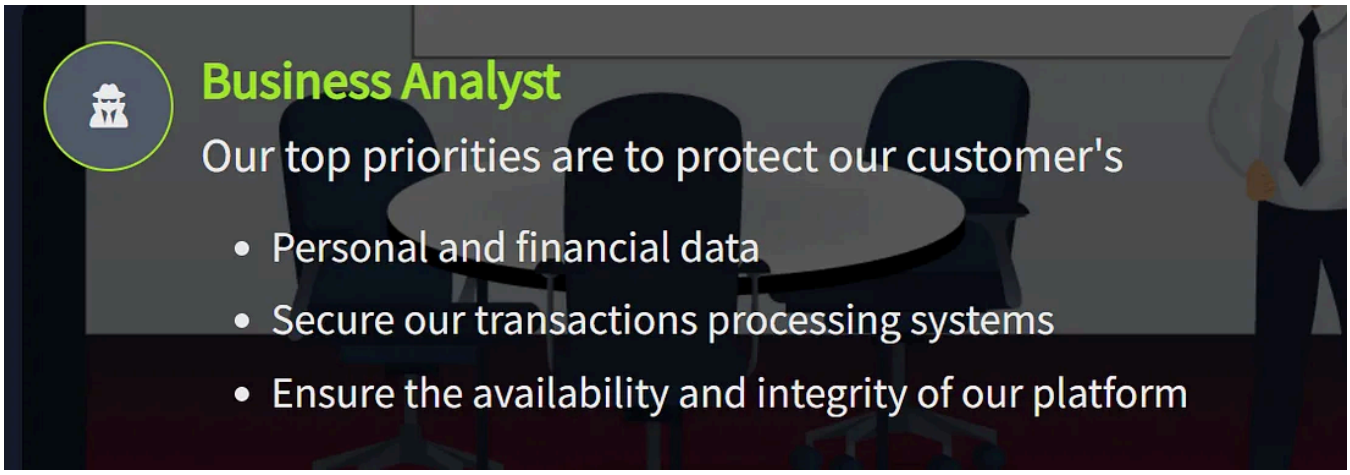

Security Engineer
In addition, our internal network can be infiltrated with phishing attacks, containing malicious payloads that may infect our employees' workstations, and obtain our internal sensitive data.

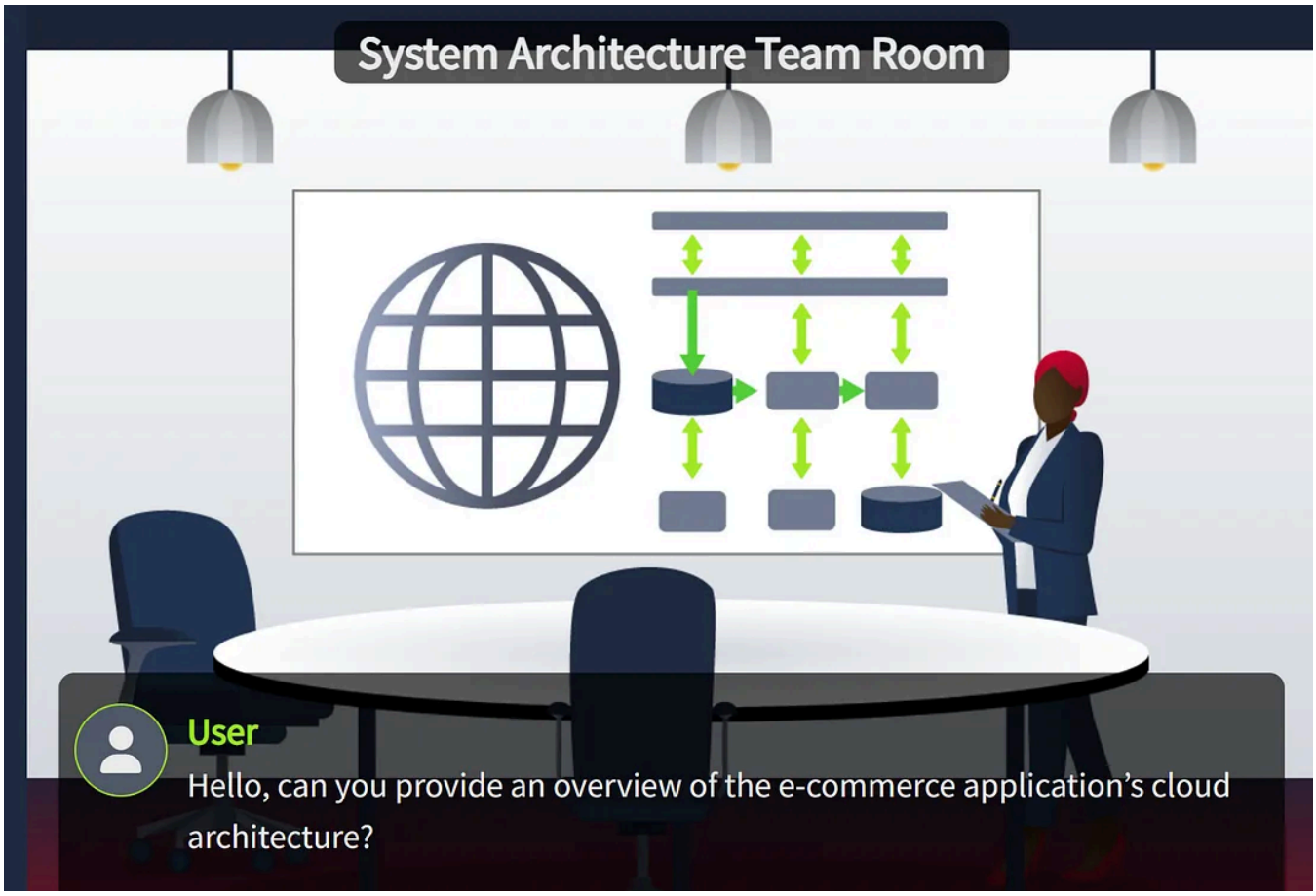

Network Infrastructure Team Room
User
Can you provide some information regarding our internal network infrastructure, including the servers you maintain and workstations used by our employees?

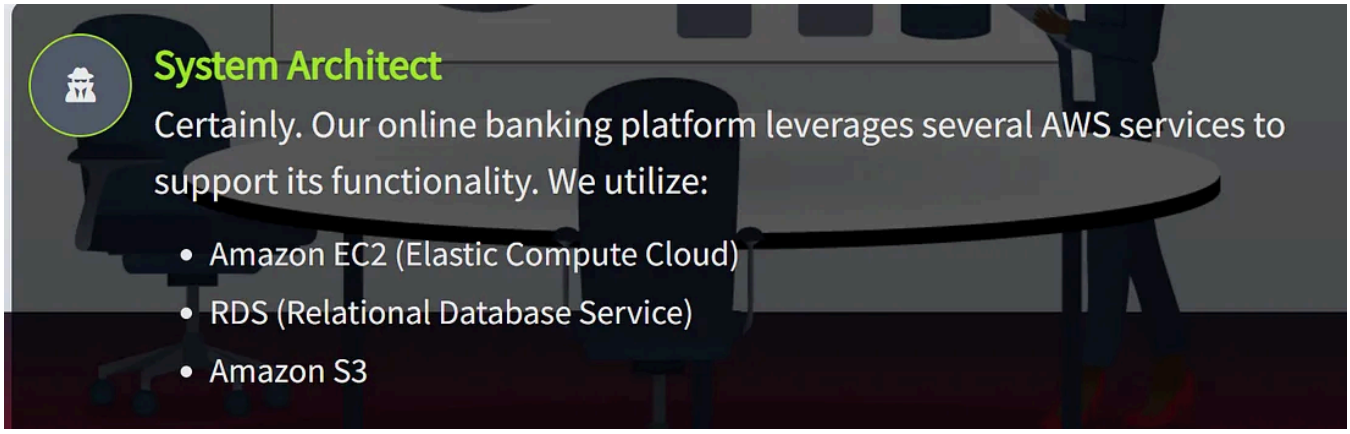

Network Engineer
Sure, we maintain servers such as:
• Database servers
• Firewalls
• Mail servers
• File servers

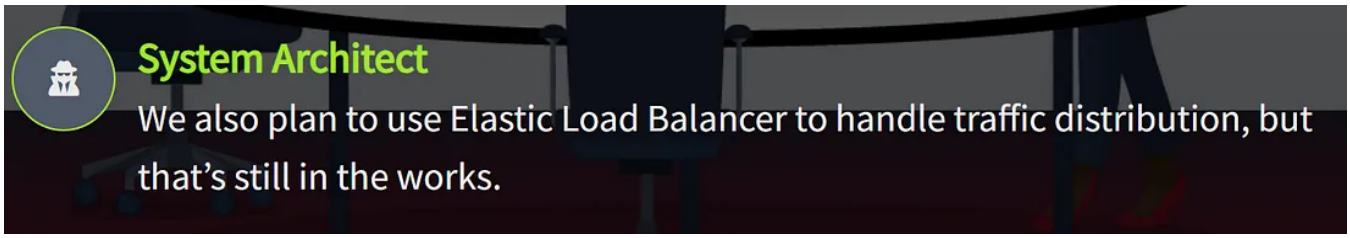

Network Engineer
Although we are still working with the logging functionality of these servers. In addition, most of the workstations the employees use are Windows 10, and we are pushing to have an automated way of pushing security updates to these assets.

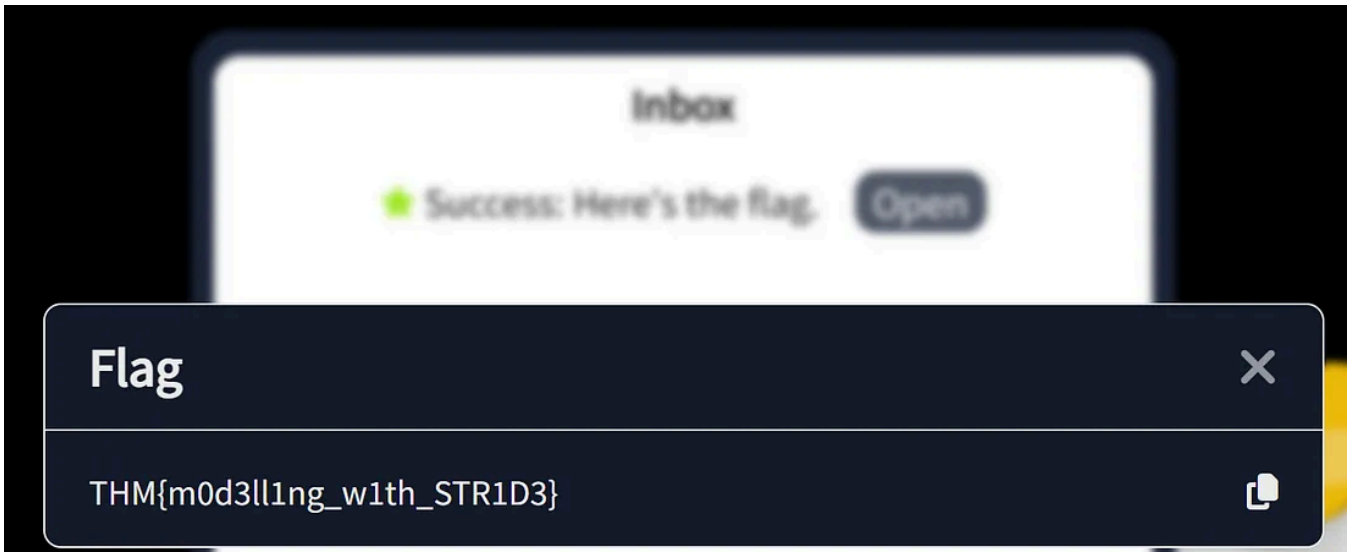

Business Stakeholder Team Room
Strategic Planning
User
What are the critical assets and processes in our e-commerce platform that we need to protect?


