7.2.4 Vulnerability Solution Facts

Vulnerability assessment is part of the scanning phase.

This lesson covers the following topics:

- Assessment solutions
- Assessment types
- Vulnerability scanning penetration steps

Assessment Solutions

There are two approaches to solving the vulnerability problems you find.

Solution	Description
Product-based	This solution involves an organization purchasing a product and administering it from inside the network. The product functions inside the firewall. This would make it inaccessible from outside penetration. An organization could implement this type of solution hoping that it solves vulnerability issues.
Service-based	A service-based solution entails hiring a professional, such as yourself, to provide a solution. This approach would involve using the vulnerability management life cycle. The professional would conduct the testing and solutions from outside the network. The risk of this approach is that an assessment based entirely from outside the network leaves potential for a hacker to gain access to the system.

An organization might be tempted not to hire a professional, but to install and run the product-based solutions themselves. However, it is likely the organization would not have the same level of protection that an ethical hacker would provide thorough analysis, assessment, remediation, verification, and continuous monitoring.

Assessment Types

There are two types of assessments.

Assessments	Description
Tree-based	With a tree-based assessment, you have a preset plan for testing and scanning based on some previous knowledge of the system. You then choose specific modes of testing for each operating system and machine.
Inference-based	In an inference-based approach, you test and discover information as you go. You then adjust your scans according to the information you discover.

The tree-based assessment relies on the professional implementing a plan based on information that may or may not be accurate and complete for the system being tested. An inference-based approach relies on a current evaluation of the system to determine the next step, testing only relevant areas of concern.

Vulnerability Scanning Penetration Steps

As you conduct vulnerability scanning, it is important to understand that there are three basic steps in penetration testing.

Steps	Description
1	Locate the live nodes in the network. You can do this using a variety of techniques, but you must know where each live host is.
2	Itemize each open port and service in the network.
3	Test each open port for known vulnerabilities.