CS437/SEC537

This lab consist of 3 parts:

- Microsoft Threat Modeling Tool lab
- Phishing Creation Lab
- Phishing Email tracker

Part 1: Microsoft Threat Modeling Tool

This lab is designed to familiarise with a tool called Microsoft Threat Modeling Tool. Threat modeling is a core element of the Microsoft Security Development Lifecycle (SDL). It's an engineering technique you can use to help you identify

- threats,
- attacks,
- vulnerabilities,
- and countermeasures that could affect your application.

You can use threat modeling to shape your application's design, meet your company's security objectives, and reduce risk. *A person using this tool does not need to be a security professional.*

According to Microsoft, there are five major threat modeling steps:

- Defining security requirements.
- Creating an application diagram.
- Identifying threats.
- Mitigating threats.
- Validating that threats have been mitigated.

Threat modeling should be part of your routine development lifecycle, enabling you to progressively refine your threat model and further reduce risk.

The tool enables anyone to:

- Communicate about the security design of their systems
- Analyze those designs for potential security issues using a proven methodology
- Suggest and manage mitigations for security issues

Here are some tooling capabilities and innovations, just to name a few:

- Guidance and feedback in drawing a model
- ***STRIDE per Element: Guided analysis of threats and mitigations***
- Reporting: Security activities and testing in the verification phase

NOTE: THIS MATERIAL IS A PROPERTY OF SABANCI UNIVERSITY. ANY UNAUTHORISED USE OR DISTRIBUTION IS STRICTLY PROHIBITED.

- Unique Methodology: Enables users to better visualize and understand threats
- Designed for Developers and Centered on Software: many approaches are centered on assets or attackers. We are centered on software. We build on activities that all software developers and architects are familiar with -- such as drawing pictures for their software architecture
- Focused on Design Analysis: The term "threat modeling" can refer to either a requirement or a design analysis technique. Sometimes, it refers to a complex blend of the two. The Microsoft SDL approach to threat modeling is a focused design analysis technique. In order to download go to :

https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

Download the Threat Modeling Tool. Only works in Windows OS.
After that if your browser asks “Do you want to keep the TMT7 application anyway”, just click on “Keep” and download the application manifest. By using an application manifest, install the software.

