PRACTICAL NO. 4

A. Perform Mobile Network Scanning using NESSUS

Aim

To perform **mobile network scanning** and identify vulnerabilities using the **Nessus vulnerability scanner**.

Tools / Software Used

- Nessus Vulnerability Scanner
- Mobile Device (Android / iOS)
- Wi-Fi Network
- Web Browser

Theory

Nessus is a vulnerability assessment tool used to scan networks, systems, and devices for security weaknesses.
Mobile devices connected to a network may contain vulnerabilities that can be detected using Nessus scanning.

Steps / Procedure

1. Start the **system with Nessus installed**.
2. Open a **web browser**.
3. Enter Nessus URL:
4. `https://localhost:8834`
5. Login using Nessus credentials.
6. Click on **New Scan**.
7. Select **Basic Network Scan**.
8. Enter scan name and description.
9. Enter **IP address of the mobile device** connected to the Wi-Fi network.
10. Click on **Save**.
11. Click **Launch Scan**.

12. Wait for scan to complete.
13. Analyze detected vulnerabilities and severity levels.

Result

Nessus successfully scanned the mobile device network and identified possible vulnerabilities.