**17 Best Vulnerability Assessment Scanning Tools**

March 23, 2020

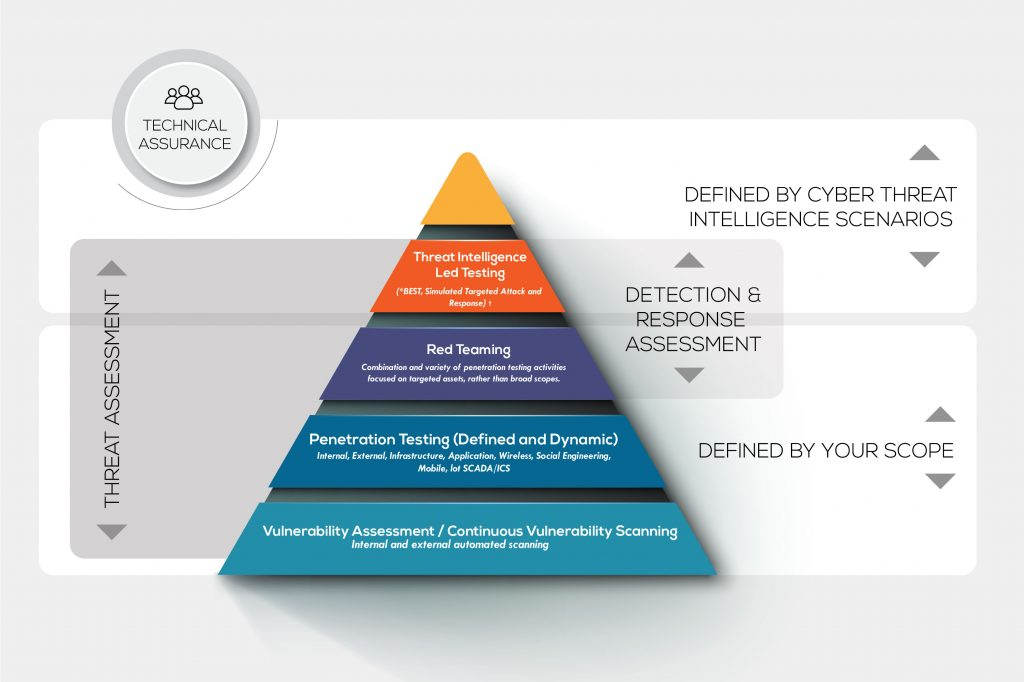
|In [Security Strategy](https://phoenixnap.com/blog/category/security-strategy), [Data Protection](https://phoenixnap.com/blog/category/data-protection)

|By [Mona Mangat](https://phoenixnap.com/blog/author/mona)

1. [Home](https://phoenixnap.com/blog/)
2. [Security Strategy](https://phoenixnap.com/blog/category/security-strategy)
3. 17 Best Vulnerability Assessment Scanning Tools

Vulnerability scanning or vulnerability assessment is a systematic process of finding security loopholes in any system addressing the potential  vulnerabilities.

The purpose of [vulnerability assessments](https://phoenixnap.com/blog/vulnerability-assessment) is to prevent the possibility of unauthorized access to systems.  Vulnerability testing preserves the confidentiality, integrity, and  availability of the system. The system refers to any computers,  networks, network devices, software, web application, cloud computing,  etc.



**Types of Vulnerability Scanners**

Vulnerability scanners have their ways of doing jobs. We can classify the vulnerability scanners into four types based on how they operate.

**Cloud-Based Vulnerability Scanners**

Used to find vulnerabilities within cloud-based systems such as web applications, WordPress, and Joomla.

**Host-Based Vulnerability Scanners**

Used to find vulnerabilities on a single host or system such as an  individual computer or a network device like a switch or core-router.

**Network-Based Vulnerability Scanners**

Used to find vulnerabilities in an internal network by scanning for  open ports. Services running on open ports determined whether  vulnerabilities exist or not with the help of the tool.

