

EXAM✓CRAM

CompTIA®  
**Security+**  
SY0-601

Save 10%  
on Exam  
Voucher

See Inside

## **CompTIA® Security+ SY0-601 Exam Cram, Companion Website**

---

Access interactive study tools on this book's companion website, including practice test software, Glossary, and Cram Sheet.

To access the companion website, simply follow these steps:

1. Go to **[www.pearsonitcertification.com/register](http://www.pearsonitcertification.com/register)**.
2. Enter the print book ISBN: **9780136798675**.
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.

If you have any issues accessing the companion website, you can contact our support team by going to **<http://pearsonitp.echelp.org>**.

# CompTIA Security+ SY0-601 Exam Cram

## Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Table of Contents

Introduction

Part I: Attacks, Threats, and Vulnerabilities

CHAPTER 1: Social Engineering Techniques

The Social Engineer

Tailgating

Dumpster Diving

Shoulder Surfing

Phishing and Related Attacks

Watering Hole Attacks

Typo Squatting

Hoaxes and Influence Campaigns

Principles of Influence (Reasons for Effectiveness)

What Next?

CHAPTER 2: Attack Basics

Malware

Viruses

Worms

Trojan

# Table of Contents

- Rootkits
- Logic Bombs
- Bots
- Crypto-Malware
- Potentially Unwanted Programs (PUPs)
  - Spyware
  - Adware
  - Cryptomining Software

## Physical Attacks

Adversarial Artificial Intelligence (AI)

Password Attacks

- Birthday Attacks

Downgrade Attacks

What Next?

## CHAPTER 3: Application Attacks

Race Conditions

Improper Software Handling

Resource Exhaustion

Overflows

Code Injections

Driver Manipulation

Request Forgeries

Directory Traversal

Replay Attack

Secure Sockets Layer (SSL) Stripping

Application Programming Interface (API) Attacks

Pass-the-Hash Attack

What Next?

## CHAPTER 4: Network Attacks

Wireless

# Table of Contents

Short-Range Wireless Communications

Bluetooth

Near-Field Communication

RFID

On-Path Attack

Layer 2 Attacks

MAC Spoofing

ARP Poisoning

MAC Flooding

Port Stealing

Domain Name System (DNS) Attacks

Domain Hijacking

Universal Resource Locator (URL) Redirection

DNS Poisoning

Denial of Service

Distributed DoS

Malicious Code and Script Execution

What Next?

## CHAPTER 5: Threat Actors, Vectors, and Intelligence

Sources

Threat Actor Attributes

Threat Actor Types

Script Kiddies

Insiders

Hacktivists

Criminal Syndicates

Competitors

State Actors

Vectors

Threat Intelligence and Research Sources

Sharing Centers

Open-Source Intelligence

# **Table of Contents**

What Next?

## **CHAPTER 6: Vulnerabilities**

Cloud-Based vs. On-Premises

Zero-Day

Weak Configurations

Improper or Weak Patch Management

Third-Party Risks

Impacts

What Next?

## **CHAPTER 7: Security Assessment Techniques**

Vulnerability Scans

Intrusive vs. Non-Intrusive

Credentialed vs. Non-Credentialed

Threat Assessment

Security Information and Event Management (SIEM)

Threat Hunting

Security Orchestration, Automation, and Response (SOAR)

What Next?

## **CHAPTER 8: Penetration Testing Techniques**

Testing Methodology

Planning

Discovery

Attack

Reporting

Team Exercises

What Next?

## **Part II: Architecture and Design**

### **CHAPTER 9: Enterprise Security Concepts**

Configuration Management

# Table of Contents

Data Confidentiality

Data Loss Prevention

- Cloud Access Security Brokers

Encryption and Data Obfuscation

- Rights Management

- Hardware Security Module (HSM)

- Encrypted Traffic Management

Data Integrity

Data Availability

- Site Resiliency

- Geographic Considerations

Deception and Disruption

What Next?

