



## Table of Contents.

- Lesson 1: Comparing Security Roles and Security Controls
- Lesson 2: Explaining Threat Actors and Threat Intelligence
- Lesson 3: Performing Security Assessments
- Lesson 4: Identifying Social Engineering and Malware
- Lesson 5: Summarizing Basic Cryptographic Concepts
- Lesson 6: Implementing Public Key Infrastructure
- Lesson 7: Implementing Authentication Controls
- Lesson 8: Implementing Identity and Account Management Controls
- Lesson 9: Implementing Secure Network Designs
- Lesson 10: Implementing Network Security Appliances
- Lesson 11: Implementing Secure Network Protocols
- Lesson 12: Implementing Host Security Solutions
- Lesson 13: Implementing Secure Mobile Solutions
- Lesson 14: Summarizing Secure Application Concepts
- Lesson 15: Implementing Secure Cloud Solutions
- Lesson 16: Explaining Data Privacy and Protection Concepts
- Lesson 17: Performing Incident Response
- Lesson 18: Explaining Digital Forensics
- Lesson 19: Summarizing Risk Management Concepts
- Lesson 20: Implementing Cybersecurity Resilience
- Lesson 21: Explaining Physical Security



## Labs Available:

- 1 - Assisted Lab: Exploring the Lab Environment
- 2 - Assisted Lab: Scanning and Identifying Network Nodes
- 3 - Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
- 4 - Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan
- 5 - Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
- 6 - Assisted Lab: Managing the Lifecycle of a Certificate
- 7 - Assisted Lab: Managing Certificates with OpenSSL
- 8 - Assisted Lab: Auditing Passwords with a Password Cracking Utility
- 9 - Assisted Lab: Managing Centralized Authentication
- 10 - Assisted Lab: Managing Access Controls in Windows Server
- 11 - Assisted Lab: Configuring a System for Auditing Policies
- 12 - Assisted Lab: Managing Access Controls in Linux
- 13 - Assisted Lab: Implementing a Secure Network Design
- 14 - Assisted Lab: Configuring a Firewall
- 15 - Assisted Lab: Configuring an Intrusion Detection System
- 16 - Assisted Lab: Implementing Secure Network Addressing Services
- 17 - Assisted Lab: Implementing a Virtual Private Network
- 18 - Assisted Lab: Implementing a Secure SSH Server
- 19 - Assisted Lab: Implementing Endpoint Protection
- 20 - Assisted Lab: Identifying Application Attack Indicators
- 21 - Assisted Lab: Identifying a Browser Attack
- 22 - Assisted Lab: Implementing PowerShell Security
- 23 - Assisted Lab: Identifying Malicious Code
- 24 - Assisted Lab: Managing Data Sources for Incident Response
- 25 - Assisted Lab: Configuring Mitigation Controls
- 26 - Assisted Lab: Acquiring Digital Forensics Evidence
- 26 - Assisted Lab: Backing Up and Restoring Data in Windows and Linux