Risk Management Report Based on Nmap Vulnerability Scan Results

1. Risk Identification

The Nmap scan results indicate the following potential risks:

- **Critical Risk 1: NULL UDP Avahi Packet DoS (CVE-2011-1002)**
    - **Explanation:** The scan detected a vulnerability related to the Avahi service, which is susceptible to a Denial of Service (DoS) attack via a NULL UDP packet. This could allow an attacker to disrupt service availability.
    - **Treatment Recommendation:** Apply patches or updates to the Avahi service to mitigate the vulnerability. If the service is not essential, consider disabling it.
    - **Mitigation Steps:**
        1. Update the Avahi service to the latest version.
        2. Disable Avahi if it is not required for network operations.
        3. Implement network filtering to block unauthorized UDP packets.
- **Critical Risk 2: Open Ports with Ignored States**
    - **Explanation:** The scan revealed that all 1000 scanned ports on the host 10.138.16.197 are in ignored states, which could indicate potential misconfigurations or overlooked services that might be exploited.
    - **Treatment Recommendation:** Conduct a thorough review of the services running on the host and ensure that only necessary ports are open.
    - **Mitigation Steps:**
        1. Perform a detailed audit of all services and ports.
        2. Close or restrict access to unnecessary ports.
        3. Implement firewall rules to limit access to essential services only.

2. Risk Monitoring Procedure

To effectively monitor the identified risks, the following procedure is recommended:

- **Procedure:**
    1. **Regular Vulnerability Scanning:** Schedule weekly Nmap scans to detect any new vulnerabilities or changes in the network configuration.
    2. **Patch Management:** Maintain a log of all software updates and patches applied, especially for services like Avahi.
    3. **Port and Service Audit:** Conduct monthly audits of open ports and running services to ensure compliance with security policies.
    4. **Incident Response Plan:** Develop and maintain an incident response plan to address any detected vulnerabilities or breaches promptly.
- **Justification:** Regular scanning and auditing help in early detection of vulnerabilities, reducing the risk of exploitation. Patch management ensures that

known vulnerabilities are mitigated promptly. An incident response plan ensures a structured approach to handling security incidents, minimizing potential damage.

3. Documentation and Justification

All identified risks, treatment recommendations, and mitigation steps have been documented to ensure a clear understanding and actionable plan. The risk monitoring procedure is designed to provide ongoing oversight and rapid response to potential threats, ensuring the security posture of the network is maintained.

This report provides a comprehensive approach to managing risks identified through the Nmap vulnerability scan, ensuring that critical vulnerabilities are addressed and monitored effectively.