

cyber security task 1

Cybersecurity Risk Assessment



INTERNCAREER

HETRICIA TSUNDZU CHAUKE

# **Task 1: Cybersecurity Risk Assessment**

**Threat identification:**

Let us say we have a sample for xyz corporation network/system setup that contains the following Network Architecture

Network Architecture:

* Internet Gateway
* Firewall
* Web Server (public-facing)
* Application Server
* Database Server
* Internal Network with Workstations

The potential threats and vulnerabilities are as follows:

1. **Phishing Attacks:**
   * Threat: Attackers may use phishing emails to trick employees into revealing sensitive information like login credentials.
   * Vulnerability: Lack of employee awareness and training on recognizing phishing attempts.
2. **Malware Infections:**
   * Threat: Malicious software (malware) could be introduced through infected email attachments or compromised websites.
   * Vulnerability: Endpoints may be susceptible if antivirus definitions are not regularly updated.
3. **Unauthorized Access:**
   * Threat: Attackers might attempt to gain unauthorized access to the network or specific systems.
   * Vulnerability: Weak passwords, insufficient access controls, or unpatched vulnerabilities in the firewall or servers.
4. **Insider Threats:**
   * Threat: Employees or contractors with malicious intent might misuse their access privileges.
   * Vulnerability: Inadequate monitoring of user activities, lack of employee background checks, or over-privileged accounts.
5. **DDoS Attacks:**
   * Threat: Distributed Denial of Service attacks could overwhelm the web server, making it unavailable to legitimate users.
   * Vulnerability: Insufficient DDoS protection measures in place.
6. **Data Breach:**
   * Threat: Unauthorized access to sensitive data (customer information, intellectual property).
   * Vulnerability: Inadequate encryption, lack of data loss prevention mechanisms, or weak database security.
7. **Social Engineering:**
   * Threat: Attackers may exploit human psychology to manipulate employees into divulging sensitive information.
   * Vulnerability: Lack of employee training on social engineering tactics.
8. **Unpatched Software:**
   * Threat: Exploitation of known vulnerabilities in software that has not been updated.
   * Vulnerability: Delayed or infrequent application of security patches.
9. **Insecure Configurations:**
   * Threat: Misconfigurations in the firewall, web server, or other systems could create security loopholes.
   * Vulnerability: Inadequate security configuration practices.
10. **Physical Security Threats:**
    * Threat: Unauthorized access to servers or network equipment.
    * Vulnerability: Insufficient physical security controls, lack of surveillance, or unsecured server rooms.

**Vulnerability scanning:**

Nmap and Nessus findings during scanning’s

1. **Nmap Scan Results:**
   * **Web Server:**
     + Vulnerability: Outdated Apache version (CVE-XXXX)
     + Severity: High
     + Potential Impact: Remote code execution; unauthorized access to the server.
   * **Database Server:**
     + Vulnerability: Weak SSL/TLS ciphers
     + Severity: Medium
     + Potential Impact: Data interception and unauthorized access.
   * **Workstations:**
     + Vulnerability: Unpatched Microsoft Office suite
     + Severity: Medium
     + Potential Impact: Malware injection through malicious documents.
2. **Nessus Scan Results:**
   * **Firewall:**
     + Vulnerability: Default credentials for firewall admin interface
     + Severity: Critical
     + Potential Impact: Unauthorized access to firewall settings.
   * **Application Server:**
     + Vulnerability: Missing security patches on the application framework
     + Severity: High
     + Potential Impact: Remote code execution; compromise of application functionality.
   * **Internal Network:**
     + Vulnerability: Lack of network segmentation
     + Severity: Medium
     + Potential Impact: Increased lateral movement in case of a breach.

