

EXAM CRAM

CompTIA

Security+ TM

SY0-401

Fourth Edition

**Save 10%
on Exam
Voucher**

See Inside



PEARSON IT
CERTIFICATION



DIANE BARRETT
MARTIN WEISS
KIRK HAUSMAN

EXAM✓CRAM

**CompTIA[®]
Security+[™]**

SY0-401

Fourth Edition

**Diane Barrett,
Kalani K. Hausman,
Martin Weiss**

CompTIA Security+ SYO-401 Exam Cram

Table of Contents

Contents

Introduction

Part I: Network Security

CHAPTER 1 Secure Network Design

Implement Security Configuration Parameters on Network Devices and Other Technologies

Firewalls

Routers

Switches

Load Balancers

Proxies

Web Security Gateways

VPN Concentrators

NIDS and NIPS

Protocol Analyzers

Spam Filter

UTM Security Appliances

Web Application Firewall Versus Network Firewall

Application-Aware Devices

Cram Quiz

Cram Quiz Answers

Given a Scenario, Use Secure Network Administration Principles

Rule-Based Management

Firewall Rules

VLAN Management

Table of Contents

Secure Router Configuration

Access Control Lists

Port Security

802.1X

Flood Guards

Loop Protection

Implicit Deny

Network Separation

Log Analysis

Unified Threat Management

Cram Quiz

Cram Quiz Answers

Explain Network Design Elements and Components

DMZ

Subnetting

VLAN

NAT

Remote Access

Telephony

NAC

Virtualization

Cloud Computing

Layered Security/Defense in Depth

Cram Quiz

Cram Quiz Answers

What Next?

CHAPTER 2 Network Implementation

Given a Scenario, Implement Common Protocols and Services

Protocols

Ports

OSI Relevance

Cram Quiz

Cram Quiz Answers

Table of Contents

Given a Scenario, Troubleshoot Security Issues Related to Wireless Networking

- WPA
- WPA2
- WEP
- EAP
- PEAP
- LEAP
- MAC Filter
- Disable SSID Broadcast
- TKIP
- CCMP
- Antenna Placement
- Power-Level Controls
- Captive Portals
- Antenna Types
- Site Surveys
- VPN (Over Open Wireless)
- Cram Quiz
- Cram Quiz Answers

What Next?

Part II: Compliance and Operational Security

CHAPTER 3 Risk Management

Explain the Importance of Risk-Related Concepts

- Control Types
- False Positives
- False Negatives
- Importance of Policies in Reducing Risk
- Risk Calculation
- Qualitative Versus Quantitative Measures
- Vulnerabilities
- Threat Vectors
- Probability/Threat Likelihood

Table of Contents

Risk-Avoidance, Transference, Acceptance, Mitigation, Deterrence

Risks Associated with Cloud Computing and Virtualization

Recovery Time Objective and Recovery Point Objective

Cram Quiz

Cram Quiz Answers

Summarize the Security Implications of Integrating Systems and Data with Third Parties

On-Boarding/Off-Boarding Business Partners

Social Media Networks and/or Applications

Interoperability Agreements

Privacy Considerations

Risk Awareness

Unauthorized Data Sharing

Data Ownership

Data Backups

Follow Security Policy and Procedures

Review Agreement Requirements to Verify Compliance and Performance
Standards

Cram Quiz

Cram Quiz Answers

Given a Scenario, Implement Appropriate Risk Mitigation Strategies

Change Management

Incident Management

User Rights and Permissions Reviews

Perform Routine Audits

Enforce Policies and Procedures to Prevent Data Loss or Theft

Enforce Technology Controls

Cram Quiz

Cram Quiz Answers

Given a Scenario, Implement Basic Forensic Procedures

Order of Volatility

Capture System Image

Table of Contents

- Network Traffic and Logs
- Capture Video
- Record Time Offset
- Take Hashes
- Screenshots
- Witnesses
- Track Man-Hours and Expense
- Chain of Custody
- Big Data Analysis
- Cram Quiz
- Cram Quiz Answers

Summarize Common Incident Response Procedures

- Preparation
- Incident Identification
- Escalation and Notification
- Mitigation Steps
- Lessons Learned
- Reporting
- Recovery/Reconstitution Procedures
- First Responder
- Incident Isolation
- Data Breach
- Damage and Loss Control
- Cram Quiz
- Cram Quiz Answers

What Next?

