[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@bd14ebecda6f42e7b64647ed82799469?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

reference <https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/>

**Best Vulnerability Scanner Tools for 2021**

[Drew Robb](https://www.esecurityplanet.com/author/drew-robb-esp/)

May 21, 2021

[Vulnerability scanning](https://www.esecurityplanet.com/networks/s/vulnerability-scanning-what-it-is-and-how-to-do-it-right/), [assessment](https://www.esecurityplanet.com/networks/s/how-to-conduct-a-vulnerability-assessment-steps-toward-better-cybersecurity/) and management all share a fundamental cybersecurity principle: the bad guys can’t get in if they don’t have a way. To that end, an essential  IT security practice is to scan for vulnerabilities and then patch them, typically via a [patch management system](https://www.esecurityplanet.com/networks/-security/patch-management.html).

Vulnerability scanning tools can make that process easier  by finding and even patching vulnerabilities for you, reducing burden on security staff and operations centers. Vulnerability scanners detect  and classify system weaknesses to prioritize fixes and sometimes predict the effectiveness of countermeasures. Scans can be performed by the IT  department or via a service provider. Typically, the scan compares the  details of the target attack surface to a database of information about  known security holes in services and ports, as well as anomalies in  packet construction, and paths that may exist to exploitable programs or scripts.

Some scans are done by logging in as an authorized user  while others are done externally and attempt to find holes that may be  exploitable by those operating outside the network. Vulnerability  scanning should not be confused with [penetration testing](https://www.esecurityplanet.com/networks/-security/penetration-testing.html), which is about exploiting vulnerabilities rather than indicating where potential vulnerabilities may lie. [Vulnerability management](https://www.esecurityplanet.com/products/vulnerability-management-software/) is a broader product that incorporates vulnerability scanning capabilities, and a complementary technology is [breach and attack simulation](https://www.esecurityplanet.com/threats/breach-and-attack-simulation-find-vulnerabilities-before-the-bad-guys-do/), which allows for continuous automated vulnerability assessment.

**Best Vulnerability Scanner Tools**

* [Qualys Vulnerability Management](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#qualys)
* [AT&T Cybersecurity](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#att)
* [Tenable Nessus](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#nessus)
* [Alibaba Cloud Managed Security Service](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#alibaba)
* [Netsparker](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#netsparker)
* [Amazon Inspector](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#aws)
* [Burp Suite](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#burp)
* [Acunetix Vulnerability Scanner](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#acunetix)
* [Intruder](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#intruder)
* [Metasploit](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#metasploit)
* [Nmap](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#nmap)
* [IBM Security QRadar](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#qradar)
* [Rapid7 InsightVM (Nexpose)](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#rapid7)

**Qualys Vulnerability Management**

The Qualys Vulnerability Management scanner operates behind the firewall in complex internal networks, can scan cloud environments  and can also detect vulnerabilities on geographically distributed  networks at the perimeter. In addition, it scans containers and  endpoints.

Its intuitive and customizable dashboard provides a unified view of all web apps and assets being monitored. Pricing may be higher  than some other services but the breadth of protection it offers is  extensive.

**AT&T Cybersecurity**

The AT&T Cybersecurity Vulnerability Scanning Solution  can be delivered either as a managed service or run from within IT. It  helps detect security vulnerabilities in systems, web applications and  network devices.

The vulnerability scanner is part of a larger tool that also includes [SIEM](https://www.esecurityplanet.com/products/siem-tools/) and [intrusion detection](https://www.esecurityplanet.com/products/intrusion-detection-and-prevention-systems/). Known vulnerability signatures are updated continually as new  vulnerabilities are identified by AlienVault Labs and Open Threat  Exchange intelligence community.

It is probably best as a managed service for IT departments lacking cybersecurity expertise.

**Tenable Nessus**

Tenable [Nessus](https://www.esecurityplanet.com/products/nessus/) is a widely used, open source vulnerability assessment tool. It is  probably best for experienced security teams, as its interface can be a  little tricky to master at first. It can be used in conjunction with  penetration testing tools, providing them with areas to target and  potential weaknesses to exploit.

Nessus comes with pre-built policies and templates for  auditing and patching a variety of IT and mobile assets, customizable  reports and automatic offline vulnerability assessment.

**Alibaba Cloud Managed Security Service**

Alibaba offers a SaaS-based managed service for port  inspection, scans for web and system vulnerability, and a vulnerability  review to eliminate false positives. The service uses machine learning  to detect web vulnerabilities and backdoors, as well as illicit content  and website defacement to prevent reputation damage.

Alibaba makes the process easy by performing unlimited  scans without any installation, updates or maintenance required. It is  focused on the cloud and is probably best for non-U.S. businesses in  light of ongoing trade hostilities between the U.S. and China.

**Netsparker**

Netsparker is very good at what it does – the scanning of  websites. But it is not designed to do anything else and so lacks the  range of many other products. One plus is its ease of use. Its automated web application security scanning capabilities can also be integrated  with third-party tools.

Operators don’t need to be knowledgeable in source code. It’s a good choice for SMBs rather than large enterprises.

**Amazon Inspector**

If you are an AWS shop, then Amazon Inspector is the  automated security assessment service for you. It scans all applications deployed on AWS and can be extended to Amazon EC2 instances, too.

After vulnerability scans and assessments, it provides a  detailed list of potential vulnerabilities that are prioritized  according to the level of risk. It can also identify a lack of best  security practices in applications both while running and before they’re deployed.