**Risk Analysis:**

Prioritization based on Severity and Likelihood:

1. **Critical (High Severity):**
   * Default credentials on the firewall.
   * Potential Impact: Unauthorized access to critical network infrastructure.
   * Likelihood: High (as default credentials are commonly exploited)
2. **High Severity:**
   * Outdated Apache version on the web server
   * Missing security patches on the application server
   * Potential Impact: Remote code execution, compromise of web and application functionality.
   * Likelihood: Medium (as outdated software is often targeted)
3. **Medium Severity:**
   * Weak SSL/TLS ciphers on the database server
   * Unpatched Microsoft Office suite on workstations
   * Lack of network segmentation in the internal network
   * Potential Impact: Data interception, malware injection, increased lateral movement.
   * Likelihood: Low to Medium (depending on the specific vulnerabilities)

**Conclusion:**

1. **Immediate Actions:**
   * Change default credentials on the firewall.
   * Update Apache on the web server and patch the application server.
2. **Short-term Actions:**
   * Strengthen SSL/TLS ciphers on the database server.
   * Patch Microsoft Office on workstations.
3. **Long-term Actions:**
   * Implement network segmentation in the internal network.
   * Establish a regular patch management process.

**Mitigation Strategies:**

High-Risk Vulnerabilities:

1. **Default Credentials on Firewall:**
   * Mitigation:
     + Change the default credentials immediately.
     + Implement multi-factor authentication (MFA) for firewall access.
   * Recommendation: Regularly update and strengthen authentication mechanisms.
2. **Outdated Apache Version on Web Server:**
   * Mitigation:
     + Update Apache to the latest version.
     + Implement a web application firewall (WAF) to filter and monitor HTTP traffic.
   * Recommendation: Establish a routine for regular software updates and patching.
3. **Missing Security Patches on Application Server:**
   * Mitigation:
     + Apply the latest security patches to the application framework.
     + Conduct code reviews and implement secure coding practices.
   * Recommendation: To integrate automated patch management and code analysis tools.

**Report and Presentation:**

Comprehensive Report:

**Overview of Assessment Purpose and Scope:**

**Purpose:** The cybersecurity assessment aims to evaluate the effectiveness of XYZ Corporation's security measures and identify potential vulnerabilities and weaknesses that could be exploited by malicious actors. The assessment is designed to enhance the organization's cybersecurity posture and reduce the risk of security breaches and incidents.

**Scope:** The assessment covers various aspects of XYZ Corporation's IT infrastructure, including:

1. Network Security: Assessment of firewall configurations, network segmentation, and intrusion detection/prevention systems.
2. Endpoint Security: Evaluation of antivirus software, endpoint protection measures, and device management practices.
3. Application Security: Review of web applications, application servers, and secure coding practices.
4. Data Security: Analysis of data encryption, access controls, and data loss prevention mechanisms.
5. User Awareness: Assessment of employee training programs, phishing awareness, and security culture.

**Major Findings:**

1. **Default Credentials on Firewall:**
   * Discovery of default credentials used for the firewall admin interface, posing a significant security risk.
   * Potential Impact: Unauthorized access to critical network infrastructure, modification of firewall settings.
   * Recommendation: Immediate change of default credentials, implementation of multi-factor authentication (MFA).
2. **Outdated Software on Web Server:**
   * Identification of an outdated version of Apache running on the web server, vulnerable to known exploits.
   * Potential Impact: Remote code execution, compromise of web server functionality.
   * Recommendation: Immediate update of Apache software, deployment of a web application firewall (WAF).
3. **Unpatched Application Server:**
   * Discovery of missing security patches on the application server, increasing the risk of exploitation.
   * Potential Impact: Remote code execution, unauthorized access to application data.
   * Recommendation: Apply latest security patches immediately, establish a patch management process.
4. **Phishing Vulnerability:**
   * Observance of employees falling prey to phishing attempts, leading to potential compromise of login credentials.
   * Potential Impact: Unauthorized access to sensitive information, increased risk of malware infection.
   * Recommendation: Enhance employee training on phishing awareness, conduct simulated phishing exercises regularly.