Business Analyst
Our top priorities are to protect our customer's
Personal and financial data
Secure our transactions processing systems
Ensure the availability and integrity of our platform


System Architecture Team Room
User
Hello, can you provide an overview of the e-commerce application's cloud architecture?


System Architect
Certainly. Our online banking platform leverages several AWS services to support its functionality. We utilize:
• Amazon EC2 (Elastic Compute Cloud)
• RDS (Relational Database Service)
• Amazon S3


System Architect
We also plan to use Elastic Load Balancer to handle traffic distribution, but that's still in the works.



Answer: **THM{m0d3ll1ng_w1th_STR1D3}**

Task 7: **PASTA Framework**

What is the PASTA Framework?

View Site

PASTA, or Process for Attack Simulation and Threat Analysis, is a structured, risk-centric threat modelling framework designed to help organisations identify and evaluate security threats and vulnerabilities within their systems, applications, or infrastructure. PASTA provides a systematic, seven-step process that enables security teams to understand potential attack scenarios better, assess the likelihood and impact of threats, and prioritise remediation efforts accordingly.

This framework was created by Tony UcedaVélez and Marco Morana. They introduced the PASTA framework in their book **"Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis"**, published in 2015.

Seven-Step Methodology

Similar to the high-level process discussed in the previous task, the PASTA framework covers a series of steps, from defining the scope of the threat modelling exercise to risk and impact analysis. Below is an overview of the seven-step methodology of the PASTA Framework.

1. **Define the Objectives**
   Establish the scope of the threat modelling exercise by identifying the systems, applications, or networks being analysed and the specific security objectives and compliance requirements to be met.
2. **Define the Technical Scope**
   Create an inventory of assets, such as hardware, software, and data, and develop a clear understanding of the system's architecture, dependencies, and data flows.
3. **Decompose the Application**
   Break down the system into its components, identifying entry points, trust boundaries, and potential attack surfaces. This step also includes mapping out data flows and understanding user roles and privileges within the system.
4. **Analyse the Threats**
   Identify potential threats to the system by considering various threat sources, such as external attackers, insider threats, and accidental exposures. This step often involves leveraging industry-standard threat classification frameworks or attack libraries.
5. **Vulnerabilities and Weaknesses Analysis**
   Analyse the system for existing vulnerabilities, such as misconfigurations, software bugs, or unpatched systems, that an attacker could exploit to achieve their objectives. Vulnerability assessment tools and techniques, such as static and dynamic code analysis or penetration testing, can be employed during this step.
6. **Analyse the Attacks**
   Simulate potential attack scenarios and evaluate the likelihood and impact of each threat. This step helps determine the risk level associated with each identified threat, allowing security teams to prioritise the most significant risks.
7. **Risk and Impact Analysis**
   Develop and implement appropriate security controls and countermeasures to address the identified risks, such as updating software, applying patches, or implementing access controls. The chosen countermeasures should be aligned with the organisation's risk tolerance and security objectives.

PASTA Methodology Guidelines

To effectively implement the PASTA framework and optimise its benefits, you may follow these practical guidelines for each step of the methodology.

Define the Objectives	• Set clear and realistic security objectives for the threat modelling exercise. • Identify relevant compliance requirements and industry-specific security standards.
Define the Technical Scope	• Identify all critical assets, such as systems and applications, that handle sensitive data owned by the organisation. • Develop a thorough understanding of the system architecture, including data flows and dependencies.
Decompose the Application	• Break down the system into manageable components or modules. • Identify and document each component's possible entry points, trust boundaries, attack surfaces, data flows, and user flows.
Analyse the Threats	• Research and list potential threats from various sources, such as external attackers, insider threats, and accidental exposures. • Leverage threat intelligence feeds and industry best practices to stay updated on emerging threats.
Vulnerabilities and Weaknesses Analysis	• Use a combination of tools and techniques, such as static and dynamic code analysis, vulnerability scanning, and penetration testing, to identify potential weaknesses in the system. • Keep track of known vulnerabilities and ensure they are addressed promptly.
Analyse the Attacks	• Develop realistic attack scenarios and simulate them to evaluate their potential consequences. • Create a blueprint of scenarios via Attack Trees and ensure that all use cases are covered and aligned with the objective of the exercise.
Risk and Impact Analysis	• Assess the likelihood and impact of each identified threat and prioritise risks based on their overall severity. • Determine the most effective and cost-efficient countermeasures for the identified risks, considering the organisation's risk tolerance and security objectives.

These guidelines provide a foundation for effectively using the PASTA framework's seven-step methodology. However, adapting and customising the approach according to your organisation's unique needs and requirements is crucial.

Benefits of Using the PASTA Framework

This framework, being risk-centric, offers numerous benefits for organisations seeking to enhance their security posture through threat modelling.

- The framework is adaptable to unique objectives and helps organisations align with compliance requirements by systematically identifying and addressing security risks while ensuring proper security controls are in place.
- Like the other frameworks, PASTA fosters collaboration between stakeholders, such as developers, architects, and security professionals, promoting a shared understanding of security risks and facilitating communication across the organisation.
- In addition, the PASTA methodology helps organisations meet compliance requirements by systematically identifying and addressing security risks and ensuring that appropriate security controls are in place.
- Lastly, the primary reason to use PASTA is its comprehensive and systematic process, ensuring a thorough analysis of the entire risk landscape. Organisations can proactively address security risks by employing PASTA, tailoring the seven-step methodology to their unique needs, and maintaining a solid security posture.

Application of PASTA Framework

To apply the concepts discussed in this task, let's simulate a scenario wherein we can use the PASTA framework.

Scenario: Your organisation is known for its online banking platform, catering to many users across the Asia Pacific region. To ensure its resiliency to potential threats, you are tasked to conduct a threat modelling exercise using the PASTA framework.

As the leader of this initiative, you will be working with different teams to create a thorough threat modelling plan. Together, you aim to identify potential security threats and protect your online banking platform, ensuring the safety of your customers' information.

As a guide, here are the roles and responsibilities of the teams joining the initiative:

Team	Roles and Responsibilities
Development Team	Responsible for building systems and applications used by the organisation.
System Architecture Team	Responsible for designing the overall architecture of the cloud services used by the organisation.
Security Team	Provide expertise on threats, vulnerabilities, and risk mitigation strategies.
Business Stakeholder Team	Provides valuable input on critical assets and business processes, and ensures alignment between the initiative and the organisation's strategic goals.

You must follow the seven-step PASTA process in choosing whom to approach for the information you need for this threat modelling exercise.

To start working, click on the green **View Site** button in this task to open the static site lab and start working on your preparation for the threat modelling exercise by following the provided instructions.

In which step of the framework do you break down the system into its components?

Answer: **Decompose the Application**

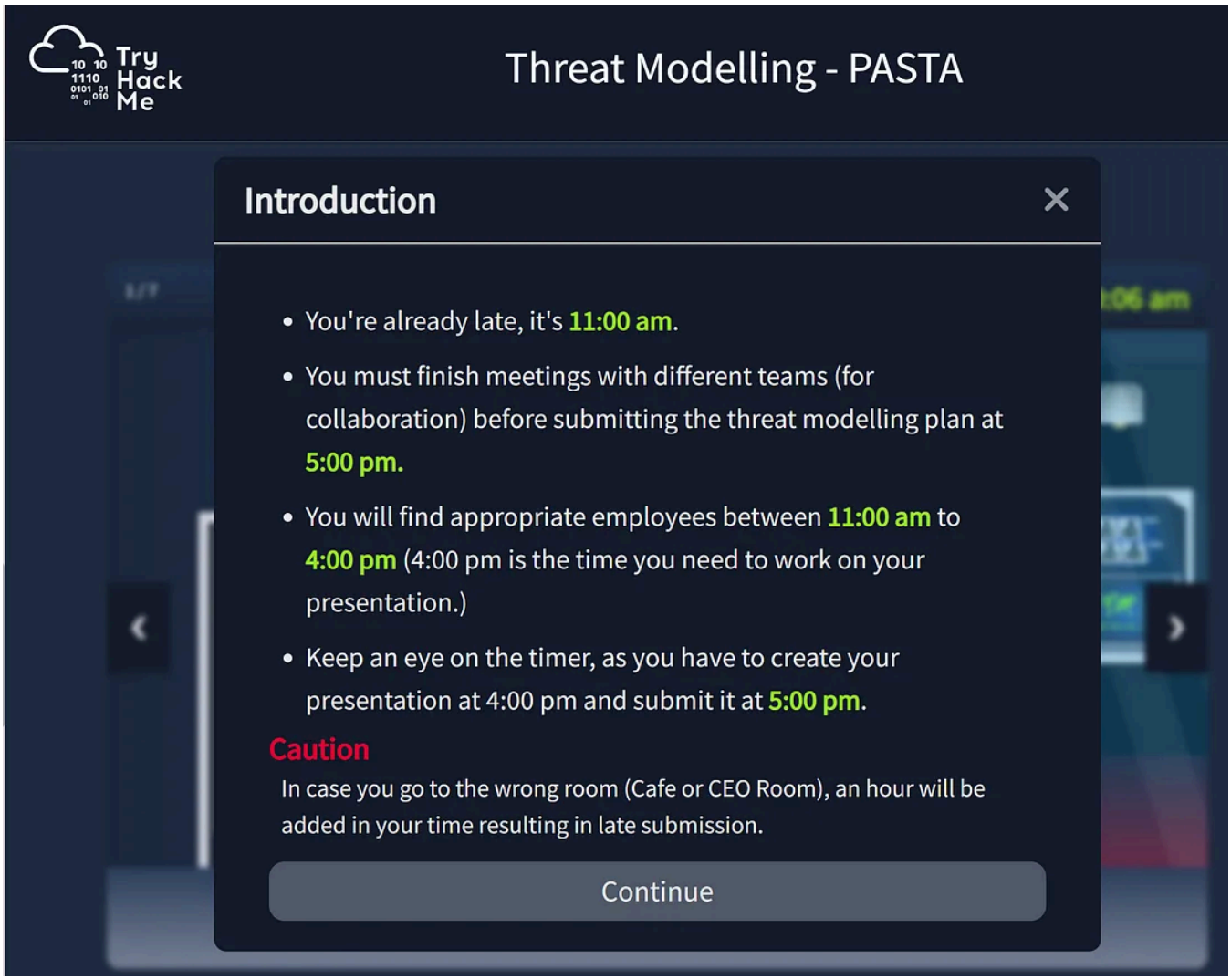
During which step of the PASTA framework do you simulate potential attack scenarios?

