**EXPERIMENT – 06**

**AIM** – To perform vulnerability scanning using Nessus tool.

**Theory**

**What is Nessus?**

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

**Why Nessus?**

If you are familiar with other network vulnerability scanners, you might be wondering what advantages Nessus has over them. Key points include:

* + Unlike other scanners, Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.
  + Nessus is very extensible, providing a scripting language for you to write tests specific to your system once you become more familiar with the tool. Its also provides a plug-in interface, and many free plug-ins are available from the Nessus plug-in site. These plugs are often specific to detecting a common virus or vulnerability.
  + Up to date information about new vulnerabilities and attacks. The Nessus team updates the list of what vulnerabilities to check for on a daily basis in order to minimize the window between an exploit appearing in the wild, and you being able to detect it with Nessus.
  + Open-source. Nessus is open source, meaning it costs nothing, and you are free to see and modify the source as you wish.
  + Patching Assistance: When Nessus detects a vulnerability, it is also most often able to suggest the best way you can mitigate the vulnerability.

**STEPS**:

1. Create a Scan. To create a scan go to top navigation bar and click Scans or go to upper right corner of the My Scans page, click on the New Scan button.
2. Choose a Scan Template. Click the scan template you want to use. Scan templates simplify the process by determining which settings are configurable and how they can be set.
3. Configure Scan Settings.

**Practical**

**OUTPUT:**











