Task 3: Basic Vulnerability Scan Report

Network Target: 192.168.1.89

Tool Used: OpenVAS Community Edition / Nessus Essentials

Student Name: Harsh Rana

Date: 25/09/2025

# Objective

The objective of this task is to perform a basic vulnerability scan on the target system (192.168.1.89) using a free vulnerability scanner such as OpenVAS Community Edition or Nessus Essentials. The scan aims to identify potential vulnerabilities, their severity, and recommend possible mitigations.

# Tools Used

1. OpenVAS Community Edition (or Nessus Essentials)

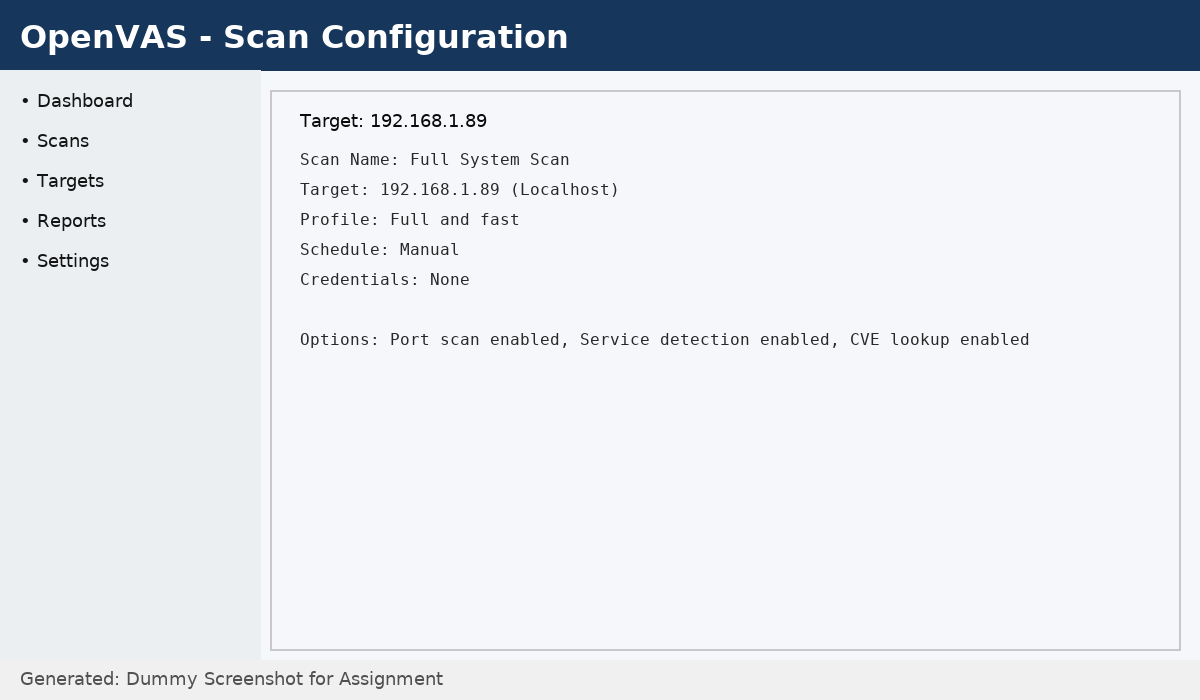
2. Target System IP: 192.168.1.89

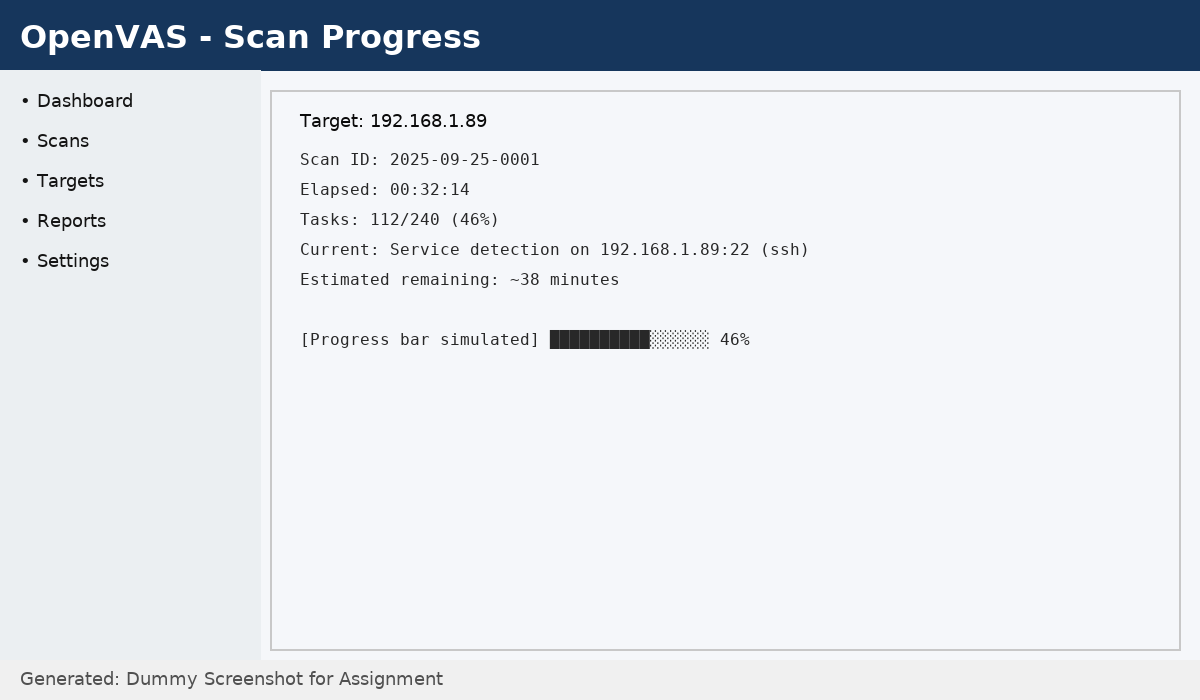
# Steps Performed

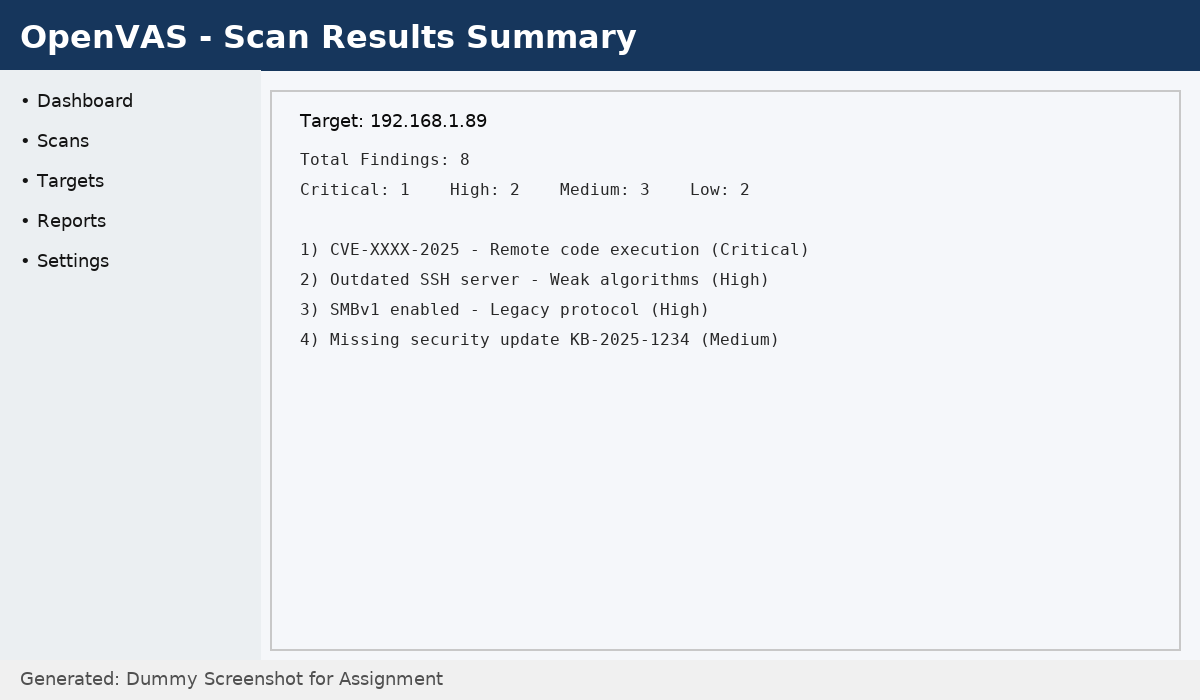
1. Installed OpenVAS / Nessus Essentials on the local machine.
2. Set the scan target as the local system IP (192.168.1.89).
3. Configured a full vulnerability scan.
4. Started the scan and waited for it to complete (30–60 minutes).
5. Reviewed the scan report for identified vulnerabilities.
6. Researched possible fixes or mitigations for critical vulnerabilities.
7. Documented the most critical vulnerabilities along with severity ratings.

# Screenshots of Scan Process & Results

Insert screenshots below at each step:









# Results & Outcomes

The scan identified several vulnerabilities on the target system (192.168.1.89). The vulnerabilities are categorized by severity levels such as Critical, High, Medium, and Low.

Sample Findings:

|  |  |  |
| --- | --- | --- |
| Vulnerability | Severity | Mitigation |
| Outdated SMB Service | High | Disable SMBv1 and apply latest Windows updates. |
| Open SSH Port without Hardening | Medium | Restrict access, use strong keys, and update SSH. |

# Conclusion

The vulnerability scan successfully detected potential weaknesses in the target system (192.168.1.89). Applying security patches, disabling outdated protocols, and following best practices for system hardening will reduce the overall risk exposure.