**Top 5 software security testing tools**

* + Astra pentest platform
  + Nmap
  + Wireshark
  + openVAS
  + Metasploit

**Introduction**

There are certain things that make a software security testing tool better than others.

| **SecurityTesting Tools** | **Key Features** |
| --- | --- |
| [Astra Pentest Platform](https://www.getastra.com/blog/security-audit/software-security-testing-tools/#astra) | Continuous pentesting, CI/CD integration, scan behind login, cloud pentest |
| [NMap](https://www.getastra.com/blog/security-audit/software-security-testing-tools/#nmap) | Network exploration, port scanning, network mapping |
| [WireShark](https://www.getastra.com/blog/security-audit/software-security-testing-tools/#wireshark) | Packet analyzer, network troubleshooting, protocol analysis |
| [OpenVAS](https://www.getastra.com/blog/security-audit/software-security-testing-tools/#openvas) | Vulnerability scanning |
| [Metasploit](https://www.getastra.com/blog/security-audit/software-security-testing-tools/#metasploit) | Helps you write, test, and execute exploit code |

### 1. Astra Security

**Astra’s solution is a solution that helps you to identify the security gaps in your network and helps you in plugging the holes.**

The Astra Network Security Solution is the most comprehensive solution to perform a complete network security assessment. The solution scans and checks your network to identify the network devices, network ports, and network protocols to find out the vulnerabilities in your network and help you fix the vulnerabilities in a timely manner.

**2. NMAP**

Nmap, is an open-source utility for network exploration, security auditing, and network discovery. It was designed to rapidly scan large networks, although it works fine against single hosts.

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

While Nmap was developed for UNIX-based operating systems, it also runs on Windows, and there are also versions available for most other major operating systems.

**3. Wireshark**

[**Wireshark**](https://www.wireshark.org/) is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark can be used to capture and interactively browse the contents of network traffic.

Wireshark is also commonly used to analyze data from a trace file, generally in the form of a pcap (the file format of libpcap). Wireshark has a GUI and comes in both 32-bit and 64-bit versions.

**4. OpenVAS**

[**OpenVAS**](https://www.openvas.org/) is a vulnerability scanner that can perform a complete vulnerability scan of the network infrastructure. OpenVAS is an international project that is used by many organizations all over the world. It is available for free and can be used with commercial products.

OpenVAS tool is owned by Green bone and the paid solution is called Green bone Security feed while the free one is called Green bone Community feed.

**5. Metasploit**

The [**Metasploit**](https://www.metasploit.com/) Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is open-source, free, and available to the public.

The project provides information about security vulnerabilities used by penetration testers during security audits and network administrators to ensure the correct configuration of the network’s devices.