**Project: Vulnerability Identification using openvas on Kali Linux**

1. **Installation of Kali Linux on VirtualBox**
   1. Download Kali Linux from the official website.
   2. Install Kali Linux on your virtual machine and set the static IP address to 192.168.56.136.
   3. Update the system: sudo apt update && sudo apt upgrade -y
2. **Install OpenVas on Kali Linux**
   1. On terminal type sudo apt install openvas -y
   2. On terminal type sudo gvm-setup
   3. On terminal type sudo gvm-check-setup
   4. On terminal type sudo gvm-start
   5. Access the OpenVas web interface by navigating to <https://127.0.0.1:9392>
   6. On web interface verify that feed status is current for SCAP, CERT & GVMD\_DATA
3. **Install and Configure Metasploitable VM on VirtualBox**
   1. Download Metasploitable from the official website.
   2. Install and configure on VirtualBox
   3. Configure Network Adapter to Host-Only
   4. Ensure the Metasploitable VM is up and running with the IP address 192.168.56.122.
4. **Performing the Nessus Scan**
   1. Open OpenVas in the web browser and log in.
   2. Create a new scan:
      1. Go to "Scans" > "Tasks"> “New Task”.
      2. Name the scan "Metasploitable Vulnerability Scan".
      3. Scan Targets
      4. Hosts>Manual>192.168.56.122
      5. Leave Exclude Hosts and others as default.
      6. Click Save twice when it appears.
   3. Running the Scan:
      1. Launch the scan and wait for it to complete.
5. **Analyzing the Results**
   1. Once the scan is complete, view the report in the OpenVas interface. Go to Scans >Reports to select the report. The information available is Results, Hosts, Ports, Applications, Operating Systems, CVEs, Closed CVEs, TLS Certificates, Error Messages, User Tags.
   2. Focus on the identified vulnerabilities, CVSS scores, and recommended solutions.