7.1.2 Vulnerability Assessment Facts

A vulnerability assessment is the process of identifying weaknesses in an organization infrastructure, including the operating system, web applications, and web server. An assessment is also used to plan additional security measures to protect the organization from attack. Every business that uses a computer to run their business is at risk of having sensitive information stolen or misused. Having an ethical hacker conduct an assessment sheds light on vulnerability to malicious attack. In a world where so much private information is stored and transferred digitally, it is essential to be proactive in determining and addressing system weaknesses.

Data obtained from a vulnerability assessment reveals security weaknesses. It will open ports and running services, configuration errors, system flaws, and weaknesses in applications and services. It is important to target multiple areas of operation in order to have a comprehensive assessment. Once the data is obtained, a plan can be made to correct, patch, or harden systems to protect data.

This lesson covers the following topics:

- Vulnerability scanning types
- Scan limitations
- Assessment types
- Vulnerability research

Vulnerability Scanning Types

There are two types of vulnerability scans. Each type of scan has advantages. Both types can be used together to provide a more comprehensive assessment.

Vulnerability Scanning	Description
Active scanning	An active scan transmits to the nodes within a network to determine exposed ports and can independently repair security flaws. It can also simulate an attack to test for vulnerabilities and can repair weak points in the system.
Passive scanning	A passive scan tries to find vulnerabilities without directly interacting with the target network. The scan identifies vulnerabilities via information exposed by systems in their normal communications. You can set a scanner to scan constantly or at specific times.

Scan Limitations

It’s important to understand that scanners are not foolproof. The following table identifies two significant limitations.

Scan Limitation	Description
Point in time	A scan can only obtain data for the time period when it runs. For example, some weaknesses may be exposed only when systems are operating at peak capacity, at certain times of day, or even at certain times of the year.
New vulnerabilities	Scans can only identify known vulnerabilities. This give an attacker that uses a new attack an advantage, as scans are written only for vulnerabilities that have been previously exploited.

Assessment Types

There is not one assessment testing tool that will cover every area to be tested. It is important to understand the goals and objectives of the organization; to gather information about the systems, network, and applications; and then to determine the best tools to make a comprehensive plan to correct security problems that you identify. Testing only one area of a system will not be sufficient to expose all vulnerabilities that exist.

Assessment Types	Description
Active assessment	In an active assessment, specifically created packets are sent to target nodes to determine the OS of the domain, the hosts, the services, and the vulnerabilities in the network. nmap is a useful tool for this assessment.
Passive assessment	Using sniffer traces from a remote system, you can determine the operating system of the remote host as well as a list of the current network work. Wireshark is a common tool for this type of information gathering and analysis.
External assessment	This type of assessment looks for ways to access the network infrastructure through open firewall ports, routers, web servers, web pages, and public DNS servers. It is external because it is working from the outside using public networks through the internet. This type of assessment may include: - Determining if maps exist for network and external service devices

	▪ Checking for vulnerabilities in web applications ▪ Examining the rule set for external network router configurations and firewalls ▪ Detecting open ports on the external network and services ▪ Identifying DNS zones
Internal assessment	The ethical hacker can also be inside the network, testing the internal networks and systems. This type of assessment can include: ▪ Inspecting physical security ▪ Checking open ports on network devices and router configurations ▪ Scanning for Trojans, spyware, viruses, and malware ▪ Evaluating remote management processes ▪ Determining flaws and patches on the internal network systems, devices, and servers
Host-based assessment	This assessment focuses on all types of user risks, including malicious users and untrained users as well as vendors and administrators. Host-based assessment can also test the vulnerability of databases, firewalls, files, and web servers, as well as flag configuration errors.
Application	Application-level scans allow the ethical hacker to scrutinize completed applications when the source code is unknown. Every application should be examined for input controls and data processing.
Wireless network assessment	A hacker can access sensitive information even from outside a building by sniffing network packets that are transmitted wirelessly through radio waves. Generally, a hacker will obtain the SSID (the name assigned to the wireless network) through sniffing and use it to hack the wireless network without ever entering the building. These assessments analyze the network for patching errors, authentication and encryption problems, and unnecessary services.

Vulnerability Research

Vulnerability research is the process of discovering vulnerabilities and design flaws that will open an operating system and its applications to attack or misuse. Time is on the attacker's side. It is crucial for an ethical hacker to put in the effort and time to research an organization from the outside in and to scan and gather information at every level.

Areas to Research	Description
Misconfigurations	The primary cause of misconfiguration is human error. Web servers, application platforms, databases, and networks are all at risk of unauthorized access. Areas to check include outdated software, unnecessary services, external systems that are incorrectly authenticated, security settings that have been disabled, and debug enabled on a running application.
Default settings	It is important to check default settings, especially for default SSIDs and admin passwords. If a company never changes the default admin passwords or the default SSID to combinations unique to the company, it is very simple for an attacker to gain access to the network.
Buffer overflows	A buffer is a temporary data storage area with limited space. Overflows occur when more data is attempted to be stored than the program was written for. Error checking should identify this problem. When overflow occurs, it can allow hackers to cause data to flow to other memory areas and to access database files or alter system files. System crashing or instability can also occur.
Unpatched servers	Hackers gain access to data in a system through misconfigured or unpatched servers. Since servers are integral part of an organization’s infrastructure, this vulnerability creates a central route for access to sensitive data and operations. Fixing bugs, patching, and simply updating software can block an attack.
Design flaws	Every operating system or device has bugs or defects in its design. Hackers take advantage of design flaws such as broken authentication and access control, cross-site scripting, insufficient logging and monitoring, and incorrect encryption.
Operating system flaws	Flaws in the OS can leave a system susceptible to malicious applications such as viruses, Trojan horses, and worms through scripts, undesirable software, or code. Firewalls, minimal software application usage, and regular system patches create protection from this form of attack.
Application flaws	Flaws in the validation and authorization of users present the greatest threat to security in transactional applications. This type of assessment evaluates deployment and communication between the server and client. It is imperative to develop tight security through user authorization and validation. Both open-source and commercial tools are recommended for this assessment.
Open services	Ports and services must be checked regularly to prevent unsecure, open, or unnecessary ports, which can lead to attacks on connected nodes or devices, loss of private information, or even denial of service.
Default usernames and passwords	Passwords should always be immediately changed after installation or setup. Passwords should always be kept secret.