***LAB 27***

***demonstrate how to use tool ....Nessus, NMAP, Prowler***

Certainly! Here’s a simplified step-by-step guide for using Nessus, Nmap, and Prowler, which are common tools for network and security assessment.

**1. Using Nessus**

Nessus is a vulnerability scanner that helps you identify potential security issues in your network.

**Step-by-Step Guide:**

1. **Download and Install Nessus:**
   * Go to the Nessus download page and download the appropriate version for your operating system.
   * Install Nessus following the installation instructions provided.
2. **Start Nessus:**
   * After installation, open your web browser and navigate to https://localhost:8834 (Nessus runs on port 8834 by default).
   * Complete the initial setup by creating an account and entering your activation code (you can get a free activation code for Nessus Essentials).
3. **Configure a New Scan:**
   * Log in to the Nessus web interface.
   * Click on the **New Scan** button.
   * Choose a scan template (e.g., "Basic Network Scan").
   * Enter the details for your scan (e.g., name, target IP addresses).
   * Click **Save** to create the scan.
4. **Run the Scan:**
   * Go to the **Scans** tab.
   * Find your newly created scan and click **Launch**.
5. **View Results:**
   * After the scan is complete, click on the scan name to view the results.
   * Review the identified vulnerabilities and recommendations.

**2. Using Nmap**

Nmap (Network Mapper) is a network scanning tool used to discover hosts and services on a network.

**Step-by-Step Guide:**

1. **Download and Install Nmap:**
   * Go to the Nmap download page and download the installer for your operating system.
   * Install Nmap by following the instructions.
2. **Open a Command Prompt:**
   * Open Command Prompt on Windows by pressing Windows Key + R, typing cmd, and pressing Enter.
3. **Basic Scan:**
   * Run a basic scan to discover live hosts on your network:

nmap -sP 192.168.1.0/24

* + Replace 192.168.1.0/24 with your target network range.

1. **Scan Specific Host:**
   * To scan a specific host for open ports, use:

nmap 192.168.1.1

* + Replace 192.168.1.1 with the IP address of the target host.

1. **Scan for Services:**
   * To get more details about services running on open ports, use:

nmap -sV 192.168.1.1

1. **View Results:**
   * Review the output in Command Prompt to see the scan results, including open ports and services.

**3. Using Prowler**

Prowler is a security tool for auditing AWS environments for compliance and security best practices.

**Step-by-Step Guide:**

1. **Download and Install Prowler:**
   * Open Command Prompt or a terminal window.
   * Clone the Prowler repository from GitHub:

git clone https://github.com/prowler-cloud/prowler

* + Navigate to the Prowler directory:

cd prowler

1. **Run a Basic Scan:**
   * To perform a basic security assessment of your AWS environment, run:

./prowler -a

* + Ensure you have AWS credentials configured in your environment.

1. **View Results:**
   * After the scan completes, Prowler will generate a report with findings related to AWS security best practices.
2. **Check Specific Checks:**
   * To run specific checks, use:

./prowler -c <check\_id>

* + Replace <check\_id> with the specific check you want to perform.

**Summary**

* **Nessus:** A vulnerability scanner that helps identify security issues. Install Nessus, create a scan, run it, and review the results.
* **Nmap:** A network scanner used to discover hosts and services. Install Nmap, run basic and detailed scans, and review the results.
* **Prowler:** A security auditing tool for AWS environments. Clone the repository, run scans, and review the security findings.

These steps provide a basic introduction to using Nessus, Nmap, and Prowler for network and security assessments.