Hello everyone in this exercise you will Learn about NESSUS, which is a proprietary vulnerability scanner developed by Tenable, Inc. It is a remote security scanning tool which scans a system and raises alert when it discovers any vulnerabilities which malicious hackers can use to gain access to any system connected to networks. Vulnerability scanning is all about identifying, evaluating, treating, and reporting security vulnerabilities in systems and software.

You can download Nessus from the given link on this page. It is available for most of the windows and Linux versions. In this exercise, you will be using it on Windows 10 64 bit. After downloading and installation, it requires activation code, which you can get while installation or separately from the given link on your registered email id. For step-by-step process of installation please go through the lab manual.

Once you have installed and launched Nessus, you're ready to start scanning. First, you have to create a scan. To create your scan: In the top navigation bar, click Scans. In the upper-right corner of the My Scans page, click the New Scan button.

Next, click the scan template you want to use. Here Basic Network Scan has been used which performs a full system

scan that is suitable for any host. Use this template to scan an asset, for example, you can perform an internal vulnerability scan on your systems.

Prepare your scan by configuring the settings available for your chosen template. The Basic Network Scan template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort. Specify the name of scan and the targets. There may be a single target or a range of targets in a CIDR notation. After Specifying the name of scan and the target IP, Click on Save.

After you have configured all your settings, you can either click the Save button to launch the scan later or launch the scan immediately. If you want to launch the scan immediately, click the Launch button. The time it takes to complete a scan involves many factors, such as network speed and congestion, so the scan may take some time to run.

Viewing scan results can help you understand your organization's security vulnerabilities. Viewing scan results by vulnerabilities gives you a view into potential risks on your assets.

To view vulnerabilities: Do one of the following: Click a specific host to view vulnerabilities found on that host. Click the Vulnerabilities tab to view all vulnerabilities.

Thank You...