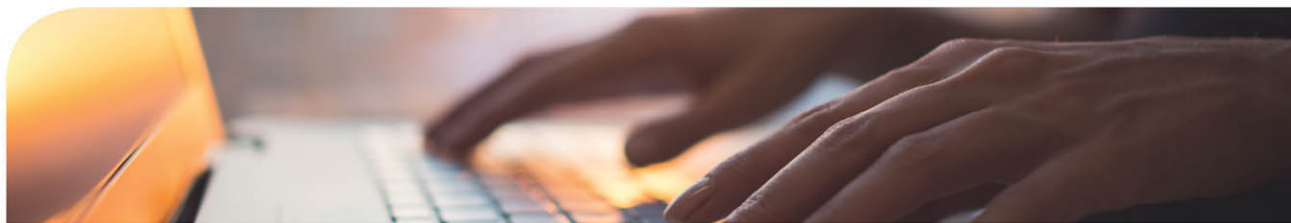


DAVID L. PROWSE



# Cert Guide

Learn, prepare, and practice for exam success



# CompTIA® Security+ SY0-501



PEARSON IT  
CERTIFICATION

**Save 10%  
on Exam  
Voucher**

See Inside

## FEATURES

Three Complete Practice Exams, More Than  
30 Videos and 30 Interactive Exercises

Exclusive Offer – 40% OFF

# Pearson IT Certification Video Training

livelessons®

[pearsonitcertification.com/video](http://pearsonitcertification.com/video)

Use coupon code PITCVIDEO40 during checkout.

## Video Instruction from Technology Experts



### Advance Your Skills

Get started with fundamentals, become an expert, or get certified.



### Train Anywhere

Train anywhere, at your own pace, on any device.



### Learn

Learn from trusted author trainers published by Pearson IT Certification.

## Try Our Popular Video Training for FREE!

[pearsonitcertification.com/video](http://pearsonitcertification.com/video)

Explore hundreds of **FREE** video lessons from our growing library of Complete Video Courses, LiveLessons, networking talks, and workshops.

PEARSON  
IT CERTIFICATION

[pearsonitcertification.com/video](http://pearsonitcertification.com/video)

# CompTIA Security+ SY0-501 Cert Guide

## Table of Contents

Cover

Title Page

Copyright Page

About the Author

Acknowledgments

About the Technical Reviewer

Table of Contents

Introduction

Chapter 1 Introduction to Security

- Foundation Topics

- Security 101

  - The CIA of Computer Security

  - The Basics of Information Security

- Think Like a Hacker

- Threat Actor Types and Attributes

- Chapter Review Activities

  - Review Key Topics

  - Define Key Terms

  - Review Questions

  - Answers and Explanations

Chapter 2 Computer Systems Security Part I

- Foundation Topics

- Malicious Software Types

# **Table of Contents**

Viruses

Worms

Trojan Horses

Ransomware

Spyware

Rootkits

Spam

Summary of Malware Threats

## **Delivery of Malware**

Via Software, Messaging, and Media

Botnets and Zombies

Active Interception

Privilege Escalation

Backdoors

Logic Bombs

## **Preventing and Troubleshooting Malware**

Preventing and Troubleshooting Viruses

Preventing and Troubleshooting Worms and Trojans

Preventing and Troubleshooting Spyware

Preventing and Troubleshooting Rootkits

Preventing and Troubleshooting Spam

You Can't Save Every Computer from Malware!

