



Practice
Tests



Video
Training



Flash
Cards



Study
Planner



Review
Exercises

Official Cert Guide

Advance your IT career with hands-on learning

Cisco CyberOps Associate

CBROPS 200-201

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to www.ciscopress.com/register.
2. Enter the print book ISBN: 9780136807834
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the Registered Products tab.
6. Under the book listing, click on the Access Bonus Content link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at PearsonTestPrep.com. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the Activate New Product button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to pearsonitp.echelp.org.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Contents

Introduction

Chapter 1 Cybersecurity Fundamentals

Do I Know This Already? Quiz

Foundation Topics

Introduction to Cybersecurity

Cybersecurity vs. Information Security (Infosec)

The NIST Cybersecurity Framework

Additional NIST Guidance and Documents

The International Organization for Standardization

Threats, Vulnerabilities, and Exploits

What Is a Threat?

What Is a Vulnerability?

What Is an Exploit?

Risk, Assets, Threats, and Vulnerabilities

Threat Actors

Threat Intelligence

Threat Intelligence Platform

Table of Contents

Vulnerabilities, Exploits, and Exploit Kits

SQL Injection

HTML Injection

Command Injection

Authentication-Based Vulnerabilities

Credential Brute-Force Attacks and Password Cracking

Session Hijacking

Default Credentials

Insecure Direct Object Reference Vulnerabilities

Cross-Site Scripting

Cross-Site Request Forgery

Cookie Manipulation Attacks

Race Conditions

Unprotected APIs

Return-to-LibC Attacks and Buffer Overflows

OWASP Top 10

Security Vulnerabilities in Open-Source Software

Network Security Systems

Traditional Firewalls

Packet-Filtering Techniques

Application Proxies

Network Address Translation

Port Address Translation

Static Translation

Stateful Inspection Firewalls

Demilitarized Zones

Firewalls Provide Network Segmentation

Application-Based Segmentation and Micro-segmentation

High Availability

Clustering Firewalls

Table of Contents

Firewalls in the Data Center

Virtual Firewalls

Deep Packet Inspection

Next-Generation Firewalls

Intrusion Detection Systems and Intrusion Prevention Systems

Pattern Matching and Stateful Pattern-Matching Recognition

Protocol Analysis

Heuristic-Based Analysis

Anomaly-Based Analysis

Global Threat Correlation Capabilities

Next-Generation Intrusion Prevention Systems

Firepower Management Center

Advanced Malware Protection

AMP for Endpoints

AMP for Networks

Web Security Appliance

Email Security Appliance

Cisco Security Management Appliance

Cisco Identity Services Engine

Security Cloud-Based Solutions

Cisco Cloud Email Security

Cisco AMP Threat Grid

Umbrella (OpenDNS)

Stealthwatch Cloud

CloudLock

Cisco NetFlow

Data Loss Prevention

The Principles of the Defense-in-Depth Strategy

Table of Contents

Confidentiality, Integrity, and Availability: The CIA Triad

- Confidentiality

- Integrity

- Availability

Risk and Risk Analysis

Personally Identifiable Information and Protected Health Information

- PII

- PHI

Principle of Least Privilege and Separation of Duties

- Principle of Least Privilege

- Separation of Duties

Security Operations Centers

Playbooks, Runbooks, and Runbook Automation

Digital Forensics

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 2 Introduction to Cloud Computing and Cloud Security