**Recommendations:**

1. **Immediate Actions:**
   * Change default credentials on the firewall promptly to prevent unauthorized access.
   * Update Apache software on the web server and apply missing security patches to the application server immediately.
2. **Long-term Improvements:**
   * Implement multi-factor authentication (MFA) for all critical systems to enhance access security.
   * Establish a patch management process to ensure timely updates of software and applications.
   * Enhance employee training programs to include regular sessions on cybersecurity awareness and best practices, with a focus on phishing prevention.
3. **Continuous Monitoring:**
   * Deploy security monitoring tools such as SIEM and IDPS to detect and respond to security threats in real-time.
   * Conduct regular vulnerability assessments and penetration testing to identify and address emerging security risks.
4. **Incident Response Planning:**
   * Develop and regularly update an incident response plan to ensure a swift and effective response to security incidents.
   * Conduct tabletop exercises to test the incident response process and improve preparedness.

**Tools Used:**

1. Nmap (Network Mapper):

**Description:** Nmap is a versatile open-source network scanning tool used for network discovery and security auditing. It provides a comprehensive range of features for network reconnaissance, including host discovery, port scanning, version detection, and OS fingerprinting.

**Key Features:**

* Host Discovery: Identifies active hosts on the network using various techniques such as ICMP, TCP, and UDP probes.
* Port Scanning: Determines which ports are open on target systems, including TCP, UDP, and SCTP ports.
* Service Version Detection: Identifies the version and type of services running on open ports, helping to assess potential vulnerabilities.
* OS Fingerprinting: Attempts to determine the operating system of target hosts based on network responses.

2. Nessus:

**Description:** Nessus is a powerful vulnerability scanning tool used to identify security vulnerabilities, misconfigurations, and compliance issues across networks, systems, and applications. It offers a wide range of vulnerability checks and extensive reporting capabilities.

**Key Features:**

* Vulnerability Scanning: Conducts thorough scans to identify known vulnerabilities in network services, operating systems, and applications.
* Compliance Auditing: Performs checks against industry standards and regulatory requirements to ensure compliance.
* Malware Detection: Identifies signs of malware infections and suspicious activities on scanned systems.
* Reporting: Generates detailed reports with actionable insights, including severity levels and remediation recommendations.

**Methodology:**

1. Pre-Assessment Planning:

* Define Scope: Determine the scope of the assessment, including the target network range, systems, and applications to be scanned.
* Obtain Permissions: Obtain necessary permissions and approvals from stakeholders to conduct the scans and perform security assessments.

2. Nmap Scanning:

* Host Discovery: Use Nmap to discover active hosts on the network using various techniques such as ICMP ping sweeps and TCP SYN scans.
* Port Scanning: Conduct port scans to identify open ports on target systems and services running on those ports.
* Service Version Detection: Identify the version and type of services running on open ports to assess potential vulnerabilities.
* OS Fingerprinting: Attempt to determine the operating system of target hosts based on network responses.

3. Nessus Vulnerability Scanning:

* Asset Discovery: Configure Nessus to discover and enumerate all assets within the defined scope, including servers, workstations, and network devices.
* Vulnerability Scanning: Conduct vulnerability scans to identify known security vulnerabilities in network services, operating systems, and applications.
* Compliance Auditing: Perform checks against industry standards and regulatory requirements to ensure compliance with security policies.
* Malware Detection: Scan for signs of malware infections and suspicious activities on scanned systems.

**Timeline of Assessment Activities:**

1. **Pre-Assessment Planning:**
   * Week 1: Define scope, obtain permissions, and approvals.
2. **Nmap Scanning:**
   * Week 2: Conduct Nmap scans to discover active hosts and open ports on the network.
3. **Nessus Vulnerability Scanning:**
   * Week 3: Configure and execute Nessus vulnerability scans on discovered assets.
4. **Analysis and Reporting:**
   * Week 4: Analyze scan results, identify vulnerabilities, and generate comprehensive reports with findings and recommendations.
5. **Mitigation Planning and Implementation:**
   * Week 5: Develop mitigation plans based on identified vulnerabilities and begin implementing remediation measures.
6. **Post-Assessment Review:**
   * Week 6: Conduct a post-assessment review to evaluate the effectiveness of mitigation efforts and plan for future assessments or improvements.

**Detailed List of Identified Vulnerabilities:**

1. Default Credentials on Firewall:

* **Severity:** Critical
* **Potential Impact:** Unauthorized access to critical network infrastructure, modification of firewall settings.