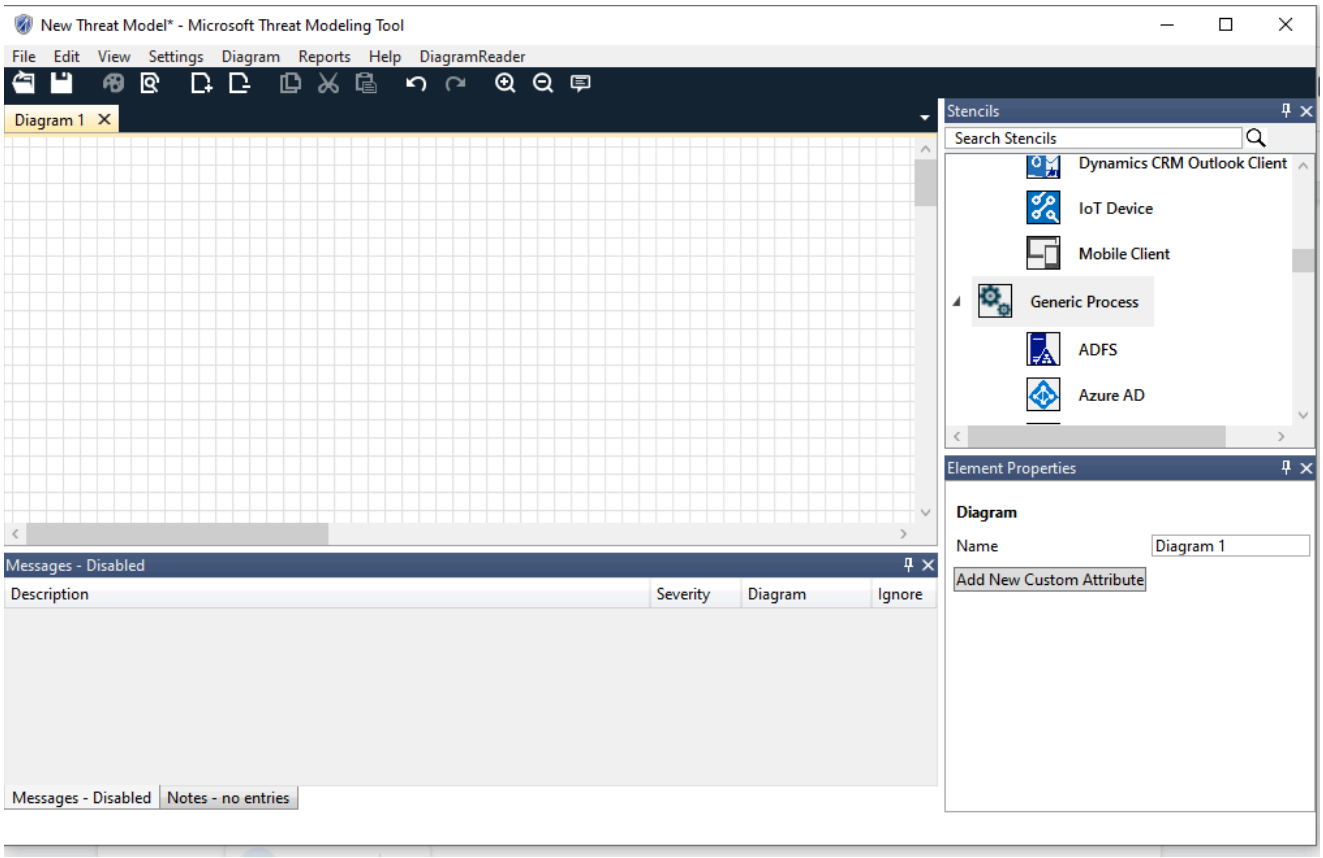


Figure 1 : Design View

Then you will see a screen like the one above (see fig 1). This page is Design View. This is a default page of the tool.
This tool provides an access to Stencils
We will draw our model by using the components offered in the Stencils panel. Below you can see Analysis View (See fig 2). You can go to this page by going to the “View” tab and then click on “Analysis View”. You can turn back to “Design View” by going to the “View” tab.

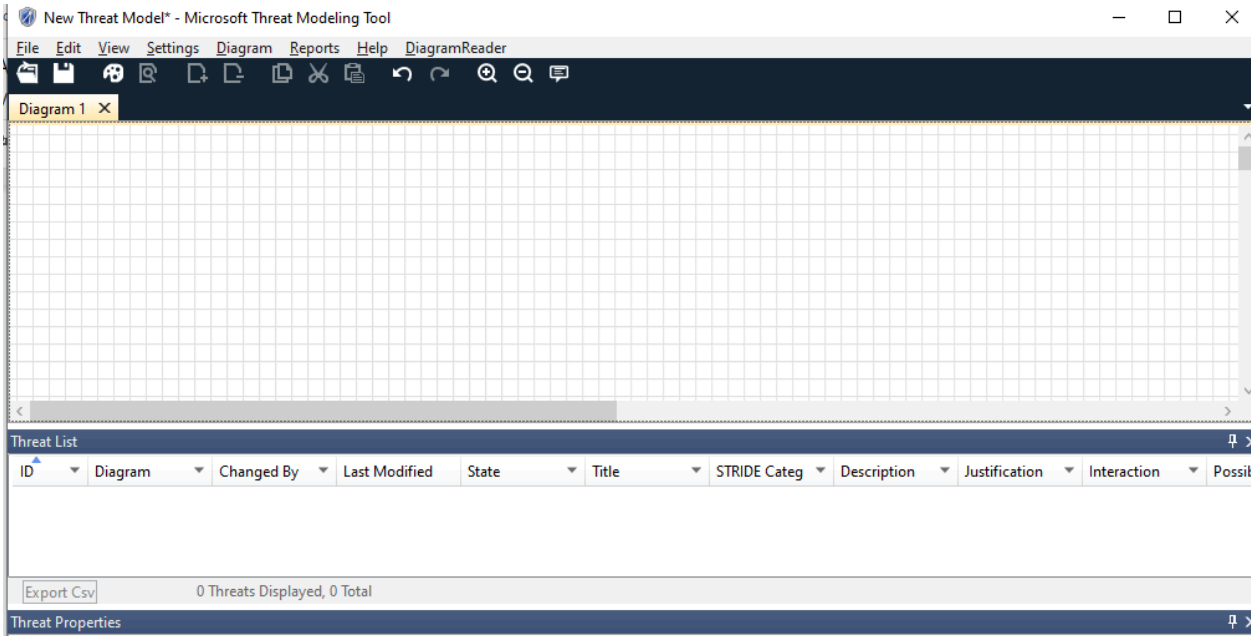
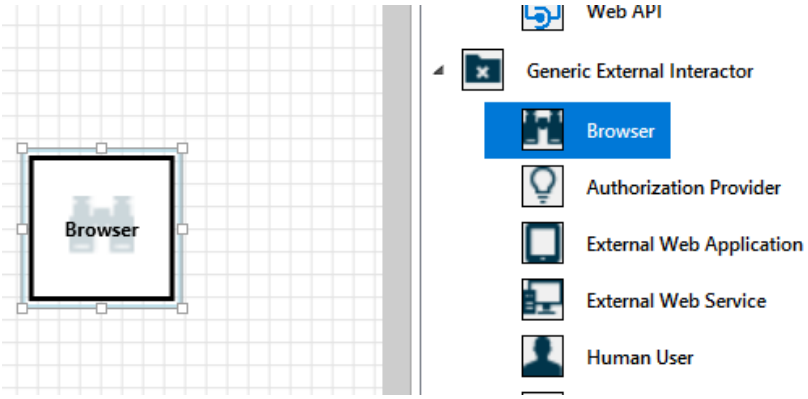