CHAPTER 4 Response and Recovery

Explain the Importance of Security-Related Awareness and Training

- Security Policy Training and Procedures
- Role-Based Training
- Personally Identifiable Information
- Information Classification

Table of Contents

Public

Data Labeling, Handling, and Disposal

Compliance with Laws, Best Practices, and Standards

User Habits

New Threats and New Security Trends/Alerts

Use of Social Networking and Peer-to-Peer Services

Follow Up and Gather Training Metrics to Validate Compliance and
Security Posture

Cram Quiz

Cram Quiz Answers

Compare and Contrast Physical and Environmental Controls

Environmental Controls

Physical Security

Control Types

Cram Quiz

Cram Quiz Answers

Summarize Risk Management Best Practices

Business Continuity Concepts

Fault Tolerance

Disaster Recovery Concepts

Cram Quiz

Cram Quiz Answers

Given a Scenario, Select the Appropriate Control to Meet the Goals of Security

Confidentiality

Integrity

Availability

Safety

Cram Quiz

Cram Quiz Answers

What Next?

Part III: Threats and Vulnerabilities

Table of Contents

CHAPTER 5 Attacks

Explain Types of Malware

- Adware
- Viruses
- Worms
- Spyware
- Trojan Horses
- Rootkits
- Backdoors
- Logic Bombs
- Botnets
- Ransomware
- Polymorphic Malware
- Armored Virus
- Cram Quiz
- Cram Quiz Answers

Summarize Various Types of Attacks

- Man-in-the-Middle
- Denial of Service
- Distributed DoS
- Replay
- DNS Poisoning
- ARP Poisoning
- Spoofing
- Spam
- Phishing and Related Attacks
- Privilege Escalation
- Malicious Insider Threat
- Transitive Access and Client-Side Attacks
- Password Attacks
- Typo Squatting/URL Hijacking
- Watering Hole Attack
- Cram Quiz
- Cram Quiz Answers

Table of Contents

Summarize Social Engineering Attacks and the Associated Effectiveness with Each Attack

- Social Engineering
- Shoulder Surfing
- Dumpster Diving
- Tailgating
- Impersonation
- Hoaxes
- Principles (Reasons for Effectiveness)
- Cram Quiz
- Cram Quiz Answers

Explain Types of Wireless Attacks

- Jamming/Interference
- Rogue Access Points
- War Driving
- Bluejacking/Bluesnarfing
- Packet Sniffing
- WEP/WPA Attacks
- WPS Attacks
- Near-Field Communication
- Cram Quiz
- Cram Quiz Answers

Explain Types of Application Attacks

- Browser Threats
- Code Injections
- Directory Traversal
- Header Manipulation
- Zero-Day
- Buffer Overflows
- Integer Overflows
- Cookies
- Arbitrary/Remote Code Execution
- Cram Quiz

Table of Contents

Cram Quiz Answers

What Next?

CHAPTER 6 Deterrents

Analyze a Scenario and Select the Appropriate Type of
Mitigation and Deterrent Techniques

Monitoring System Logs

Hardening

Network Security

Security Posture

Reporting

Detection Controls Versus Prevention Controls

Cram Quiz

Cram Quiz Answers

Given a Scenario, Use Appropriate Tools and Techniques to
Discover Security Threats and Vulnerabilities

Interpret Results of Security Assessment Tools

Tools

Risk Calculation

Assessment Technique

Cram Quiz

Cram Quiz Answers

Explain the Proper Use of Penetration Testing Versus
Vulnerability Scanning

Penetration Testing

Vulnerability Scanning

Testing

Cram Quiz

Cram Quiz Answers

What Next?

