CompTIA Security+ SY0-501

Practice Labs™

CompTIA Security+

Powered by Practice Labs

CompTIA AUTHORIZED PARTNER

Lab Outline

The CompTIA Security+ Practice Lab will provide you with the necessary platform to gain hands on skills in information security. By completing the lab tasks you will improve your practical skills in identifying threats, attacks and vulnerabilities, access and identity management and risk management.

These same tasks will help you understand the objectives and competencies required by the CompTIA Security+ (SY0-501) certification exam.and competencies required by the CompTIA CASP (CAS-002) certification exam.

Outcomes

After completing this Practice Lab, students will be able to:

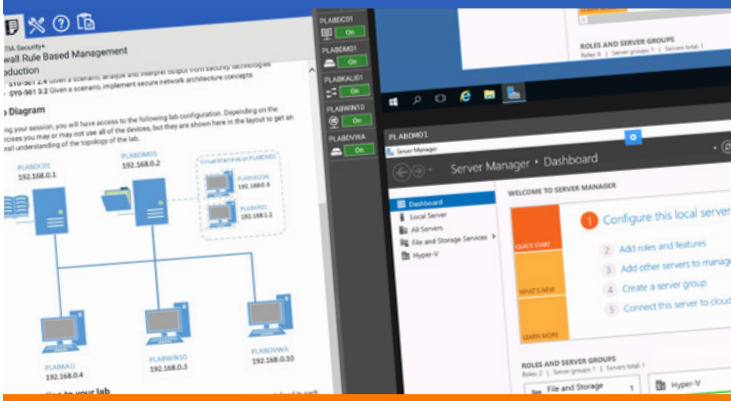
- Configure firewall rules to protect against network vulnerabilities
- Implement software RAID
- Configure IDS and honeypots
- Install and configure load balancing
- Describe and protect against social engineering
- Use password cracking tools
- Scan and remediate vulnerabilities
- Understand backup and recovery procedures
- Use WSUS to rollout patches
- Manage certificates and implement AD federation services
- Use encryption and hashing techniques
- Perform data encryption
- Use basic forensics techniques

Course Code
SY0-501

Skill Level
Intermediate

Released
Oct 2017

Duration
25 hours



Prerequisites

It is recommended that you have gained the following certification before attempting the CompTIA Security+ exam:

- Network+

No prior hands-on experience is required to use or complete this Practice Lab, however it would be beneficial to be familiar with basic networking technologies and information security concepts.

Who is it For?

The CompTIA Security+ certificate is aimed at IT security analysts, vulnerability analysts, threat intelligence analysts, or IT professionals seeking to advance into the industry.

