**10) Perform the following:**

**1) Vulnerability scanning with Nessus**

**2) Web application assessment with nekton**

**3) Perform Web application assessment using Burp suite**

1) Vulnerability scanning with Nessus

Aim:

The main aim of vulnerability scanning with Nessus is to proactively identify and fix security weaknesses or vulnerabilities within an organization's IT infrastructure before cyber attackers can exploit them

**Procedure:**

Vulnerability scanning with Nessus

1. First, the Welcome to the InstallShield Wizard for Tenable, Inc. Nessus screen

appears. Select Next to continue.

2. On the License Agreement screen, read the terms of the Tenable, Inc. Nessus software

license and subscription agreement.

3. Select the I accept the terms of the license agreement option, and then click Next.

4. On the Destination Folder screen, select the Next button to accept the default

installation folder. Otherwise, select the Change button to install Nessus to a different

folder.

5. On the Ready to Install the Program screen, select the Install button.

The Installing Tenable, Inc. Nessus screen appears and a Status indication bar shows the

installation progress. The process may take several minutes.

After the InstallShield Wizard completes, the Welcome to Nessus page loads in your default

browser.

If the page does not load, do one of the following steps to open Nessus in your browser.

 To access a remotely installed Nessus instance, go to https://&lt;remote IP

address&gt;:8834 (for example, https://111.49.7.180:8834).

 To access a locally installed Nessus instance, go to https://localhost:8834.

**2) Web application assessment with nekton**

**Aim:**

The primary goal of a web application assessment, often involving tools like Nekton, is to identify and assess security weaknesses in a web application, ultimately aiming to improve its security posture and resilience against attacks.

Procedure Steps:

1. Install Nikto:
   1. Install via package manager (e.g., apt-get install nikto on Debian-based systems).
2. Nikto –help
3. Nikto –h <target url> -ssl
4. Nikto –h <target url> -tuning 1,2
5. Run Nikto Scan:
   1. Basic scan:
      1. nikto -h <target\_URL>
   2. Specify output file:
      1. nikto -h <target\_URL> -o report.txt
6. Analyze Results:
   1. Look for issues such as:
      1. Server misconfigurations.
      2. Directory traversal vulnerabilities.
      3. Default credentials.

**3. Web Application Assessment Using Burp Suite**

**Aim:**

Perform a detailed and interactive assessment of a web application for vulnerabilities using Burp Suite.

**Procedure:**

**Downloading and Setting Up Burp Suite on Windows**

1. Go to the Burp Suite website and download the installer
2. Run the installer and follow the prompts to complete the installation process, select “new temporary project”, followed by “use burp defaults”
3. Click on **Start Burp**

**Configuring Burp Suite**

1. ***Set up the Proxy***: In order to intercept traffic, you need to configure the proxy settings in Burp Suite.  
   Go to the “Proxy” tab, then click on the sub-tab “Options/Proxy Setting”
2. You should see an entry in the table with a ticked Checkbox in the Running column, and “127.0.0.1:8080” showing in the Interface column.
3. Go to the **Proxy > Intercept** tab and Click the **Intercept is off** button, so it toggles to **Intercept is on.**This toggle allows you to intercept any request or response, and modify it before forwarding it.