Answer: **Analyse the Attacks**

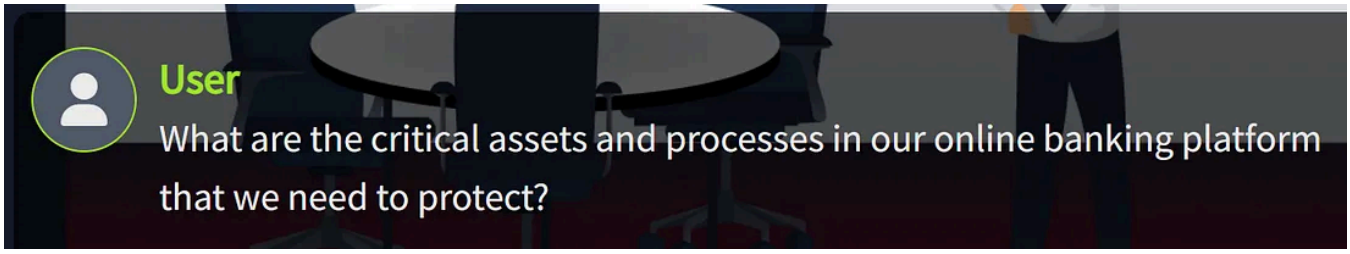
In which step of the PASTA framework do you create an inventory of assets?

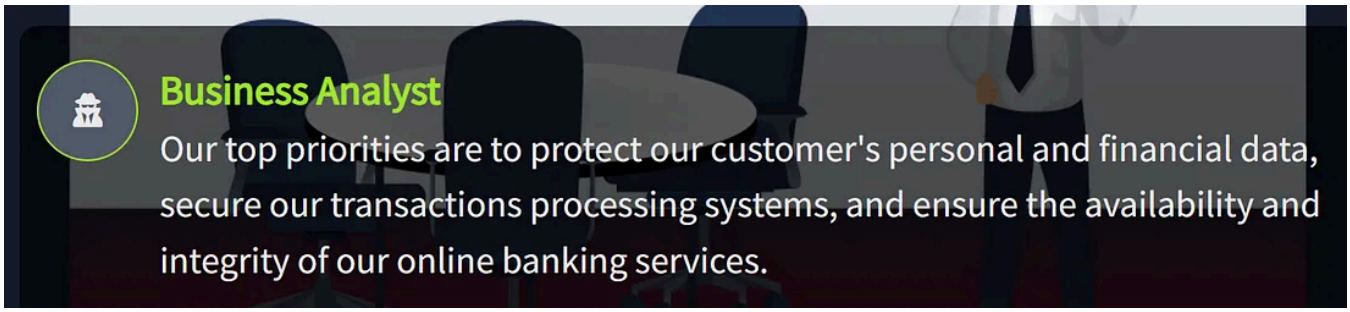
Answer: **Define the Technical Scope**

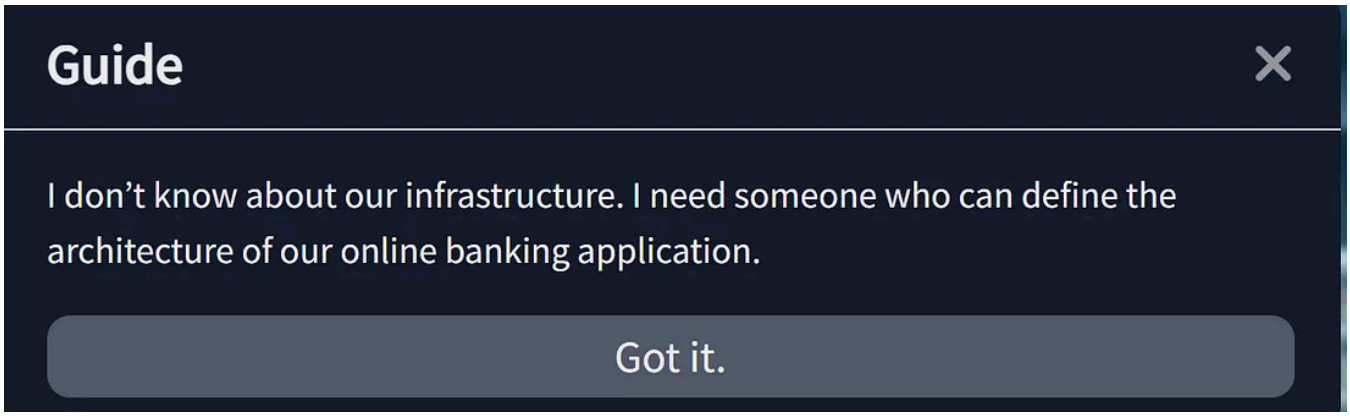
Provide the flag for the simulated threat modelling exercise.

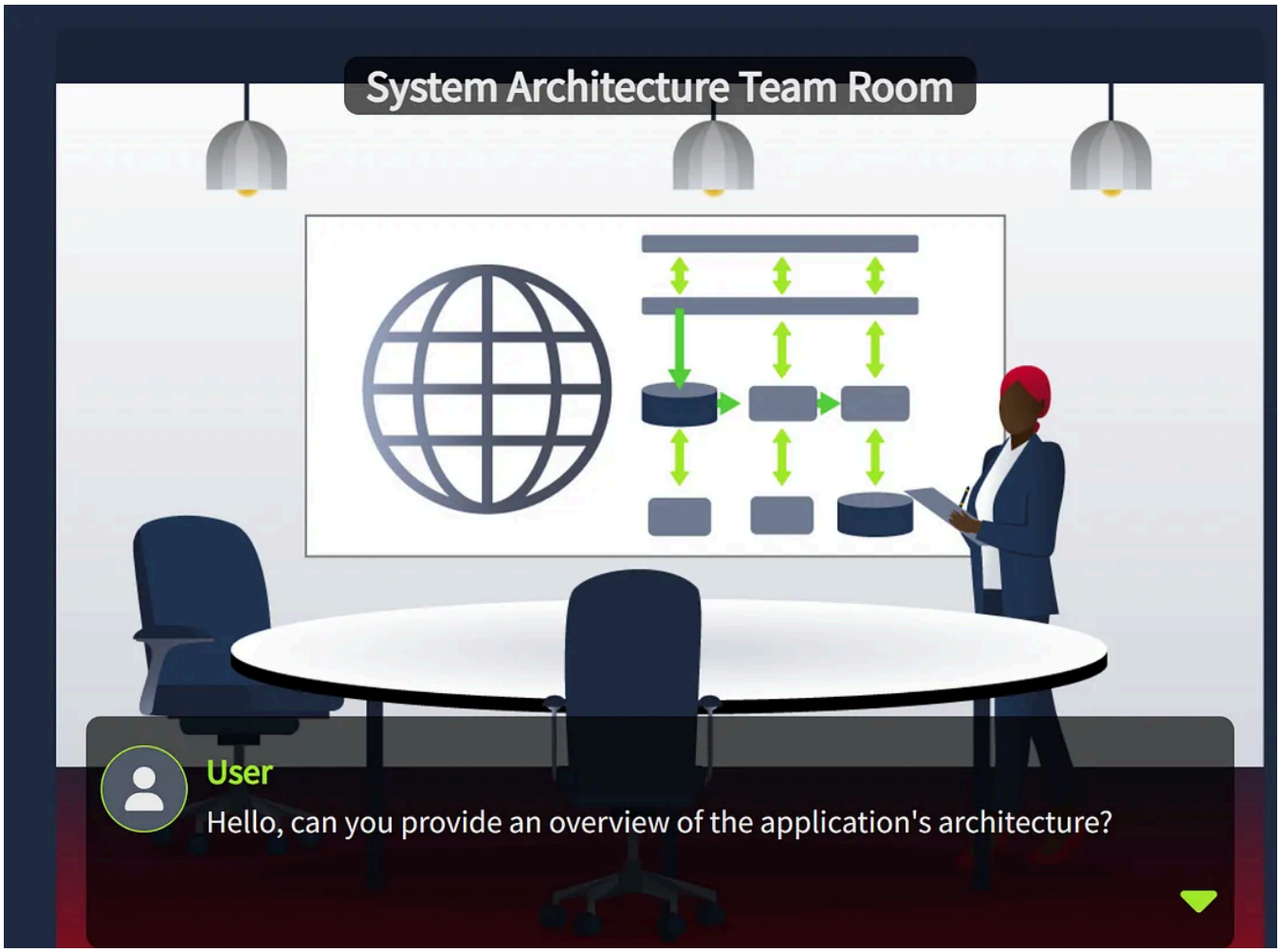

Try Hack Me
Threat Modelling - PASTA
Introduction
You're already late, it's 11:00 am.
You must finish meetings with different teams (for collaboration) before submitting the threat modelling plan at 5:00 pm.
You will find appropriate employees between 11:00 am to 4:00 pm (4:00 pm is the time you need to work on your presentation.)
Keep an eye on the timer, as you have to create your presentation at 4:00 pm and submit it at 5:00 pm.
Caution
In case you go to the wrong room (Cafe or CEO Room), an hour will be added in your time resulting in late submission.
Continue

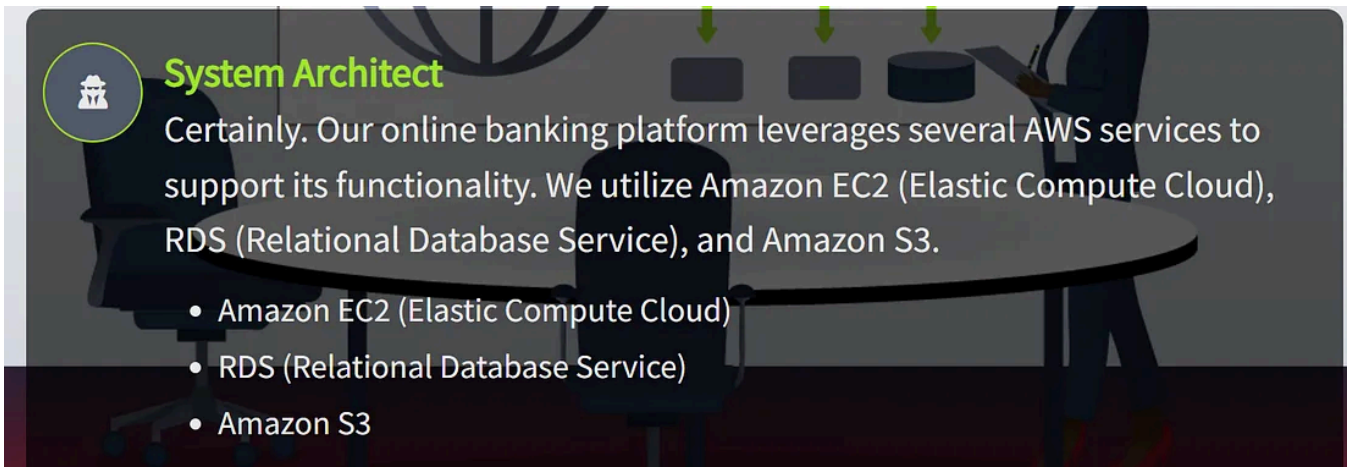

Business Stakeholder Team Room
Strategic Planning
User
Hey, I'm currently working on a Threat Modelling plan and I would like to ask for your expertise.

