uCertify

Systems Security Certified Practitioner (SSCP)

Lesson Practice test Live-Lab

01 Sep 2023

8. 1 Introduction

   2 The Business Case for Decision Assurance and Information Security

   3 Information Security Fundamentals

   4 Integrated Information Risk Management

   5 Operationalizing Risk Mitigation

   6 Communications and Network Security

   7 Identity and Access Control

   8 Cryptography

   9 Hardware and Systems Security

   10 Applications, Data, and Cloud Security

   11 Incident Response and Recovery

   12 Business Continuity via Information Security and People Power

   13 Cross-Domain Challenges

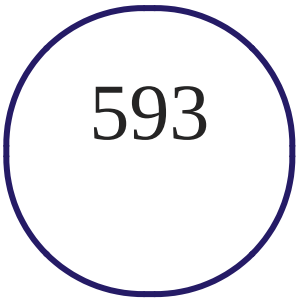
10.

1

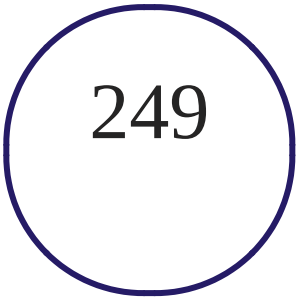
Get hands-on experience in system security with the Systems Security Certified Practitioner (SSCP) course and lab. The course contains interactive tools such as live labs, test preps, and SSCP exam objective-based lessons with knowledge checks, quizzes, flashcards, and glossary terms to get a detailed understanding of critical aspects of information security. It will be a great source to learn about Security Operations and Administration, Access Controls, Risk Identification, Monitoring, and Analysis, Incident Response and Recovery, Cryptography, Network and Communications Security, and Systems and Application Security.

2

3



4



5

6

7

8

9

•

10

- **2014**
  1.
- **2015**
  5.
- **2016**
  5.
- **2017**
  3.
- **2018**
  3.
- **2019**
  3.
- **2020**
  3.

11

1: Introduction

- About This Course
- What Is an SSCP?
- Using This Course

- Let's Get Started!

2: The Business Case for Decision Assurance and Information Security

- Information: The Lifeblood of Business
- Policy, Procedure, and Process: How Business Gets Business Done
- Who Runs the Business?
- Summary
- Exam Essentials

3: Information Security Fundamentals

- The Common Needs for Privacy, Confidentiality, Integrity, and Availability
- Training and Educating Everybody
- SSCPs and Professional Ethics
- Summary
- Exam Essentials

4: Integrated Information Risk Management

- It’s a Dangerous World

- The Four Faces of Risk
- Getting Integrated and Proactive with Information Defense
- Risk Management: Concepts and Frameworks
- Risk Assessment
- Four Choices for Limiting or Containing Damage
- Summary
- Exam Essentials

5: Operationalizing Risk Mitigation

- From Tactical Planning to Information Security Operations
- Operationalizing Risk Mitigation: Step by Step
- The Ongoing Job of Keeping Your Baseline Secure
- Ongoing, Continuous Monitoring
- Reporting to and Engaging with Management
- Summary
- Exam Essentials

6: Communications and Network Security

- Trusting Our Communications in a Converged World
- Internet Systems Concepts
- Two Protocol Stacks, One Internet
- Wireless Network Technologies
- IP Addresses, DHCP, and Subnets
- IPv4 vs. IPv6: Important Differences and Options
- CIANA Layer by Layer
- Securing Networks as Systems
- Summary
- Exam Essentials

7: Identity and Access Control

- Identity and Access: Two Sides of the Same CIANA+PS Coin
- Identity Management Concepts
- Access Control Concepts
- Network Access Control
- Implementing and Scaling IAM
- User and Entity Behavior Analytics (UEBA)

