Sure, here's a report based on the rubric provided, using the context from the "Vulnerability Assessment Report.pdf" and "Vulnerability Assessment Report.markdown" files:

Risk Management Report: Vulnerability Assessment Findings

Introduction

This report details the risk management strategies applied to the findings of a vulnerability assessment conducted on the target network. The assessment identified several vulnerabilities, and this report outlines the critical risks, treatment recommendations, and a risk monitoring procedure to ensure ongoing security.

Identification of Critical Risks

The vulnerability assessment revealed several risks, with two classified as critical:

1. **CVE-2017-1000083: Remote Code Execution in OpenSSH**

- **Affected System:** 192.168.1.10 (Port 22)

- **Explanation:** The outdated OpenSSH version is vulnerable to remote code execution. This vulnerability could allow an attacker to gain unauthorized access to the system, potentially leading to the compromise of sensitive data or escalation of privileges.

- **Treatment Recommendation:** Patch Management. Update OpenSSH on 192.168.1.10 to mitigate CVE-2017-1000083.

- **Basic Mitigation Steps:**
  - Apply the latest security patches to the OpenSSH service.
  - Restrict SSH access to trusted IP ranges.
  - Enforce the use of key-based authentication instead of passwords.

2. **Directory Traversal Vulnerability**

- **Affected System:** 192.168.1.10 (Port 80)

- **Explanation:** The web server is exposed to a directory traversal vulnerability, which could allow unauthorized access to sensitive files. This exposure could lead to the disclosure of configuration files or sensitive data, potentially enabling further exploitation.

- **Treatment Recommendation:** Patch Management. Patch the web server on 192.168.1.10 to fix the directory traversal vulnerability.

- **Basic Mitigation Steps:**
  - Apply security patches to the web server software.
  - Implement proper input validation and sanitization.
  - Configure the web server to restrict access to sensitive directories.

Risk Monitoring Procedure

To effectively track and manage the identified risks, the following risk monitoring procedure will be implemented:

1. **Regular Vulnerability Scanning:** Conduct regular vulnerability scans (e.g., monthly or quarterly) using Nmap or similar tools to identify any new or recurring vulnerabilities.

2. **Patch Management Tracking:** Maintain a detailed log of all patches applied to systems, including the date of application, patch version, and systems patched. Regularly verify that all critical systems are up-to-date.

3. **Intrusion Detection System (IDS) Monitoring:** Continuously monitor IDS logs for any suspicious activity that may indicate exploitation attempts related to the identified vulnerabilities. Configure alerts for high-risk events.

4. **Security Log Analysis:** Regularly review system and application logs for any signs of unauthorized access or malicious activity. Implement a Security Information and Event Management (SIEM) system to aggregate and correlate logs for more effective monitoring.

5. **Risk Review Meetings:** Conduct regular meetings (e.g., monthly) to review the status of identified risks, track mitigation efforts, and discuss any new security concerns. Update the risk register as needed.
6. **Reporting:** Generate regular reports (e.g., quarterly) on the status of risk management activities, including vulnerability scan results, patch management status, IDS alerts, and any security incidents.

Justification for Decisions

- The treatment recommendations prioritize patch management and service hardening, as these are the most effective ways to directly address the identified vulnerabilities.

- The risk monitoring procedure includes a combination of technical measures (vulnerability scanning, IDS monitoring, log analysis) and procedural measures (patch management tracking, risk review meetings, reporting) to provide comprehensive and ongoing risk management.

- Regular reporting ensures that stakeholders are informed of the organization's security posture and risk management efforts.

Conclusion

This risk management report outlines the steps necessary to address the critical vulnerabilities identified in the vulnerability assessment. By implementing the recommended treatment strategies and adhering to the risk monitoring procedure, the organization can significantly reduce its risk exposure and enhance the overall security of its network.