## CHAPTER 10: Virtualization and Cloud Computing

Virtualization

- Hypervisors

  - Type I Hypervisors

  - Type II Hypervisors

  - Type I vs. Type II Hypervisors

- Containers and Microservices

- Virtual Desktop Infrastructure (VDI)

- Virtual Machine (VM) Sprawl Avoidance

- VM Escape Protection

- Software-Defined Networking (SDN)

- Infrastructure as Code (IaC)

On-Premises vs. Off-Premises

Cloud Models

- Service Models

  - IaaS

  - PaaS

  - SaaS

- Deployment Models

# Table of Contents

Private

Public

Hybrid

Community

What Next?

## CHAPTER 11: Secure Application Development, Deployment, and Automation

Application Environment

Development and Testing

Staging and Production

Provisioning and Deprovisioning

Integrity Measurement

Change Management and Version Control

Secure Coding Techniques

Normalization

Stored Procedures

Encryption, Obfuscation, and Camouflage

Code Reuse and Dead Code

Use of Third-Party Libraries and SDKs

Server-Side vs. Client-Side Execution and Validation

Data Exposure

Proper Error Handling

Proper Input Validation

Code Signing

Memory Management

Automation and Scripting

Secure DevOps

Scalability and Elasticity

What Next?

## CHAPTER 12: Authentication and Authorization Design

Identification and Authentication, Authorization, and Accounting (AAA)

Multifactor Authentication

# Table of Contents

## Single Sign-on

- Federation

- Transitive Trust

## Authentication Technologies

- Tokens

- Biometrics

- Card Authentication

- Certificate-Based Authentication

## What Next?

## CHAPTER 13: Cybersecurity Resilience

### Redundancy

- High Availability

- Load Balancers

  - NIC Teaming

- RAID

### Backups

- Full Backups

- Differential Backups

- Incremental Backups

- Copies and Snapshots

- Non-persistence

  - Revert to Known State or Good Configuration

  - Live Boot Media

### Defense in Depth

### What Next?

## CHAPTER 14: Embedded and Specialized Systems

### Embedded Systems

- SoC and RTOS

### SCADA and ICS

### Smart Devices and IoT

- Heating, Ventilation, Air Conditioning (HVAC)

- Multifunction Devices

# Table of Contents

Surveillance Systems

Special-Purpose Devices

Medical Devices

Vehicles

Aircraft and UAV

Resource Constraints

What Next?

## CHAPTER 15: Physical Security Controls

### Perimeter Security

Signs, Fencing, and Gates

Lighting

Barricades and Bollards

Cameras

Security Guards

### Internal Security

Alarms

Motion and Infrared Detection

Access Control Vestibules

Locks and Lock Types

### Equipment Security

Cable Locks

Cages and Safes

Locking Cabinets and Enclosures

Screen Filters

Air Gaps

### Environmental Controls

Protected Cabling, Protected Distribution, and Faraday Cages

HVAC

Fire Suppression

Hot and Cold Aisles

Secure Data Destruction

What Next?

# **Table of Contents**

## **CHAPTER 16: Cryptographic Concepts**

### **Cryptosystems**

#### **Keys**

##### **Key Exchange**

#### **Symmetric Algorithms**

#### **Asymmetric Algorithms**

#### **Elliptic Curve and Emerging Cryptography**

#### **Session Keys**

#### **Nonrepudiation and Digital Signatures**

#### **Hashing**

### **Use of Proven Technologies and Implementation**

### **Steganography**

### **Cryptography Use Cases**

### **Cryptography Constraints**

### **What Next?**

## **Part III: Implementation**

## **CHAPTER 17: Secure Protocols**

### **Secure Web Protocols**

#### **Internet Protocol Security (IPsec)**

### **Secure File Transfer Protocols**

### **Secure Email Protocols**

### **Secure Internet Protocols**

#### **Lightweight Directory Access Protocol (LDAP)**

#### **Secure Real-Time Transport Protocol (SRTP)**

#### **Simple Network Management Protocol (SNMP)**

### **Secure Protocol Use Cases**

#### **Secure Web Communication**

##### **Using HTTPS for Web Communications**

##### **Using SSL/TLS for Remote Access**

##### **Using DNSSEC for Domain Name Resolution**

#### **Secure File Transfer Communication**

# Table of Contents

Using FTPS and SFTP for File Transfer

## Secure Email Communications

Using S/MIME, POP3S, and IMAPS for Email

## Securing Internal Communications

Using SRTP for Voice and Video

Using LDAPS for Directory Services

Using SNMPv3 with Routing and Switching

Using Network Address Allocation

Using Time Synchronization

Using Subscription Services

## What Next?

## CHAPTER 18: Host and Application Security Solutions

### Endpoint Protection

Firewalls and HIPS/HIDS Solutions

#### Anti-Malware and Other Host Protections

Endpoint Detection and Response (EDR)

