Vulnerability Assessment with OpenVAS

Project Overview

This project was conducted to assess potential security risks on a Raspberry Pi device running on the same local network. The analysis focused on identifying exploitable vulnerabilities using industry-standard scanning techniques and providing actionable security recommendations.

Objective:

- This project aimed to analyze the network security of a Raspberry Pi device within a controlled environment.
- Identifying vulnerabilities and providing recommendations to strengthen the security system.

Scope:

- The assessment focused on common vulnerabilities in network services, specifically examining DNS and SSH configurations.

Methodology

Environment Setup:

- The scan was conducted using a Kali Linux virtual machine running on VMware, connected to the same network as the Raspberry Pi.

Tools used:

- The Greenbone Vulnerability Manager (OpenVAS) was utilized to conduct the vulnerability scan, leveraging its extensive database of known vulnerabilities.

Scanning Procedure:

- The OpenVAS scan was initiated using the 'Full and Fast' profile, targeting the Raspberry Pi to assess the presence of vulnerabilities on ports 53 (DNS) and 22 (SSH). The scan results were monitored in real-time to capture any critical findings.

Summary of Findings:

Vulnerability 1: DNS Cache Snooping

- Port: 53
- Severity: Medium
- CVSS Score: 5.0

Description: This vulnerability allows external parties to query the DNS server's cached records, which may expose sensitive information.

Impact: Unauthorized access to DNS cache could disclose the browsing habits or sensitive data of internal users.

Mitigation: Disable DNS recursion for external requests, restrict DNS access to internal trusted network only.

Vulnerability 2: Weak MAC Algorithm Supported

- Port: 22/tcp
- Severity: Low
- CVSS Score: 2.6

Description: The SSH server is configured to allow weak MAC algorithms, which may not provide strong encryption.

Impact: Attackers could potentially decrypt SSH sessions, weakening the security of data in transit.

Mitigation: Update the SSH configuration to disable weak MAC algorithms.

Recommendations

DNS Configuration:

- Disable DNS recursion for external DNS requests to limit cache snooping risks.
- Restrict DNS server access to trusted internal IP addresses to prevent unauthorized external access.

SSH Configuration:

- Remove weak MAC algorithms from the SSH configuration to enforce stronger encryption.
- Regularly review and update SSH settings to align with best security practices.

Ongoing Monitoring:

- Schedule periodic vulnerability scans to catch new risks and validate the effectiveness of implemented security controls.
- Stay updated with Greenbone feed updates to ensure OpenVAS is scanning with the latest vulnerability information.

Conclusion

In conclusion, the Raspberry Pi vulnerability assessment uncovered two specific security concerns, focusing on DNS and SSH configurations. By implementing the recommended actions, the system’s security against external threats will be significantly strengthened. The findings showcase the importance of regular scans and proactive security measures to maintain an optimal secure system.