Task 1: Cybersecurity Risk Assessment

Introduction:

In the realm of cybersecurity, risk assessment plays a pivotal role in safeguarding networks and systems against potential threats and vulnerabilities. By systematically identifying, analyzing, and mitigating risks, organizations can fortify their defenses and mitigate the likelihood of security incidents. In this task, we will explore various techniques and methodologies involved in cybersecurity risk assessment through a sample network or system setup.

1. Threat Identification:

Sample Network/System Setup:

For the purpose of this assessment, let's consider a medium-sized company with the following network/system setup:

1. **Internet Connection**:
    - High-speed broadband connection provided by an ISP.
2. **Firewall**:
    - Hardware firewall appliance deployed at the network perimeter to filter incoming and outgoing traffic.
3. **Router**:
    - Connects the internal network to the internet.
    - Manages traffic routing between internal devices and the internet.
4. **Switch**:
    - Connects various devices within the internal network, such as servers, workstations, and printers.
    - Provides network connectivity at the local level.
5. **Server Infrastructure**:
    - **File Server**: Stores and manages company files and documents.
    - **Email Server**: Hosts corporate email accounts and facilitates internal and external communication.
    - **Database Server**: Stores and manages sensitive business data.
    - **Web Server**: Hosts the company's website and web applications.

6. **Workstations**:
    - Desktop computers or laptops used by employees for daily work tasks.
    - Running operating systems such as Windows, macOS, or Linux.
7. **Wireless Access Points (WAPs)**:
    a. Provide wireless network connectivity for mobile devices and laptops.
    b. Enable employees to access the network from various locations within the office premises.
8. **Intrusion Detection System (IDS)**:
    a. Monitors network traffic for suspicious activity or signs of potential security breaches.
    b. Alerts administrators in real-time about potential threats.

Potential Threats and Vulnerabilities:

1. **Unauthorized Access**:
    - Weak or default passwords on network devices, servers, or user accounts.
    - Lack of proper access controls, allowing unauthorized users to gain access to sensitive data.
2. **Malware Infections**:
    - Introduction of malware through email attachments, malicious websites, or infected USB drives.
    - Outdated antivirus software or insufficient malware protection measures.
3. **Insider Threats**:
    - Employees intentionally or unintentionally leaking sensitive information.
    - Disgruntled employees attempting to sabotage systems or steal data.
4. **Phishing Attacks**:
    - Employees falling victim to phishing emails and disclosing sensitive information such as login credentials.
    - Lack of employee training and awareness regarding phishing threats.

5. **Unpatched Software**:
    - Failure to apply security patches and updates to operating systems, applications, and network devices.
    - Exploitation of known vulnerabilities by attackers to gain unauthorized access or disrupt services.
6. **Social Engineering**:
    a. Attackers exploiting human psychology to manipulate employees into divulging confidential information or performing unauthorized actions.
7. **Physical Security Breaches**:
    a. Unauthorized individuals gaining physical access to server rooms, network equipment, or sensitive documents.
    b. Lack of proper security measures such as access control systems, surveillance cameras, and security guards.

Identifying and addressing these potential threats and vulnerabilities is essential for maintaining the security and integrity of the company's network and data assets.

2. Vulnerability Scanning:

For vulnerability scanning, we will utilize tools such as Nmap and Nessus to identify potential weaknesses within the network/system. After conducting scans, we will document identified vulnerabilities along with their severity ratings and potential impact on the system's security.

3. Risk Analysis:

Following vulnerability identification, we will assess the risks associated with each vulnerability in terms of their potential impact on the system's confidentiality, integrity, and availability. Prioritization of vulnerabilities will be based on severity ratings and the likelihood of exploitation.

4. Mitigation Strategies:

High-risk vulnerabilities will be addressed through effective mitigation strategies, including:

- Implementing multi-factor authentication to combat unauthorized access.
- Deploying antivirus and anti-malware software to detect and remove malicious threats.
- Enforcing strict access controls and monitoring mechanisms to mitigate insider threats.
- Conducting regular employee training on identifying and avoiding phishing attacks.
- Configuring firewalls and intrusion detection/prevention systems to mitigate DoS attacks.
- Enforcing password policies requiring strong, regularly updated passwords.
- Establishing a patch management process to promptly apply software updates.
- Encrypting sensitive data both at rest and in transit to prevent unauthorized access.