Figure 2: Analysis View

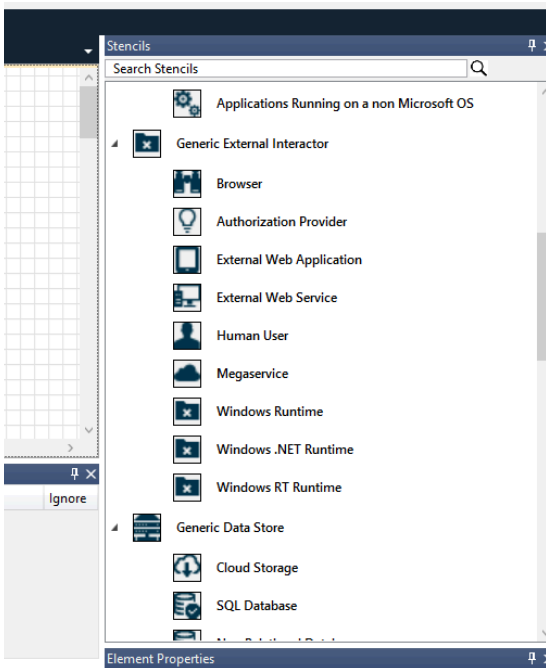
Canvas

The canvas is the space where you drag and drop elements. Drag and drop is the quickest and most efficient way to build models. You can also right-click and select items from the menu to add generic versions of elements, as shown:



NOTE: THIS MATERIAL IS A PROPERTY OF SABANCI UNIVERSITY. ANY UNAUTHORISED USE OR DISTRIBUTION IS STRICTLY PROHIBITED.

You can drag and drop stencil on the canvas.



Stencils

Based on the template you select, you can find all the stencils available to use. If you can't find the right elements, use another template. Or you can modify a template to fit your needs. Generally, you can find a combination of categories like these:

Process: Applications, browser plug-ins, threads, virtual machines
External interactor: Authentication providers, browsers, users, web applications
Data store: Cache, storage, configuration files, databases, registry
Data flow: Binary, ALPC, HTTP, HTTPS/TLS/SSL, IOCTL, IPSec, named pipe, RPC/DCOM, SMB, UDP
Trust line/Border boundary

Element properties (See fig 3)
Element properties vary by the elements you select. Apart from trust boundaries, all other elements contain three general selections:

Name: Useful for naming your processes, stores, interactors, and flows so that they're easily recognized.
Out of scope: If selected, the element is taken out of the threat-generation matrix (not recommended).
Reason for out of scope: Justification field to let users know why out of scope was selected.