2. Outdated Apache Version on Web Server:

* **Severity:** High
* **Potential Impact:** Remote code execution, compromise of web server functionality, unauthorized access to sensitive data.

3. Missing Security Patches on Application Server:

* **Severity:** High
* **Potential Impact:** Remote code execution, unauthorized access to application data, compromise of application functionality.

4. Weak SSL/TLS Ciphers on Database Server:

* **Severity:** Medium
* **Potential Impact:** Increased risk of data interception and unauthorized access to database contents.

5. Unpatched Microsoft Office Suite on Workstations:

* **Severity:** Medium
* **Potential Impact:** Malware injection through malicious documents, potential compromise of sensitive data.

**Categorization Based on Criticality:**

Critical Vulnerabilities:

1. **Default Credentials on Firewall:**
   * Immediate action required due to critical severity.
   * Potential for unauthorized access to critical network infrastructure poses a significant risk.

High-Severity Vulnerabilities:

1. **Outdated Apache Version on Web Server:**
   * Requires immediate attention to prevent remote code execution and compromise of web server functionality.
2. **Missing Security Patches on Application Server:**
   * High severity due to the potential for remote code execution and compromise of application data.

Medium-Severity Vulnerabilities:

1. **Weak SSL/TLS Ciphers on Database Server:**
   * Medium severity; while the risk of data interception exists, it's less critical compared to high-severity vulnerabilities.
2. **Unpatched Microsoft Office Suite on Workstations:**
   * Medium severity; although there's a risk of malware injection, it's not as immediate as high-severity vulnerabilities.

**Prioritization of Vulnerabilities Based on Severity and Likelihood:**

Risk Assessment Criteria:

1. **Severity:**
   * **Critical:** Vulnerabilities with the potential for severe impact on the organization's security posture, including unauthorized access to critical systems or data, and compromise of essential services.
   * **High:** Vulnerabilities that pose significant risks, such as remote code execution, unauthorized access to sensitive data, or compromise of key infrastructure components.
   * **Medium:** Vulnerabilities with moderate impact, including potential data exposure, service disruption, or compromise of less critical systems.
2. **Likelihood:**
   * **High:** Vulnerabilities that are highly likely to be exploited due to known exploits, widespread attack vectors, or weak security controls.
   * **Medium:** Vulnerabilities with a moderate likelihood of exploitation, such as commonly targeted systems or applications.
   * **Low:** Vulnerabilities with a low likelihood of exploitation, often due to limited attack vectors or less common configurations.

Prioritization Process:

1. **Critical Vulnerabilities:**
   * Identified critical vulnerabilities, such as default credentials on the firewall, are prioritized regardless of likelihood due to their severe impact potential.
   * Immediate action is necessary to mitigate critical vulnerabilities and prevent severe security incidents.
2. **High-Severity Vulnerabilities:**
   * Vulnerabilities with high severity, like outdated software on the web server and missing security patches on the application server, are prioritized next.
   * These vulnerabilities have significant impact potential and require urgent attention to mitigate risks effectively.
3. **Medium-Severity Vulnerabilities:**
   * Medium-severity vulnerabilities, such as weak SSL/TLS ciphers on the database server and unpatched software on workstations, are addressed after critical and high-severity vulnerabilities.
   * While not as immediate, they still pose significant risks and should be remediated promptly to ensure comprehensive security measures.

Explanation of Risk Assessment Criteria:

* **Severity:** The severity of a vulnerability indicates the potential impact it could have on the organization's security posture and operations. Critical vulnerabilities pose the highest risk due to their severe impact potential, while high and medium-severity vulnerabilities also require attention based on their respective impact levels.
* **Likelihood:** Likelihood refers to the probability of a vulnerability being exploited by malicious actors. Vulnerabilities with a high likelihood of exploitation are more urgent to address, as they are more likely to result in security incidents. However, even vulnerabilities with a lower likelihood of exploitation should not be ignored, as they still pose risks and could be targeted in future attacks.

