Security+ SY0-501 Cybrary Course Study Guide

Description

There are many career opportunities for IT and cybersecurity professionals. If you're wondering where to start to help fill this gap, start with the CompTIA Security+ SY0-501 certification. This certification course helps you prove your competency in topics such as threats, vulnerabilities, and attacks, system security, network infrastructure, access control, cryptography, risk management, and organizational security.

This study guide along with the Cybrary videos covers each of the six domains for the Security+ SY0-501 certification to help you prepare for that exam. It contains the supplementary material you can use as a part of your study while you watch the instructional videos. As a part of this study guide, the domains are separated into sections. Each section has links to the presentation slide decks with specific information on each Security+ SY0-501 objective requirement. You can use these while watching the Cybrary videos as part of your study process. Each section also contains sample questions to help you prepare for your certification exam.

Course Introduction

Cybersecurity is a rising career field with a need for more security professionals in all industries and types of organizations. One of the greatest hindrances to mitigating cybercrime is the lack of qualified and skilled professionals trained in cybersecurity.

If you're wondering where to start in cybersecurity to help fill this gap, start with Security+. The CompTIA Security+ SY0-501 exam is an internationally recognized validation of foundation-level security skills and knowledge and is used by organizations and security professionals around the globe. The CompTIA Security+ certification proves an IT security professional's competency in topics such as threats, vulnerabilities, and attacks, system security, network infrastructure, access control, cryptography, risk management, and organizational security. This course covers those topics to prepare students for the CompTIA SY0-501 certification exam. The fundamentals taught in this class will prepare you for a career as a cybersecurity analyst.

Contents

Description	
Course Introduction	1
Module Outline	4
Series Introduction	4
CompTIA Security+ 501 Domains & Objectives – Top Level	6
CompTIA Security+ 501 Domains & Objectives – Details	8
Domain 1.0 Threats, Attacks and Vulnerabilities	14
Domain 1 Introduction	14
1.1 Indicators of compromise and types of malware	14
1.2 Types of attacks	14
1.3 Threat actor types and attributes	16
1.4 Penetration testing concepts	16
1.5 Vulnerability scanning concepts	17
1.6 Impact of vulnerabilities	17
Domain 2.0 Technologies and Tools	18
Domain 2 Introduction	18
2.1 Network components supporting security	18
2.2 Security assessment tools	19
2.3 Common security issues	20
2.4 Output from security technologies	20
2.5 Mobile device security	21
2.6 Secure protocols	21
Domain 3.0 Architecture and Design	22
Domain 3 Introduction	22
3.1 Frameworks, best practice and secure configuration guides	22
3.2 Secure network architecture concepts	23
3.3 Secure systems design	23
3.4 Secure staging and deployment	24
3.5 Embedded systems security	24
3.6 Secure application development	24
3.7 Cloud and virtualization security	25
3.8 Resiliency and automation strategies	25

3.9 Physical security controls	26
Domain 4.0 Identity and Access Management	27
Domain 4 Introduction	27
4.1 Identity and access management concepts	27
4.2 Install and configure identity and access services	27
4.3 Implement identity and access management controls	28
4.4 Common account management practices	29
Domain 5.0 Risk Management	30
Domain 5 Introduction	30
5.1 Security policies, plans and procedures	30
5.2 Business impact analysis (BIA)	30
5.3 Risk management concepts and processes	31
5.4 Incident response procedures	31
5.5 Digital forensics	32
5.6 Disaster recovery and business continuity	32
5.7 Types of security controls	33
5.8 Data security and privacy	33
Domain 6.0 Cryptography and PKI	34
Domain 6 Introduction	34
6.1 Basic concepts of cryptography	34
6.2 Cryptographic algorithms	35
6.3 Wireless security	36
6.4 Public kev infrastructure (PKI)	36

Module Outline

Series Introduction

The outline below will help you to understand the basics of the CompTIA Security+ 501 exam and the Cybrary video series.