Data Execution Prevention (DEP)

Data Loss Prevention (DLP)

Removable Media Control

Application Allow/Block Lists

Web Application Firewall

### Application Security

#### Code Analyzers

Static Code Analyzers

Dynamic Analysis

Stress Testing

Application Sandboxing

### Hardware and Firmware Security

FDE and SED

TPM and HSM

Boot Integrity

Boot Attestation

Hardware Root of Trust

### Operating System Security

# **Table of Contents**

- Patch Management
- Disabling Unnecessary Ports and Services
- Least Functionality
- Secure Configurations
- Trusted Operating System

What Next?

## **CHAPTER 19: Secure Network Design**

### **Network Devices and Segmentation**

- Routers
  - Network Address Translation (NAT)
- Switches
  - Port Security
- Virtual Local Area Network (VLAN)
- Bridges

### **Security Devices and Boundaries**

- Screened Subnet
- Web Application Firewalls
- Proxies
- Unified Threat Management (UTM)
- VPN Concentrators
- NIDS and NIPS
  - Detection Methods
  - Analytics
- Network Access Control (NAC)

What Next?

## **CHAPTER 20: Wireless Security Settings**

### **Access Methods**

### **Wireless Cryptographic Protocols**

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
  - Temporal Key Integrity Protocol
  - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
- Wi-Fi Protected Access Version 2 (WPA2)

# **Table of Contents**

Wi-Fi Protected Access Version 3 (WPA3)

Authentication Protocols

Wireless Access Installations

Antenna Types, Placement, and Power

MAC Filter

Disabling SSID Broadcast

What Next?

## **CHAPTER 21: Secure Mobile Solutions**

Communication Methods

Mobile Device Management Concepts

Device, Application, and Content Management

Mobile Device Management

Mobile Content Management

Mobile Application Management

Protections

Screen Locks, Passwords, and PINs

Biometrics and Context-Aware Authentication

Remote Wiping

Geolocation, Geofencing, and Push Notifications

Storage Segmentation and Containerization

Full Device Encryption (FDE)

Enforcement and Monitoring

Jailbreaking and Rooting

Custom Firmware, Carrier Unlocking, and OTA Updates

Third-Party App Stores and Sideloading

Storage and USB OTG

Enforcement for Normal Device Functions

Wi-Fi Methods, Tethering, and Payments

Deployment Models

BYOD, CYOD, COPE, and Corporate-Owned Devices

Virtual Desktop Infrastructure

Deployment Strategies

Architecture/Infrastructure Considerations

# **Table of Contents**

Adherence to Corporate Policies and Acceptable Use

Legal Concerns

Privacy

Data Ownership and Support

Patch and Antivirus Management

Forensics

What Next?

## **CHAPTER 22: Cloud Cybersecurity Solutions**

### **Cloud Workloads**

Regions and Availability Zones

Virtual Private Cloud (VPC)

Security Groups

Policies

Managing Secrets

Central Logging

### **Third-Party Cloud Security Solutions**

What Next?

## **CHAPTER 23: Identity and Account Management Controls**

### **Account Types**

### **Account Management**

Onboarding and Offboarding

Least Privilege

Access Auditing and Reviews

Time of Day and Location Restrictions

Logical Access Controls

### **Account Policy Enforcement**

Password Complexity

Account Expiration

Forgotten Passwords

Account Lockout

Password Age and History

# **Table of Contents**

Password Length and Rotation

What Next?

## **CHAPTER 24: Authentication and Authorization Solutions**

### **Authentication**

Unencrypted Plaintext Credentials

Filesystem Permissions

Access Violations

Authentication Issues

Authentication Protocols

802.1X

AAA Protocols and Services

Federated Services

Kerberos

### **Access Control**

Privileged Access Management

What Next?