Amazon Inspector can’t scan Azure, Google Cloud or  on-premises data centers and server rooms. Thus, it’s only recommended  for those enterprises and SMBs running mainly on the Amazon cloud.

**Burp Suite**

[Burp Suite](https://www.esecurityplanet.com/products/burp-scanner/) is a web vulnerability scanner used in a great many organizations.  Although there is a free version available, it is limited in  functionality, with no automation capabilities. Those wishing for the  complete package for enterprise-wide scalability and automation should  be prepared to pay well. Security professionals needing only a good  automated vulnerability scanner for testing of code can make do with the Professional version, which is cheaper.

Burp includes a power crawl engine that can crawl web apps  and find a wide range of vulnerabilities. It uses an advanced algorithm  for scanning dynamic content to better uncover more attack surfaces.

**Acunetix Vulnerability Scanner**

Acunetix is another tool that only scans web-based  applications. But its multi-threaded scanner can crawl across hundreds  of thousands of pages rapidly and it also identifies common web server  configuration issues. It is particularly good at scanning WordPress.  Therefore, those with a heavy WordPress deployment should consider it.

The Acunetix Vulnerability Scanner also includes other  integration with other helpful tools, such as Jenkins, Jira and GitHub.  It also boasts an impressively low false-positive rate.

**Intruder**

Intruder is a cloud-based proactive vulnerability scanner  that concentrates on perimeter scanning. Any deeper in the enterprise  and it needs to be supplemented by other tools. But it is strong at  discovering new vulnerabilities. Therefore, it’s a good choice for those looking to harden the perimeter.

It includes more than 10,000 memorable security checks, including WannaCry, Heartbleed and SQL Injection.

**Metasploit**

[Metasploit](https://www.esecurityplanet.com/products/metasploit/) covers the scanning and testing of vulnerabilities. Backed by a huge  open-source database of known exploits, it also provides IT with an  analysis of pen testing results so remediation steps can be done  efficiently. However, it doesn’t scale up to enterprise level and some  new users say it is difficult to use at first.

**Nmap**

[Nmap](https://www.esecurityplanet.com/products/nmap/) is a port scanner that also aids pen testing by flagging the best areas to target in an attack. That is useful for ethical hackers in  determining network weaknesses. As it’s open source, it’s free. That  makes it handy for those familiar with the open source world, but it may be a challenge for someone new to such applications. Although it runs  on all major OSes, Linux users will find it more familiar.

**IBM Security QRadar**

IBM Security is a world-leading cybersecurity provider and  QRadar lives up to the vendor’s reputation. After scanning a network and correlating the information with network topology and connection data,  it manages risk using a policy engine with automated [compliance](https://www.esecurityplanet.com/networks/s/security-compliance/) checks.

Its advanced analytics are a powerful tool for preventing  security breaches, prioritizing and performing remediation and  maintaining regulatory compliance. It also includes an intuitive  dashboard that consolidates all of this information into a single view.

**Rapid7 Nexpose**

Rapid7 Nexpose is a top-rated open source vulnerability  scanning solution. It’s able to automatically scan and assess physical,  cloud and virtual infrastructures. The tool provides live and  interactive dashboards, solution-based remediation and risk scoring and  prioritization.

Nexpose automatically detects and scans all new devices  connected to a network to provide real time vulnerability  identification. It also offers a lightweight endpoint agent for  processing information while consuming minimal bandwidth.

**What are vulnerability scanners?**

Vulnerability scanners are software that searches for,  identifies and assesses network and network resources for known  weaknesses. They discover and inventory all network access points and  connected devices, then compare the findings from the scans to known  vulnerabilities in a database. These tools are also capable of detecting anomalies in packet construction and paths that may exist to  exploitable programs or scripts.

**Key features of vulnerability scanners**

The key features of vulnerability scanning software can be  broken down into two primary groups, identification and correlation, as  well as evaluation.

**Identification and correlation**

Vulnerability scanners discover and classify devices, open  ports, operating systems and software connected to a network, then  correlate this information with the latest known vulnerabilities. They  can also detect misconfigurations and a lack of security controls and  policies.

**Evaluation**

After identifying a vulnerability, these tools also  evaluate and assess the level of risk for each one. They can also  perform root cause analysis to find the source of the issue. This  information informs which vulnerabilities to prioritize.

**External vs. internal vulnerability scanning**

External scans are run from outside the network perimeter  to identify vulnerabilities for servers and applications that are  accessible directly from the internet. Internal scans, on the other  hand, identify vulnerabilities that could allow attackers to move  laterally throughout a network.

**Authenticated vs non-authenticated scanning**

Authenticated scans are performed by authenticated users  with legitimate login credentials. These scans are typically more  comprehensive than non-authenticated scans. They are able to identify  poor configurations, insecure registry entries and malicious code and  plug-ins.

Non-authenticated scans do not use any login credentials.  This is because they are solely a surface-level scan. They identify  backdoors, expired certificates, unpatched software, weak passwords and  poor encryption protocols.

**Penetration testing vs vulnerability scanning**

Penetration testing and vulnerability scanning serve  similar purposes but use different methods. Penetration testing is used  to actually exploit vulnerabilities. Scanning is used to identify where  potential vulnerabilities may exist before penetration testing is  carried out.

**How to select a vulnerability scanning tool**

When looking for a vulnerability scanning tool, there are two things to keep in mind:

1. Ensure it can define compliance rules based on regulations and standards relevant to your organization.
2. Opt for a tool with an intuitive dashboard that clearly shows risk scores and reports to help prioritize patching efforts.
3. And look for one that can scan your most critical systems and defenses.