7.4.2 Vulnerability Assessment Tool Facts

As an ethical hacker, your value will depend on your ability to accurately find and fix vulnerabilities in an organization. Your ability to do this greatly depends on having the right tools for the job. Let’s go through a few of the top tools available to you.

This lesson covers the following topics:

- Assessment tools
- Open source tools
- Mobile tools
- Assessment reports

Assessment Tools

Here are two tools for overall scanning, reporting, remediation, and ongoing monitoring.

Tools	Description
Qualys Vulnerability Management	Qualys Vulnerability Management is a cloud-based service that keeps all your data in a virtual private database. Qualys is easy to use and is capable of scanning large enterprises. Data is always encrypted during transit and at rest, so even though it is cloud-based, your data is secure; only their scanners reside in your network.
Nessus Professional	Nessus Professional is an assessment solution that resides on your network. This makes it more suitable for smaller organizations. It scans for known vulnerabilities, malware, and misconfigurations. Nessus also provides reporting and remediation, as well as ongoing monitoring.

Open-Source Tools

Open-source tools are free to use, and it is legal for anyone to modify and share them.

Tools	Description
OpenVAS	OpenVAS is a vulnerability scanner that boasts more than 50, 000 vulnerability tests with daily updates. It is capable of various high-level and low-level internet and industrial protocols, as well as unauthenticated and authenticated testing.
Nikto	Nikto is a web server scanner. It tests for outdated versions of more than 1250 servers. It also scans for more than 6,000 files and programs that can be exploited. It checks for version-specific problems on more than 270 servers. It is important to note that this tool creates a large footprint by leaving a high volume of entries in the web servers log files.

Mobile Tools

It may not be the first thing you think of when looking for vulnerabilities on an organization's network, but mobile devices are important to include in a thorough assessment.

Tool	Description
Retina CS for Mobile	Provides comprehensive vulnerability management for smartphones, mobile devices, and tablets. This program can scan, prioritize, and fix smartphone vulnerabilities. Then it analyzes and reports its findings from a centralized data warehouse.
SecurityMetrics Mobile	Detects vulnerabilities in mobile devices. It can help you protect customers' data, avoid unwanted app privileges, mobile malware, device theft, connectivity issues, and threats to device storage and unauthorized account access. You can expect a report containing a total risk score, a summary of revealed vulnerabilities, and remediation suggestions.
Nessus	Offers scanning on mobile devices and will let you know which devices are unauthorized or non-compliant. It also finds outdated versions of Apple IOS. Nessus highlights devices that have not connected for a period of time. It helps to overcome the difficulty of identifying network vulnerabilities when mobile devices are connecting and disconnecting between testing.
Net Scan	Provides discovery through network and port scanning. Net Scan can find vulnerabilities, security flaws, and open ports in your network.
Network Scanner	Provides an understanding of the use of a network. Network Scanner generates reports of security issues and vulnerabilities. These reports are autosaved and can be backed up to your web storage.

Assessment Reports

Assessment reports come in two categories.

Report Type	Description
Security vulnerability report	Here, you will find information on all the scanned devices and servers including open and detected ports, new vulnerabilities, and suggestions for remediation with links to patches.
Security vulnerability summary	This report covers every device or server that was scanned. It provides information on current security flaws and categories of vulnerabilities including severity level. It also lists resolved vulnerabilities.

Assessment reports provide detailed information on the vulnerabilities that are found in the network.

Information	Description
Scan information	The name of the scanning tool, its version, and the network ports that have been scanned.
Target information	The target system's name and address are listed.
Results	This section provides a complete scanning report. It contains the following sub-topics: ▪ Target: this sub-topic includes each host's detailed information. ▪ Services: this sub-topic defines the network services by their names and ports. ▪ Classification: the origin of the scan can be found here. ▪ Assessment: the scanner's assessment of the vulnerability.