Do I Know This Already? Quiz

Foundation Topics

Cloud Computing and the Cloud Service Models

Cloud Security Responsibility Models

- Patch Management in the Cloud

- Security Assessment in the Cloud

DevOps, Continuous Integration (CI), Continuous Delivery (CD), and

DevSecOps

- The Agile Methodology

Table of Contents

DevOps

CI/CD Pipelines

The Serverless Buzzword

A Quick Introduction to Containers and Docker

Container Management and Orchestration

Understanding the Different Cloud Security Threats

Cloud Computing Attacks

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 3 Access Control Models

Do I Know This Already? Quiz

Foundation Topics

Information Security Principles

Subject and Object Definition

Access Control Fundamentals

Identification

Authentication

Authentication by Knowledge

Authentication by Ownership

Authentication by Characteristic

Multifactor Authentication

Authorization

Accounting

Access Control Fundamentals: Summary

Access Control Process

Asset Classification

Table of Contents

Asset Marking

Access Control Policy

Data Disposal

Information Security Roles and Responsibilities

Access Control Types

Access Control Models

Discretionary Access Control

Mandatory Access Control

Role-Based Access Control

Attribute-Based Access Control

Access Control Mechanisms

Identity and Access Control Implementation

Authentication, Authorization, and Accounting Protocols

RADIUS

TACACS+

Diameter

Port-Based Access Control

Port Security

802.1x

Network Access Control List and Firewalling

VLAN Map

Security Group-Based ACL

Downloadable ACL

Firewalling

Identity Management and Profiling

Network Segmentation

Network Segmentation Through VLAN

Firewall DMZ

Cisco TrustSec

Table of Contents

Intrusion Detection and Prevention

Network-Based Intrusion Detection and Protection System

Host-Based Intrusion Detection and Prevention

Antivirus and Antimalware

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 4 Types of Attacks and Vulnerabilities

Do I Know This Already? Quiz

Foundation Topics

Types of Attacks

Reconnaissance Attacks

Social Engineering

Privilege Escalation Attacks

Backdoors

Buffer Overflows and Code Execution

Man-in-the Middle Attacks

Denial-of-Service Attacks

Direct DDoS

Botnets Participating in DDoS Attacks

Reflected DDoS Attacks

Attack Methods for Data Exfiltration

ARP Cache Poisoning

Spoofing Attacks

Route Manipulation Attacks

Password Attacks

Wireless Attacks

Types of Vulnerabilities

Table of Contents

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 5 Fundamentals of Cryptography and Public Key

Infrastructure (PKI)

Do I Know This Already? Quiz

Foundation Topics

Cryptography

 Ciphers and Keys

 Ciphers

 Keys

Key Management

Block and Stream Ciphers

 Block Ciphers

 Stream Ciphers

Symmetric and Asymmetric Algorithms

 Symmetric Algorithms

 Asymmetric Algorithms

 Elliptic Curve

 Quantum Cryptography

 More Encryption Types

 One-Time Pad

 PGP

 Pseudorandom Number Generators

Hashes

 Hashed Message Authentication Code

Digital Signatures

Table of Contents

Digital Signatures in Action

Next-Generation Encryption Protocols

IPsec and SSL/TLS

IPsec

Secure Sockets Layer and Transport Layer Security

SSH

Fundamentals of PKI

Public and Private Key Pairs

RSA Algorithm, the Keys, and Digital Certificates

Certificate Authorities

Root and Identity Certificates

Root Certificate

Identity Certificates

X.500 and X.509v3

Authenticating and Enrolling with the CA

Public Key Cryptography Standards

Simple Certificate Enrollment Protocol

Revoking Digital Certificates

Using Digital Certificates

PKI Topologies

Single Root CA

Hierarchical CA with Subordinate CAs

Cross-Certifying CAs

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 6 Introduction to Virtual Private Networks (VPNs)

Table of Contents

Do I Know This Already? Quiz

Foundation Topics

What Are VPNs?

Site-to-Site vs. Remote-Access VPNs

An Overview of IPsec

- IKEv1 Phase 1

- IKEv1 Phase 2

- IKEv2

SSL VPNs

- SSL VPN Design Considerations

- User Connectivity

- VPN Device Feature Set

- Infrastructure Planning

- Implementation Scope

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 7 Introduction to Security Operations Management

Do I Know This Already? Quiz

Foundation Topics

Introduction to Identity and Access Management

- Phases of the Identity and Access Life Cycle

- Registration and Identity Validation

- Privileges Provisioning

- Access Review

- Access Revocation

- Password Management

Table of Contents

- Password Creation
- Multifactor Authentication
- Password Storage and Transmission
- Password Reset
- Password Synchronization
- Directory Management
- Single Sign-On
- Kerberos
- Federated SSO
- Security Assertion Markup Language
- OAuth
- OpenID Connect

