6.9.2 Vulnerability Assessment Facts

Vulnerability assessment is the process of identifying the vulnerabilities in a system or network. Attackers attempt to take advantage of vulnerabilities to gain access to information or to a network to which they are not authorized. An administrator checks a network for vulnerabilities to plug security holes and provide a more secure network.

Tools that can be used to monitor the vulnerability of systems are explained in the following table:

Tool	Description
Vulnerability Scanner	A *vulnerability scanner* is a software program that passively searches an application, computer, or network for weaknesses such as: ▪ Open ports ▪ Active IP addresses ▪ Running applications or services ▪ Missing critical patches ▪ Default user accounts that have not been disabled ▪ Default or blank passwords ▪ Misconfigurations ▪ Missing security controls Vulnerability scanners: ▪ Should be updated regularly to include the latest known vulnerabilities. ▪ Are the least intrusive methods for checking the environment for known software flaws. Port scanners and penetration testers are potentially more intrusive. Protocol analyzers cannot check for known software flaws. ▪ Can be used to scan again after a security hole has been patched to verify that the vulnerability has been removed and the system is secure. Vulnerability scans can be conducted with or without authentication credentials. Each method has benefits and drawbacks: ▪ In a credentialed scan, the security administrator authenticates to the system prior to starting the scan. A credentialed scan usually provides more detailed information about potential vulnerabilities. For example, a credentialed scan of a Windows workstation allows the registry to be probed for security vulnerabilities. ▪ In a non-credentialed scan, the security administrator does not authenticate to the system prior to running the scan. A non-credentialed scan can be valuable because it allows the scanner to see the system from the same perspective that an attacker would see it. However, a non-credentialed scan does not typically produce the same level of detail as a credentialed scan. Security tools that can be used for vulnerability scanning include: ▪ Nessus, which is a comprehensive vulnerability assessment tool. ▪ Microsoft Baseline Security Analyzer (MBSA), which is used to evaluate security vulnerabilities in Microsoft products. ▪ Retina Vulnerability Assessment Scanner, which is used to remotely scan an organization's network for vulnerabilities.
Ping Scanner	A *ping scanner* is a tool that sends ICMP echo/request packets to one or multiple IP addresses. Use a ping scanner to quickly identify systems on the network that respond to ICMP packets. To protect against attacks that use ICMP, use a ping scanner to identify systems that allow ICMP, and then configure those systems to block ICMP messages. A vulnerability scanner often includes a ping scanner.
Port Scanner	A *port scanner* is a tool that probes systems for open ports. A TCP SYN scan is the most common type of port scanning tool: ▪ It performs a two-way handshake, also called a half-open scan, which does not complete the TCP three-way handshake process (the TCP session is not established). ▪ Devices that respond indicate devices with ports that are in a listening state. ▪ The port scan output is a combination of IP address and port number separated by a colon (e.g., 192.168.0.1:*x* where *x* is the port number) for both the source of the port scan and the destination of the port scan. A vulnerability scanner often includes a port scanner.
Network Mapper	A *network mapper* is a tool that can discover devices on the network and then display the devices in a graphical representation. Network mappers typically use a ping scanner to discover devices as well as a port scanner to identify open ports on those devices. Many port scanners are technically network mappers.
Password Cracker	A *password cracker* is a tool that performs cryptographic attacks on passwords. Use a password cracker to identify weak passwords or passwords protected with weak encryption. Common password cracking tools include:

	▪ John the Ripper ▪ Cain and Abel ▪ L0phtcrack
Open Vulnerability and Assessment Language (OVAL)	The *Open Vulnerability and Assessment Language* (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system. ▪ OVAL is sponsored by the National Cyber Security Division of the U.S. Department of Homeland Security. ▪ OVAL identifies the XML format for identifying and reporting system vulnerabilities. ▪ Each vulnerability, configuration issue, program, or patch that might be present on a system is identified as a definition. ▪ OVAL repositories are like libraries or databases that contain multiple definitions.