**Task 3: Vulnerability Assessment Report**

**1. Introduction**

This report provides a detailed analysis of vulnerabilities discovered through a basic vulnerability scan using **OpenVAS** (Greenbone Vulnerability Management).  
The goal of this task is to understand how vulnerability scanners work and how to interpret their results.

**2. Tools Used**

* **OpenVAS** (Greenbone Vulnerability Manager)
* **Kali Linux**
* **Web Browser (Firefox/Chromium)** to access OpenVAS Dashboard
* **VirtualBox** (if used in a virtualized setup)

**3. Scanning Process**

1. **Started GVM (Greenbone Vulnerability Manager) Services** using the terminal:

* sudo gvm-start

1. **Opened the OpenVAS Web Interface** by navigating to:

* https://127.0.0.1:9392

1. **Logged in** using the default or created credentials.
2. **Created a New Target**:
   * Gave the target a name
   * Entered the IP address of the machine to be scanned
3. **Created a Task**:
   * Linked the task to the created target
   * Chose scan configurations (Full and fast)
   * Saved and started the scan
4. **Waited for the Scan to Complete**, then viewed the detailed **report** from the **Scans → Reports** section.

**4. Key Findings**

The scan provided a list of vulnerabilities categorized as:

* **High**
* **Medium**
* **Low**
* **Log**

Common issues detected:

* Outdated or vulnerable services
* Open ports with weak configurations
* Missing security headers
* Potential for brute-force attacks

Each finding included:

* A summary
* CVSS score (severity)
* Suggested remediation steps

**5. Recommendations**

To reduce risk and strengthen system security:

* Regularly apply security patches and updates.
* Close unused and unnecessary ports.
* Configure firewall rules properly.
* Disable vulnerable services and protocols.
* Conduct periodic vulnerability scans.
* Use strong, complex passwords and implement multi-factor authentication (MFA).

**6. Conclusion**

This task demonstrated how vulnerability scanners like OpenVAS help identify weaknesses in a system.  
By performing this scan, we gained insights into real-world risks and learned how to remediate them.  
Regular vulnerability assessments are essential to maintaining a secure environment.

1. **Screnshot**





