**Project: Vulnerability Identification using Nessus 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 Nessus on Kali Linux**
   1. Download the Nessus Debian package from the official Tenable website.
   2. Verify the checksum of the downloaded package: sha256sum Nessus-10.7.4-debian10\_amd64.deb
   3. Install Nessus essential: sudo dpkg -i Nessus-10.7.4-debian10\_amd64.deb
   4. Sudo apt install -f
   5. Start Nessus scanner by typing /bin/systemctl start nessusd.service on terminal
   6. Access the Nessus web interface by navigating to <https://127.0.0.1:8834>
   7. Follow the prompts to configure Nessus and install plugins.
3. **Install and Configure Metasploitable VM on VirtualBox**
   1. Download Metasploitable from the official website.
   2. Install and configure on VirtualBox
   3. Ensure the Metasploitable VM is up and running with the IP address 192.168.56.122.
4. **Performing the Nessus Scan**
   1. Open Nessus in the web browser and log in.
   2. Create a new scan:
      1. Go to "Scans" > "New Scan".
      2. Select "Basic Network Scan".
      3. Name the scan "Metasploitable Vulnerability Scan".
      4. Set the target to 192.168.56.122.
      5. Under the "Discovery" tab, specify the ports to scan: Port scan (all ports)
      6. Under the "Assessment” tab, specify the scab type: Scan for all web vulnerabilities (complex)
   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 Nessus interface.
   2. Focus on the identified vulnerabilities, CVSS scores, and recommended solutions.
   3. Vulnerabilities (13 as Critical, 10 as High, 43 as Medium, 12 as Low & 180 as Info)
   4. Here are some of the vulnerabilities below:
      1. Port 2049 UDP RPC-NFS
         1. Vulnerability: NFS Exported Share Information Disclosure
         2. CVSS:10.0
         3. Solution: Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
      2. Port 5900 TCP VNC
         1. Vulnerability: VNC Server 'password' Password
         2. CVSS:10.0
         3. Solution: Secure the VNC service with a strong password
      3. Port n/a
         1. Vulnerability: Unix Operating System Unsupported Version Detection
         2. CVSS:10.0
         3. Solution: Upgrade to a version of the Unix Operating system that is currently supported.
      4. Port 1524 TCP Wild\_Shell
         1. Vulnerability: Bind Shell Backdoor Detection
         2. CVSS:9.8
         3. Solution: Verify if the remote host has been compromised, and reinstall the system if necessary
      5. Port 25 TCP SMTP
         1. Vulnerability: SSL Version 2 and 3 Protocol Detection
         2. CVSS:9.8
         3. Solution: Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 or higher instead.