**TASK1**

**Step 1: Threat Identification**

**1. Sample Network/System Setup**

**Network/System Description:**

* The sample network/system consists of:
  + Workstations running Windows 10
  + File server with Windows Server 2016
  + Cisco routers and switches for network connectivity
  + Applications include Microsoft Office suite, web browsers, and email clients
  + Devices are connected via Ethernet LAN

**2. Identified Threats and Vulnerabilities**

**Threats:**

1. Malware:
   * Risk of ransomware attacks targeting critical data on file server
2. Unauthorized Access:
   * Weak password policies may lead to unauthorized access to workstations
3. Phishing Attacks:
   * Employees could fall victim to email phishing scams, compromising sensitive information
4. Denial-of-Service (DoS) Attacks:
   * Routers and servers may be vulnerable to DoS attacks disrupting network services
5. Insider Threats:
   * Employees with access to sensitive data pose risks of intentional or accidental data breaches

**Vulnerabilities:**

1. Outdated Software:
   * Workstations and server may have outdated operating systems and applications
2. Weak Authentication:
   * Lack of multi-factor authentication exposes systems to unauthorized access
3. Inadequate Security Patching:
   * Delayed application of security patches leaves systems vulnerable to exploits
4. Default Passwords:
   * Default passwords on network devices are not changed, posing security risks
5. Lack of Network Segmentation:
   * Flat network architecture increases exposure to lateral movement by attackers

**STEP2**

**Vulnerability Scan Results**

**Host: 192.168.1.100**

Identified Vulnerabilities:

1. **CVE-2021-1234** (Critical)
   * Description: Remote code execution vulnerability in Apache HTTP Server.
   * Potential Impact: Attacker can execute arbitrary code on the server.
   * Recommendation: Apply vendor patch immediately.
2. **CVE-2022-5678** (High)
   * Description: SQL injection vulnerability in web application.
   * Potential Impact: Attacker can extract sensitive data from the database.
   * Recommendation: Implement input validation and parameterized queries.

**Host: 192.168.1.101**

Identified Vulnerabilities:

1. **CVE-2021-8765** (Medium)
   * Description: Outdated software version susceptible to known exploits.
   * Potential Impact: Attacker can gain unauthorized access to the system.
   * Recommendation: Update software to the latest version.
2. **CVE-2022-4321** (Low)
   * Description: Information disclosure vulnerability in SSH service.
   * Potential Impact: Attacker can obtain system configuration details.
   * Recommendation: Limit SSH access and review configuration settings.

**STEP3**

**Risk Analysis**

**Vulnerability Prioritization:**

1. **CVE-2021-1234** (Critical)
   * **Severity**: Critical
   * **Likelihood of Exploitation**: High
   * **Risk Assessment**: This vulnerability poses a significant risk to the system's integrity and confidentiality. With a critical severity rating and a high likelihood of exploitation, immediate action is necessary to mitigate the threat.
2. **CVE-2021-8765** (Medium)
   * **Severity**: Medium
   * **Likelihood of Exploitation**: Medium
   * **Risk Assessment**: While this vulnerability is not as severe as CVE-2021-1234, it still presents a notable risk to the system's security. A medium severity rating and likelihood of exploitation indicate that timely measures should be taken to address the issue and prevent potential unauthorized access.
3. **CVE-2022-5678** (High)
   * **Severity**: High
   * **Likelihood of Exploitation**: Low
   * **Risk Assessment**: Despite its high severity rating, the likelihood of exploitation for this vulnerability is currently low. However, proactive measures should still be implemented to reduce the risk of exploitation in the future and ensure the system's overall security posture.
4. **CVE-2022-4321** (Low)
   * **Severity**: Low
   * **Likelihood of Exploitation**: Low
   * **Risk Assessment**: While the severity of this vulnerability is low and the likelihood of exploitation is also low, it should not be overlooked. Addressing this vulnerability can help strengthen the system's defenses and mitigate potential security risks.

**STEP 4**

**Mitigation Strategies**

**Devise Mitigation Strategies for High-Risk Vulnerabilities:**

1. **CVE-2021-1234** (Critical)
   * **Mitigation Strategy**: Immediately apply vendor-supplied patches or security updates to remediate the vulnerability.
   * **Recommendation**: Implement network segmentation to limit the exposure of vulnerable systems to potential attacks.
   * **Action Plan**: Schedule regular vulnerability scans and patch management processes to ensure ongoing security updates.
2. **CVE-2022-5678** (High)
   * **Mitigation Strategy**: Implement strict access controls and authentication mechanisms to protect vulnerable systems.
   * **Recommendation**: Conduct regular security awareness training for system users to mitigate the risk of social engineering attacks.
   * **Action Plan**: Monitor system logs and network traffic for suspicious activities associated with the identified vulnerability.

**Recommendations to Address Identified Risks Effectively:**

1. **Network Hardening**:
   * Implement firewall rules and intrusion detection/prevention systems (IDS/IPS) to monitor and block malicious network traffic.
   * Regularly update and patch all network devices and software components to minimize security vulnerabilities.
2. **Security Awareness and Training**:
   * Conduct periodic security training sessions for employees to raise awareness about cybersecurity best practices.
   * Encourage employees to report any suspicious activities or security incidents promptly.
3. **Incident Response Plan**:
   * Develop and maintain an incident response plan outlining procedures for responding to security breaches and mitigating risks.
   * Regularly test the incident response plan through tabletop exercises and simulations to ensure readiness.
4. **Continuous Monitoring**:
   * Implement continuous security monitoring tools to detect and respond to emerging threats in real-time.
   * Establish security controls for logging and monitoring critical system events for early threat detection.

**Action Plan for Implementation:**

* Assign responsible personnel or teams to oversee the implementation of mitigation strategies and recommendations.
* Define timelines and milestones for completing each action item.
* Conduct regular reviews and assessments to evaluate the effectiveness of implemented security measures.