

Practical lab - 13

Drawing a threat model

1. Threat model

Threat modeling is a structured process with these objectives: identify security requirements, pinpoint security threats and potential vulnerabilities, quantify threat and vulnerability criticality, and prioritize remediation methods.

2. Installation and implementation

Step 1: go to chrome and install draw.io and click on open (on) download and install draw.io for your operating system.

Step 2: open draw.io application and create a new blank diagram.

Step 3: and finally start diagramming by using shapes that are available in draw.io to implement threat model as shown in the picture.

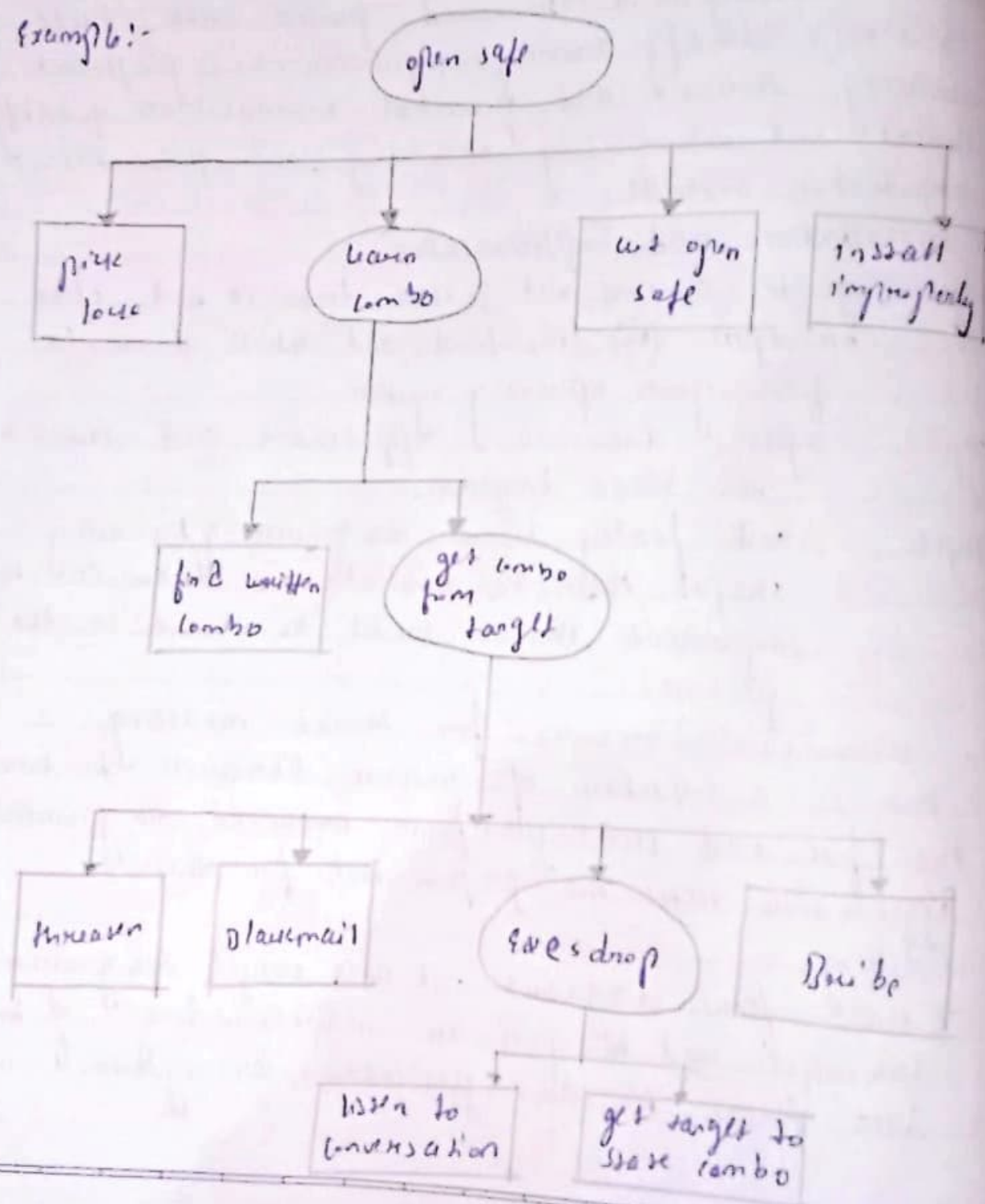
3. Draw.io libraries for threat modeling

This is a collection of custom libraries to turn the free and cross-platform draw.io diagramming application into the perfect tool for threat modelling.

→ Data flow diagrams - it is a simple diagramming technique used to gain an understanding of how data flows in an application (on) system.

Attack Trees - attack trees are another kind of diagramming method that is great for explaining how a threat actor might attain a specific goal.