**Database-Based Vulnerability Scanners**

Used to find vulnerabilities in database management systems.  Databases are the backbone of any system storing sensitive information.  Vulnerability scanning is performed on database systems to [prevent attacks like SQL Injection](https://phoenixnap.com/blog/what-is-sql-injection).

****

**Vulnerability Scanning Tools**

Vulnerability scanning tools allow for the detection of  vulnerabilities in applications using many ways. Code analysis  vulnerability tools analyze coding bugs. Audit vulnerability tools can  find well-known rootkits, backdoor, and trojans.

There are many vulnerability scanners available in the market. They  can be free, paid, or open-source. Most of the free and open-source  tools are available on GitHub. Deciding which tool to use depends on a  few factors such as vulnerability type, budget, frequency of how often  the tool is updated, etc.

**1. Nikto2**

[Nikto2](https://cirt.net/Nikto2) is an open-source vulnerability scanning software that focuses on web  application security. Nikto2 can find around 6700 dangerous files  causing issues to web servers and report outdated servers based  versions. On top of that, Nikto2 can alert on server configuration  issues and perform web server scans within a minimal time.  
 Nikto2 doesn’t offer any countermeasures for vulnerabilities found nor  provide risk assessment features. However, Nikto2 is a frequently  updated tool that enables a broader coverage of vulnerabilities.

**2. Netsparker**

[Netsparker](https://www.netsparker.com/) is another web application vulnerability tool with an automation  feature available to find vulnerabilities. This tool is also capable of  finding vulnerabilities in thousands of web applications within a few  hours.  
 Although it is a paid enterprise-level vulnerability tool, it has many  advanced features.  It has crawling technology that finds  vulnerabilities by crawling into the application. Netsparker can  describe and suggest mitigation techniques for vulnerabilities found.  Also, security solutions for advanced vulnerability assessment are  available.

**3. OpenVAS**

[OpenVAS](https://www.openvas.org/) is a powerful vulnerability scanning tool that supports large-scale  scans which are suitable for organizations. You can use this tool for  finding vulnerabilities not only in the web application or web servers  but also in databases, operating systems, networks, and virtual  machines.  
 OpenVAS receives updates daily, which broadens the vulnerability  detection coverage. It also helps in risk assessment and suggests  countermeasures for the vulnerabilities detected.

**4. W3AF**

[W3AF](http://w3af.org/) is a  free and open-source tool known as Web Application Attack and  Framework. This tool is an open-source vulnerability scanning tool for  web applications. It creates a framework which helps to secure the web  application by finding and exploiting the vulnerabilities. This tool is  known for user-friendliness. Along with vulnerability scanning options,  W3AF has exploitation facilities used for penetration testing work as  well.  
 Moreover, W3AF covers a high-broaden collection of vulnerabilities.  Domains that are attacked frequently, especially with newly identified  vulnerabilities, can select this tool.

**5. Arachni**

[Arachni](https://www.arachni-scanner.com/) is also a dedicated vulnerability tool for web applications. This tool  covers a variety of vulnerabilities and is updated regularly. Arachni  provides facilities for risk assessment as well as suggests tips and  countermeasures for vulnerabilities found.  
 Arachni is a free and open-source vulnerability tool that supports  Linux, Windows, and macOS. Arachni also assists in penetration testing  by its ability to cope up with newly identified vulnerabilities.

**6. Acunetix**

[Acunetix](https://www.acunetix.com/) is a paid web application security scanner (open-source version also  available) with many functionalities provided. Around 6500  vulnerabilities scanning range is available with this tool. In addition  to web applications, it can also find vulnerabilities in the network as  well.  
 Acunetix provides the ability to automate your scan. Suitable for large  scale organizations as it can handle many devices. HSBC, NASA, USA Air  force are few industrial giants who use Arachni for vulnerability tests.

