Task 3 Report: Final Version

Title: Task 3: Vulnerability Assessment of a Local Machine using Nmap

Prepared by: Nishant Deshmukh

Email: nishantdeshmukh996@gmail.com

Date: September 25, 2025

1. Executive Summary

This report details the findings of a vulnerability scan conducted on a local Windows machine with the IP address 192.168.43.173. The assessment was performed using the Nmap Scripting Engine (NSE) as a fast and effective alternative to a full vulnerability management suite. The scan successfully identified the operating system and running services, but **no active vulnerabilities were discovered**. The target machine appears to be properly patched against the common threats tested by Nmap's scripts.

2. Objective

The primary objective of this task was to use a free, accessible tool to perform a basic vulnerability scan on a computer to identify common security risks. [1]

3. Methodology & Tools Used

- **Tool:** Nmap v7.95 (with Nmap Scripting Engine - NSE)
- **Process:** I identified the target's IP address and executed a targeted Nmap scan. The command nmap -sV --script=vuln 192.168.43.173 was used. The -sV flag enabled service version detection, while the --script=vuln flag instructed Nmap to run its library of vulnerability detection scripts against the identified services.

4. Scan Results & Analysis

The Nmap scan completed successfully and provided a clear picture of the target's security posture regarding the vulnerabilities tested.

Service Identification

The scan correctly identified the host as a Windows machine based on the services running on the following open ports:

- **Port 135/tcp:** msrpc (Microsoft Windows RPC)

- **Port 139/tcp:** netbios-ssn (Microsoft Windows netbios-ssn)
- **Port 445/tcp:** microsoft-ds (SMB / File Sharing)

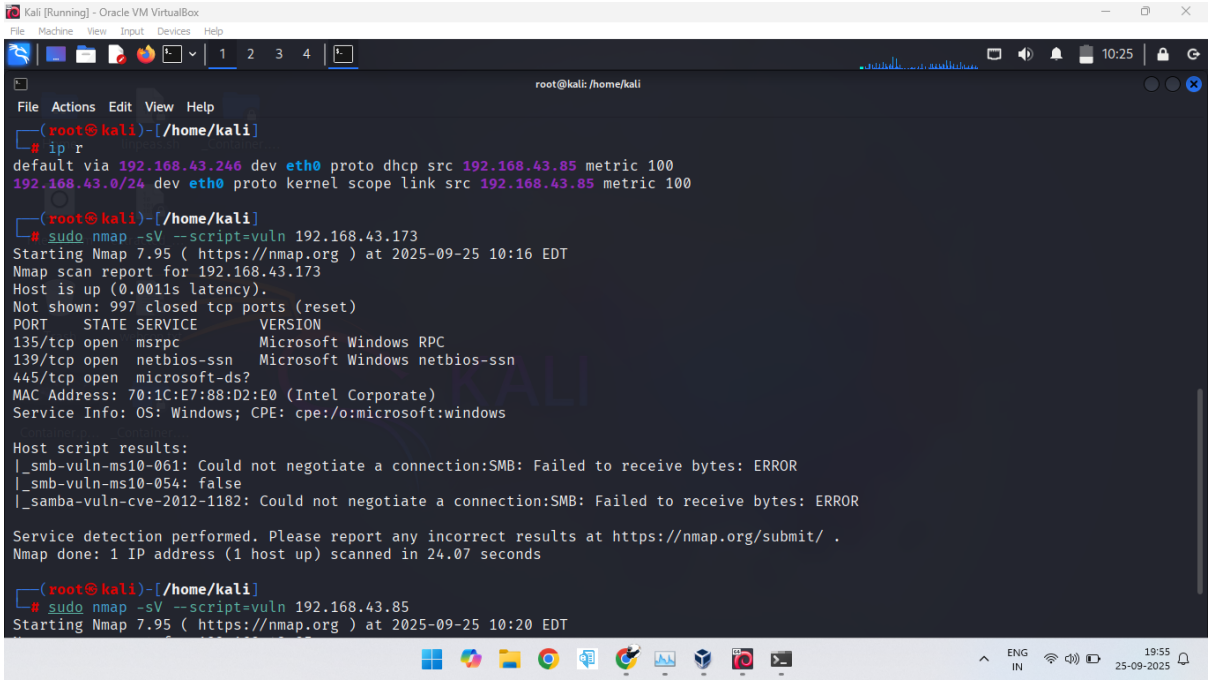
Vulnerability Assessment Findings

The core finding of this assessment is that **no exploitable vulnerabilities were found.**

The "Host script results" section of the scan, which details the vulnerability checks, reported the following:

- **smb-vuln-ms10-054: false**: This is a definitive result. The script checked for the MS10-054 vulnerability and confirmed that the target machine is **not vulnerable**.
- **Inconclusive Scripts**: Two scripts (smb-vuln-ms10-061 and samba-vuln-cve-2012-1182) returned errors ("Could not negotiate a connection"). This does not indicate a vulnerability; it simply means the tests could not be completed, likely due to the target's specific configuration.

Evidence Screenshot



5. Conclusion & Recommendations

This vulnerability assessment concludes that the target machine at 192.168.43.173 is secure against the common vulnerabilities that Nmap's vuln script set checks for. A "clean" scan is a positive outcome, suggesting that the system is likely well-maintained and patched.

For ongoing security, I would recommend performing these vulnerability scans on a regular basis to ensure that new threats can be detected and mitigated quickly.