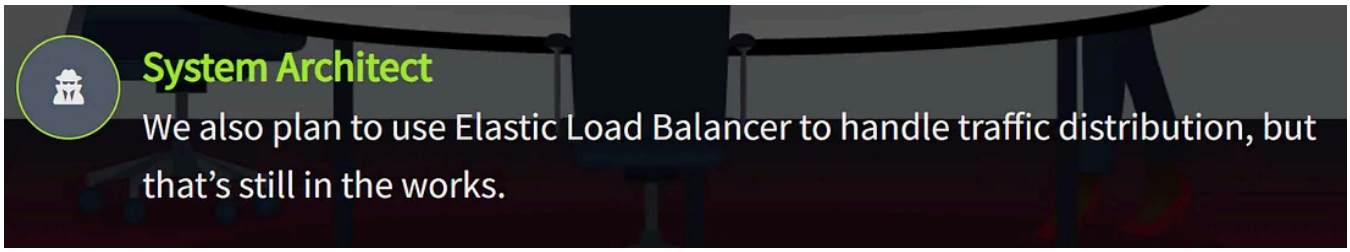

User
What are the critical assets and processes in our online banking platform that we need to protect?

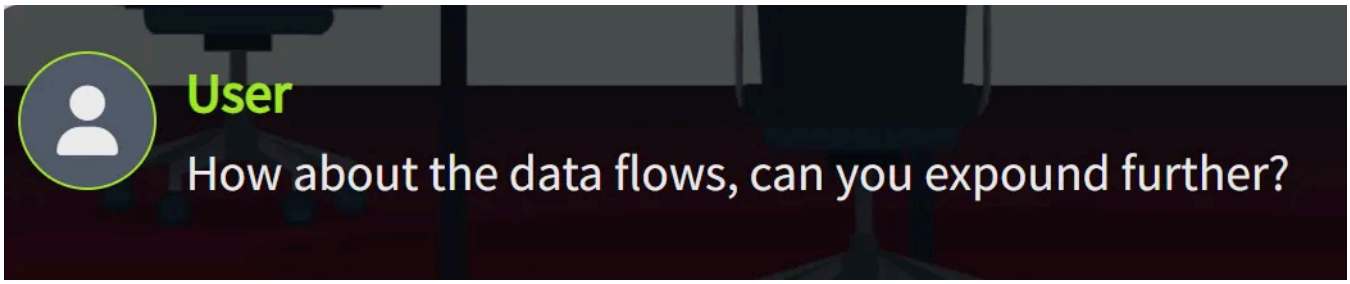

Business Analyst
Our top priorities are to protect our customer's personal and financial data, secure our transactions processing systems, and ensure the availability and integrity of our online banking services.

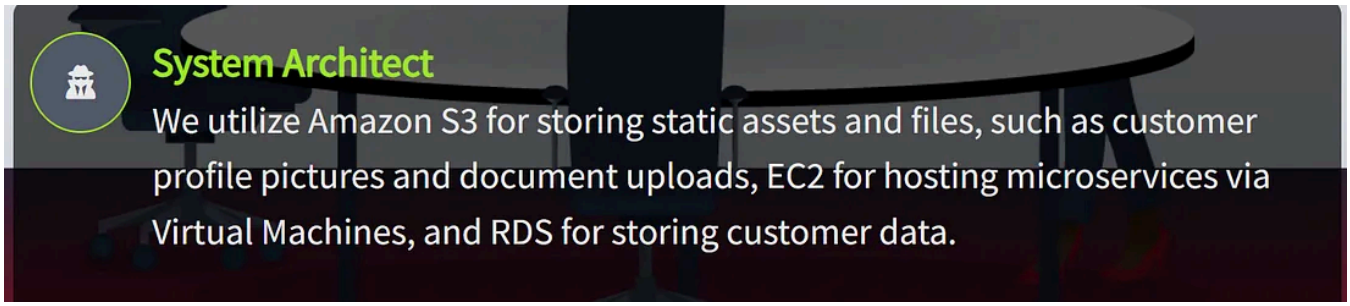

Guide
I don’t know about our infrastructure. I need someone who can define the architecture of our online banking application.
Got it.

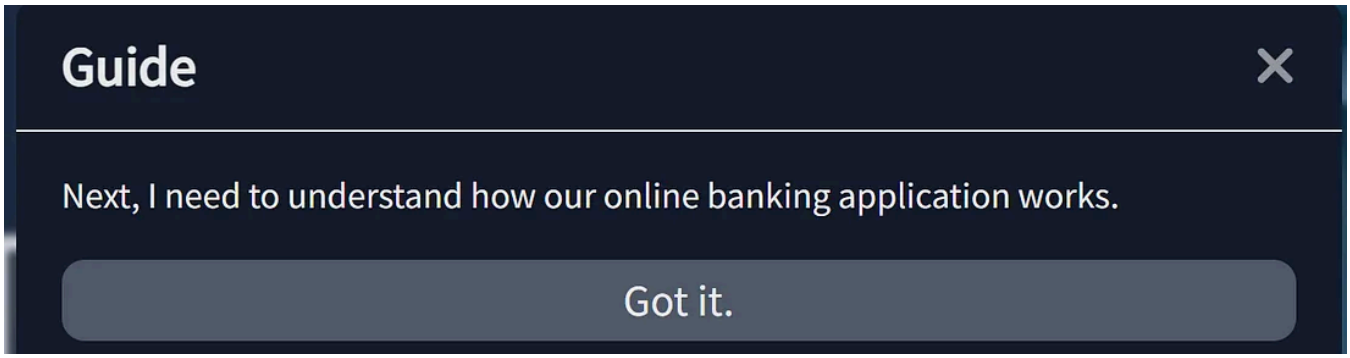

System Architecture Team Room
User
Hello, can you provide an overview of the application's architecture?

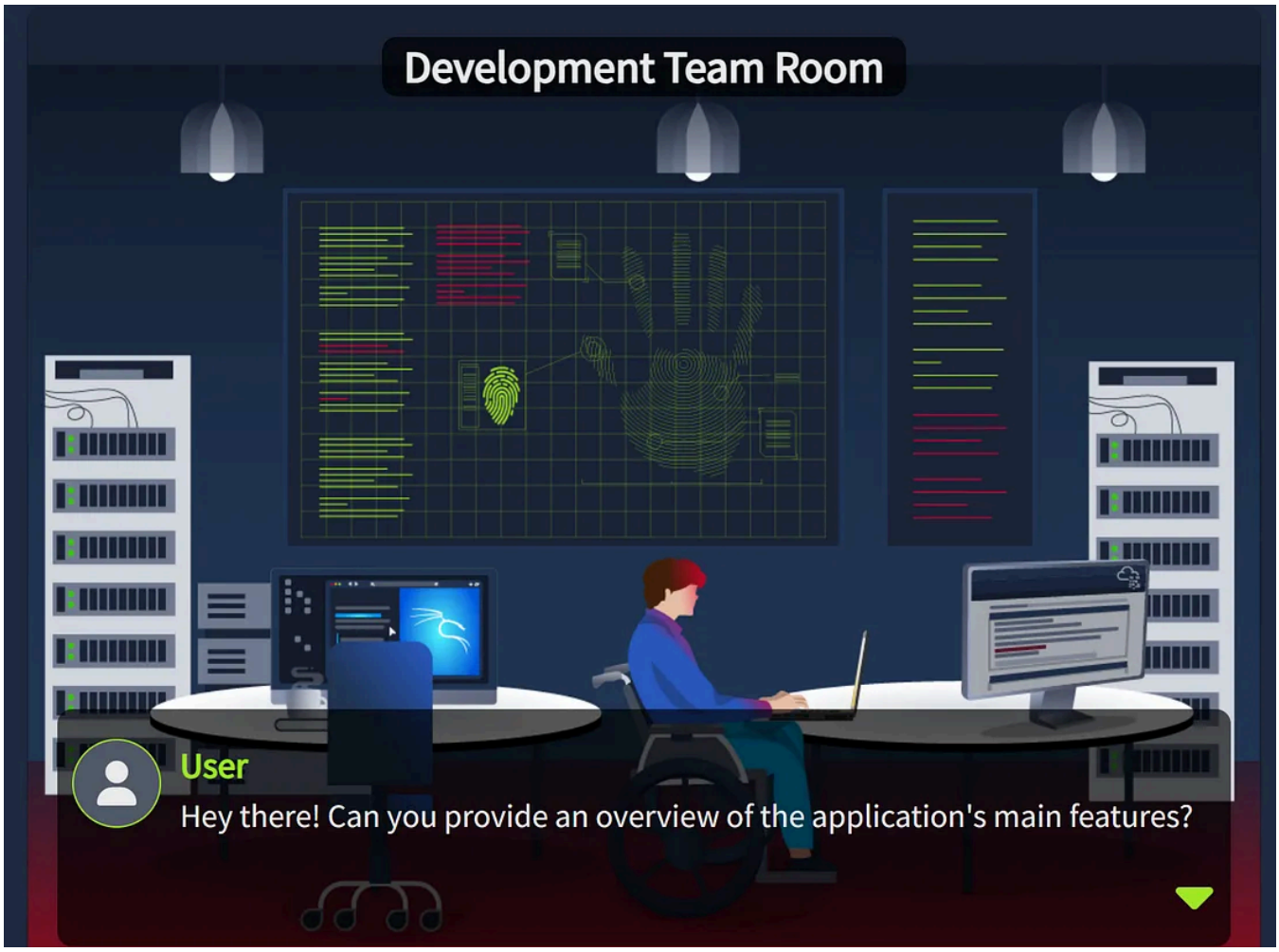

System Architect
Certainly. Our online banking platform leverages several AWS services to support its functionality. We utilize Amazon EC2 (Elastic Compute Cloud), RDS (Relational Database Service), and Amazon S3.
Amazon EC2 (Elastic Compute Cloud)
RDS (Relational Database Service)
Amazon S3

