**TASK 3:** Perform a Basic Vulnerability Scan on your PC

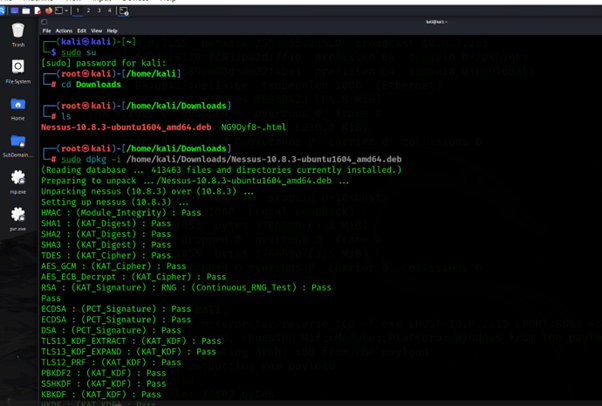
**Nessus** is a widely used vulnerability scanner developed by Tenable, designed to identify security weaknesses in computer systems, networks, and applications. It helps organizations detect potential vulnerabilities such as outdated software, misconfigurations, missing patches, and other security risks that could be exploited by attackers.

**Step-by-Step Guide to Configuring and Running a Network Scan in Nessus**

**1. Access Nessus Web Interface**

• **Start Nessus:** Ensure that Nessus is running on your machine or server. Typically, Nessus runs as a service, and you can access its web interface by navigating to https://<Nessus\_Server\_IP>:8834/ in a web

• **Login:** Once you open the Nessus web interface, log in with your username and password. If you’re using Nessus Essentials for the first time, you may be prompted to activate your license.



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a login screen

AI-generated content may be incorrect.

**2. Configure a New Scan**

Once logged in, you can configure a scan.

• **Go to the "Scans" Tab:** This is where all your scans are listed.

• **Click "New Scan":** In the upper-right corner of the screen, click on the “New Scan” button. This will open a list of available scan templates.

A screenshot of a computer

AI-generated content may be incorrect.**3. Choose a Scan Template**

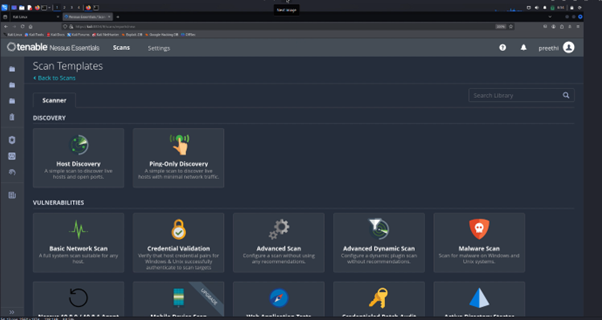
Nessus provides various scan templates, each designed for specific use cases. The most common for a network scan are:

• **Basic Network Scan:** This is used for general network vulnerability scanning.

• **Advanced Scan:** Offers more flexibility and detailed configuration options.

• **Web Application Tests:** Designed specifically for web application vulnerability assessments.

For a general network scan, select Basic Network Scan.



**4. Configure Scan Settings**

Now, configure the scan settings according to your network scan needs.

• **Name the Scan:** Provide a meaningful name for the scan. For example, "Network Scan – Internal Network".

• **Description (Optional):** You can add a brief description for easier reference.

**Target Settings**

• Targets: In the "Targets" section, enter the IP address range, hostname(s), or CIDR block you want to scan. For example:

o A specific IP: 192.168.1.10

o A range of IPs: 192.168.1.10-50

o A network block: 192.168.1.0/24

• If you're scanning multiple subnets or a more complex network, you can add more targets by separating them with commas.

Scan Credentials (Optional but Recommended)

• Credentialed Scans: If you want to perform a more thorough scan (credentialed), you can configure the scan to use SSH (Linux/Unix) or Windows Credentials. This allows Nessus to log into the target systems and run a deeper scan, checking for vulnerabilities that may only be visible with privileged access.

o Windows Credentials: Provide the username, password, and domain if applicable.

o SSH Credentials: Provide the SSH username and password (or private key).

Port Scanning Options:

• Nessus automatically scans a range of ports, but you can specify custom ports if needed under the Port Scanning section.

• You can choose between All Ports, Common Ports, or specify a Custom Port Range.

**5. Configure Advanced Scan Settings**

Click the Advanced tab for additional configuration options, if necessary:

• Scan Options: You can adjust the scanning options such as Performance Tuning to balance between scan speed and system load.