Summary of Malware Prevention Techniques

## **Chapter Summary**

## **Chapter Review Activities**

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

# **Table of Contents**

## **Chapter 3 Computer Systems Security Part II**

### **Foundation Topics**

### **Implementing Security Applications**

- Personal Software Firewalls

- Host-Based Intrusion Detection Systems

- Pop-Up Blockers

- Data Loss Prevention Systems

### **Securing Computer Hardware and Peripherals**

- Securing the BIOS

- Securing Storage Devices

- Removable Storage

- Network Attached Storage

- Whole Disk Encryption

- Hardware Security Modules

- Securing Wireless Peripherals

### **Securing Mobile Devices**

- Malware

- Botnet Activity

- SIM Cloning and Carrier Unlocking

- Wireless Attacks

- Theft

- Application Security

- BYOD Concerns

### **Chapter Summary**

### **Chapter Review Activities**

- Review Key Topics

- Define Key Terms

- Complete the Real-World Scenarios

- Review Questions

# **Table of Contents**

Answers and Explanations

## **Chapter 4 OS Hardening and Virtualization**

Foundation Topics

Hardening Operating Systems

Removing Unnecessary Applications and Services

Windows Update, Patches, and Hotfixes

Patches and Hotfixes

Patch Management

Group Policies, Security Templates, and Configuration Baselines

Hardening File Systems and Hard Drives

Virtualization Technology

Types of Virtualization and Their Purposes

Hypervisor

Securing Virtual Machines

Chapter Summary

Chapter Review Activities

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 5 Application Security**

Foundation Topics

Securing the Browser

General Browser Security Procedures

Implement Policies

Train Your Users

Use a Proxy and Content Filter

Secure Against Malicious Code

# **Table of Contents**

Web Browser Concerns and Security Methods

Basic Browser Security

Cookies

LSOs

Add-ons

Advanced Browser Security

## **Securing Other Applications**

## **Secure Programming**

Software Development Life Cycle

Core SDLC and DevOps Principles

Programming Testing Methods

White-box and Black-box Testing

Compile-Time Errors Versus Runtime Errors

Input Validation

Static and Dynamic Code Analysis

Fuzz Testing

Programming Vulnerabilities and Attacks

Backdoors

Memory/Buffer Vulnerabilities

Arbitrary Code Execution/Remote Code Execution

XSS and XSRF

More Code Injection Examples

Directory Traversal

Zero Day Attack

## **Chapter Summary**

## **Chapter Review Activities**

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

# **Table of Contents**

Answers and Explanations

## **Chapter 6 Network Design Elements**

Foundation Topics

Network Design

The OSI Model

Network Devices

Switch

Bridge

Router

Network Address Translation, and Private Versus Public IP

Network Zones and Interconnections

LAN Versus WAN

Internet

Demilitarized Zone (DMZ)

Intranets and Extranets

Network Access Control (NAC)

Subnetting

Virtual Local Area Network (VLAN)

Telephony

Modems

PBX Equipment

VoIP

Cloud Security and Server Defense

Cloud Computing

Cloud Security

Server Defense

File Servers

Network Controllers

E-mail Servers

Web Servers



# **Table of Contents**

FTP Server

Chapter Summary

Chapter Review Activities

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 7 Networking Protocols and Threats**

Foundation Topics

Ports and Protocols

Port Ranges, Inbound Versus Outbound, and Common Ports

Protocols That Can Cause Anxiety on the Exam

Malicious Attacks

DoS

DDoS

Sinkholes and Blackholes

Spoofing

Session Hijacking

Replay

Null Sessions

Transitive Access and Client-Side Attacks

DNS Poisoning and Other DNS Attacks

ARP Poisoning

Summary of Network Attacks

Chapter Summary

Chapter Review Activities

Review Key Topics

Define Key Terms

# **Table of Contents**

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 8 Network Perimeter Security**

Foundation Topics

Firewalls and Network Security

Firewalls

Proxy Servers

Honeypots and Honeynets

Data Loss Prevention (DLP)

NIDS Versus NIPS

NIDS

NIPS

Summary of NIDS Versus NIPS

The Protocol Analyzers Role in NIDS and NIPS

Unified Threat Management

Chapter Summary

Chapter Review Activities

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 9 Securing Network Media and Devices**

Foundation Topics

Securing Wired Networks and Devices

Network Device Vulnerabilities

Default Accounts

Weak Passwords

# **Table of Contents**

Privilege Escalation

Back Doors

Network Attacks

Other Network Device Considerations

Cable Media Vulnerabilities

Interference

Crosstalk

Data Emanation

Tapping into Data and Conversations

## **Securing Wireless Networks**

Wireless Access Point Vulnerabilities

The Administration Interface

SSID Broadcast

Rogue Access Points

Evil Twin

Weak Encryption

Wi-Fi Protected Setup

Ad Hoc Networks

VPN over Open Wireless

Wireless Access Point Security Strategies

Wireless Transmission Vulnerabilities

Bluetooth and Other Wireless Technology Vulnerabilities

Bluejacking

Bluesnarfing

RFID and NFC

More Wireless Technologies

## **Chapter Summary**

## **Chapter Review Activities**

Review Key Topics

Define Key Terms

# **Table of Contents**

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 10 Physical Security and Authentication Models**

### **Foundation Topics**

#### **Physical Security**

General Building and Server Room Security

Door Access

Biometric Readers

#### **Authentication Models and Components**

Authentication Models

Localized Authentication Technologies

802.1X and EAP

LDAP

Kerberos and Mutual Authentication

Remote Desktop Services

Remote Authentication Technologies

Remote Access Service

Virtual Private Networks

RADIUS Versus TACACS

### **Chapter Summary**

### **Chapter Review Activities**

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 11 Access Control Methods and Models**

### **Foundation Topic**

# **Table of Contents**

## **Access Control Models Defined**

- Discretionary Access Control
- Mandatory Access Control
- Role-Based Access Control (RBAC)
- Attribute-based Access Control (ABAC)
- Access Control Wise Practices

## **Rights, Permissions, and Policies**

- Users, Groups, and Permissions
- Permission Inheritance and Propagation
- Moving and Copying Folders and Files
- Username and Passwords
- Policies
- User Account Control (UAC)

## **Chapter Summary**

## **Chapter Review Activities**

- Review Key Topics
- Define Key Terms
- Complete the Real-World Scenarios
- Review Questions
- Answers and Explanations

