

Security+ CertMaster Labs Course Outline



Brief Table of Contents

1.0 Summarize Fundamental Security Concepts.....	3
2.0 Compare Threat Types.....	4
3.0 Explain Cryptographic Solutions.....	5
4.0 Implement Identity and Access Management.....	6
5.0 Secure Enterprise Network Architecture.....	7
6.0 Secure Cloud Network Architecture.....	8
7.0 Explain Resiliency and Site Security Concepts.....	9
8.0 Explain Vulnerability Management.....	10
9.0 Evaluate Network Security Capabilities.....	11
10.0 Assess Endpoint Security Capabilities.....	12
11.0 Enhance Application Security Capabilities.....	13
12.0 Explain Incident Response and Monitoring Concepts.....	14
13.0 Analyze Indicators of Malicious Activity.....	15
14.0 Summarize Security Governance Concepts.....	16
15.0 Explain Risk Management Processes.....	17
16.0 Summarize Data Protection and Compliance Concepts.....	18

1.0 Summarize Fundamental Security Concepts

- 1.1 Security Concepts
 - 1.1.1 Assisted Live Lab: Exploring The Lab Environment
 - 1.1.2 Assisted Live Lab: Perform System Configuration Gap Analysis
- 1.2 Security Controls
 - 1.2.1 Assisted Live Lab: Configuring Examples Of Security Control Types

2.0 Compare Threat Types

- 2.1 Attack Surfaces
 - 2.1.1 Assisted Live Lab: Finding Open Service Ports
- 2.2 Social Engineering
 - 2.2.1 Assisted Live Lab: Using Set To Perform Social Engineering

3.0 Explain Cryptographic Solutions

- 3.1 Cryptographic Algorithms
 - 3.1.1 Applied Live Lab: Using Storage Encryption
- 3.2 Cryptographic Solutions
 - 3.2.1 Assisted Live Lab: Using Hashing And Salting

4.0 Implement Identity and Access Management

- 4.1 Authentication
 - 4.1.1 Assisted Live Lab: Managing Password Security
- 4.2 Authorization
 - 4.2.1 Assisted Live Lab: Managing Permissions

5.0 Secure Enterprise Network Architecture

- 5.1 Secure Communications
 - 5.1.1 Assisted Live Lab: Setting Up Remote Access
 - 5.1.2 Assisted Live Lab: Using Ipsec Tunneling

6.0 Secure Cloud Network Architecture

- 6.1 Cloud Infrastructure
 - 6.1.1 Assisted Live Lab: Using Containers
 - 6.1.2 Assisted Live Lab: Using Virtualization

7.0 Explain Resiliency and Site Security Concepts

- 7.1 Asset Management
 - 7.1.1 Applied live Lab: Implement Backups
 - 7.1.2 Assisted Live Lab: Performing Drive Sanitization

8.0 Explain Vulnerability Management

- 8.1 Application and Cloud Vulnerabilities
 - 8.1.1 Assisted Live Lab: Exploiting And Detecting Sqli
- 8.2 Vulnerability Identification Methods
 - 8.2.1 Assisted Live Lab: Working With Threat Feeds
- 8.3 Vulnerability Analysis and Remediation
 - 8.3.1 Assisted Live Lab: Performing Vulnerability Scans

9.0 Evaluate Network Security Capabilities

- 9.1 Network Security Baselines
 - 9.1.1 Assisted Live Lab: Understanding Security Baselines
- 9.2 Network Security Capability Enhancement
 - 9.2.1 Applied Live Lab: Implementing A Firewall

10.0 Assess Endpoint Security Capabilities

- 10.1 Implement Endpoint Security
 - 10.1.1 Assisted Live Lab: Using Group Policy
 - 10.1.2 Applied Live Lab: Hardening

11.0 Enhance Application Security Capabilities

- 11.1 Application Protocol Security Baselines
 - 11.1.1 Assisted Live Lab: Performing Dns Filtering
- 11.2 Cloud and Web Application Security Concepts
 - 11.2.1 Assisted Live Lab: Configuring System Monitoring

12.0 Explain Incident Response and Monitoring Concepts

- 12.1 Incident Response
 - 12.1.1 Applied Live Lab: Incident Response Detection
- 12.2 Digital Forensics
 - 12.2.1 Applied Live Lab: Performing Digital Forensics
- 12.3 Data Sources
 - 12.3.1 Applied Live Lab: Using Network Sniffers
- 12.4 Alerting and Monitoring Tools
 - 12.4.1 Assisted Live Lab: Performing Root Cause Analysis

13.0 Analyze Indicators of Malicious Activity

- 13.1 Malware Attack Indicators
 - 13.1.1 Assisted Live Lab: Detecting And Responding To Malware
- 13.2 Physical and Network Attack Indicators
 - 13.2.1 Assisted Live Lab: Understanding Onpath Attacks

14.0 Summarize Security Governance Concepts

- 14.1 Policies, Standards, and Procedures
 - 14.1.1 Adaptive Live Lab: Using A Playbook
- 14.2 Change Management
 - 14.2.1 Assisted Live Lab: Implementing Allow Lists And Deny Lists
- 14.3 Automation and Orchestration
 - 14.3.1 Assisted Live Lab: Use Cases Of Automation And Scripting

15.0 Explain Risk Management Processes

- 15.1 Audits and Assessments
 - 15.1.1 Assisted Live Lab: Performing Reconnaissance
 - 15.1.2 Assisted Live Lab: Performing Penetration Testing

16.0 Summarize Data Protection and Compliance Concepts

- 16.1 Personnel Policies
 - 16.1.1 Assisted Live Lab: Training And Awareness Through Simulation
 - 16.1.2 Challenge Live Lab: Network Incident Investigation And Remediation