**7. Nmap**

[Nmap](https://nmap.org/) is one of the well-known free and open-source network scanning tools  among many security professionals. Nmap uses the probing technique to  discover hosts in the network and for operating system discovery.  
 This feature helps in detecting vulnerabilities in single or multiple  networks. If you are new or learning with vulnerabilities scanning, then Nmap is a good start.

**8. OpenSCAP**

[OpenSCAP](https://www.open-scap.org/) is a framework of tools that assist in vulnerability scanning,  vulnerability assessment, vulnerability measurement, creating security  measures. OpenSCAP is a free and open-source tool developed by  communities. OpenSCAP only supports Linux platforms.  
 OpenSCAP framework supports vulnerability scanning on web applications,  web servers, databases, operating systems, networks, and virtual  machines. Moreover, they provide a facility for risk assessment and  support to counteract threats.

**9. GoLismero**

[GoLismero](http://www.golismero.com/) is a free and open-source tool used for vulnerability scanning.  GoLismero focuses on finding vulnerabilities on web applications but  also can scan for vulnerabilities in the network as well. GoLismero is a convenient tool that works with results provided by other vulnerability tools such as OpenVAS, then combines the results and provides feedback.  
 GoLismero covers a wide range of vulnerabilities, including database and network vulnerabilities. Also, GoLismero facilitates countermeasures  for vulnerabilities found.

**10. Intruder**

[Intruder](https://www.intruder.io/) is a paid vulnerability scanner specifically designed to scan  cloud-based storage. Intruder software starts to scan immediately after a vulnerability is released. The scanning mechanism in Intruder is  automated and constantly monitors for vulnerabilities.  
 Intruder is suitable for enterprise-level vulnerability scanning as it  can manage many devices. In addition to monitoring cloud-storage,  Intruder can help identify network vulnerabilities as well as provide  quality reporting and suggestions.

**11. Comodo HackerProof**

With [Comodo Hackerproof](https://www.comodo.com/hackerproof) you will be able to reduce cart abandonment, perform daily  vulnerability scanning, and use the included PCI scanning tools. You can also utilize the drive-by attack prevention feature and build valuable  trust with your visitors. Thanks to the benefit of Comodo Hackerproof,  many businesses can convert more visitors into buyers.

Buyers tend to feel safer when making a transaction with your  business, and you should find that this drives your revenue up. With the patent-pending scanning technology, SiteInspector, you will enjoy a new level of security.

**12. Aircrack**

Aircrack also is known as [Aircrack-NG](https://www.aircrack-ng.org/), is a set of tools used for assessing the WiFi network security. These  tools can also be utilized in network auditing, and support multiple  OS’s such as Linux, OS X, Solaris, NetBSD, Windows, and more.

The tool will focus on different areas of WiFi security, such as  monitoring the packets and data, testing drivers and cards, cracking,  replying to attacks, etc. This tool allows you to retrieve the lost keys by capturing the data packets.

**13. Retina CS Community**

[Retina CS Community](https://www.beyondtrust.com/docs/archive/vulnerability-management/documents/6-2-0/retina-community-users-guide.pdf) is an open-source web-based console that will enable you to make a more centralized and straightforward vulnerability management system. Retina CS Community has features like compliance reporting, patching, and  configuration compliance, and because of this, you can perform an  assessment of cross-platform vulnerability.

The tool is excellent for saving time, cost, and effort when it comes to managing your network security. It features an automated  vulnerability assessment for DBs, web applications, workstations, and  servers. Businesses and organizations will get complete support for  virtual environments with things like virtual app scanning and vCenter  integration.

**14. Microsoft Baseline Security Analyzer (MBSA)**

An entirely free vulnerability scanner created by Microsoft, it’s  used for testing your Windows server or windows computer for  vulnerabilities. The [Microsoft Baseline Security Analyzer](https://www.microsoft.com/en-us/download/details.aspx?id=19892) has several vital features, including scanning your network service  packets, checking for security updates or other windows updates, and  more. It is the ideal tool for Windows users.