## **CHAPTER 25: Public Key Infrastructure**

### **PKI Components**

#### **Certificate Authority (CA)**

Certification Practice Statement

Trust Models

Key Escrow

#### **Digital Certificate**

Public and Private Key Usage

Certificate Signing Request

Certificate Policy

Certificate Types

Certificate Formats

#### **Certificate Revocation**

#### **OCSP Stapling**

#### **Pinning**

# **Table of Contents**

What Next?

## **Part IV: Operations and Incident Response**

### **CHAPTER 26: Organizational Security**

Shell and Script Environments

Network Reconnaissance and Discovery

Exploitation Frameworks

Packet Capture and Replay

Password Crackers

Forensics and Data Sanitization

What Next?

### **CHAPTER 27: Incident Response**

Attack Frameworks

Cyber Kill Chain

MITRE ATT&CK

Diamond Model of Intrusion Analysis

Incident Response Plan

Documented Incident Type/Category Definitions

Roles and Responsibilities

Reporting Requirements and Escalation

Cyber-Incident Response Teams

Training, Tests, and Exercises

Incident Response Process

Preparation

Incident Identification and Analysis

Containment, Eradication, and Recovery

Post-Incident Activities

Continuity and Recovery Plans

Disaster Recovery

Continuity of Operations Planning

What Next?

# **Table of Contents**

## **CHAPTER 28: Incident Investigation**

- SIEM Dashboards

- Logging

- Network Activity

  - Protocol Analyzers

  - Network Flow

- What Next?

## **CHAPTER 29: Incident Mitigation**

- Containment and Eradication

  - Quarantining

  - Configuration Changes

    - Firewalls

    - Application Control

  - Secure Orchestration, Automation, and Response (SOAR)

- What Next?

## **CHAPTER 30: Digital Forensics**

- Data Breach Notifications

- Strategic Intelligence/Counterintelligence Gathering

- Track Person-hours

- Order of Volatility

- Chain of Custody

- Data Acquisition

  - Capture System Images

  - Capture Network Traffic and Logs

  - Capture Video and Photographs

  - Record Time Offset

  - Take Hashes

  - Capture Screenshots

  - Collect Witness Interviews

- What Next?

## **Part V: Governance, Risk, and Compliance**

# **Table of Contents**

## **CHAPTER 31: Control Types**

Nature of Controls

Functional Use of Controls

Deterrent Controls

Preventive Controls

Detective Controls

Corrective Controls

Compensating Controls

What Next?

## **CHAPTER 32: Regulations, Standards, and Frameworks**

Industry-Standard Frameworks and Reference Architectures

Regulatory and Non-regulatory Requirements

Industry-Specific Frameworks

Benchmarks and Secure Configuration Guides

Platform- and Vendor-Specific Guides

General-Purpose Guides

What Next?

## **CHAPTER 33: Organizational Security Policies**

Policy Framework

Human Resource Management Policies

Background Checks

Onboarding and Offboarding

Mandatory Vacations

Separation of Duties

Job Rotation

Clean Desk Policies

Role-Based Awareness and Training

Continuing Education

Acceptable Use Policy/Rules of Behavior

Internet Usage

Nondisclosure Agreements

# Table of Contents

Disciplinary and Adverse Actions

Exit Interviews

Third-Party Risk Management

Interoperability Agreements

What Next?

## CHAPTER 34: Risk Management

Risk Analysis

Risk Register

Risk Response Techniques

Threat Assessment

Risk Assessment

Qualitative vs. Quantitative Measures

Single Loss Expectancy

Annual Rate of Occurrence

Annual Loss Expectancy

Business Impact Analysis

Critical Functions

Identification of Critical Systems

Single Points of Failure

Recovery Objectives

MTTF, MTBF, and MTTR

Impact

What Next?

## CHAPTER 35: Sensitive Data and Privacy

Sensitive Data Protection

Data Sensitivity Labeling and Handling

Privacy Laws and Regulatory Compliance

Data Roles and Responsibilities

Data Retention and Disposal

Privacy Impact Assessment

What Next?

# **Table of Contents**

## Glossary of Essential Terms and Components

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X-Z

Index