NOTE: THIS MATERIAL IS A PROPERTY OF SABANCI UNIVERSITY. ANY UNAUTHORISED USE OR DISTRIBUTION IS STRICTLY PROHIBITED.

Properties are changed under each element category. Select each element to inspect the available options. Or you can open the template to learn more. Let's review the features.

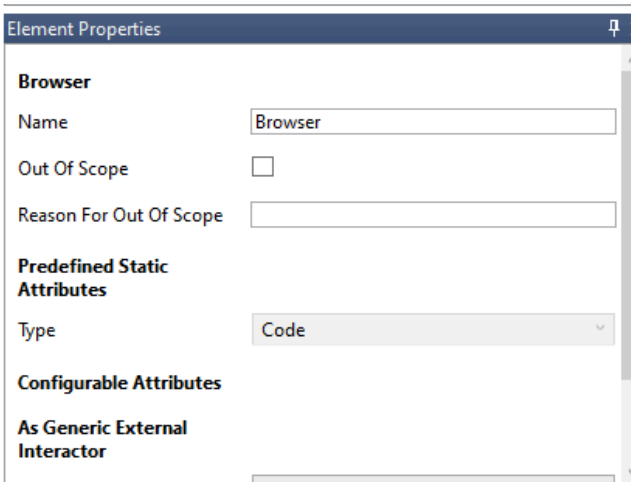
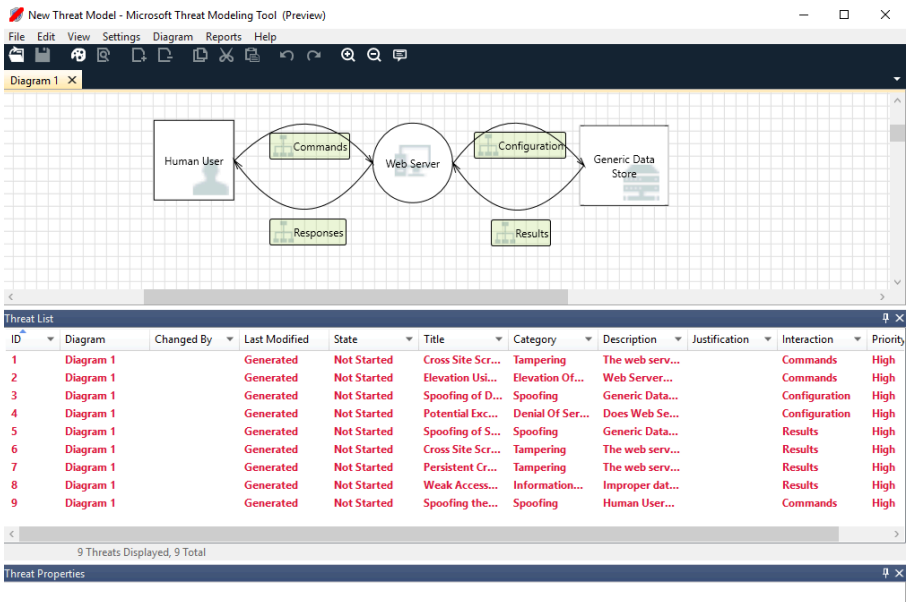


Figure 3 : Element properties

Analysis view

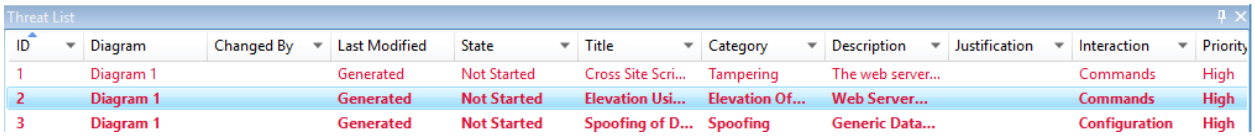
After you build your diagram, select the Analysis symbol (the magnifying glass) on the shortcuts toolbar to switch to the Analysis view.



