**Assignment 1: Vulnerability Assessment using Nessus**

Nessus is a popular vulnerability assessment tool that helps identify security vulnerabilities in a network or system. Below are the general steps for performing a vulnerability assessment using Nessus:

1. **Installation and Setup**: Install Nessus on a computer that has access to the network you want to assess. After installation, launch the Nessus interface and set up the necessary configurations, such as configuring scanning policies, target hosts, and scan schedules.
2. **Create a Scanning Policy**: Define a scanning policy that suits your requirements. This policy includes various settings and preferences that Nessus will use during the assessment, such as the type of vulnerabilities to check for, the intensity of the scan, and any specific compliance checks.
3. **Target Selection**: Identify the target hosts or IP ranges that you want to assess. Ensure that you have the proper authorization to perform the assessment on these systems.
4. **Start the Scan**: Initiate the vulnerability scan by selecting the appropriate scanning policy and specifying the target hosts. Nessus will then start scanning the target systems for vulnerabilities.
5. **Scan Progress Monitoring**: Monitor the progress of the scan in real-time. Depending on the size of the target network and the selected policy, the scan may take some time to complete.
6. **Vulnerability Identification**: Once the scan is complete, Nessus will generate a report detailing the vulnerabilities found on the target systems. The report will include information about the severity of each vulnerability, affected services, and possible solutions or mitigation measures.
7. **Vulnerability Prioritization**: Prioritize the vulnerabilities based on their severity and potential impact on your network. Focus on addressing the critical vulnerabilities first.
8. **Remediation Planning**: Plan the remediation process for the identified vulnerabilities. This may involve applying patches, updating configurations, or implementing security measures to mitigate the risks.
9. **Reporting**: Generate a comprehensive report that summarizes the assessment results, including a list of vulnerabilities, their severity levels, and recommendations for remediation. This report is valuable for communicating the security status to stakeholders and management.