Network Penetration Testing Methodology-External

1 Hr 9 Min Remaining

Instructions Resources Help  100%

Module 05: Network Penetration Testing Methodology-External

Objective

The objective of this lab is to help students in conducting network scanning, network vulnerability analysis, and network security maintenance.

You need to perform network scans to:

* Check live systems and open ports
* Perform banner grabbing and OS fingerprinting
* Identify network vulnerabilities
* Draw network diagrams of vulnerable hosts
* Pentest vulnerabilities to gain unauthorized access

Scenario

External Penetration Testing determines the possibility of network security attacks from outside of the network perimeter. It evaluates the organization’s systems and network for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption.

An attacker uses vulnerabilities to disrupt the confidentiality, availability or integrity of the network, thereby allowing the organization to address each weakness. Vulnerability scanning is a critical component of any penetration testing assignment. As an expert Penetration Tester or a Security Administrator, you need to conduct penetration testing and list the threats and vulnerabilities found in an organization’s network, perform port scanning, network scanning, and vulnerability scanning to identify IP/hostname, live hosts, and vulnerabilities. Then, you need to take specific preventive countermeasures to overcome them.