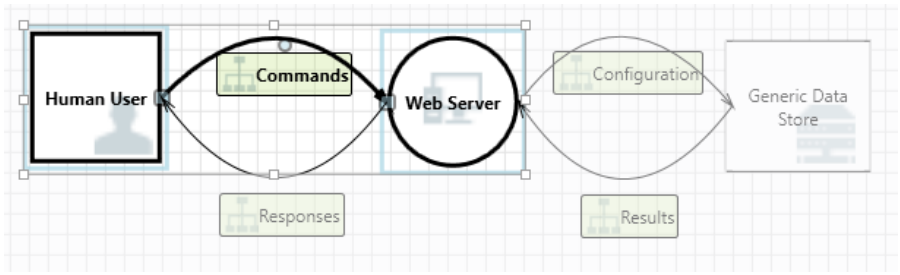
Generated threat selection

When you select a threat, you can use three distinct functions:

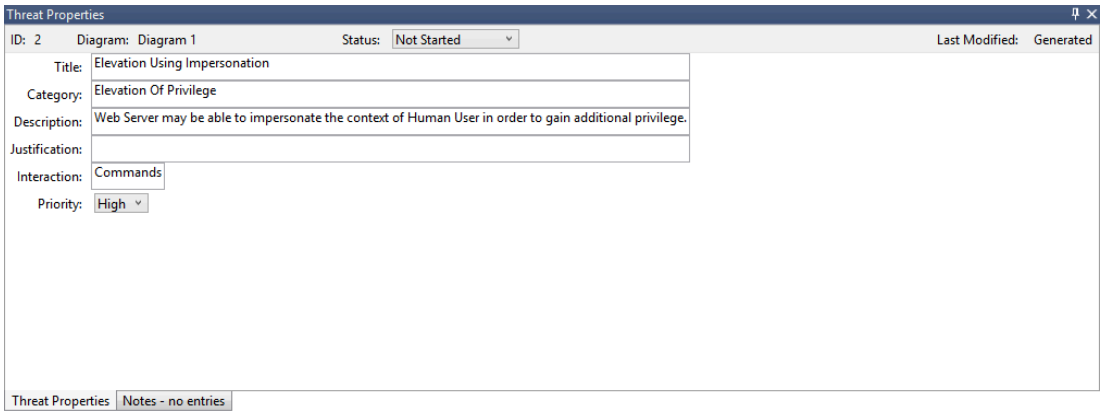
Read indicator : The threat is marked as read, which helps you keep track of the items you reviewed.



Interaction focus: Interaction in the diagram that belongs to a threat is highlighted.

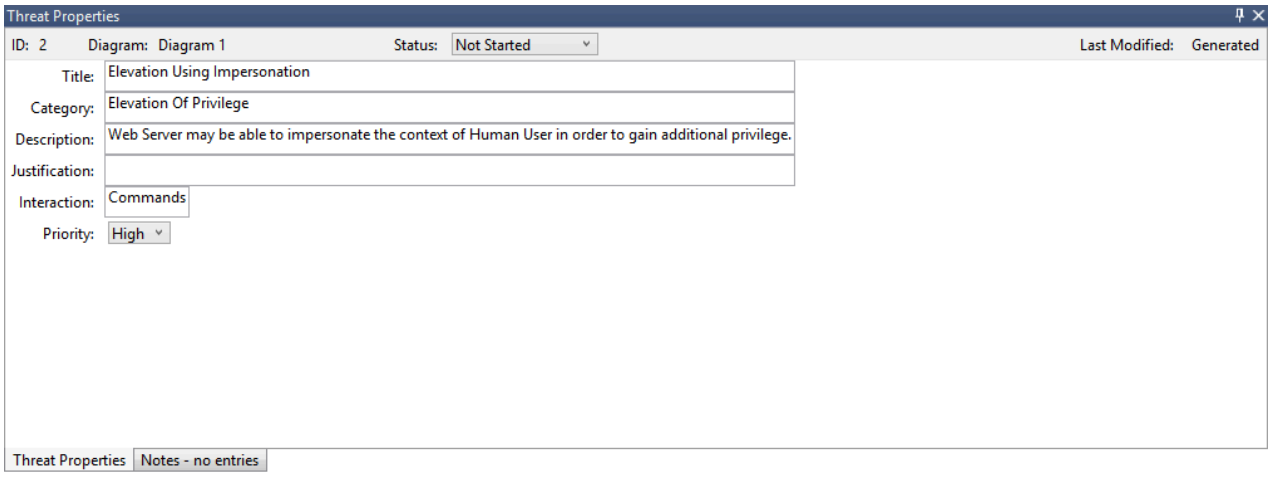


Threat properties: Additional information about the threat appears in the Threat Properties window.