- Zero Trust Architectures
- Summary
- Exam Essentials

8: Cryptography

- Cryptography: What and Why
- Building Blocks of Digital Cryptographic Systems
- Keys and Key Management
- Modern Cryptography: Beyond the “Secret Decoder Ring”
- “Why Isn't All of This Stuff Secret?”
- Cryptography and CIANA+PS
- Public Key Infrastructures
- Applying Cryptography to Meet Different Needs
- Managing Cryptographic Assets and Systems
- Measures of Merit for Cryptographic Solutions
- Attacks and Countermeasures
- PKI and Trust: A Recap

- On the Near Horizon
- Summary
- Exam Essentials

9: Hardware and Systems Security

- Infrastructure Security Is Baseline Management
- Securing the Physical Context
- Infrastructures 101 and Threat Modeling
- Endpoint Security
- Malware: Exploiting the Infrastructure's Vulnerabilities
- Privacy and Secure Browsing
- “The Sin of Aggregation”
- Updating the Threat Model
- Managing Your Systems' Security
- Summary
- Exam Essentials

10: Applications, Data, and Cloud Security

- It's a Data-Driven World…At the Endpoint
- Software as Appliances
- Applications Lifecycles and Security
- CIANA+PS and Applications Software Requirements
- Application Vulnerabilities
- “Shadow IT:” The Dilemma of the User as Builder
- Information Quality and Information Assurance
- Protecting Data in Motion, in Use, and at Rest
- Into the Clouds: Endpoint App and Data Security Considerations
- Legal and Regulatory Issues
- Countermeasures: Keeping Your Apps and Data Safe and Secure
- Summary
- Exam Essentials

11: Incident Response and Recovery

- Defeating the Kill Chain One Skirmish at a Time
- Harsh Realities of Real Incidents
- Incident Response Framework

- Preparation
- Detection and Analysis
- Containment and Eradication
- Recovery: Getting Back to Business
- Post-Incident Activities
- Summary
- Exam Essentials

12: Business Continuity via Information Security and People Power

- What Is a Disaster?
- Surviving to Operate: Plan for It!
- Timelines for BC/DR Planning and Action
- Options for Recovery
- Cloud-Based “Do-Over” Buttons for Continuity, Security, and Resilience
- People Power for BC/DR
- Security Assessment: For BC/DR and Compliance
- Converged Communications: Keeping Them Secure During BC/DR Actions

- Summary
- Exam Essentials

13: Cross-Domain Challenges

- Operationalizing Security Across the Immediate and Longer Term
- Supply Chains, Security, and the SSCP
- Other Dangers on the Web and Net
- On Our Way to the Future
- Enduring Lessons
- Your Next Steps
- At the Close
- Exam Essentials

125
PRE-ASSESSMENTS QUESTIONS

2
FULL LENGTH TESTS

125
POST-ASSESSMENTS QUESTIONS

13 Live Labs

Information Security Fundamentals

- Encrypting Files with EFS

Integrated Information Risk Management

- Conducting Vulnerability Scanning Using Nessus
- Using Social Engineering Techniques to Plan an Attack
- Configuring a VPN

Communications and Network Security

- Configuring a Router
- Configuring Default Routing
- Configuring Network Address Translation
- Finding the Physical and Logical Address of a LAN Adapter
- Getting the UDP Settings and the Current Connection Statistics of UDP

- Tracing Route Using Tracert
- Intercepting Packets
- Configuring VLANs
- Obtaining the ARP Cache and Getting Information about DNS
- Obtaining Information about Different IP Versions and the IP Version of a Network Adapter
- Getting the TCP Settings and Information about the Current Connection Statistics of TCP
- Adding an IPv6 Address
- Assigning Different Classes of IP Addresses
- Using Burp Suite
- Performing ARP Spoofing

Identity and Access Control

- Creating ACL in a Router

Cryptography

- Observing an MD5-Generated Hash Value
- Observing an SHA-Generated Hash Value
- Performing Symmetric Key Encryption
- Using OpenSSL to Create a Public/Private Key Pair

Hardware and Systems Security

- Creating a Virtual Machine

14

support@ucertify.com