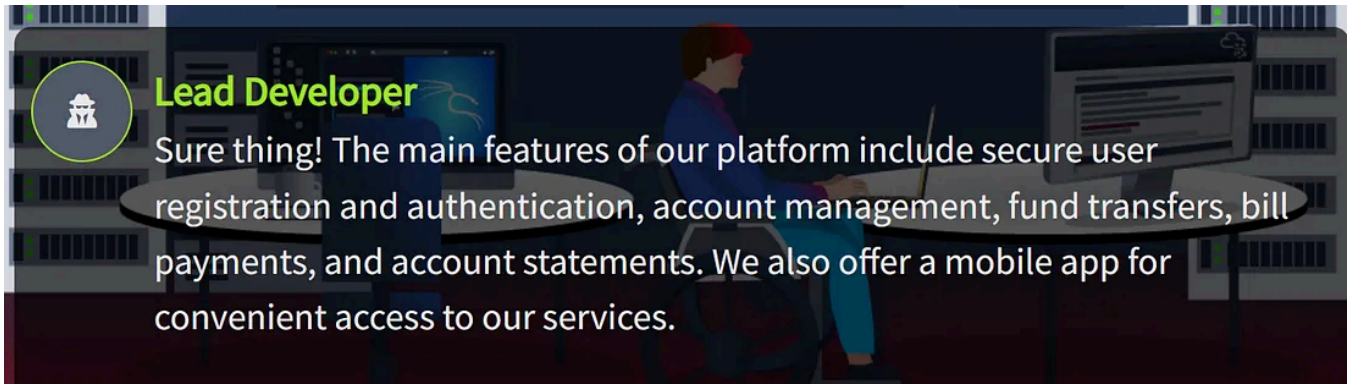

System Architect
We also plan to use Elastic Load Balancer to handle traffic distribution, but that's still in the works.

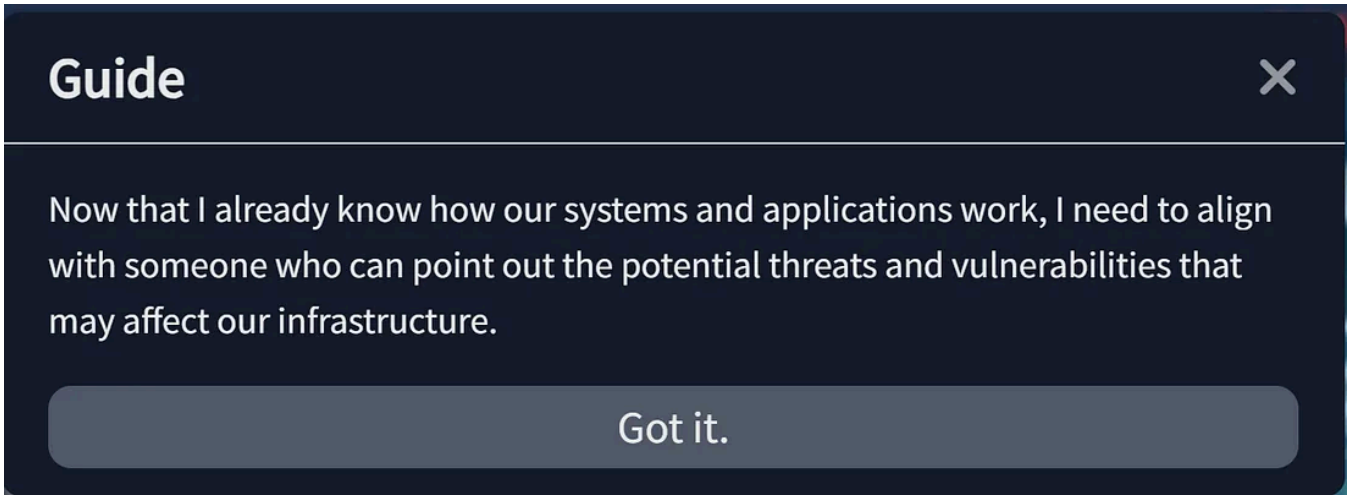

User
How about the data flows, can you expound further?


System Architect
We utilize Amazon S3 for storing static assets and files, such as customer profile pictures and document uploads, EC2 for hosting microservices via Virtual Machines, and RDS for storing customer data.

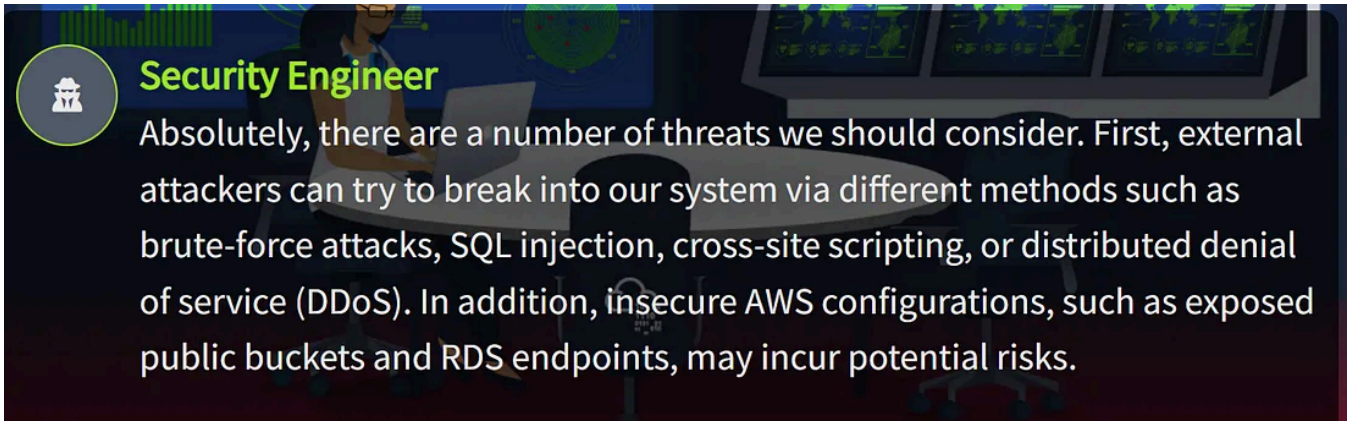

Guide
Next, I need to understand how our online banking application works.
Got it.

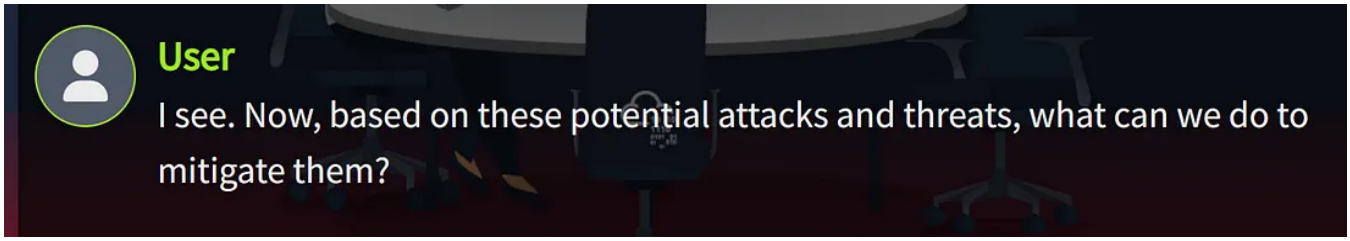

Development Team Room
User
Hey there! Can you provide an overview of the application's main features?

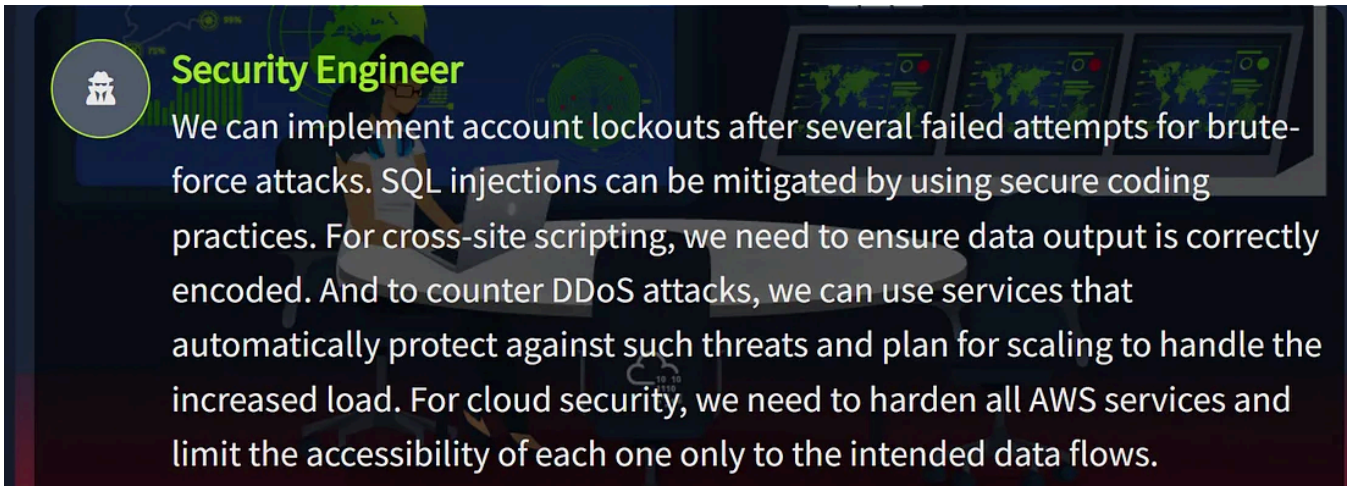

Lead Developer
Sure thing! The main features of our platform include secure user registration and authentication, account management, fund transfers, bill payments, and account statements. We also offer a mobile app for convenient access to our services.