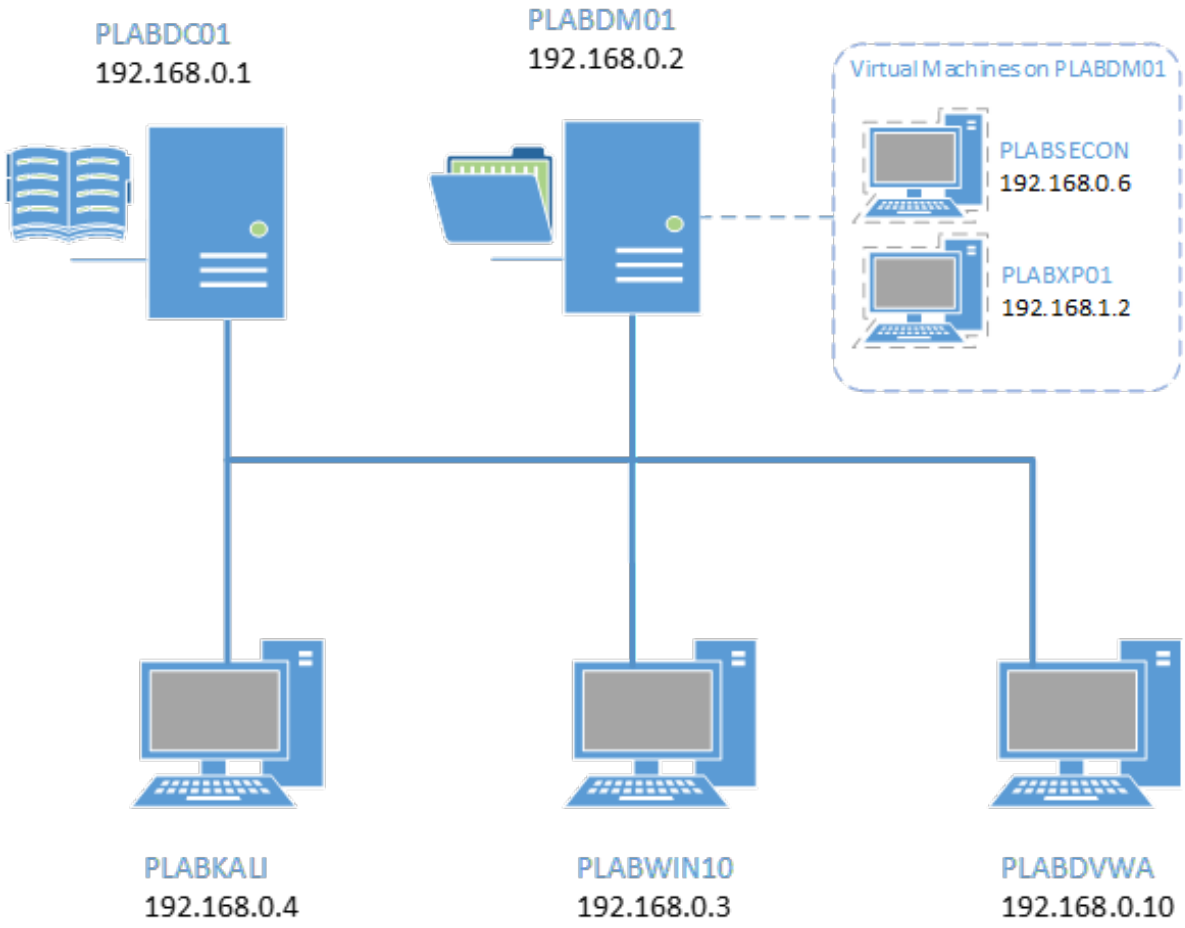
Additional Info

This Practice Lab focuses on the practical aspects of the CompTIA Security+ (SY0-501) exam objectives. It is therefore advised to refer to your own course materials to gain a deeper understanding of any theoretical aspects of the exam objectives.

Support 9am-5pm(GMT) : +44 (0) 203 588750
E-mail: sales@practice-labs.com

Lab Topologies

You will also have access to the following topologies:



CompTIA Security+

Powered by Practice Labs

CompTIA AUTHORIZED PARTNER

Modules and Exercises

Firewall Rule Based Management
- Introduction
- Exercise 1 - Configuring Firewall Rules Using Windows Firewall
- Exercise 2 - Configuring Firewall Rules using Windows Firewall with Advanced Security
- Exercise 3 - Configuring Firewall Rules using Remote Desktop
- Exercise 4 - Configuring Firewall Rules from the Command Line Interface
- Summary

Firewalls and Evasion
- Introduction
- Exercise 1 - Connecting to Hyper V Manager
- Exercise 2 - Install ZoneAlarm Firewall and Antivirus
- Exercise 3 - Configuring ZoneAlarm
- Exercise 4 - Using Anonymous Proxy Sites
- Summary

NAT and OpenSSH
- Introduction
- Exercise 1 - Installing NAT Firewall
- Exercise 2 - Installing OpenSSH
- Summary

Network Vulnerabilities Part 1
- Introduction
- Exercise 1 - Network Footprinting
- Exercise 2 - Packet Sniffing
- Summary

Network Vulnerabilities Part 2
- Introduction
- Exercise 1 - Denial of Service
- Exercise 2 - Anti-Phishing Toolbar
- Summary

Application Data - Establish Host Security
- Introduction
- Exercise 1 - Anti-virus Programs
- Summary

Configuring IDS and Honeypots
- Introduction
- Exercise 1 - Snort Installation
- Exercise 2 - Test Snort
- Exercise 3 - Configure and Re-Test Snort
- Summary

Password Cracking Tools
- Introduction
- Exercise 1 - Password Cracking Tools
- Summary

