2025

# THREAT MODELING ACTIVITY: PATCH & PROTECT

## Overview

This hands-on activity will introduce you to real-world cybersecurity practices through threat modeling. You'll work in groups to analyze your own systems, identify potential vulnerabilities, and apply mitigations while documenting your findings.

**Activity Time: 40 Minutes**

Akaanksha Sinha

Linkedin/in/cybergirlak

3/11/2025

# Table of Content



# THREAT MODELING ACTIVITY: PATCH & PROTECT

## Activity Overview:

👥 Group Size: 4–5 participants per team

Each team will act as a cybersecurity task force for their own "company." Using your laptops as assets, you'll:

1. Identify critical files and sensitive data.
2. Detect potential threats and attack vectors.
3. Apply basic security measures (mitigations).
4. Document your findings in a Threat Model Worksheet.

At the end of the activity, two groups will be randomly selected to present their findings.

## Group Formation & Roles:

- Team Leader: Coordinates tasks and ensures everyone participates.
- Technical Specialist: Runs the commands and gathers results.
- Documentation Lead: Fills out the Threat Model Worksheet.
- Presenter: Summarizes findings for the group's presentation.

## Submission Guidelines:

- Each group must complete the **Threat Model Worksheet**.
- Ensure the following sections are filled:
    - **Assets Identified**
    - **Threats Found**
    - **Attack Vectors**
    - **Mitigations Applied**

Two groups will be randomly selected to present their findings in a short 3-minute presentation.

## Timing Breakdown:

- **5 mins:** Group formation & role assignment
- **5 mins:** Identify Assets
- **10 mins:** Identify Threats
- **10 mins:** Find Attack Vectors
- **10 mins:** Apply Mitigations
- **5 mins:** Finalize the worksheet

## Expected Outcome:

By the end of the session, you will:

- Understand how threat modeling works in a real-world environment.
- Recognize common vulnerabilities and attack vectors.
- Apply basic security best practices on your own system.
- Work collaboratively in a cybersecurity team environment.

## Step-by-Step Instructions:

### Step 1: Identify Assets (5 minutes)

- Locate the sensitive files from the **Security Starter Pack** on your Desktop.

- **Windows Command:**

```
cd Desktop\Security-Starter-Pack
dir
```

- **macOS/Linux Command:**

```
cd ~/Desktop/Security-Starter-Pack
ls
```

- List:
  - Important system files (e.g., personal documents, photos, financial data)
  - Files from the starter pack (e.g., passwords.txt, confidential_notes.docx)
- Document all critical assets on the worksheet.

### Step 2: Identify Threats (10 minutes)

- Check for vulnerabilities using the following commands:

- **Open Ports:**
  - Windows:

```
netstat -an | find "LISTEN"
```

  - macOS/Linux:

```
lsof -i -P -n | grep LISTEN
```

- **User Accounts & Permissions:**
  - Windows:

```
net user
```

  - macOS/Linux:

```
whoami
id
```

- **File Permissions:**
  - Windows:

```
icacls sensitive_file.txt
```

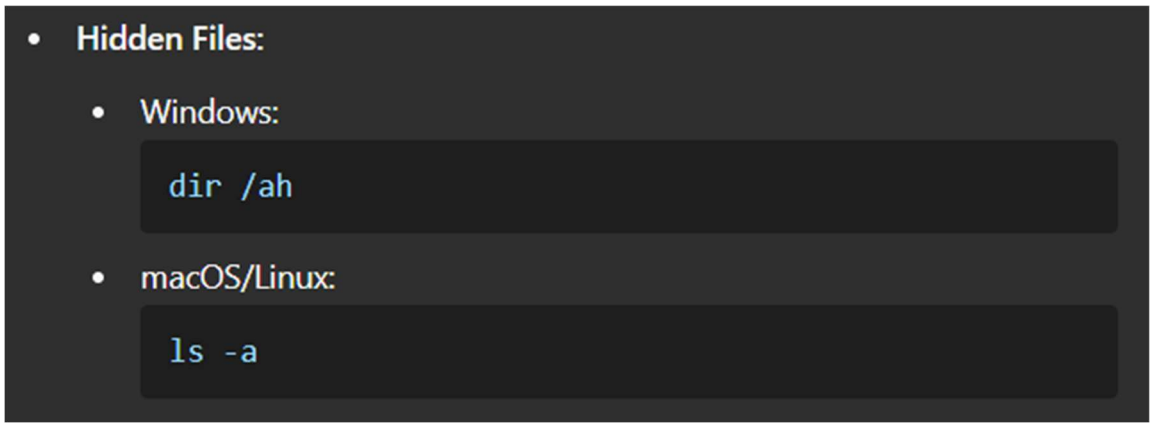
  - macOS/Linux:

```
ls -l sensitive_file.txt
```

- Record all detected vulnerabilities in the worksheet.

## Step 3: Find Attack Vectors (10 minutes)

- Look for weak points:




    - Manually inspect files for:
        - Passwords in plain text
        - Personal or sensitive data stored without encryption
- Document any potential attack vectors identified.

## Step 4: Apply Mitigations (10 minutes)

- Apply security fixes:
    - **Close Unnecessary Ports (Manual via firewall settings):**
    - **Windows:**
        1. Open the **Control Panel** → **System and Security** → **Windows Defender Firewall** → **Advanced settings**.
        2. In the left-hand menu, click on **Inbound Rules**.
        3. Locate the port or application you want to block.
        4. Right-click → **Disable Rule** or **Block Connection**.
    - **macOS:**
        1. Open **System Preferences** → **Security & Privacy** → **Firewall** → **Firewall Options**.
        2. Click on the **+** button to add applications.
        3. Set the connection status to **Block incoming connections**.

- **Linux:**

1. Use the Uncomplicated Firewall (UFW) command:

```
sudo ufw deny [port_number]
sudo ufw reload
```

2. Verify the status with:

```
sudo ufw status
```

- **Restrict File Permissions:**
  - Windows:

```
icacls sensitive_file.txt /remove Everyone
```

  - macOS/Linux:

```
chmod 600 sensitive_file.txt
```

- Document each mitigation applied.