**Strategies for Addressing High-Risk Vulnerabilities:**

1. Immediate Actions:

1. **Change Default Credentials on Firewall:**
   * Immediately change default credentials for the firewall admin interface to prevent unauthorized access.
   * Implement multi-factor authentication (MFA) to enhance access security.
2. **Update Apache Version on Web Server:**
   * Promptly update the Apache software on the web server to the latest version to address known vulnerabilities.
   * Deploy a web application firewall (WAF) to provide an additional layer of protection against web-based attacks.
3. **Apply Missing Security Patches on Application Server:**
   * Apply the latest security patches to the application server to mitigate potential risks of remote code execution and unauthorized access.
   * Conduct thorough testing to ensure the stability of the application after patching.

2. Long-term Recommendations for Improving Overall Security Posture:

1. **Establish Patch Management Process:**
   * Implement a robust patch management process to ensure timely updates of software, applications, and firmware across the organization.
   * Automate patch deployment where possible to streamline the process and reduce the window of vulnerability.
2. **Implement Continuous Monitoring:**
   * Deploy security monitoring tools such as Security Information and Event Management (SIEM) systems and Intrusion Detection and Prevention Systems (IDPS) to detect and respond to security threats in real-time.
   * Monitor network traffic, system logs, and user activity for signs of malicious behavior or unauthorized access.
3. **Enhance Employee Training and Awareness:**
   * Conduct regular security awareness training sessions for employees to educate them about cybersecurity best practices, including phishing awareness, password hygiene, and social engineering tactics.
   * Encourage employees to report suspicious activities or security incidents promptly.
4. **Enforce Least Privilege and Access Controls:**
   * Implement least privilege access controls to limit user access rights and permissions to the minimum necessary for their roles.
   * Regularly review and update access controls based on changes in job roles or responsibilities.
5. **Implement Network Segmentation:**
   * Segment the network into separate zones to limit the spread of potential security breaches and mitigate lateral movement by attackers.
   * Implement strict access controls between network segments to restrict unauthorized communication.
6. **Establish Incident Response Plan:**
   * Develop and regularly update an incident response plan to ensure a swift and coordinated response to security incidents.
   * Conduct tabletop exercises and simulations to test the effectiveness of the incident response plan and identify areas for improvement.
7. **Regular Security Assessments and Audits:**
   * Conduct regular vulnerability assessments, penetration tests, and security audits to identify and address emerging threats and vulnerabilities.
   * Engage third-party security experts to provide independent assessments and recommendations for improving security posture.

**Key Takeaways:**

1. **Urgent Action Needed:** Address critical and high-risk vulnerabilities immediately to mitigate potential security risks and prevent severe impact on the organization's operations.
2. **Comprehensive Approach:** Implement a holistic approach to cybersecurity, focusing on patch management, continuous monitoring, employee training, access controls, network segmentation, and incident response planning.
3. **Proactive Measures:** Take proactive measures to enhance security posture, including regular security assessments, audits, and vulnerability scans to identify and address emerging threats.
4. **Employee Awareness:** Invest in employee training and awareness programs to educate staff about cybersecurity best practices, including phishing prevention, password hygiene, and incident reporting.
5. **Continuous Improvement:** Establish a culture of continuous improvement by regularly reviewing and updating security measures, policies, and procedures to adapt to evolving threats and technologies.

**Call to Action:**

1. **Immediate Remediation:** Take immediate action to address critical vulnerabilities identified in the assessment, such as changing default credentials, updating software versions, and applying security patches.
2. **Long-Term Planning:** Develop a comprehensive plan for implementing recommended changes and improving overall security posture over time. Assign responsibilities, set timelines, and allocate resources accordingly.
3. **Employee Training:** Prioritize employee training and awareness initiatives to build a strong security culture within the organization. Schedule regular training sessions and communicate the importance of cybersecurity to all staff members.
4. **Regular Assessments:** Schedule regular security assessments, vulnerability scans, and audits to proactively identify and address security weaknesses. Use the findings to refine security measures and enhance protection against cyber threats.
5. **Incident Response Planning:** Develop and test an incident response plan to ensure a coordinated and effective response to security incidents. Conduct tabletop exercises and simulations to evaluate the plan's effectiveness and identify areas for improvement.

PRESENTATION:

KINDLY DOUBLE CLICK THE IMAGE ABOVE!!!

