STRIDE threat modeling

## Summary

This lab uses the OWASP’s ThreatDargon to model threats based on Microsoft’s STRIDE framework.

## Tools/Resources

Parrot, Docker, ThreatDragon

## Walkthrough

1. The configuration of docker and running of the ThreatDragon container were covered by the previous lab.
2. Pull and run ThreatDragon

docker run -d -p 8080:3000 -v $(pwd)/.env:/app/.env owasp/threat-dragon:stable

1. In a browser visit the locally hosted ThreatDragon

<http://localhost:8080/>

1. Login, Explore existing Threat Model, Version2 Demo Model, click around to review elementsA screenshot of a computer

   Description automatically generated
2. Red elements are in scope.
   1. Select the “Web Application” element.
   2. Check in scope
   3. For each STRIDE threat type create one new threat.
3. Save your threat model “<your-email-id>.json”

## Submission

Upload to Canvas your saved threat model “<your-email-id>.json”

## Additional Thoughts

How often do multiple elements share the same threat?

How do the STRIDE threats types map to the OWASP top 10 risks?