Part IV: Application, Data, and Host Security

CHAPTER 7 Application Security

Explain the Importance of Application Security Controls and

Table of Contents

Techniques

Fuzzing

Secure Coding Concepts

Cross-Site Scripting Prevention

Cross-Site Request Forgery Prevention

Application Configuration Baseline (Proper Settings)

Application Hardening

Application Patch Management

NoSQL Databases Versus SQL Databases

Server-Side Versus Client-Side Validation

Cram Quiz

Cram Quiz Answers

What Next?

CHAPTER 8 Host Security

Summarize Mobile Security Concepts and Technologies

Device Security

Application Security

BYOD Concerns

Cram Quiz

Cram Quiz Answers

Given a Scenario, Select the Appropriate Solution to Establish Host Security

Operating System Security and Settings

OS Hardening

Anti-malware

Patch Management

White Listing Versus Black Listing Applications

Trusted OS

Host-Based Firewalls

Host-Based Intrusion Detection

Hardware Security

Host Software Baselineing

Virtualization

Table of Contents

Cram Quiz

Cram Quiz Answers

What Next?

CHAPTER 9 Data Security

Implement the Appropriate Controls to Ensure Data Security

Cloud Storage

SAN

Handling Big Data

Data Encryption

Hardware-Based Encryption Devices

Data In-Transit, Data At-Rest, Data In-Use

Permissions/ACL

Data Policies

Cram Quiz

Cram Quiz Answers

Compare and Contrast Alternative Methods to Mitigate
Security Risks in Static Environments

Environments

Methods

Cram Quiz

Cram Quiz Answers

What Next?

Part V: Access Control and Identity Management

CHAPTER 10 Authentication, Authorization, and Access Control

Compare and Contrast the Function and Purpose of
Authentication Services

RADIUS

TACACS+

Kerberos

LDAP

XTACACS

Table of Contents

SAML

Secure LDAP

Cram Quiz

Cram Quiz Answers

Given a Scenario, Select the Appropriate Authentication, Authorization, or Access Control

Identification Versus Authentication Versus Authorization

Authorization

Authentication

Authentication Factors

Identification

Federation

Transitive Trust/Authentication

Cram Quiz

Cram Quiz Answers

What Next?

CHAPTER 11 Account Management

Install and Configure Security Controls When Performing Account Management, Based on Best Practices

Mitigate Issues Associated with Users with Multiple Account/ Roles and/or Shared Accounts

Account Policy Enforcement

Group-Based Privileges

User-Assigned Privileges

User Access Reviews

Continuous Monitoring

Cram Quiz

Cram Quiz Answers

What Next?

Part VI: Cryptography

CHAPTER 12 Cryptography Tools and Techniques

Given a Scenario, Utilize General Cryptography Concepts

Table of Contents

Symmetric Versus Asymmetric
Elliptic Curve and Quantum Cryptography
In-Band Versus Out-of-Band Key Exchange
Session Keys
Transport Encryption
Nonrepudiation and Digital Signatures
Hashing
Key Escrow
Steganography
Use of Proven Technologies
Cram Quiz
Cram Quiz Answers

Given a Scenario, Use Appropriate Cryptographic Methods

Wireless Encryption Functions
Cryptographic Hash Functions
HMAC
Symmetric Encryption Algorithms
Asymmetric Encryption Algorithms
One-Time Pads
PGP
Use of Algorithms with Transport Encryption
Cipher Suites
Key Stretching
Cram Quiz
Cram Quiz Answers

What Next?

CHAPTER 13 Public Key Infrastructure

Given a Scenario, Use Appropriate PKI, Certificate Management, and Associated Components

Public Key Infrastructure Standards
PKI
Certificate Policies
Public and Private Key Usage

Table of Contents

Revocation

Trust Models

Cram Quiz

Cram Quiz Answers

What Next?

PRACTICE EXAM 1

Exam Questions

Answers at a Glance

Answers with Explanations

INDEX

On the CD: Practice Exam 2

Glossary

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Table of Contents

R

S

T

UV

W

XYZ