## **Chapter 12 Vulnerability and Risk Assessment**

### **Foundation Topics**

### **Conducting Risk Assessments**

- Qualitative Risk Assessment
- Quantitative Risk Assessment
- Security Analysis Methodologies
- Security Controls
- Vulnerability Management
- Penetration Testing

# **Table of Contents**

OVAL

Additional Vulnerabilities

## **Assessing Vulnerability with Security Tools**

Network Mapping

Vulnerability Scanning

Network Sniffing

Password Analysis

## **Chapter Summary**

## **Chapter Review Activities**

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 13 Monitoring and Auditing**

### **Foundation Topics**

### **Monitoring Methodologies**

Signature-Based Monitoring

Anomaly-Based Monitoring

Behavior-Based Monitoring

### **Using Tools to Monitor Systems and Networks**

Performance Baselining

Protocol Analyzers

Wireshark

SNMP

Analytical Tools

Use Static and Dynamic Tools

### **Conducting Audits**

Auditing Files

# **Table of Contents**

Logging

Log File Maintenance and Security

Auditing System Security Settings

SIEM

Chapter Summary

Chapter Review Activities

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 14 Encryption and Hashing Concepts**

Foundation Topics

Cryptography Concepts

Symmetric Versus Asymmetric Key Algorithms

Symmetric Key Algorithms

Asymmetric Key Algorithms

Public Key Cryptography

Key Management

Steganography

Encryption Algorithms

DES and 3DES

AES

RC

Blowfish and Twofish

Summary of Symmetric Algorithms

RSA

Diffie-Hellman

Elliptic Curve

# Table of Contents

More Encryption Types

One-Time Pad

PGP

Pseudorandom Number Generators

## Hashing Basics

Cryptographic Hash Functions

MD5

SHA

RIPEMD and HMAC

LANMAN, NTLM, and NTLMv2

LANMAN

NTLM and NTLMv2

Hashing Attacks

Pass the Hash

Happy Birthday!

Additional Password Hashing Concepts

## Chapter Summary

## Chapter Review Activities

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## Chapter 15 PKI and Encryption Protocols

### Foundation Topics

### Public Key Infrastructure

Certificates

SSL Certificate Types

Single-Sided and Dual-Sided Certificates



# **Table of Contents**

Certificate Chain of Trust

Certificate Formats

Certificate Authorities

Web of Trust

## **Security Protocols**

S/MIME

SSL/TLS

SSH

PPTP, L2TP, and IPsec

PPTP

L2TP

IPsec

## **Chapter Summary**

## **Chapter Review Activities**

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 16 Redundancy and Disaster Recovery**

### **Foundation Topics**

### **Redundancy Planning**

Redundant Power

Redundant Power Supplies

Uninterruptible Power Supplies

Backup Generators

Redundant Data

Redundant Networking

Redundant Servers

# **Table of Contents**

Redundant Sites

Redundant People

## **Disaster Recovery Planning and Procedures**

Data Backup

DR Planning

## **Chapter Summary**

Chapter Review Activities

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 17 Social Engineering, User Education, and Facilities Security**

### **Foundation Topics**

### **Social Engineering**

Pretexting

Malicious Insider

Diversion Theft

Phishing

Hoaxes

Shoulder Surfing

Eavesdropping

Dumpster Diving

Baiting

Piggybacking/Tailgating

Watering Hole Attack

Summary of Social Engineering Types

### **User Education**

# **Table of Contents**

## Facilities Security

- Fire Suppression
- Fire Extinguishers
- Sprinkler Systems
- Special Hazard Protection Systems
- HVAC
- Shielding
- Vehicles

## Chapter Summary

## Chapter Review Activities

- Review Key Topics
- Define Key Terms
- Complete the Real-World Scenarios
- Review Questions
- Answers and Explanations

## Chapter 18 Policies and Procedures

### Foundation Topics

### Legislative and Organizational Policies

- Data Sensitivity and Classification of Information
- Personnel Security Policies
- Privacy Policies
- Acceptable Use
- Change Management
- Separation of Duties/Job Rotation
- Mandatory Vacations
- Onboarding and Offboarding
- Due Diligence
- Due Care
- Due Process

# **Table of Contents**

User Education and Awareness Training

Summary of Personnel Security Policies

How to Deal with Vendors

How to Dispose of Computers and Other IT Equipment Securely

Incident Response Procedures

IT Security Frameworks

Chapter Summary

Chapter Review Activities

Review Key Topics

Define Key Terms

Complete the Real-World Scenarios

Review Questions

Answers and Explanations

## **Chapter 19 Taking the Real Exam**

Getting Ready and the Exam Preparation Checklist

Tips for Taking the Real Exam

Beyond the CompTIA Security+ Certification

## **Practice Exam 1: SY0-501**

Answers to Practice Exam 1

Answers with Explanations

## **Glossary**

A

B

C

D

E

F

G

# **Table of Contents**

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Index

Where are the companion content files?