Security Events and Log Management

- Log Collection, Analysis, and Disposal
- Syslog
- Security Information and Event Manager
- Security Orchestration, Automation, and Response (SOAR)
- SOC Case Management (Ticketing) Systems

Asset Management

- Asset Inventory
- Asset Ownership
- Asset Acceptable Use and Return Policies
- Asset Classification
- Asset Labeling
- Asset and Information Handling
- Media Management

Introduction to Enterprise Mobility Management

- Mobile Device Management
- Cisco BYOD Architecture

Table of Contents

Cisco ISE and MDM Integration

Cisco Meraki Enterprise Mobility Management

Configuration and Change Management

Configuration Management

Planning

Identifying and Implementing the Configuration

Controlling the Configuration Changes

Monitoring

Change Management

Vulnerability Management

Vulnerability Identification

Finding Information About a Vulnerability

Vulnerability Scan

Penetration Testing (Ethical Hacking Assessments)

Product Vulnerability Management

Vulnerability Analysis and Prioritization

Vulnerability Remediation

Patch Management

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 8 Fundamentals of Intrusion Analysis

Do I Know This Already? Quiz

Foundation Topics

Introduction to Incident Response

The Incident Response Plan

The Incident Response Process

Table of Contents

The Preparation Phase

The Detection and Analysis Phase

Containment, Eradication, and Recovery

Post-Incident Activity (Postmortem)

Information Sharing and Coordination

Incident Response Team Structure

Computer Security Incident Response Teams

Product Security Incident Response Teams

Security Vulnerabilities and Their Severity

Vulnerability Chaining Role in Fixing Prioritization

How to Fix Theoretical Vulnerabilities

Internally Versus Externally Found Vulnerabilities

National CSIRTs and Computer Emergency Response Teams

Coordination Centers

Incident Response Providers and Managed Security Service Providers (MSSPs)

Common Artifact Elements and Sources of Security Events

The 5-Tuple

File Hashes

Tips on Building Your Own Lab

False Positives, False Negatives, True Positives, and True Negatives

Understanding Regular Expressions

Protocols, Protocol Headers, and Intrusion Analysis

How to Map Security Event Types to Source Technologies

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 9 Introduction to Digital Forensics

Table of Contents

Do I Know This Already? Quiz

Foundation Topics

Introduction to Digital Forensics

The Role of Attribution in a Cybersecurity Investigation

The Use of Digital Evidence

- Defining Digital Forensic Evidence

- Understanding Best, Corroborating, and Indirect or Circumstantial Evidence

- Collecting Evidence from Endpoints and Servers

- Using Encryption

- Analyzing Metadata

- Analyzing Deleted Files

- Collecting Evidence from Mobile Devices

- Collecting Evidence from Network Infrastructure Devices

Evidentiary Chain of Custody

Reverse Engineering

Fundamentals of Microsoft Windows Forensics

- Processes, Threads, and Services

- Memory Management

- Windows Registry

- The Windows File System

- Master Boot Record (MBR)

- The Master File Table (\$MFT)

- Data Area and Free Space

- FAT

- NTFS

- MFT

- Timestamps, MACE, and Alternate Data Streams

- EFI

Fundamentals of Linux Forensics

Table of Contents

Linux Processes

Ext4

Journaling

Linux MBR and Swap File System

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 10 Network Infrastructure Device Telemetry and Analysis

Do I Know This Already? Quiz

Foundation Topics

Network Infrastructure Logs

Network Time Protocol and Why It Is Important

Configuring Syslog in a Cisco Router or Switch

Traditional Firewall Logs

Console Logging

Terminal Logging

ASDM Logging

Email Logging

Syslog Server Logging

SNMP Trap Logging

Buffered Logging

Configuring Logging on the Cisco ASA

Syslog in Large-Scale Environments

Splunk

Graylog

Elasticsearch, Logstash, and Kibana (ELK) Stack

Next-Generation Firewall and Next-Generation IPS Logs

Table of Contents

NetFlow Analysis

What Is a Flow in NetFlow?

