**1. Installing OpenVAS or Nessus Essentials**

The PDF shows that Nessus Essentials was chosen and installed on a Linux environment. The service was started using system commands (sudo systemctl start nessusd), and the status confirmed the scanner was running.​

**2. Setting Up the Scan Target**

The scan target was set to the local machine, specifically 127.0.0.1 (localhost), as indicated in the scan's configuration and report summary screens in the PDF.​

**3. Starting a Full Vulnerability Scan**

A "Basic Network Scan" template was used to perform a complete vulnerability assessment of the local system. The scan was initiated from the Nessus web interface and its progress was shown by the report screenshots.​

**4. Waiting for Completion**

The scan began at 12:45 PM and ended at 1:00 PM, showing completion within about 15 minutes (timing may vary in different runs), as summarized on the report dashboard.​

**5. Reviewing the Report**

The scan report identified 62 vulnerabilities on the localhost. The vulnerabilities were categorized by severity: Critical, High, Medium, Low, and Informational. Specific issues are mentioned in detail throughout the report screens in the PDF.​

**6. Researching Simple Fixes or Mitigations**

Here are some highlight vulnerabilities and recommended mitigations:

* **SSL Certificate Cannot Be Trusted (Medium, CVSS 6.5):**
  + Cause: Uses a self-signed or improperly chained X.509 certificate.
  + Mitigation: Obtain and install a valid SSL certificate from a trusted Certificate Authority.
* **SSL Certificate Common Name Mismatch (Info):**
  + The certificate common name (laptop-917tmoeo) does not match the accessed host (localhost).
  + Mitigation: Re-issue the SSL certificate with the correct common name or use the correct hostname when connecting.
* **Apache mod\_status Information Disclosure (Medium, CVSS 5.3):**
  + The server’s mod\_status page is accessible, leaking sensitive operational info.
  + Mitigation: Restrict access to /server-status in the Apache configuration so only administrative IPs can view it, or disable the module entirely.
* **Other Information Vulnerabilities:**
  + Items related to SSH, HTTP, certificates, and service version disclosures.
  + Mitigation: Regularly patch and configure services; restrict unnecessary information exposure.​

**7. Documenting the Most Critical Vulnerabilities**

Below is a table summarizing the most significant findings:

| **Vulnerability** | **Severity** | **Description** | **Suggested Fix** |
| --- | --- | --- | --- |
| SSL Cert. Cannot Be Trusted | Medium | Self-signed or untrusted SSL certificate on local service | Use CA-signed SSL certificate |
| SSL Cert. CN Mismatch | Info | Hostname in certificate does not match actual host | Correct CN in certificate or connect using correct hostname |
| Apache mod\_status Disclosure | Medium | Exposes Apache server activity, requests, and resource info without authentication | Restrict access to mod\_status or disable for public interfaces |
| Multiple Information Disclosure | Info | SSH/HTTP/service version and system info available to unauthenticated connections | Harden service configuration, apply least-privilege access |

​

**8. Screenshots of Scan Results**

The PDF contains multiple screenshots taken from the Nessus Essentials web dashboard, showing:

* The scan dashboard with total vulnerabilities identified
* Details for each vulnerability, including SSL and Apache findings
* Expanded views with CVSS scores, descriptions, and suggested fixes

The screenshots confirm the vulnerability count and details as described above and match the steps of the scan process.