Threat properties editable fields

As seen in the preceding image, you can change the information generated by the tool. You can also add information to certain fields, such as justification. These fields are generated by the template. If you need more information for each threat, you can make modifications.



Priority change

You can change the priority level of each generated threat. Different colors make it easy to identify high-, medium-, and low-priority threats.

Threat List

ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
1	Diagram 1	REDMOND\ro...	8/16/2017 3:13:...	Not Started	Cross Site Scri...	Tampering	The web server...		Commands	Mediu
2	Diagram 1	REDMOND\ro...	8/16/2017 3:13:...	Not Started	Elevation Usin...	Elevation Of Pr...	Web Server ma...		Commands	Low
3	Diagram 1	REDMOND\ro...	8/16/2017 3:13:...	Not Started	Spoofing of De...	Spoofing	Generic Data S...		Configuration	Mediu
4	Diagram 1	REDMOND\ro...	8/16/2017 3:13:...	Not Started	Potential Exces...	Denial Of Servi...	Does Web Serv...		Configuration	Mediu
5	Diagram 1		Generated	Not Started	Spoofing of So...	Spoofing	Generic Data S...		Results	High
6	Diagram 1		Generated	Not Started	Cross Site Scri...	Tampering	The web server...		Results	High
7	Diagram 1	REDMOND\ro...	8/16/2017 3:13:...	Not Started	Persistent Cros...	Tampering	The web server...		Results	Low
8	Diagram 1		Generated	Not Started	Weak Access...	Information...	Improper dat...		Results	High
9	Diagram 1		Generated	Not Started	Spoofing the...	Spoofing	Human User...		Commands	High

Reports

After you finish changing priorities and updating the status of each generated threat, you can save the file and/or print out a report. Go to Report > Create Full Report. Name the report, and you should see something similar to the following image:

Threat Modeling Report

Created on 7/31/2017 12:35:42 PM
Threat Model Name:
Owner:
Reviewer:
Contributors:
Description:
Assumptions:
External Dependencies:

Threat Model Summary:

Not Started	9
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	9
Total Migrated	0

Diagram: Diagram 1

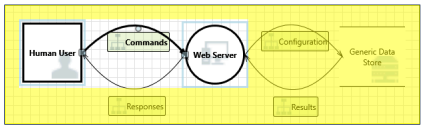
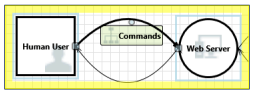


Diagram 1 Diagram Summary:

Not Started	9
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	9
Total Migrated	0

Interaction: Commands



1. Spoofing the Human User External Entity [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	Human User may be spoofed by an attacker and this may lead to unauthorized access to Web Server. Consider using a standard authentication mechanism to identify the external entity.
Justification:	<no mitigation provided>
Possible Mitigation(s):	
SDL Phase:	Design

2. Cross Site Scripting [State: Not Started] [Priority: High]

Category:	Tampering
Description:	The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification:	<no mitigation provided>
Possible Mitigation(s):	
SDL Phase:	Design

Threat Modelling Tool - Pros and Cons

Pros

Free
Easy to learn
Can be used by anyone
Automatically identifies threats
Automatically Generates Reports
Customizable threat templates

Cons

Platform dependent
Single user experience
Limited visual configuration
Limited prioritization capabilities
Security controls not mapped
Limited documentation

Diagram layers

• Context Diagram
– Very high-level; entire component / product / system
• Level 1 Diagram
– High level; single feature / scenario
• Level 2 Diagram
– Low level; detailed sub-components of features
• Level 3 Diagram
– More detailed
– Rare to need more layers, except in huge projects or when you're drawing more trust boundaries

Lab Questions

Scenario 1: Threat Modeling at OrcunCorp for Document sharing tool.

We will start out with identifying security objectives:

What is the application used for ?
Simple application that allows employees to securely share documents such as reports and other sensitive files with third parties.
Who uses the application?
All users at Orcun Corp will have access to use this particular system.
Are there compliance requirements?

