Introduction to Network Security Tools, Skill Labs

Course Specifications

Course Number: ACI76-052SL_rev1.0
Lab Length: Approximately 12 hours

Topology Discovery - Part 1 (PLAB-WS-NMAP

Introduction
Objective

The Topology Discovery - Part 1 module provides you with the instructions and devices needed to develop your hands-on skills in the following topics:

- Basic Scanning
- Discovering Network Topologies
- Topology Discovery against Firewalls

Topology Discovery - Part 2 (PLAB-WS-NMAP)

Introduction
Objective

The Topology Discovery - Part 2 module provides you with the instructions and devices needed to develop your hands-on skills in the following topics:

- OS Fingerprinting
- Output Logs
- Zenmap the NMAP GUI

Scanning Networks Part - 1 (PLAB-WS-NMAP)

Introduction
Objective

The Scanning Networks Part - 1 module provides you with the instruction and server hardware to develop your hands-on skills in the defined topics. This module includes the following exercises:

- Network Scanner—Advanced IP Scanner
- Nmap Scanner
- MyLanViewer
- Network Topology Mapper

Scanning Networks Part - 2 (PLAB-WS-NMAP)

Introduction
Objective

The Scanning Networks Part - 2 module provides you with the instruction and server hardware to develop your hands-on skills in the defined topics. This module includes the following exercises:

- NetworkView
- The Dude
- Nessus
- Banner Grabbing: ID Serve
- SSH Tunnelling: Bitvise

Understand Network Protocols - HTTP, HTTPS, NetBIOS, TCP, UDP (PLAB-WS-NMAP)

Introduction
Objective

The Understand Network Protocols - HTTP, HTTPS, NetBIOS, TCP, UDP module provides you with the instructions and computer hardware needed to develop your hands-on skills in the defined topics. This module includes the following exercises:

- Verifying Port 80 for HTTP
- Verifying Port 443 for HTTPS
- Verify Port 139 for NetBIOS
- Understanding TCP and UDP
- Using a Port Scanner

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- 2.1 Given a scenario, use appropriate monitoring tools (port scanner).
- 3.2 Compare and contrast common network vulnerabilities and threats (HTTP).
- 5.9 Compare and contrast the following ports and protocols (HTTP, HTTPS, NetBIOS).

Network Security - Protocol Analyzers (PLAB-WS-NMAP)

Introduction
Objective

The Security+ Network Security - Protocol Analyzers module provides you with the instructions and computer hardware needed to develop your hands-on skills in the defined topics. This module includes the following exercises:

- Investigating the ARP Cache Table
- Using Wireshark to Capture Packets
- ARP Problems
- Using a Port Scanner
- Using Nmap

Threats - Network Vulnerability (PLAB-WS-NMAP)

Introduction
Objective

The Security+ ThreatsNetwork - Vulnerabilities module provides you with the instruction and server hardware to develop your hands-on skills in the defined topics. This module includes the following exercises:

- Network Footprinting
- Packet Sniffing
- MITM with ARP Spoofing
- Denial of Service
- Anti-Phishing Toolbar

Threats - Network Vulnerability Scanning (PLAB-WS-NMAP)

Introduction
Objective

The module Threats - Network Vulnerability Scanning provides you with the instructions and devices needed to develop your hands-on skills in the following topics:

- OpenVAS Scanning
- Applying Windows Secure Updates
- Validating Security Changes with OpenVAS

Overview
Exam Objectives

The following exam objectives are covered in this lab:

- SY0-501 1.5: Explain vulnerability scanning concepts.

Network Security - Routing Protocols (PLAB-WS-NMAP)

Introduction
Objective

The SY0-401 – Network Security - Routing Protocols module provides you with the instructions and server hardware needed to develop your hands-on skills in the defined topics. This module includes the following exercises:

- Configuring a Network
- Sniffing Routing Traffic
- Injecting Poison Routes
- Configuring Authentication for RIP Packets

Network Security - Spam Filter (PLAB-WS-NMAP)

Introduction
Objective

The Network Security - Spam Filter module provides you with the instruction and computer hardware to develop your hands on skills in the defined topics. This module includes the following exercises:

- Configuring an Email Service
- Configuring a Mail Client
- Using Telnet to Spoof a Sender

Understand Common Ports and Protocols (SY0-401)

Introduction
Objective

The Understanding Common Ports and Protocols module provides you with the instruction and computer hardware to develop your hands on skills in the defined topics. This module includes the following exercises:

- Verifying Port 80 for HTTP
- Verifying Port 443 for HTTPS
- Verify Port 139 for NetBIOS
- Understanding TCP and UDP

Understanding IDS Firewall Evasion and Honeypots (PLAB-WS-NMAP)

Introduction
Objective

The Understanding IDS, Firewall Evasion and Honeypots module provides you with the instruction and server hardware to develop your hands on skills in the defined topics. This module includes the following exercises:

- Install and Configure ZoneAlarm Firewall
- Install and Configure Snort
- Using Anonymous Proxy Sites