CERBERUS

Security Assessment Report

Date: March 29, 2025

Report ID: CERB-20250329-001

Table of Contents

Executive Summary 2

Key Findings 3

Risk Assessment 4

Recommendations 5

Knowledge Graph Insights 6

Executive Summary

This report summarizes the security assessment conducted on the target system, scanme.nmap.org. The assessment identified no critical vulnerabilities or high-risk security issues, but potential vulnerabilities were found that require further investigation and remediation. This report provides detailed findings, risk assessments, and practical recommendations to address these potential vulnerabilities, incorporating insights from the knowledge graph data.

Key Findings

1. Outdated Software Versions

- Description: The target system is running outdated versions of OpenSSH (6.6.1p1) and Apache HTTP Server (2.4.7).
- OWASP Reference: OWASP Top 10:2021 - A6:2021-Vulnerable and Outdated Components
- Impact: Outdated software versions are susceptible to known vulnerabilities that have been patched in newer releases. This increases the risk of exploitation by attackers.
- Remediation: Update OpenSSH and Apache HTTP Server to their latest stable versions to mitigate the risk of known vulnerabilities.

2. Unusual Service on Port 31337

- Description: An unusual service, "Elite?", is running on port 31337. This port is often associated with backdoors or malware.
- OWASP Reference: OWASP Top 10:2021 - A7:2021-Identification and Authentication Failures
- Impact: The presence of an unknown service on a non-standard port could indicate a potential backdoor or unauthorized access point.
- Remediation: Investigate the purpose of the service and ensure it is legitimate. If it is not needed, disable the service and close the port.

3. Potential for Unauthorized Access via SSH

- Description: The SSH service is running on the default port (22/tcp) and uses an outdated version of OpenSSH.
- OWASP Reference: OWASP Top 10:2021 - A2:2021-Cryptographic Failures
- Impact: Outdated SSH versions may have vulnerabilities that could be exploited for unauthorized access. Additionally, running SSH on the default port increases the risk of automated attacks.
- Remediation: Update OpenSSH to the latest version. Consider changing the SSH port to a non-standard port to reduce the risk of automated attacks.

4. Additional Open Ports

- Description: The knowledge graph data indicates that additional ports are open on the target system, including port 9929, which runs the Nping echo service.
- Impact: Open ports that are not necessary can provide additional attack vectors for malicious actors.
- Remediation: Investigate the purpose of each open port and ensure that only necessary services are running. Disable or close any unnecessary ports.

Risk Assessment

- High Risk: The presence of outdated software versions and an unusual service on a non-standard port increases the risk of exploitation.
- Medium Risk: Running SSH on the default port and using an outdated version of OpenSSH increases the risk of unauthorized access.
- Medium Risk: Additional open ports that are not necessary can provide additional attack vectors.
- Low Risk: No critical vulnerabilities or high-risk security issues were detected.

Recommendations

1. Update Software Versions: Ensure that all software, including OpenSSH and Apache HTTP Server, is updated to the latest stable versions to mitigate known vulnerabilities.
2. Investigate Unusual Services: Investigate the purpose of the service running on port 31337 and ensure it is legitimate. If it is not needed, disable the service and close the port.
3. Secure SSH Configuration: Update OpenSSH to the latest version and consider changing the SSH port to a non-standard port to reduce the risk of automated attacks.
4. Review Open Ports: Conduct a thorough review of all open ports on the system. Ensure that only necessary services are running and disable or close any unnecessary ports.
5. Regular Security Assessments: Conduct regular security assessments to identify and address potential vulnerabilities in a timely manner.

By following these recommendations, the organization can significantly reduce the risk of security breaches and ensure the integrity and confidentiality of its systems.

Knowledge Graph Insights

- IP Addresses: The target system resolves to two IP addresses: 2600:3c01::f03c:91ff:fe18:bb2f (IPv6) and 45.33.32.156 (IPv4).
- Open Ports: Both IP addresses have the following open ports: 22 (SSH), 80 (HTTP), 9929 (Nping echo), and 31337 (unknown service).
- Software Versions: The HTTP service on both IP addresses is running Apache httpd 2.4.7, and the SSH service is running OpenSSH 6.6.1p1.

These insights confirm the findings from the security assessment and provide additional context for the identified vulnerabilities and recommendations.