Risk Management Strategies: Identification, Treatment, and Monitoring

1. Identification of Risks

The provided vulnerability assessment using Nmap did not detect any open ports or critical vulnerabilities. However, potential risks still exist based on the scan results and general security best practices.

Critical Risks Identified

Risk 1: Lack of Continuous Monitoring

- **Description**: While the scan did not find open ports or vulnerabilities, this does not guarantee long-term security. If new services or ports are exposed in the future, they could introduce risks.
- **Treatment Recommendation**: Implement continuous vulnerability monitoring and scheduled scanning.
- **Mitigation Steps**:
  1. Set up automated vulnerability scans using Nmap or other tools on a weekly/monthly basis.
  2. Configure alerts for any newly detected open ports or service changes.
  3. Maintain an updated asset inventory to track changes in the network environment.

Risk 2: Broadcast-avahi-dos (CVE-2011-1002)

- **Description**: This vulnerability is associated with Avahi, a service commonly used for local network service discovery. It can be exploited for a Denial of Service (DoS) attack via NULL UDP packets.
- **Treatment Recommendation**: Disable Avahi if not required and apply appropriate firewall rules.
- **Mitigation Steps**:
  1. Identify systems running Avahi and determine if it is necessary.
  2. If not needed, disable Avahi service: `sudo systemctl disable avahi-daemon`
  3. Configure firewall rules to block incoming NULL UDP packets from untrusted sources.
  4. Regularly check for security patches related to Avahi and apply updates.

2. Risk Monitoring Procedure

To effectively track and manage risks, the following monitoring procedure should be implemented:

Risk Monitoring Procedure for Network Vulnerabilities

1. **Define Monitoring Scope**
   - Monitor all networked assets within the organization.
   - Focus on critical servers, workstations, and IoT devices.
2. **Set Up Automated Scanning**
   - Schedule automated vulnerability scans using Nmap (`nmap -sV --script vuln <IP>`).
   - Utilize other tools such as OpenVAS or Nessus for deeper scanning.
3. **Log and Review Scan Results**
   - Store scan results in a centralized logging system.
   - Compare results with previous scans to identify new risks.
4. **Implement Alerting Mechanisms**
   - Configure alerts for changes such as newly open ports or unpatched vulnerabilities.
   - Send notifications to security teams for immediate action.
5. **Conduct Periodic Security Audits**
   - Perform manual reviews and penetration testing quarterly.
   - Verify firewall and security configurations against best practices.
6. **Update Risk Assessments and Take Action**
   - Update risk registers with newly identified vulnerabilities.
   - Apply patches and reconfigure security settings as needed.

Justification for Decisions

- **Continuous monitoring** is necessary because security postures change over time due to software updates, network changes, and evolving threats.
- **Avahi mitigation** is recommended because services that are not required should be disabled to reduce the attack surface.
- **Risk monitoring procedures** ensure that vulnerabilities are tracked proactively, minimizing exposure to potential attacks.