It’s excellent for helping you to identify missing updates or  security patches. Use the tool to install new security updates on your  computer. Small to medium-sized businesses find the tool most useful,  and it helps save the security department money with its features. You  won’t need to consult a security expert to resolve the vulnerabilities  that the tool finds.

**15. Nexpose**

[Nexpose](https://www.rapid7.com/products/nexpose/) is an open-source tool that you can use for no cost. Security experts  regularly use this tool for vulnerability scanning. All the new  vulnerabilities are included in the Nexpose database thanks to the  Github community. You can use this tool with the Metasploit Framework,  and you can rely on it to provide a detailed scanning of your web  application. Before generating the report, it will take various elements into account.

Vulnerabilities are categorized by the tool according to their risk  level and ranked from low to high. It’s capable of scanning new devices, so your network remains secure. Nexpose is updated each week, so you  know it will find the latest hazards.

**16. Nessus Professional**

[Nessus](https://www.tenable.com/products/nessus/nessus-professional) is a branded and patented vulnerability scanner created by Tenable  Network Security. Nessus will prevent the networks from attempts made by hackers, and it can scan the vulnerabilities that permit remote hacking of sensitive data.

The tool offers an extensive range of OS, Dbs, applications, and  several other devices among cloud infrastructure, virtual and physical  networks. Millions of users trust Nessus for their vulnerability  assessment and configuration issues.

**17. SolarWinds Network Configuration Manager**

[SolarWinds Network Configuration Manager](https://www.solarwinds.com/network-configuration-manager) has consistently received high praise from users. The vulnerability  assessment tool features that it includes addresses a specific type of  vulnerability that many other options do not, such as misconfigured  networking equipment. This feature sets it apart from the rest. The  primary utility as a vulnerability scanning tool is in the validation of network equipment configurations for errors and omissions. It can also  be used to check device configurations for changes periodically.

It integrates with the National Vulnerability Database and has access to the most current CVE’s to identify vulnerabilities in your Cisco  devices. It will work with any Cisco device running ASA, IOS, or Nexus  OS.

**Vulnerability Assessment Secures Your Network**

If an attack starts by modifying device networking configuration, the tools will be able to identify and put a stop to it. They assist you  with regulatory compliance with their ability to detect out-of-process  changes, audit configurations, and even correct violations.

To implement a vulnerability assessment, you should follow a systematic process as the one outlined below.

**Step 1** – Begin the process by documenting, deciding what tool/tools to use, obtain the necessary permission from stakeholders.

**Step 2** – Perform vulnerability scanning using the relevant tools. Make sure to save all the outputs from those vulnerability tools.

**Step 3** – Analyse the output and decide which  vulnerabilities identified could be a possible threat. You can also  prioritize the threats and find a strategy to mitigate them.

**Step 4** – Make sure you document all the outcomes and prepare reports for stakeholders.

**Step 5** – Fix the vulnerabilities identified.

****

**Advantages of Scanning for Vulnerabilities**

Vulnerability scanning keeps systems secure from external threats. Other benefits include:

* Affordable – Many vulnerability scanners are available free of charge.
* Quick – Assessment takes a few hours to complete.
* Automate – can use automated functions available in the  vulnerability tools to perform scans regularly without manual  involvement.
* Performance – vulnerability scanners perform almost all the well-known vulnerability scan.
* Cost/Benefit – reduce cost and increase benefits by optimizing security threats.

**Vulnerability Testing Decreases Risk**

Whichever vulnerability tool you decide to use, choosing the ideal  one will depend on security requirements and the ability to analyze your systems. Identify and deal with security vulnerabilities before it’s  too late.

Take this opportunity now to look into the features provided by each  of the tools mentioned, and select one that’s suitable for you. If you  need help, reach out to one of our experts today [for a consultation](https://phoenixnap.com/contact-us#get-a-quote).

Learn about more of [the best networking tools](https://phoenixnap.com/blog/best-network-security-tools) to improve your overall security.