Sometimes compliance needs will drive additional security requirements.
Find out what these requirements are!
In this case, orcun corp has agreed that this document sharing tool will not be used for transmission or store of any regulated data.
Is there data that needs to be protected?
Regulated data is not to be shared using this tool, other data such as customer listing, price information, and supplier information should definitely be kept secure.
Does the application interact with our internal servers?
Does not directly interact with their internal server. This will be a completely segmented system and application.
Are there any third parties involved?
We will use our own infrastructure

Try to get better at asking questions. You will be asking better questions as you get more experienced with the process.

Application review
Do your homework first, understand what is needed. Then you can get more out of the TMT software.
Consider following:
Users
What type of users and what kind of data will be used by them?
Use cases
Describe common request that a user would have about the application
Also what the users are trying to do
Technology
Underlying technology stack
Specific threats that affect the particular technology stack that you are working with at the moment.

OrcunCorp Document Sharing Tool Application review

Internal users will have access to sensitive files. We don't know what external users will do.
Users will securely share electronic documents with external clients.

Microsoft technology stack Microsoft web servers and databases .NET framework with the primary programming language being C#

Having this information in advance helps us identify vulnerabilities and limitations.

Questions

0. Take a screenshot of your full msinfo. For this question, only provide your *full* msinfo.In Window 10 :Type “system information“ into the initial search box, and then select the result. Without this information do not submit!

1.1 Draw a simple data flow diagram (DFD) for scenarios using Design View.

Things to do:

External users (Use Human User Stencils) **(Change its name with yours)**

Make sure to check Authenticates itself Yes(Important)

File sharing application (Use Web server Stencils)

Storage (Use SQL Database Stencils)

And then draw bi-directional connection between External users and File sharing application

After that draw bi-directional connection between File sharing application and storage.

Once this is done. Take a screenshot of the design view. Make sure to include msinfo. And system time.

1.2 Save your DFD as a TM7 file. Name your file as yourname_context-diagram.tm7. Include this in your submission folder.

1.3 Let’s take a look at the analysis page. Please write down how many unique threats we have ?

Number: ?

Screenshot!

1.4 Please give a descriptive analysis of the attack categories.

How many for Spoofing?

How many for Tampering?

How many for Repudiation?

….

1.5 Please take a look at the threat properties description section and suggest one security mechanism that could help fix any Authentication problems. Explain why you pick this security mechanism.

1.6 For this question,let's improve this model. Create another diagram. Copy the same model. And start adding one generic trust line boundary between Human and Web server and name it “Internet”. Add another one between Webserver and SQL database and name it “Secured”.

Now do you see more threats? Screenshot needed. Explain how many more?

NOTE: THIS MATERIAL IS A PROPERTY OF SABANCI UNIVERSITY. ANY UNAUTHORISED USE OR DISTRIBUTION IS STRICTLY PROHIBITED.

1.7 Find out what needs to be added to the *Web server* in order to get rid of Cross site scripting (XSS)? Explain and screenshots needed! Explain the screenshot as well. Basically why did you add this screenshot?

1.8 Once you find a way to mitigate XSS, Generate a full report.

Your lab submission must include: PDF document containing explanations and screenshots. (1st file)
Output from question 1.2(2nd file)
Full report from 1.7 (3rd file) (Report details must be completed - name must be your name and rest must be according to the homework details -no details no points)
And the final DFD AS TM7 file.
And Save your final version of DFD as a TM7 file. Name your file as yourname_final-diagram.tm7.(4th file)

The 4th file is the final question.

Part 2: Phishing Creation Lab

The purpose of this homework is to help students understand how phishing attacks are designed, structured, and contextualized. By creating realistic phishing scenarios, students will learn to analyze attacker psychology, social-engineering tactics, linguistic markers, and operational security elements commonly found in phishing campaigns.

Part 2.1:Create 5 Phishing Emails (5 Distinct Concepts)
Each student must design **five different** phishing emails, each based on one unique phishing concept listed below.
Each email must have convincing :

- **HTML body,**
- **images,**
- **psychological techniques (embedded in text or images or html)**
- **Logo of companies (Not exact logo but similar one!)**
- **text, Button or other form of links that could allow attackers to redirect victims into malicious websites.**
- **You should learn how and where to host these images and other components.**
- **We are looking for creativity and new possible techniques which can be used by attackers.**
- **Each email must be sent to : cs437.2025@gmail.com**
    - **Email send here first contain your name in the title and then real title**
        - **Example: Fariz İbadov - Important update**

NOTE: THIS MATERIAL IS A PROPERTY OF SABANCI UNIVERSITY. ANY UNAUTHORISED USE OR DISTRIBUTION IS STRICTLY PROHIBITED.

    - **Fariz İbadov -> Your name goes there**
    - **- This is a separator**
    - **Important update -> Find a creative title about your email**
  - **They would be able to get through the email mailbox**
  - **You can try this with your own mailbox**
  - **Create a temporary mailbox just to**

Phishing Concepts to Use:

Part 2.1.1: Credential Harvesting – Fake Login Alert
Create a phishing email pretending to be from: popularly used platforms.
Goal: Trick users into entering their credentials.
We are looking for HTML content, and in the report you should mention what kind of psychological techniques are used. You should be able to justify your psychological techniques with scientific articles.
Additionally add a screenshot into the report that shows how it looks.
Moreover email to cs437.2025@gmail.com. If it fails to get through (caught by spam filter) then your marks will be reduced.

Part 2.1.2:Spear-Phishing – Executive Impersonation

Create a personalized message pretending to be from a head of an organization or department

It should request urgent action, such as:

- Sending a document
- Approving a financial request
- Sharing confidential data via link!

Goal: Social-engineer a specific target using authority pressure.

We are looking for HTML content, and in the report you should mention what kind of psychological techniques are used. You should be able to justify your psychological techniques with scientific articles.
Additionally add a screenshot into the report that shows how it looks.
Moreover email to cs437.2025@gmail.com. If it fails to get through (caught by spam filter) then your marks will be reduced.

Part 2.1.3,Part 2.1.4,Part 2.1.5: Link click

Create 3 more emails which would force/ convince/ trick users to click on links (in buttons or emails) and redirect them to random websites.

NOTE: THIS MATERIAL IS A PROPERTY OF SABANCI UNIVERSITY. ANY UNAUTHORISED USE OR DISTRIBUTION IS STRICTLY PROHIBITED.

We are looking for HTML content, and in the report you should mention what kind of psychological techniques are used. You should be able to justify your psychological techniques with scientific articles.
Additionally add a screenshot into the report that shows how it looks.
Moreover email to cs437.2025@gmail.com. If it fails to get through (caught by spam filter) then your marks will be reduced.

Part 3 : Technical Component: Create a Tracking Mechanism Used by Phishers

Modern phishers rarely send emails without tracking. In this part you are asked to create a python based system which tracks the emails.
You should be able to answer the following question:
Was the email opened?

Email providers like Gmail, Outlook, Office365, and some corporate gateways automatically click links to scan them, this creates false positives for phishers.

Your system must detect the difference.

Students must implement logic that labels an event as:

- Provider Scan / Security Bot
- Real Human Click

Indicators of automated scanners

- User-Agent strings such as
  “GoogleImageProxy”, “Microsoft Defender SmartScreen”, “Cisco IronPort”, “Barracuda”, “Proofpoint URL Defense”
- Clicking the link immediately after email delivery (0–2 sec)
- Clicking from data center IP ranges
- Accessing URLs multiple times in quick sequence
- HEAD requests instead of GET requests
- No JavaScript execution (bots do not execute JS consistently)

NOTE: THIS MATERIAL IS A PROPERTY OF SABANCI UNIVERSITY. ANY UNAUTHORISED USE OR DISTRIBUTION IS STRICTLY PROHIBITED.

Indicators of real human interaction

- Normal browser UAs: Chrome, Safari, Edge, Firefox
- Time delay: human interactions typically > 5 seconds after email viewing
- Typical residential or mobile IP ranges
- Mouse movement signals (if JS added)
- JS execution returning real browser fingerprint

You are asked to submit:

- **the code & requirements**
- **Video which explain how code works**
- **Video showing how tracking system works**
    - **Also including real tests with gmail and outlook**
- **Explanation of the code and requirements should be also mentioned in the report!**

NOTE: THIS MATERIAL IS A PROPERTY OF SABANCI UNIVERSITY. ANY UNAUTHORISED USE OR DISTRIBUTION IS STRICTLY PROHIBITED.