**📋 Threat Modeling Workbook Template**

# **🔐 Group Information:**

* **Company Name:**

|  |  |  |
| --- | --- | --- |
| S# | Role Assignments | Team Members |
| 1 | **Team Leader** |  |
| 2 | **Technical Specialist:** |  |
| 3 | **Documentation Lead** |  |
| 4 | **Presenter** |  |
| 5 | **Timekeeper** |  |

# **📝 Step 1: Identify Assets**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S# | Asset Name | Owner | Description | Asset Type | Open Ports |
| Eg | Laptop | John Doe | Work laptop used for company access | System |  |
| Eg | Config file | Sysadmin | Stores customer information | Data |  |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |
| 11 |  |  |  |  |  |
| 12 |  |  |  |  |  |
| 13 |  |  |  |  |  |
| 14 |  |  |  |  |  |
| 15 |  |  |  |  |  |
| 16 |  |  |  |  |  |
| 17 |  |  |  |  |  |
| 18 |  |  |  |  |  |

# **⚠️ Step 2: Identify Threats and Attack Vectors**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S# | Asset Name | Asset Owner | Detected Threat | Attack Vector | Open Ports |
| Eg | Laptop | John Doe | Work laptop used for company access | High |  |
| Eg | Config file | Sysadmin | Stores customer information | High |  |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |
| 11 |  |  |  |  |  |
| 12 |  |  |  |  |  |
| 13 |  |  |  |  |  |
| 14 |  |  |  |  |  |
| 15 |  |  |  |  |  |
| 16 |  |  |  |  |  |
| 17 |  |  |  |  |  |
| 18 |  |  |  |  |  |

# **🔓 Step 3: Identify and Assess Vulnerabilities**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S# | Name | Vulnerability | Severity | Discovery Method |
| Eg | Laptop 1 | Weak Remote Desktop Password | High | Manual Inspection |
| Eg | Laptop 2 | Outdated macOS Version | Medium | System Information Command |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 15 |  |  |  |  |
| 16 |  |  |  |  |
| 17 |  |  |  |  |
| 18 |  |  |  |  |

# **💥 Step 4: Develop Mitigation Strategies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S# | Name | Potential Impact | Mitigation Strategy | Status |
| Eg | Laptop 1 | Unauthorized data access | Enforce strong RDP password policy | Open |
| Eg | Laptop 2 | System compromise due to malware | Enable and update antivirus software | Closed |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 15 |  |  |  |  |
| 16 |  |  |  |  |
| 17 |  |  |  |  |
| 18 |  |  |  |  |

# **📊 Step 5: Group Summary Section**

|  |  |  |
| --- | --- | --- |
| #N | Answer | |
| Number of Assets Analyzed | Unauthorized data access | |
| Total # of Vulnerabilities Detected | System compromises due to malware | |
| Total # of Critical Vulnerabilities |  | |
| List 3 Critical Vulnerabilities identified | **Critical Vuln. Details** | **Remediation Complete** |
|  |  |
|  |  |
|  |  |
|  |  | |
|  |  | |
|  |  | |

# **🔍 Reflection Questions:**

1. What was the most significant vulnerability your group identified?
2. Which mitigation strategy worked best and why?
3. What improvements would you suggest for future threat assessments?

# **📚 Additional Notes:**

(Record additional observations, technical difficulties, or any key lessons learned during the activity.)

# **Instructions:**

Each group should complete the tables in the appropriate steps while conducting their threat assessments. All worksheets should be submitted for review at the end of the session.