Cybersecurity Task 3: Vulnerability Scan Report

Executive Summary

This report provides the findings from a security scan conducted on a personal computer using Nessus Essentials. The purpose was to uncover any existing vulnerabilities and assess the general security posture of the device. The results have been documented to guide future hardening efforts.

Tool Used & Scan Context

The scan was carried out using Tenable Nessus Essentials on the localhost (127.0.0.1). The scan type was a Basic Network Scan designed to detect common vulnerabilities, misconfigurations, and exposed ports.

Approach

- Configured Nessus Essentials and set up local scan
- Ran a Basic Network Scan on 127.0.0.1
- Analyzed scan results, severity levels, and risk exposure
- Interpreted the raw output to validate findings
- Formulated remediation steps to strengthen the system

Results Summary

The scan detected a total of 73 vulnerabilities:

- 2 High-severity issues
- 71 Medium-severity issues

No critical or low-severity vulnerabilities were explicitly listed. The scan also identified several open and listening ports that should be reviewed for necessity and security.

Network Exposure

Detected open TCP ports include: 135, 139, 445, 5040, 902, 912, 7680, 8834, and others.

Detected open UDP ports include: 123, 500, 4500, 5353, 5355, 62831.

Of particular concern are SMB (445) and VMware service ports, which may pose risks if not

hardened.

Key Security Insights

- SMB (Server Message Block) running on port 445 has a history of being exploited in past ransomware campaigns.

- VMware service ports were exposed and may leak sensitive info or allow unauthorized access.

- Several services were listening on all interfaces, which should be minimized.

Suggested Mitigation Steps

- Apply all available OS and application security updates.

- Disable or firewall unused services and ports.

- Avoid exposing sensitive ports to all network interfaces.

- Enforce loopback binding where applicable.

- Regularly schedule vulnerability scans and reviews.

Humanized Summary of Raw Data

During the scan, Nessus identified 62 open ports and 47 active connections.

The system was identified as running: Windows 11.

A total of 3872 plugin checks were launched to evaluate known vulnerabilities.

Notably, port 8834 (Nessus interface) supports SSL, indicating encrypted web communication.

The list of open ports includes:

0.0.0.0:123, 0.0.0.0:135, 0.0.0.0:445, 0.0.0.0:4500, 0.0.0.0:49664, 0.0.0.0:49665, 0.0.0.0:49666, 0.0.0.0:49667, 0.0.0.0:49668, 0.0.0.0:49669, 0.0.0.0:500, 0.0.0.0:5040, 0.0.0.0:5050, 0.0.0.0:5353, 0.0.0.0:5355, 0.0.0.0:53914, 0.0.0.0:7680, 0.0.0.0:8834, 0.0.0.0:902, 0.0.0.0:912, 127.0.0.1:1900, 127.0.0.1:24830, 127.0.0.1:62837, 192.168.131.1:137, 192.168.131.1:138, 192.168.131.1:139, 192.168.131....

This raw technical data helps validate the higher-level observations and reinforces the trust in scan output.

Detailed Open Port List (From Nessus Scan)

Based on the raw scan data, here is the full list of open ports detected:

TCP Ports (0):

UDP Ports (0):

Conclusion

This scan offered a clear view into the current vulnerabilities affecting the system. By following the recommended mitigation steps, the system's security posture can be significantly enhanced. Routine assessments like this ensure proactive defense against evolving cyber threats.

Cybersecurity Task 3: Vulnerability Scan Report