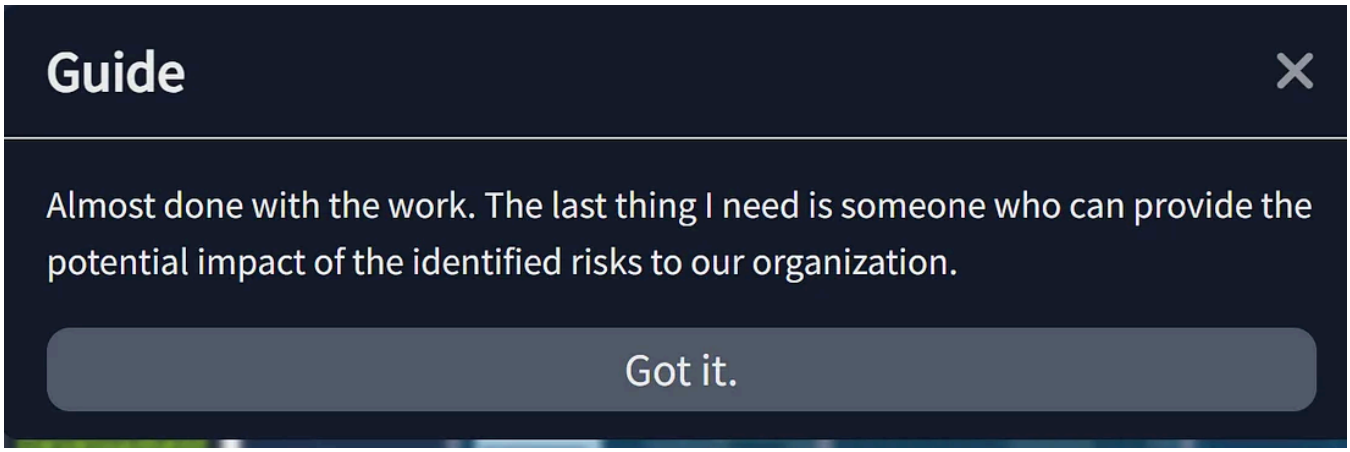

Guide
Now that I already know how our systems and applications work, I need to align with someone who can point out the potential threats and vulnerabilities that may affect our infrastructure.
Got it.

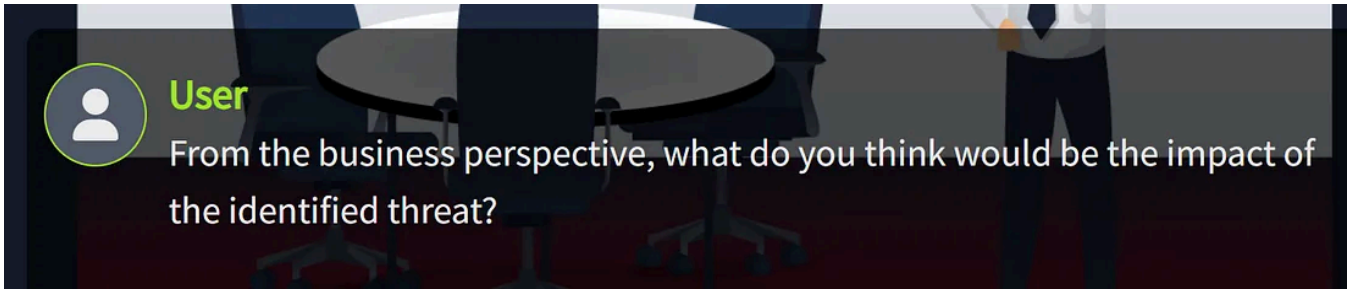

Security Team Room
User
Hi! Can you help me identify potential threats and vulnerabilities to our online banking system?

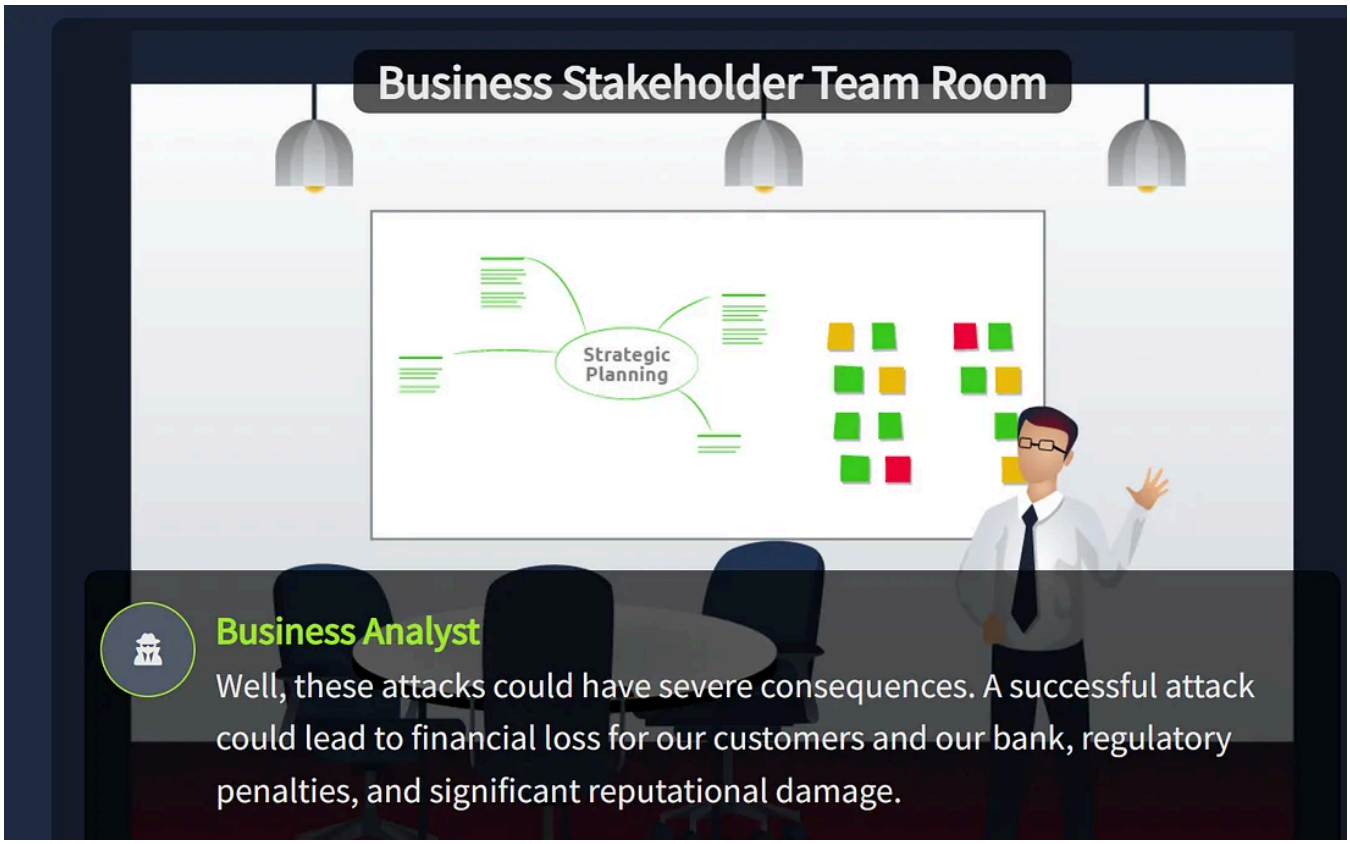

Security Engineer
Absolutely, there are a number of threats we should consider. First, external attackers can try to break into our system via different methods such as brute-force attacks, SQL injection, cross-site scripting, or distributed denial of service (DDoS). In addition, insecure AWS configurations, such as exposed public buckets and RDS endpoints, may incur potential risks.

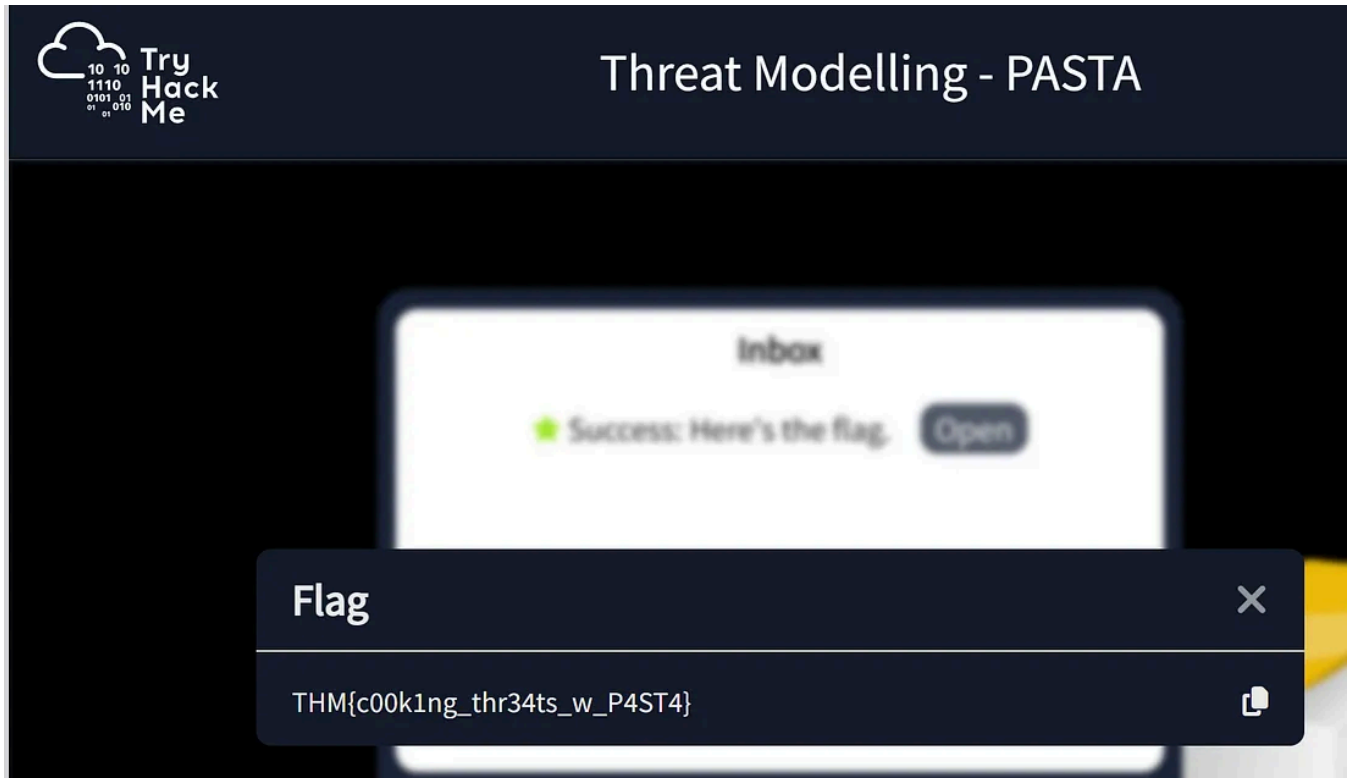

User
I see. Now, based on these potential attacks and threats, what can we do to mitigate them?


Security Engineer
We can implement account lockouts after several failed attempts for brute-force attacks. SQL injections can be mitigated by using secure coding practices. For cross-site scripting, we need to ensure data output is correctly encoded. And to counter DDoS attacks, we can use services that automatically protect against such threats and plan for scaling to handle the increased load. For cloud security, we need to harden all AWS services and limit the accessibility of each one only to the intended data flows.


Guide
Almost done with the work. The last thing I need is someone who can provide the potential impact of the identified risks to our organization.
Got it.


User
From the business perspective, what do you think would be the impact of the identified threat?





Answer: **THM{c00k1ng_thr34ts_w_P4ST4}**

Task 8: **Conclusion**

Congratulations! You have completed the Threat Modelling room.

