

Exp 10 : Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities.

Using NESSUS on Kali Linux to Scan Networks for Vulnerabilities

Nessus is a widely-used vulnerability scanner that can identify a range of security vulnerabilities in systems, networks, and applications. It helps penetration testers, security professionals, and system administrators to find and fix vulnerabilities before they can be exploited by attackers.

Kali Linux comes pre-installed with a lot of useful tools, but Nessus is not pre-installed. You can manually install Nessus on Kali Linux to start scanning for vulnerabilities.

Here's a step-by-step guide to install and use Nessus on Kali Linux:

1. Install Nessus on Kali Linux

Step 1: Download Nessus

1. Go to the official Nessus website to download the Nessus installer for Kali Linux.
 - Visit: Nessus Downloads
 - Select Linux as the platform.
 - Download the correct package for your system (e.g., Debian package for Kali).
2. Alternatively, you can use `wget` to download the `.deb` package directly to your Kali system. Open a terminal and run:

```
https://www.tenable.com/downloads/api/v1/public/pages/nessus/downloads/12010/download?i_agree_to_tenable_license_agreement=true -O nessus.deb
```

Step 2: Install Nessus

Once you have downloaded the `.deb` file, install Nessus using `dpkg`:

```
sudo dpkg -i nessus.deb
```

This will install Nessus on Kali Linux. If there are any missing dependencies, you can fix them by running:

```
sudo apt --fix-broken install
```

Step 3: Start Nessus Service

To start the Nessus service, use the following command:

```
sudo systemctl start nessusd.service
```

You can check the status of the Nessus service with:

```
sudo systemctl status nessusd.service
```

Step 4: Open Nessus in Browser

Nessus runs a web server that you can access via your browser. Open a browser on your Kali machine and go to:

<https://localhost:8834>

This will take you to the Nessus web interface. You might see a warning about the self-signed SSL certificate, but you can safely ignore it.

Step 5: Configure Nessus

1. **Sign up for a Nessus Account:** You will need to create a Tenable account to get an activation code for Nessus. After creating an account, you can get your activation code from the Tenable website.
 2. **Enter Activation Code:** Once you have the activation code, enter it in the web interface to start the Nessus setup.
 3. **Choose the Version:** Nessus has a free version (Nessus Essentials) and a commercial version. If you are using the free version, select Nessus Essentials.
-

2. Running Vulnerability Scans with Nessus

After you've set up Nessus, you can start scanning for vulnerabilities on your network or specific devices. Here's how to perform a basic scan:

Step 1: Create a New Scan

1. Log in to Nessus Web Interface using your browser and credentials.
2. In the Nessus dashboard, click on "New Scan".

Step 2: Choose a Scan Type

Nessus offers various scan types, such as:

- **Basic Network Scan:** Scans for common vulnerabilities on a specified range of IP addresses.
- **Advanced Scan:** A more customizable scan, allowing you to configure detailed scan parameters.
- **Web Application Scan:** Specifically designed to detect vulnerabilities in web applications.

For now, let's go with a Basic Network Scan.

1. Select "Basic Network Scan".
2. Enter a Name for your scan (e.g., "Network Scan").
3. Under Targets, enter the IP range or domain of the network or device you want to scan. Example:
 - 192.168.1.1-192.168.1.254 (for a whole subnet).
 - 192.168.1.10 (for a specific host).
4. Set up Credentials (optional, but recommended) for deeper scans (especially for authenticated scans that need login credentials).

Step 3: Configure Scan Settings (Optional)

You can customize your scan settings under the Settings tab. Some of the key options include:

- **Scan Type:** Choose between a full scan or a quick scan.
- **Port Scanning:** You can adjust which ports to scan.
- **Vulnerability Families:** You can configure which types of vulnerabilities to search for (e.g., Web Servers, Operating Systems, etc.).

Once you're happy with the settings, click on Save.

Step 4: Run the Scan

After configuring your scan, you'll see the new scan listed in the Nessus dashboard. To start the scan:

1. Click on your newly created scan.
2. Click the "Launch" button to start scanning.

Nessus will begin scanning the target IP range or host for known vulnerabilities. It will check for issues such as:

- Open ports
- Misconfigurations
- Outdated software versions
- Known CVEs (Common Vulnerabilities and Exposures)

Step 5: View Results

Once the scan is complete, you can view the results in the Nessus dashboard:

- **Severity Levels:** Nessus classifies vulnerabilities by severity: Critical, High, Medium, Low, or Information.
- **Detailed Report:** You can view details of each vulnerability, including a description, CVE number, affected software versions, and remediation steps.
- **Export Results:** You can export the results in formats such as PDF, CSV, or HTML for reporting purposes.

3. Scan with Nmap (Optional)

If you prefer to use Nmap for scanning and vulnerability detection, you can install Nmap on Kali Linux and use it in combination with Nessus.

Install Nmap:

Nmap is pre-installed on Kali Linux, but if you need to install it manually, use:

```
sudo apt install nmap
```

Run Nmap Scan:

To scan for open ports or services on a target, use Nmap. For example:

```
nmap -sV -p 1-65535 192.168.1.1
```

This scans the target (192.168.1.1) for open ports from 1-65535 and detects the version of the services running on those ports.

You can also use the Nmap + Nessus Integration feature, where Nessus can run an Nmap scan automatically as part of its vulnerability scanning.

4. Using ISO Kali Linux for Vulnerability Scanning

If you are using a Kali Linux ISO (live USB or virtual machine) to run Nessus, the installation process for Nessus is exactly the same as in the steps above. Simply install Nessus on the live Kali system, configure it, and start scanning.

You can also use Nessus plugins on Kali for network mapping, vulnerability assessment, and reporting. By integrating tools like Metasploit (which is pre-installed in Kali), you can perform penetration testing after identifying vulnerabilities using Nessus.