- I. Security+ Certification
 - a. What is the certification
 - b. Why is it valuable
 - c. Certification goals
 - d. Who is it for
 - e. Test details
 - f. Exam Domains
 - g. See the CompTIA Security+ Certification Exam Objectives, EXAM NUMBER: SY0-501
- II. What is Security+
 - a. The CompTIA Security+ certification is a vendor-neutral credential
 - b. An internationally recognized validation of foundation-level security skills and knowledge
 - c. Demonstrates you have the competence required to apply knowledge of security concepts, tools, and procedures to react to security incidents
 - d. Tests knowledge held by a security professional with at least 2 years of full-time security-related work experience
- III. Why Security+
 - a. Provides proof of professional achievement
 - b. Increases credibility, marketability and opportunity for advancement
 - c. Recognized worldwide
 - d. Fulfills training requirements
 - e. Entry point for security certifications
- IV. Certification Goals
 - a. The successful candidate has the knowledge and skills required to:
 - i. Install and configure systems to secure applications, networks and devices
 - ii. Perform threat analysis and respond with appropriate mitigation techniques
 - iii. Participate in risk mitigation activities
 - iv. Operate with an awareness of applicable policies, laws and regulations
 - b. The successful candidate will perform these tasks to support the principles of confidentiality, integrity, and availability.
- V. Who Security+ is for
 - a. The CompTIA Security+ certification is aimed at an IT security professional who has:
 - i. A minimum of two years full-time experience
 - ii. Day-to-day technical information security experience
 - iii. Broad knowledge of security issues, concerns and implementation
- VI. Exam Domains
 - a. 1.0 Threats, Attacks and Vulnerabilities: 21%
 - b. 2.0 Technologies and Tools: 22%c. 3.0 Architecture and Design: 15%

c. 3.0 Architecture and Design: 15%

d. 4.0 Identity and Access Management: 16%

e. 5.0 Risk Management: 14%

f. 6.0 Cryptography and PKI: 12%

VII. Test Details

a. Required exam: SY0-501

b. Number of questions: Maximum of 90

c. Types of questions: Multiple choice and performance-based

d. Length of test: 90 minutes

e. Recommended experience: At least two years of experience in IT administration with a focus on security

f. Passing score: 750 (on a scale of 100–900

VIII. Resources:

- a. Cybrary's Security+ Study Guide (501) [this document]
- b. CompTIA Security+ Website
- c. Cybrary Security+ Responsive Practice Exam
- d. Cybrary CompTIA Security+ Hands-On Practice Labs
- e. OP3N | Security+
- f. Sybex: Security+ Study Guide (SY0-501) 7th Edition Paperback or 4th Edition Deluxe
- g. Pearson CompTIA Security+ SY502 Exam Cram, 5th Edition

IX. Moving Forward

- a. Videos will be in order of listed CompTIA Domains
- b. Keep taking practice exams and quizzes
- c. Know your strengths and weaknesses
- d. Final video Test taking strategies & techniques

CompTIA Security+ 501 Domains & Objectives – Top Level

This section contains a high-level outline of the <u>CompTIA Security+ Certification Exam Objectives</u>. This is available for your convenience. See the official <u>CompTIA website</u> for details.

Domain 1.0 Threats, Attacks and Vulnerabilities

- 1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.
- 1.2 Compare and contrast types of attacks
- 1.3 Explain threat actor types and attributes
- 1.4 Explain penetration testing concepts
- 1.5 Explain vulnerability scanning concepts
- 1.6 Explain the impact associated with types of vulnerabilities

Domain 2.0 Technologies and Tools

- 2.1 Install and configure network components, both hardware and software-based, to support organizational security.
- 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization
- 2.3 Given a scenario, troubleshoot common security issues
- 2.4 Given a scenario, analyze and interpret output from security technologies
- 2.5 Given a scenario, deploy mobile devices securely
- 2.6 Given a scenario, implement secure protocols

Domain 3.0 Architecture and Design

- 3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides
- 3.2 Given a scenario, implement secure network architecture concepts.
- 3.3 Given a scenario, implement secure systems design
- 3.4 Explain the importance of secure staging deployment concepts.
- 3.5 Explain the security implications of embedded systems.
- 3.6 Summarize secure application development and deployment concepts.
- 3.7 Summarize cloud and virtualization concepts.
- 3.8 Explain how resiliency and automation strategies reduce risk.
- 3.9 Explain the importance of physical security controls.