To conclude the room, let's summarise the use case applications of each framework:

Framework	Use Case Applications
MITRE ATT&CK	Unlike DREAD and STRIDE, which focus more on potential risks and vulnerabilities, ATT&CK provides a practical and hands-on approach by mapping adversary tactics. • Assess the effectiveness of existing controls against known attack techniques used by threat actors.
DREAD	DREAD offers a more numerical and calculated approach to threat analysis than STRIDE or MITRE ATT&CK, making it excellent for clearly prioritising threats. • Qualitatively assess the potential risks associated with specific threats. • Prioritise risk mitigation based on the collective score produced by each DREAD component.
STRIDE	While other frameworks like MITRE ATT&CK focus on real-world adversary tactics, STRIDE shines in its structure and methodology, allowing for a systematic review of threats specific to software systems. • Analyse and categorise threats in software systems. • Identify potential vulnerabilities in system components based on the six STRIDE threat categories. • Implement appropriate security controls to mitigate specific threat types.
PASTA	Excellent for aligning threat modelling with business objectives. Unlike other frameworks, PASTA integrates business context, making it a more holistic and adaptable choice for organisations. • Conduct risk-centric threat modelling exercises aligned with business objectives. • Prioritise threats based on their potential impact and risk level to the organisation. • Build a flexible methodology that can be adapted to different organisational contexts.

In general, all these frameworks significantly aid in reducing risks in organisations by:

- Enhancing threat awareness and identifying vulnerabilities
- Prioritising risk mitigation efforts and optimising security controls
- Continuous improvement and adaptation to evolving threats

All four frameworks have their unique strengths and applications in threat modelling. Leveraging these frameworks in real-world scenarios can significantly enhance an organisation's ability to identify and mitigate risks, thereby reducing the overall risk landscape and improving resilience against potential threats.

Now that you have completed this room, you may proceed to Atomic Red Team and CALDERA (coming soon!) rooms to practice emulating threats!

Tryhackme Walkthrough | Tryhackme Writeup

Follow

Written by Daniel Schwarzentraub

116 Followers · 4 Following

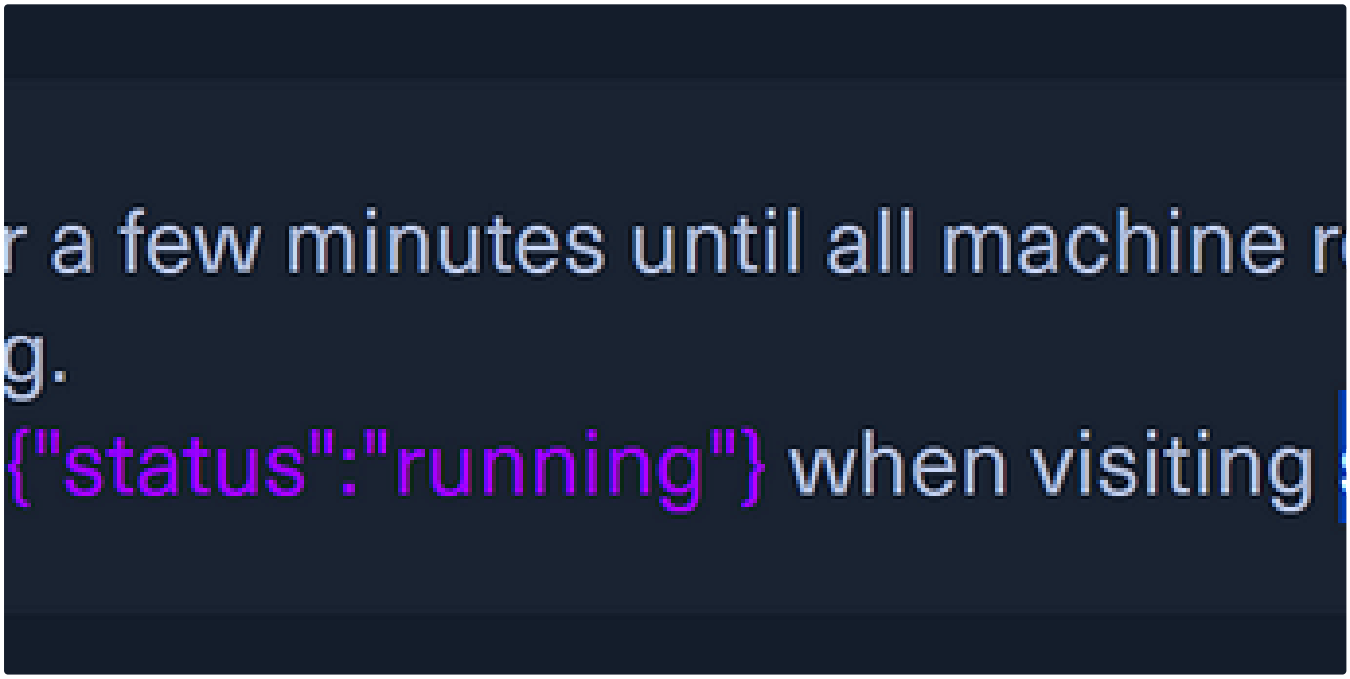
PNW_Hacker

No responses yet

What are your thoughts?

Respond

More from Daniel Schwarzentraub

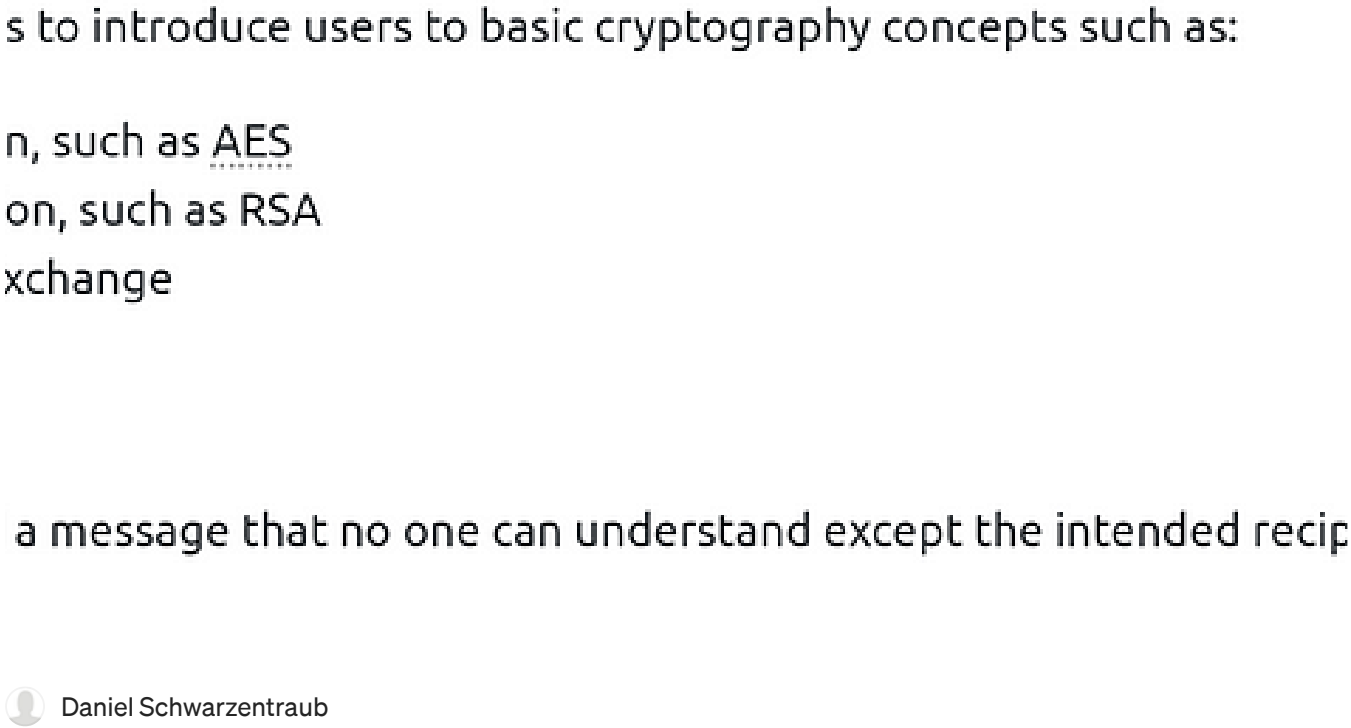


Daniel Schwarzentraub

HTB—Tier 1 Starting Point: Three

HTB—Tier 1 Starting Point: Three

Jul 20, 2023 4 2

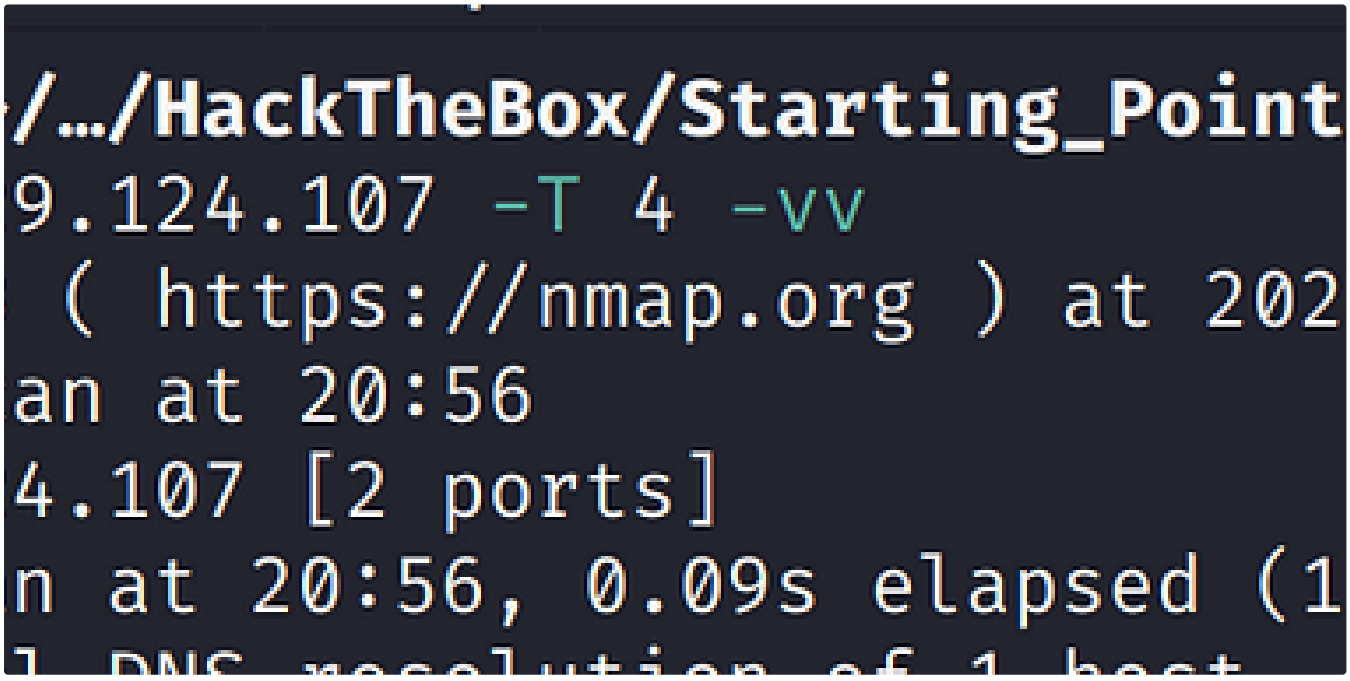


Daniel Schwarzentraub

Tryhackme: Introduction to Cryptography

Tryhackme: Introduction to Cryptography

Sep 26, 2023 2



Daniel Schwarzentraub

HTB—Tier 2 Starting Point: Archetype

HTB—Tier 2 Starting Point: Archetype

Jul 21, 2023

erative that we understand and can protect against common attacks.