The NetFlow Cache

NetFlow Versions

IPFIX

IPFIX Architecture

IPFIX Mediators

IPFIX Templates

Commercial NetFlow Analysis Tools

Open-Source NetFlow Analysis Tools

Big Data Analytics for Cybersecurity Network Telemetry

Cisco Application Visibility and Control (AVC)

Network Packet Capture

tcpdump

Wireshark

Network Profiling

Throughput

Measuring Throughput

Used Ports

Session Duration

Critical Asset Address Space

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 11 Endpoint Telemetry and Analysis

Do I Know This Already? Quiz

Foundation Topics

Table of Contents

Understanding Host Telemetry

- Logs from User Endpoints

- Logs from Servers

Host Profiling

- Listening Ports

- Logged-in Users/Service Accounts

- Running Processes

- Applications Identification

Analyzing Windows Endpoints

- Windows Processes and Threads

- Memory Allocation

- The Windows Registry

- Windows Management Instrumentation

- Handles

- Services

- Windows Event Logs

Linux and macOS Analysis

- Processes in Linux

- Forks

- Permissions

- Symlinks

- Daemons

- Linux-Based Syslog

- Apache Access Logs

- NGINX Logs

Endpoint Security Technologies

- Antimalware and Antivirus Software

- Host-Based Firewalls and Host-Based Intrusion Prevention

- Application-Level Whitelisting and Blacklisting

Table of Contents

System-Based Sandboxing

Sandboxes in the Context of Incident Response

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 12 Challenges in the Security Operations Center (SOC)

Do I Know This Already? Quiz

Foundation Topics

Security Monitoring Challenges in the SOC

Security Monitoring and Encryption

Security Monitoring and Network Address Translation

Security Monitoring and Event Correlation Time Synchronization

DNS Tunneling and Other Exfiltration Methods

Security Monitoring and Tor

Security Monitoring and Peer-to-Peer Communication

Additional Evasion and Obfuscation Techniques

Resource Exhaustion

Traffic Fragmentation

Protocol-Level Misinterpretation

Traffic Timing, Substitution, and Insertion

Pivoting

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 13 The Art of Data and Event Analysis

Table of Contents

Do I Know This Already? Quiz

Foundation Topics

Normalizing Data

Interpreting Common Data Values into a Universal Format

Using the 5-Tuple Correlation to Respond to Security Incidents

Using Retrospective Analysis and Identifying Malicious Files

Identifying a Malicious File

Mapping Threat Intelligence with DNS and Other Artifacts

Using Deterministic Versus Probabilistic Analysis

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 14 Classifying Intrusion Events into Categories

Do I Know This Already? Quiz

Foundation Topics

Diamond Model of Intrusion

Cyber Kill Chain Model

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Action on Objectives

The Kill Chain vs. MITREs ATT&CK

Exam Preparation Tasks

Review All Key Topics

Table of Contents

Define Key Terms

Review Questions

Chapter 15 Introduction to Threat Hunting

Do I Know This Already? Quiz

Foundation Topics

What Is Threat Hunting?

Threat Hunting vs. Traditional SOC Operations vs. Vulnerability Management

The Threat-Hunting Process

Threat-Hunting Maturity Levels

Threat Hunting and MITREs ATT&CK

Automated Adversarial Emulation

Threat-Hunting Case Study

Threat Hunting, Honeypots, Honeynets, and Active Defense

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 16 Final Preparation

Hands-on Activities

Suggested Plan for Final Review and Study

Summary

Glossary of Key Terms

A

B

C

D

E

Table of Contents

F
H
I
J
K
L
M
N
O
P
R
S
T
V
W
Z

Appendix A Answers to the Do I Know This Already?

Quizzes and Review Questions

Appendix B Understanding Cisco Cybersecurity Operations

Fundamentals CBROPS 200-201 Exam Updates

Index