Top 7 Free Server Security Testing Tools - Protect Your System More Effectively

With the increase in external and internal threats, using security testing tools is essential to ensure the safety of your data and systems. In this article, we will explore the Top 7 Free Server Security Testing Tools that you can apply today to

Nmap

Nmap (Network Mapper) is one of the most popular network scanning tools available today. It is widely used by security professionals and system administrators to discover active hosts and services on a network.

Nmap provides many useful features that help users easily identify network structures. One of the most prominent features of Nmap is the ability to scan network ports. Through this, it can identify the services running on each port and remove unnecessary services.

In addition to port scanning, Nmap also supports OS detection. This means you can see what operating system is running on the host you are scanning. This feature is extremely useful when you want to find out about security vulnerabilities that may exist on a specific version of the operating system.

OpenVAS

OpenVAS (Open Vulnerability Assessment System) is a powerful and completely free vulnerability testing platform. It is an ideal tool for performing comprehensive security scans.

OpenVAS provides a very powerful vulnerability scanning capability, allowing users to detect many different types of vulnerabilities on servers and applications. One of the strengths of OpenVAS is that it regularly updates its vulnerability database, keeping users up to date with the latest threats.

OpenVAS's reporting system is also very detailed. Once the scan is complete, it generates a full report of the vulnerabilities it found, along with instructions on how to fix them. This makes it easy for administrators to take the necessary remediation measures.

Burp Suite Community Edition

Burp Suite Community Edition is a popular web application security testing tool that helps developers and security professionals find vulnerabilities in web applications.

Burp Suite comes with many powerful tools like Proxy Intercepting, Scanner, Intruder and Repeater. This allows you to directly interact with requests and responses between the browser and the web application, thereby finding security vulnerabilities.

The Proxy Intercepting feature allows you to view and modify HTTP/HTTPS requests before they are sent to the server. This is useful for testing common vulnerabilities such as SQL Injection or Cross-Site Scripting (XSS).

Nikto

Nikto is a web server scanner that helps detect common security issues. It is designed to test web servers for misconfigurations, security vulnerabilities, and other issues that could compromise security.

Nikto supports a wide range of security scanning issues, including checking web server software versions, identifying unsafe files and folders, and detecting server configuration errors. In particular, Nikto uses a large database to check for millions of security vulnerabilities, helping you quickly identify weaknesses.

Since Nikto is an open source tool, you can customize it to your needs by adding plugins or changing scanning parameters.

OWASP ZAP

OWASP ZAP (Zed Attack Proxy) is an open source project that aims to make web application security testing easy and efficient. This tool is suitable for both beginners and security experts.

One of the key features of OWASP ZAP is its automated scanning feature. You simply specify the URL of the web application you want to test, and ZAP will automatically scan and detect security vulnerabilities.

In addition, ZAP also supports many features such as Proxy, Scanner, Fuzzer and Passive Scanning. These features help you to examine your application more deeply and detect vulnerabilities that other tools may miss.

Acunetix Free Edition

Acunetix Free Edition is a web security testing tool with a free version. While the free version has some limitations in features, it still provides enough tools for you to perform basic tests.

Acunetix stands out for its ability to quickly scan and detect various types of vulnerabilities such as SQL Injection, XSS and many other common security issues. The user-friendly graphical interface makes it easy to operate and monitor the scanning process.

Additionally, Acunetix also provides detailed reports of detected security issues, making it easy for you to take necessary remediation measures.

Metasploit Community

Metasploit Community is a penetration testing platform that allows users to find and exploit security vulnerabilities. It is an indispensable tool in any security professional's toolkit.

Metasploit provides a large collection of exploits and payloads, making it easy for users to test security vulnerabilities in the system. With a friendly user interface, you can easily search and select the exploits you want to use.

The software also supports a variety of attack options, from simple attacks to more complex ones. This gives you a better understanding of how security vulnerabilities work and how they can be exploited.

Conclude

Above are the Top 7 Free Server Security Testing Tools that you can apply to protect your system. Each tool has its own advantages and disadvantages, so you should choose based on your needs and usability.

Hopefully this article will help you gain a better understanding of the security testing tools available and guide you in applying them most effectively. Remember, security is not just a task but a continuous process.