Example:-



Final lab - 20

using the microsoft threat modeling methodologies evaluate threat model for a given application architecture using microsoft threat modeling tools.

- threat modeling is the process of using hypothetical scenarios, system diagrams, and testing to help secure systems and data.
- There are eight main methodologies security teams can use while threat modeling, here we use STRIDE methodology.
- STRIDE stands for spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege.

→ Installation of threat modeling tool 2016:

step 1:- go to chrome and search for threat modeling tool 2016 (<http://aka.ms/mt2016>) and

step 2:- ensure that .NET framework 4.5 or later is installed on your computer.

step 3:- after installing the threat modeling tool 2016, run the application by following the instructions to complete the installation.

step 4:- double-click on the application to implement the STRIDE methodology.

7 starting the threat modeling process

when you launch the threat modeling tool, you'll notice a few things, as seen in the picture:

Threat model section -

component	Details
feedback, suggestions and issues Button	saves you the mason form for all things SOL
create a model	opens a blank canvas for you to draw your diagram
template for new models	you must select which template to use before creating a model

open a model

opens previously saved threat models

• open from this component - classic way of opening a file using local storage.

3. Building a model

step 1:- go to file and click on new and start implementing STRIDE by using the below tools/components

1. Human user
2. generic external interaction
3. generic data flow
4. generic trust line boundary
5. generic trust Border Boundary
6. generic data store
7. native application.

steps → human user → native application (src/passwd) → generic data flow → generic trust Border Boundary → file system (src/shadow) → generic data frame → finally click on Analysis view

4. Analyzing threats → once ~~the~~^{we} click on the analysis view from the icon menu selection, we can see the list of generated threats the threat modeling tool found based on the default template, which use the SOL approach called STRIDE.

5. save the project

→ click on file ^{menu} and click on save as, finally save the file with the name "STADOB methodology". ~~finally~~
~~click on save button.~~



Practice lab - 21

1. Demonstrate a tool like owasp dependency check.

owasp dependency-check is a software composition analysis utility that detects publicly disclosed vulnerabilities in application dependencies.

Dependency-check is a software composition analysis (SCA) tool that attempts to detect publicly disclosed vulnerabilities contained within a project's dependencies.

1. Installation of owasp dependency check using github.

step 1: go to  login into github  search for <https://github.com/jeremylog/dependencycheck>.

step 2: there we can see the latest version of dependency check install by double click on it..

step 3: after completing the installation unzip the file.

2. to unzip the file

Step 1:- go to ubuntu terminal and type the below commands

```
# cd /opt
```

```
# unzip -/downloads/dependency-check-6.2.2-release.zip
```

```
# ls
```

```
# cd dependency-check/
```

```
# cd dependency-check/bin/
```

```
# ls
```

```
# pwd (present working directory)
```

• here we should copy the location to paste it in next command.

```
# ln -s /opt/dependency-check/bin/dependency-check.sh /usr/bin/dependency-check.sh
```

```
# dependency-check.sh
```

3. to scan your project using owasp dependency check

• type the below commands

```
# ls (select any file @ directory)
```

```
# dependency-check.sh --scan multiples/
```

```
# ls
```

```
# firefox dependency-check-report.html
```

(the final output will display on the firefox).

lab practice - 22

install and configure apparmor in ubuntu

apparmor is a mandatory access control (MAC) system which confines programs to a limited set of resources. apparmor confinement is provided via profiles loaded into the kernel.

1- installation of apparmor (root user)

step 1:- go to ubuntu terminal and type the below command to install apparmor

```
# sudo apt-get install apparmor-utils auditd
# sudo apt install -y apparmor-utils apparmor
  - profiles
# aa-status
```

(apparmor-status is used to view the current status of apparmor profiles. sudo apparmor-status)

2. command line utilities (creating and viewing a python script in apparmor)

below are the commands used to create the script

step 1:- go to vi editor by typing vi test.py
filename

```
# vim test.py
```

```
#!/usr/bin/python 3
FILE = 'mytextfile'
try:
    open(FILE, 'a').close()
    print(f'created file: {FILE}')
except:
    print(f'failed to create file {FILE}')
    exit(1)
```

```
# chmod u+x test.py
```

(chmod u+x will make the file executable for your user, it will only add it for your user, though it may be already executable by the group owner, or "other").

```
# ./test.py
# ls
```


(the ls command is used to list files 07 directories in linux & other unix-based operating systems).

• we can also remove the existing file by using the below command.

rm mytextfile

3. generating a profile

step 1: # ~~sudo~~ aa-genprof test.py
(while executing this command, it will ask for scan(s) (on) to finish (F)). we should click on S (scan) to scan our system).

step 2: after the scanning is finished, it will ask for the permission and there we should type for letter 'o' (owner permission) it will change the permission.

step 3: after the change permission is done, we can also choose (on) type the letter 'A' (Allow) to allow.