• Scan Policies: Customize the scan by enabling or disabling certain checks (for example, web application security checks, compliance audits, etc.).

• Plugin Preferences: Enable or disable specific plugins based on the vulnerabilities you want to focus on.

**6. Save the Scan Configuration**

After configuring the scan, click the Save button in the bottom-right corner to save your scan configuration.

**7. Run the Scan**

• Start the Scan: Once the scan is saved, you will return to the main Scans tab, where you should see your newly created scan listed.

• Launch the Scan: Click the Launch button (a play icon) next to your scan to start the scanning process.

• Monitor the Scan: The status of the scan will be displayed in real-time. Nessus will show progress such as "Scanning", "Finished", and any issues it encounters during the scan.

**8. View Scan Results**

Once the scan completes, you can view the results by clicking on the scan name in the Scans tab.

• Severity Levels: Results will be categorized into severity levels (Critical, High, Medium, Low, Informational), helping you prioritize vulnerabilities.

• Detailed Information: Each finding will provide detailed information, including the type of vulnerability, affected system(s), risk level, and remediation recommendations.

• Export Reports: You can export the scan results in various formats (HTML, PDF, CSV) for further analysis or to share with stakeholders.

**9. Remediation Actions**

After analyzing the scan results, you can:

• Patch Vulnerabilities: Apply patches for critical or high severity vulnerabilities.

• Fix Configuration Issues: Remediate misconfigurations identified in the scan (e.g., disable unnecessary services, update software versions).

• Perform Additional Scans: Run additional scans after remediation to verify that the vulnerabilities have been fixed.

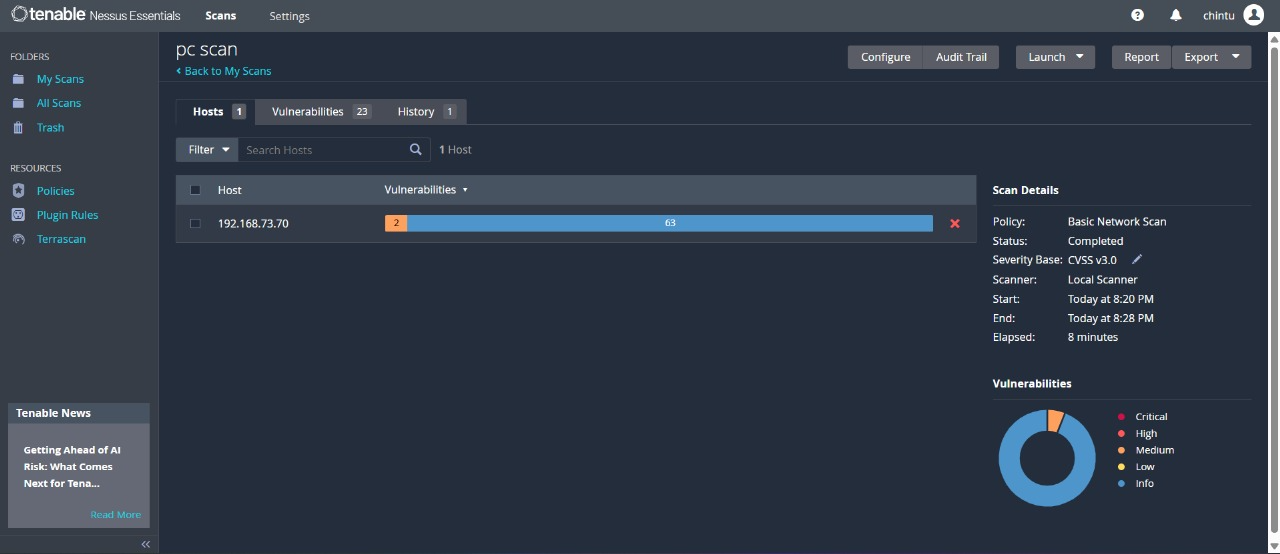
**10. Set up Scheduled Scans**

If you need to run this scan regularly (e.g., daily, weekly, or monthly), you can schedule it:

• Go to your saved scan.

• Click the Schedule button (clock icon).

• Set the frequency and time for the scan to run automatically.



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* Nessus scan results categorize vulnerabilities based on severity levels, which help prioritize remediation efforts. These levels are based on the risk a vulnerability poses to the system, from low-impact issues to critical threats. Here's how each severity level is typically interpreted:

