(ISC)² SSCP – Systems Security Certified Practitioner

This (ISC)² Systems Security Certified Practitioner (SSCP) training is designed for cybersecurity professionals seeking hands-on expertise in securing IT systems. This course covers application security, network defense, access control mechanisms, cryptographic solutions, and incident response techniques. It also covers cutting-edge topics like the MITRE ATT&CK framework, quantum cryptography, organizational compliance, and advanced network security appliances.□□A premier credential for systems administrators, the SSCP certifies your ability to implement, monitor, and manage secure infrastructure environments following globally recognized (ISC)² standards. The course includes interactive virtual labs and realistic practice exams, ensuring you're ready to pass the SSCP exam and succeed in real cybersecurity roles.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Discussing Ethics and Security Concepts

Code of Ethics

The CIA Triad

Accountability, Privacy and Non-repudiation

Least privilege & Segregation of Duties

Security Controls

Security Control Categories

Other Security Concepts

Validation

Exploring Security Controls and Asset Protection

Introduction

Functions of Security Controls

Asset Management Lifecycle Pt1

Asset Management Lifecycle Pt2

Change Management Lifecycle

Implementing Security Awareness Training

Physical Security Operations

Validation

Exploring Access Controls

Introduction

Methods of Authentication

Biometric Factors

SSO and Device Authentication

Identity Federations

Trust Relationships

Zero Trust Architecture

Zero Trust In Action

WEEK 2

Validation

Learning Network Trust Architecture

Overview

Support Internetwork Trust Architectures

Third Party Connections

The Identity Management Lifecycle

Seeing the Identity Management Lifecycle in Action

Managing by groups instead of individual accounts

Types of Access Control

Validation

Understand the risk management process

Introduction

Risk Visibility and Reporting

Methods of Risk Analysis

Vulnerability Management and CVSS

Risk Management Concepts

Risk Management Frameworks

Risk Tolerance

Risk Treatment

The MITRE ATT&CK Framework

Validation

Examining Security Monitoring and Analysis

Introduction

Legal and Regulatory Concerns

Security Assessment Activities

Organizational Risk Reviews

Vulnerability Management Lifecycle

Source Systems and Events of Interest

Log Management and Event Analysis Systems

WEEK 3

Analyze Monitoring Results

Validation

Supporting the Incident Response Lifecycle

Introduction

The Incident Response Lifecycle

Security Event vs Security Incident

Phase 1

Phase 2

Phase 3

Phase 3 Continued

Phase 4

Security Policy Compliance

Validation

Understanding BC and DR Planning

Introduction

Disaster Recovery and Business Continuity

BCDR Planning Process

Interim or Alternate Processing Strategies

Creating a Business Continuity Plan

Creating a Disaster Recovery Plan

Resiliency and Redundancy

Testing and Drills

Validation

Understand and Support Forensic Investigations

Introduction

Legality and the Process

Ethical Principles

Identifying Forensic Evidence

Evidence Collection Part 1

WEEK 4

Evidence Collection Part 2

Preserving Forensic Evidence

Lets Hash

Reporting of Analysis

Validation

Examining the Basics of Cryptography

Introduction

What Does Cryptography Provide?

Data Sensitivity

Regulatory and Industry Best Practice

Basics of Encryption

Encryption Cipher Types

Cryptographic Entropy

Strength of Encryption Algorithms and Keys

Cryptographic Attacks, Cryptanalysis, and Countermeasures

Validation

Discussing Cryptography and Its Uses

Introduction

Symmetric and Asymmetric Encryption

Elliptic Curve Cryptography

Hashing and Salting

Non-Repudiation

Secure Protocols

Understand Public Key Infrastructure (PKI) and Web of Trust (WoT)

Blockchain

Validation

Understanding Networking Fundamentals

Introduction

The Open System Interconnection (OSI) Model

The TCP/IP Model

Network Topologies and Relationships

Transmission Media Types

Software Defined Networking (SDN)

WEEK 5

Networking Ports

Common Applications

Validation

Managing Network Security

Introduction

Types of Network Attacks

Managing Network Access

Virtual Private Networks (VPNs)

Network Device Placement

Network Segmentation

Secure Device Management

Validation

Securing Networks and Wireless Communications

Introduction

Firewalls

Web Application Firewall (WAF)

Intrusion Detection / Prevention Systems

NAC, DLP and UTM

LANs, Routers, and Switches

Traffic Shaping

Wireless Technologies

Internet of Things (IoT)

Validation

Identify Malicious Code and Endpoint Security

Introduction

Malware and Countermeasures Part 1

Malware and Countermeasures Part 2

Malicious activities and Countermeasures Part 1

Malicious activities and Countermeasures Part 2

Endpoint Device Security Part 1

Endpoint Device Security Part 2

Endpoint Device Security In Action

Social Engineering Attack Methods

Behavior Analytics

Understanding Cloud Security

Introduction

Cloud Deployment Models

Cloud Service Models

Virtualization

Containerization

Legal and Regulatory Concerns

Data Storage, Processing, and Transmission

Third Party/Outsourcing Requirements

Shared Responsibility Model

Validation

Managing Mobile Devices and Virtual Environments

Introduction

Mobile Device Management

MDM Models

MDM Containerization and MAM

Securing Virtualized Systems

Virtualization Components

WEEK 6

WEEK 7

Virtualization Vulnerabilities

Hypervisor Tour

Validation

Last updated 6.30.2025