Implementing DNSSEC
- Introduction
- Exercise 1 - Preparing DNS Setup for DNSSEC
- Exercise 2 - Configuring DNSSEC
- Exercise 3 - Customizing DNSSEC
- Summary

Social Engineering Reconnaissance
- Introduction
- Exercise 1 - Social Engineering Reconnaissance
- Summary

Encryption and Hashing
- Introduction
- Exercise 1 - Cryptographic Basics
- Exercise 2 - Comparing Hashing Algorithms
- Exercise 3 - Comparing Hash Values
- Summary

Understanding PKI Concepts
- Introduction
- Exercise 1 - Install and Configure Active Directory Certificate Services
- Exercise 2 - Configure Certificate Revocation Lists (CRLs)
- Summary

Backup and Recovery
- Introduction
- Exercise 1 - Install Windows Server Backup
- Exercise 2 - Backup and Restore using Windows Server Backup
- Summary

Implement Patching using WSUS
- Introduction
- Exercise 1 - Install Windows Server Backup
- Exercise 2 - Backup and Restore using Windows Server Backup
- Exercise 3 - Configure GPO Policy for WSUS
- Summary

Company No. 05939037 VAT No. 900079851

CompTIA Security+

Powered by Practice Labs

CompTIA AUTHORIZED PARTNER

Managing Local Storage and Virtual Hard Disks

- Introduction
- Exercise 1 - Creating Disk Volumes
- Exercise 2 - Managing Virtual Hard Disks
- Summary

Implementing a Network Policy Server

- Introduction
- Exercise 1 - Managing Certificate Templates
- Exercise 2 - Configuring Certificate Auto Enrollment
- Exercise 3 - Implementing Key Archival
- Exercise 4 - Enrolling for User Certificate
- Exercise 5 - Managing Key Recovery
- Summary

Managing Certificates

- Introduction
- Exercise 1 - Managing Certificate Templates
- Exercise 2 - Configuring Certificate Auto Enrollment
- Exercise 3 - Implementing Key Archival
- Exercise 4 - Enrolling for User Certificate
- Exercise 5 - Managing Key Recovery
- Summary

Protocols and Services - SNMP

- Introduction
- Exercise 1 - Installing the Monitoring Software
- Exercise 2 - Installing and Configuring SNMP
- Exercise 3 - Performing a Network Inventory
- Summary

Data Encryption

- Introduction
- Exercise 1 - Configure Software RAID
- Summary

Implementing Software RAID

- Introduction
- Exercise 1 - Configure Software RAID
- Summary

Introduction to Digital Forensics

- Introduction
- Exercise 1 - Acquiring an Image of Evidence Media
- Exercise 2 - Analyzing Your Digital Evidence
- Exercise 3 - Analysis Example
- Exercise 4 - Report Example
- Exercise 5 - Keyword Search Example
- Summary

Implementing AD Federation Services

- Introduction
- Exercise 1 - Prepare System Requirements for ADFS Resource Partner
- Exercise 2 - Prepare System Requirements for ADFS Accounts Partner
- Exercise 3 - Enable Name Resolution for Resource and Account Domains
- Exercise 4 - Prepare Requirements for AD FS Server Resource Partner
- Exercise 5 - Install and Configure AD Federation Services
- Exercise 6 - Create AD Federation Services Trusts
- Summary

Configuring RADIUS

- Introduction
- Exercise 1 - Install and Configure Network Policy Server
- Exercise 2 - Install and Configure Remote Access Server
- Exercise 2 - Install and Configure Remote Access Server
- Exercise 4 - Viewing the NPS Logs
- Summary

Install and Configure Network Load Balancing

- Introduction
- Exercise 1 - Installing Network Load Balancing Nodes
- Exercise 2 - Configuring a New NLB Cluster
- Exercise 3 - Adding a Secondary Node to an NLB Cluster
- Exercise 4 - Examining the Working of an NLB Cluster
- Exercise 5 - Configuring and Validating Port Rules for NLB
- Summary

Scanning and Remediating Vulnerabilities with OpenVAS

- Introduction
- Exercise 1 - Connecting to Kali
- Exercise 2 - OpenVAS Scanning
- Exercise 3 - Securing Active Directory Access LDAP
- Exercise 4 - Validating Security Changes with OpenVAS
- Summary

Company No. 05939037 VAT No. 900079851