

Forum:[Hack Forums](#)

Thread: [What Is Nessus and How Do You Use It for Ethical Hacking?](#)

JoseMar - January 22, 2025, 6:06 am

What Is Nessus and How Do You Use It for Ethical Hacking?

Nessus, developed by Tenable, is one of the most incredible scanning tools for vulnerabilities that one may come across. It assists security experts in determining the gaps, misconfigurations and risks that exist in the application systems, networks, or any other application. It is an invaluable tool for ethical hackers and pen-testers as well as IT security personnel intending to secure proactively their infrastructure.

What's More Important With Nessus?

What brings Nessus to the spotlight is its extensive vulnerability structure, its flexibility, and of course, its ease of use. It can scan different kinds of systems such as servers, network devices, databases, and even web applications. Heuristic scans can be performed using plugins offering broad range of detection and these plugins are updated regularly to cover the latest threats. People who use these can also scan and search for old and weak software, report services that are misconfigured and -886489833167559017find weak and outdated passwords.

How to Use Nessus for Ethical Hacking

While the use of Nessus is relatively straightforward, it is important to adequately comprehend the environment you are targeting and what you are hoping to achieve. This article serves as a guide to help you get started:

Step 1: Installing Nessus

Nessus is compatible with Windows, Linux, and macOS, and it can be found on the Tenable website. When it has been downloaded and saved, follow the instructions to install it. Once the installation is complete, remember to activate Nessus to utilize the features, using the provided key: (#Nessus_Essentials - a free version is to be used for personal use.)

Step 2: Set Up Your Scan

1: Log in to Nessus: Open your browser and navigate to the Nessus web interface (usually <https://localhost:8834>).

2: Create a New Scan:

Select "New Scan" on the screen.

Select one of the scan templates that suits your needs, for example:

Basic Network Scan: This is good for most general purpose vulnerability scans.

Web Application Tests: For web applications, generally for vulnerabilities scans.

Step 3: Running the New Scan

After the configurations have been completed, press launch, this will initiate Nessus to begin the scan within the target system. This can take anywhere from a few minutes to several hours based on the size of the network, therefore, keep in mind this is quite a time consuming process.

Step 4: Results Interpretation

Now that the scan has been fully completed, Nessus is going to produce an in depth report, and based on the standard where these scan are always reported, it includes:

Vulnerable Results: This report covers everything that has worked on a discovered vulnerability, arranged in order of decreasing rank (Critical, High, Medium, Low).

Remediation Steps: Suggestions for anything touching the problem.

Risk Scores: CVSS score explaining weakness severity for easy fixes.

As an example, the server would be vulnerable if Nessus shows that an obsolete version of Apache is being used. The recommended update is to the last version.

Step 5: Take Action

You can achieve the maximum worth of Nessus by focusing on how the results are utilized. Make sure to disseminate the report for the context of your team. Make sure you focus on the most critical vulnerabilities and implement the recommended changes. Ensure that you regularly scan your systems for safety purposes and to capture newer vulnerabilities.

Nessus in Use:

Example 1: Scanning Web Server

Imagine you have been given the task of securing a company's webserver. So you conduct a Nessus scan, and you find the following:

There is an unsupported version of OpenSSL (High) running on the server.

Port 22 (SSH) is enabled to the world and has weak passwords.

Nessus gives you detailed steps like change OpenSSL and change the password policy to sophisticated ones. Now you can set up fixing coordination with the IT team.

Example 2: Network Audit

You are requested to conduct an audit for a small office network. Conducting a network scan using Nessus over all the IPs reveals that:

Many devices have not been updated with important security patches.

A printer using an easily guessable password for a default administrator account is open to attackers.

With this information, you will change the print password and patch the devices improving security over the network significantly.

Why Nessus is Essential for Ethical Hackers

Nessus is more than just a scanner, it's a proactive tool for staying ahead of cyber threats. By identifying vulnerabilities before attackers do, you can:

- Prevent data breaches.

- Comply with security regulations (e.g., GDPR, HIPAA).

- Build trust with clients by demonstrating a commitment to security.

Tips for Using Nessus Effectively

- Stay Updated:** Regularly update Nessus plugins to detect the latest vulnerabilities.

- Use Credentialed Scans:** Provide Nessus with login credentials to perform deeper, more accurate scans.

- Schedule Scans:** Set up automated scans to run at regular intervals.

- Combine with Other Tools:** Use Nessus alongside tools like Metasploit or Burp Suite for a more comprehensive security assessment.

Conclusion

Nessus is a very good tool for ethical hackers and security professionals. Its ability to identify vulnerabilities, provide actionable insights, and help secure systems makes it a cornerstone of modern, but keep in mind, if you dig a little deeper, you'll discover even more powerful tools that can take your ethical hacking skills to the next level. The world of cybersecurity is vast, and there's always something new to learn and explore!