SAD LAB EXPERIMENT - 3

AIM:- Understanding the concept of threat modeling with an exercise using microsoft threat modeling tool .

THEORY:-

Threat modeling is a method of optimizing network security by locating vulnerabilities, identifying objectives, and developing countermeasures to either prevent or mitigate the effects of cyber-attacks against the system.While security teams can conduct threat modeling at any point during development, doing it at the start of the project is best practice. This way, threats can be identified sooner and dealt with before they become an issue. Microsoft Threat Modelling Tool applies STRIDE threat classification scheme to the identified threats.

Steps :-

1. **Creating New Threat Model**: A new model for the system is created by drawing the diagram. We will be discussing this scenario in detail. By default template for the new model is SDL TM Knowledge Base(Core) (4.1.0.9)
2. **Modifying an Existing Threat Model:** Open existing model and analyze threats against your system. One can open the existing model for making changes either by selecting the desired model from the list of recently opened models on the initial screen or by navigating to open option in the file menu.
3. **Create New Template:** Define stencils, threat types and custom threat properties for your threat model from scratch.
4. **Modifying Existing Template:** Open existing template to make modifications to better suit your specific threat analysis

STRIDE threat modeling: STRIDE is a threat model, created by Microsoft engineers, which is meant to guide the discovery of threats in a system. It is used along with a model of the target system. This makes it most effective for evaluating individual systems.

STRIDE is an acronym for the types of threats it covers, which are:

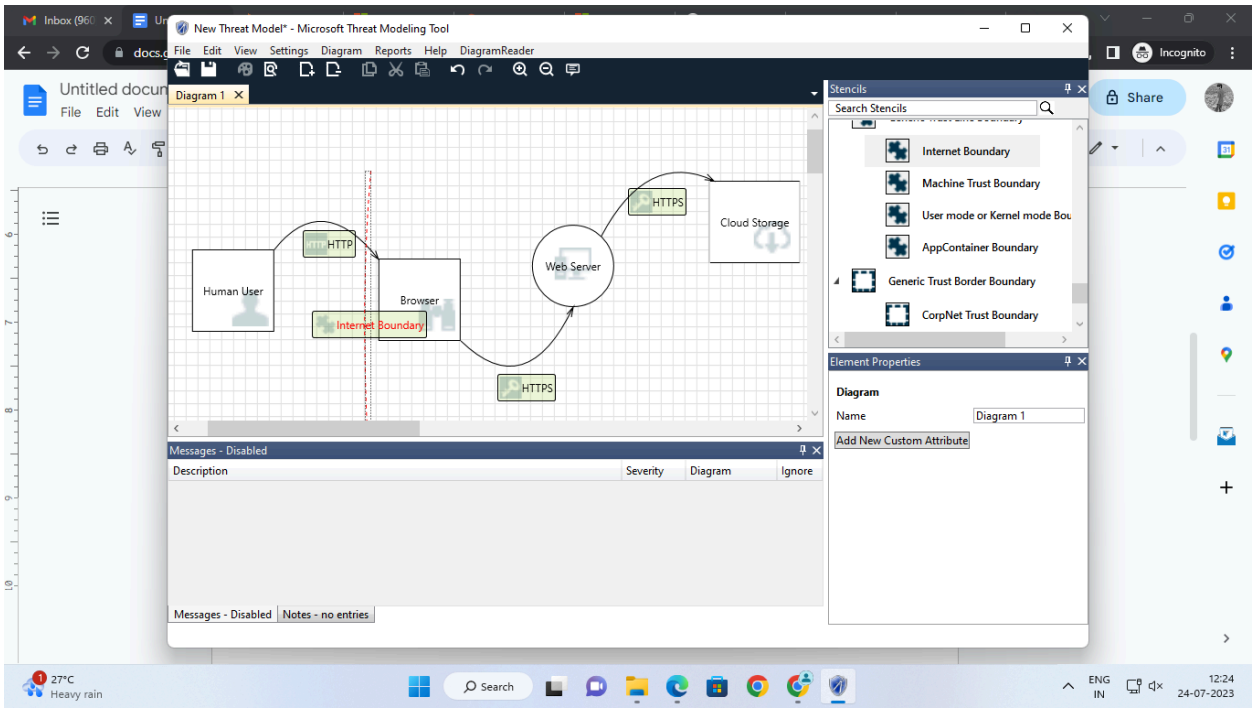
- **Spoofing** — a user or program pretends to be another
- **Tampering** — attackers modify components or code
- **Repudiation** — threat events are not logged or monitored
- **Information disclosure** — data is leaked or exposed
- **Denial of service (DoS)** — services or components are overloaded with traffic to prevent legitimate use
- **Elevation of Privilege** — attackers grant themselves additional privileges to gain greater control over a system

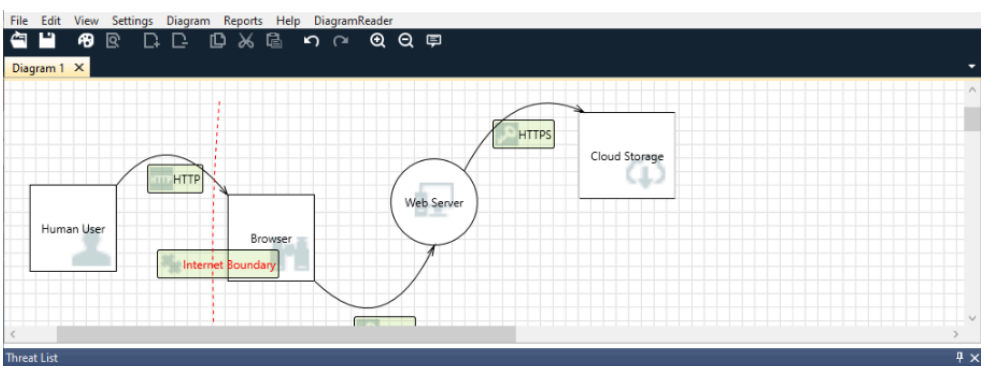
Microsoft threat modeling tools :-
The Threat Modeling Tool is a core element of the Microsoft Security Development Lifecycle (SDL). It allows software architects to identify and mitigate potential security issues early, when they are relatively easy and cost-effective to resolve. As a result, it greatly reduces the total cost of development. Also, we designed the tool with non-security experts in mind, making threat modeling easier for all developers by providing clear guidance on creating and analyzing threat models.

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

Automation: 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
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





Threat Modeling Report

Created on 24-07-2023 12:19:38

Threat Model Name:

Threat Model Summary:

Not Started	7
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	7
Total Migrated	0

Diagram: Diagram 1

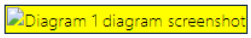
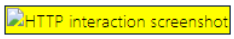


Diagram 1 Diagram Summary:

Not Started	7
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	7
Total Migrated	0

Interaction: HTTP



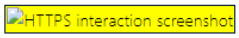
1. External Entity Browser Potentially Denies Receiving Data [State: Not Started] [Priority: High]

Category: Repudiation
Description: Browser claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the re
Justification: <no mitigation provided>

2. Data Flow HTTP Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: <no mitigation provided>

Interaction: HTTPS



3. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Web Server may be able to impersonate the context of Browser in order to gain additional privilege.
Justification: <no mitigation provided>

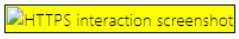
4. Cross Site Scripting [State: Not Started] [Priority: High]

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>

5. Spoofing the Browser External Entity [State: Not Started] [Priority: High]

Category: Spoofing
Description: Browser 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>

Interaction: HTTPS



6. Spoofing of Destination Data Store Cloud Storage [State: Not Started] [Priority: High]

6. Spoofing of Destination Data Store Cloud Storage [State: Not Started] [Priority: High]

Category: Spoofing
Description: Cloud Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Cloud Storage. Consider using a standard authentication mechanism to identif
destination data store.
Justification: <no mitigation provided>

7. Potential Excessive Resource Consumption for Web Server or Cloud Storage [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: Does Web Server or Cloud Storage take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS
job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification: <no mitigation provided>

STRIDE :-

Spoofing :-

Identify spoofing occurs when the hacker pretends to be another person, assuming the identity and information in that identity to commit fraud. A very common example of this threat is when an email is sent from a false email address, appearing to be someone else (also called a phishing attack).
Typically, these emails request sensitive data. A vulnerable or unaware recipient provides the requested data and the hacker is then easily able to assume the new identity.

Tampering :-

Data tampering occurs when data or information is changed without authorization. Ways that a bad actor can execute tampering could be through changing a configuration file to gain system control, inserting a malicious file, or deleting/modifying a log file.

Change monitoring, also known as file integrity monitoring (FIM) is essential to integrate into your business to identify if and when data tampering occurs. This process critically examines files with a baseline of what a ‘good’ file looks like. Proper logging and storage is critical to support file monitoring. Read the Security Playbook here to understand the risks of insufficient or excessive logging and auditing.

Repudiation :-

Repudiation threats happen when a bad actor performs an illegal or malicious operation in a system and then denies their involvement with the attack. In these attacks, the system lacks the ability to actually trace the malicious activity to identify a hacker.

Repudiation attacks are relatively easy to execute on e-mail systems, as very few systems check outbound mail for validity. Most of these attacks begin as access attacks.

Information Disclosure:-

Information disclosure is also known as information leakage. It happens when an application or website unintentionally reveals data to unauthorized users. This type of threat can affect the process, data flow and data storage in an application. Some examples of information disclosure include unintentional access to source code files via temporary backups, unnecessary exposure of sensitive information such as credit card numbers, and revealing database information in error messages.

These issues are common, and can arise from internal content that is shared publicly, insecure application configurations, or flawed error responses in the design of the application.

DOS:-

Denial of Service (DoS) attacks restrict an authorized user from accessing resources that they should be able to access. This affects the process, data flow and data storage in an application. DoS attacks are getting bigger and more frequent, with an estimated 12.5 million DDos weapons detected in 2020. In the State of Penetration Testing as a Service report for 2022, it was reported that DoS attacks increased in frequency by 133% last year.

One of the most famous attacks was on Google in 2017. In their statement, Google said, "*The attacker used several networks to spoof 167 Mpps (millions of packets per second) to 180,000 exposed CLDAP, DNS, and SMTP servers, which would then send large responses to us. This demonstrates the volumes a well-resourced attacker can achieve: This was four times larger than the record-breaking 623 Gbps attack from the Mirai botnet a year earlier.*"

Elevation of privilege:-

Through the elevation of privileges, an authorized or unauthorized user in the system can gain access to other information that they are not authorized to see. An example of this attack could be as simple as a missed authorization check, or even elevation through data tampering where the attacker modifies the disk or memory to execute non-authorized commands.

CONCLUSION:- STRIDE threat model, which is a framework used in cybersecurity to identify and categorize potential threats to a system or application. We understood the concept of Threat modeling and used software such as Microsoft Threat modeling tool and also implemented the Concept of STRIDE .