mon techniques used by attackers to target people online. It will also teach some of the best wa

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

See all from Daniel Schwarzentraub

Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

Sep 7, 2024 10

Lists

Staff picks

796 stories · 1560 saves

Stories to Help You Level-Up at Work

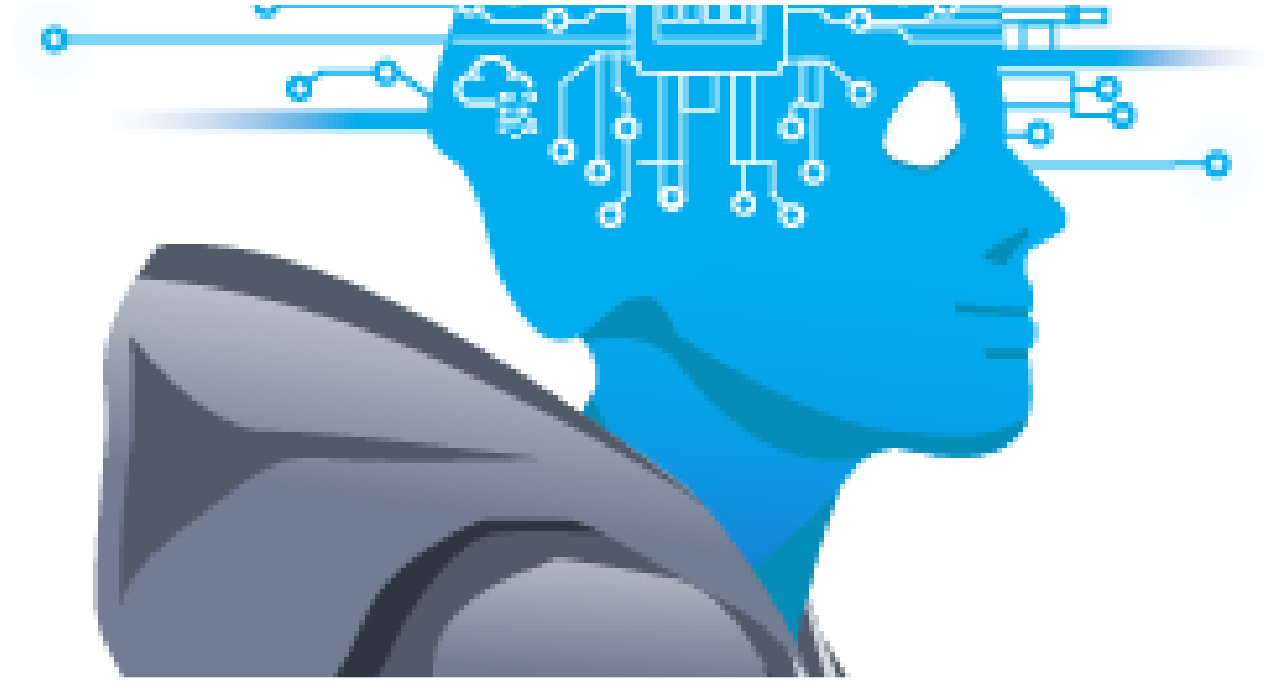
19 stories · 912 saves

Self-Improvement 101

20 stories · 3196 saves

Productivity 101

20 stories · 2707 saves

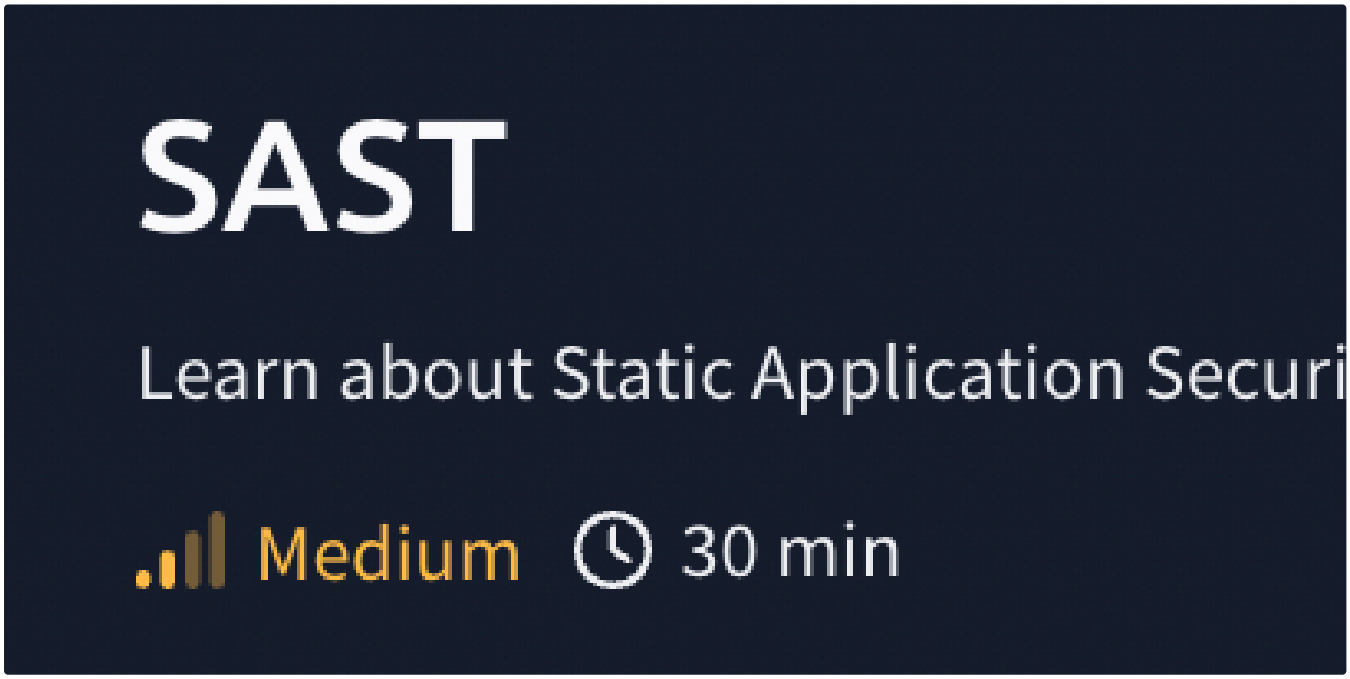


Haircutfish

TryHackMe Room—Threat Intelligence for SOC

This is a free room on TryHackMe. It was created by TryHackMe and ar33zy. Here it the link to said room, TryHackMe Room—Threat...

Jul 19, 2024 95



In OSINT Team by Angie

SAST TryHackMe Writeup | THM Walkthrough

Hello everyone! For today, I will do a TryHackMe walkthrough of the SAST room. I will note that this is a paid room. The SAST room is from...

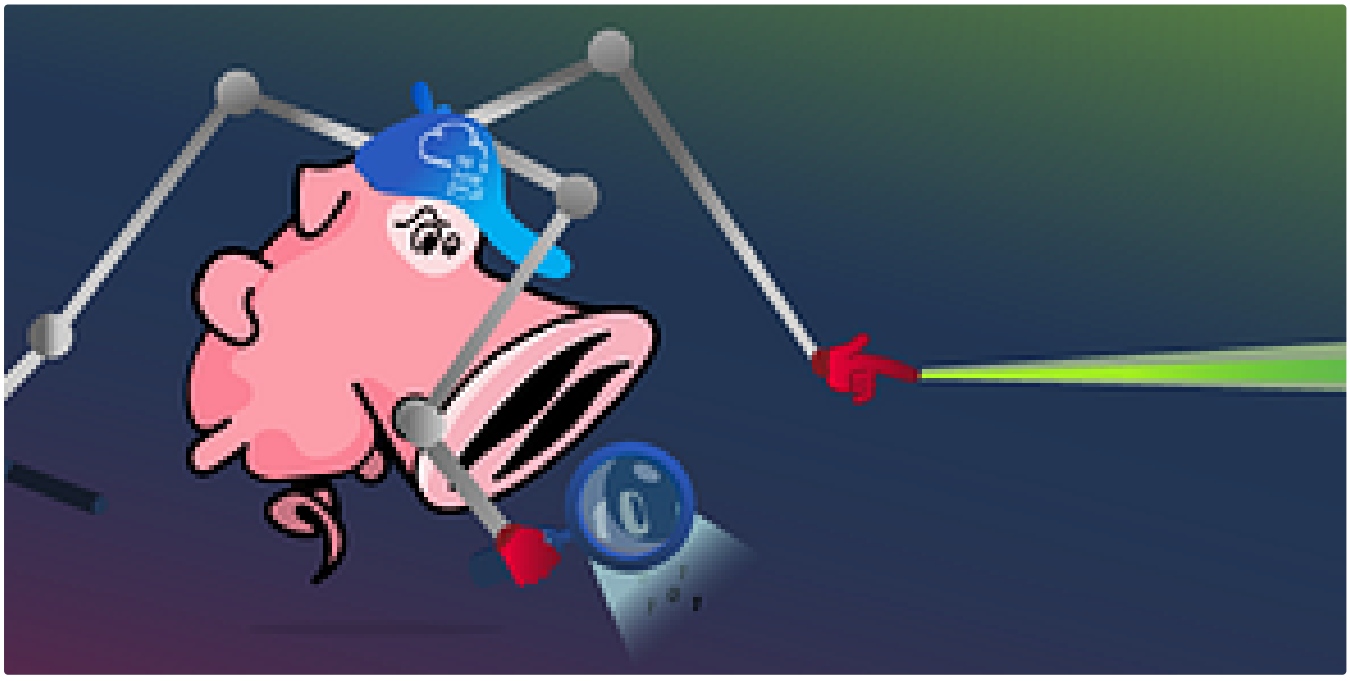
Aug 23, 2024 131

In T3CH by Axoloth

TryHackMe | Vulnerability Scanner Overview | WriteUp

Learn about vulnerability scanners and how they work in a practical scenario

Nov 23, 2024 50



In T3CH by Axoloth

TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

Nov 9, 2024 100