uCertify

CompTIA Security+ (SY0-601)

Lesson Practice test Live-Lab

01 Sep 2023

8. 1 Introduction

   2 Today's Security Professional

   3 Cybersecurity Threat Landscape

   4 Malicious Code

   5 Social Engineering, Physical, and Password Attacks

   6 Security Assessment and Testing

   7 Secure Coding

   8 Cryptography and the Public Key Infrastructure

   9 Identity and Access Management

   10 Resilience and Physical Security

   11 Cloud and Virtualization Security

   12 Endpoint Security

   13 Network Security

   14 Wireless and Mobile Security

   15 Incident Response

   16 Digital Forensics

   17 Security Policies, Standards, and Compliance

   18 Risk Management and Privacy

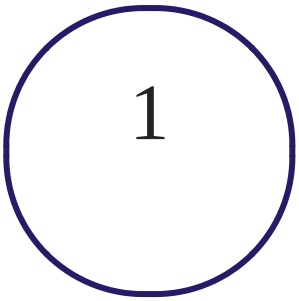
10.

1

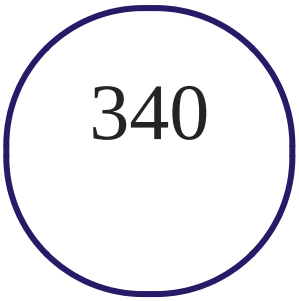
Gain hands-on experience to pass the CompTIA Security+ certification exam with the CompTIA Security+ (SY0-601) course and lab. Interactive chapters and hands-on labs comprehensively cover the SY0-601 exam objectives and provide knowledge in areas such as security concepts, operating systems, application systems, and many more. The CompTIA Security+ study guide will help you get a full understanding of the challenges you'll face as a security professional.

2

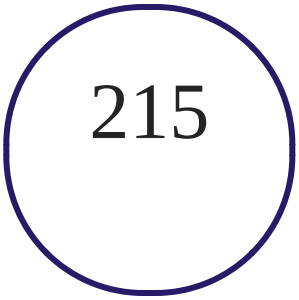
3



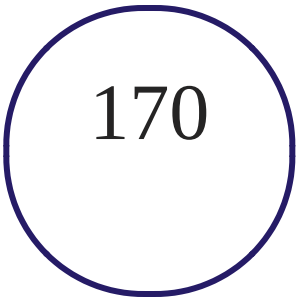
4



5



6



7

8

9

10

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

11

1: Introduction

- The Security+ Exam
- What Does This Course Cover?
- Exam SY0-601 Exam Objectives

- Malicious Code
- Adversarial Artificial Intelligence
- Summary
- Exam Essentials

5: Social Engineering, Physical, and Password Attacks

- Social Engineering
- Password Attacks
- Physical Attacks
- Summary
- Exam Essentials

6: Security Assessment and Testing

- Vulnerability Management
- Security Vulnerabilities
- Penetration Testing
- Training and Exercises
- Summary

- Exam Essentials

7: Secure Coding

- Software Assurance Best Practices
- Designing and Coding for Security
- Software Security Testing
- Injection Vulnerabilities
- Exploiting Authentication Vulnerabilities
- Exploiting Authorization Vulnerabilities
- Exploiting Web Application Vulnerabilities
- Application Security Controls
- Secure Coding Practices
- Summary
- Exam Essentials

8: Cryptography and the Public Key Infrastructure

- An Overview of Cryptography
- Goals of Cryptography

- Cryptographic Concepts
- Modern Cryptography
- Symmetric Cryptography
- Asymmetric Cryptography
- Hash Functions
- Digital Signatures
- Public Key Infrastructure
- Asymmetric Key Management
- Cryptographic Attacks
- Emerging Issues in Cryptography
- Summary
- Exam Essentials

9: Identity and Access Management

- Identity
- Authentication and Authorization
- Authentication Methods
- Accounts

- Access Control Schemes
- Summary
- Exam Essentials

10: Resilience and Physical Security

- Building Cybersecurity Resilience
- Response and Recovery Controls
- Physical Security Controls
- Summary
- Exam Essentials

11: Cloud and Virtualization Security

- Exploring the Cloud
- Virtualization
- Cloud Infrastructure Components
- Cloud Security Issues
- Cloud Security Controls
- Summary

- Exam Essentials

12: Endpoint Security

- Protecting Endpoints
- Service Hardening
- Operating System Hardening
- Securing Embedded and Specialized Systems
- Summary
- Exam Essentials

13: Network Security

- Designing Secure Networks
- Secure Protocols
- Attacking and Assessing Networks
- Network Reconnaissance and Discovery Tools and Techniques
- Summary
- Exam Essentials

14: Wireless and Mobile Security

- Building Secure Wireless Networks
- Managing Secure Mobile Devices
- Summary
- Exam Essentials

15: Incident Response

- Incident Response
- Incident Response Data and Tools
- Mitigation and Recovery
- Summary
- Exam Essentials

16: Digital Forensics

- Digital Forensic Concepts
- Conducting Digital Forensics
- Reporting
- Digital Forensics and Intelligence

- Summary
- Exam Essentials

17: Security Policies, Standards, and Compliance

- Understanding Policy Documents
- Personnel Management
- Third-Party Risk Management
- Complying with Laws and Regulations
- Adopting Standard Frameworks
- Security Control Verification and Quality Control
- Summary
- Exam Essentials

18: Risk Management and Privacy

- Analyzing Risk
- Managing Risk
- Risk Analysis
- Disaster Recovery Planning

- Privacy
- Summary
- Exam Essentials

81	12:56
VIDEOS	HOURS

12

90	2	90
PRE-ASSESSMENTS QUESTIONS	FULL LENGTH TESTS	POST-ASSESSMENTS QUESTIONS

13 Live Labs

-

Malicious Code

- Identifying Virus Threats
- Detecting Rootkits

Social Engineering, Physical, and Password Attacks

- Using Social Engineering Techniques to Plan an Attack
- Cracking a Linux Password Using John the Ripper

Security Assessment and Testing

- Conducting Vulnerability Scanning Using Nessus

Secure Coding

- Exploiting a Website Using SQL Injection
- Conducting a Cross-Site Request Forgery Attack
- Attacking a Website Using XSS Injection
- Defending Against a Buffer Overflow Attack

Cryptography and the Public Key Infrastructure

- Performing Symmetric Encryption
- Examining Asymmetric Encryption
- Observing an SHA-Generated Hash Value
- Observing an MD5-Generated Hash Value
- Examining PKI Certificates
- Using Rainbow Tables to Crack Passwords

Identity and Access Management

- Examining Kerberos Settings

- Installing a RADIUS Server

Resilience and Physical Security

- Configuring RAID 5

Endpoint Security

- Using the chmod Command
- Examining File Manipulation Commands

Network Security

- Configuring a Standard ACL
- Implementing Port Security
- Configuring a BPDU Guard on a Switch Port
- Configuring VLANs
- Using Windows Firewall
- Performing ARP Poisoning
- Using the ifconfig Command
- Using the traceroute Command
- Capturing Packets Using Wireshark
- Performing Reconnaissance on a Network
- Using the theHarvester Tool to Gather Information about a Victim
- Using the hping Program
- Using Reconnaissance Tools

Incident Response

- Viewing Linux event logs
- Using Event Viewer
- Making Syslog Entries Readable

Digital Forensics

- Using FTK Imager

Security Policies, Standards, and Compliance

- Configuring a Password Policy

38	38	01:03
LIVE LABS	VIDEO TUTORIALS	HOURS

14