Domain 4.0 Identity and Access Management

- 4.1 Compare and contrast identity and access management concepts.
- 4.2 Given a scenario, install and configure identity and access services.
- 4.3 Given a scenario, implement identity and access management controls.
- 4.4 Given a scenario, differentiate common account management practices.

Domain 5.0 Risk Management

- 5.1 Explain the importance of policies, plans and procedures related to organizational security
- 5.2 Summarize business impact analysis concepts.
- 5.3 Explain risk management processes and concepts.
- 5.4 Given a scenario, follow incident response procedures.
- 5.5 Summarize basic concepts of forensics.
- 5.6 Explain disaster recovery and continuity of operations concepts.

- 5.7 Compare and contrast various types of controls.
- 5.8 Given a scenario, carry out data security and privacy practices.

Domain 6.0 Cryptography and PKI

- 6.1 Compare and contrast basic concepts of cryptography.
- 6.2 Explain cryptography algorithms and their basic characteristics
- 6.3 Given a scenario, install and configure wireless security settings
- 6.4 Given a scenario, implement public key infrastructure

CompTIA Security+ 501 Domains & Objectives – Details

This section contains a detailed outline of the <u>CompTIA Security+ Certification Exam Objectives</u>. It contains more information on each Security+ 501 domain objective. See the <u>official CompTIA website</u> for details.

Domain 1.0 Threats, Attacks and Vulnerabilities

- 1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.
- 1.2 Compare and contrast types of attacks
 - 1.2.1 Social Engineering
 - 1.2.2 Application / Service attacks
 - 1.2.3 Cryptographic attacks
 - 1.2.4 Hijacking
 - 1.2.5 Network / Wireless attacks
- 1.3 Explain threat actor types and attributes
 - 1.3.1 Types of actors
 - 1.3.2 Attributes of actors
- 1.4 Explain penetration testing concepts
 - 1.4.1 Penetration testing process
 - 1.4.1.1 Reconnaissance
 - 1.4.1.2 Initial exploitation
 - 1.4.1.3 Persistence
 - 1.4.1.4 Pivot
 - 1.4.1.5 Escalation of privilege
 - 1.4.2 Penetration testing vs. Vulnerability scanning
 - 1.4.3 Black box vs. Gray box vs. White box
- 1.5 Explain vulnerability scanning concepts
 - 1.5.1 Identifying
 - 1.5.1.1 Vulnerability / Unpatched system or application
 - 1.5.1.2 Lack of security controls
 - 1.5.1.3 common misconfigurations
 - 1.5.2 Intrusive vs. non-intrusive
 - 1.5.3 Credentialed vs. non-credentialed
- 1.6 Explain the impact associated with types of vulnerabilities
 - 1.6.1 Configuration issues
 - 1.6.2 Access control
 - 1.6.3 Cryptography, certificate and key management
 - 1.6.4 Application vulnerabilities
 - 1.6.5 Application input handling

Domain 2.0 Technologies and Tools

- 2.1 Install and configure network components, both hardware and software-based, to support organizational security
 - 2.1.1 Network equipment: Router, Switch, Bridge, Load Balancer, Proxy
 - 2.1.2 Gateways: Email, Media
 - 2.1.3 Access Points
 - 2.1.4 Firewall
 - 2.1.5 NAC
 - 2.1.6 VPN / SSL/TLS accelerators & decryptors
 - 2.1.7 NIPS/NIDS
 - 2.1.8 DLP
 - 2.1.9 SIEM
- 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization
 - 2.2.1 Network scanners
 - 2.2.2 Protocol analyzer
 - 2.2.3 Wireless scanners / crackers
 - 2.2.4 Exploitation frameworks
 - 2.2.5 Passive vs Active
 - 2.2.6 Scanners: Vulnerability, Configuration compliance and inventory
 - 2.2.7 Password crackers
 - 2.2.8 Backup Utilities
 - 2.2.9 Honeypot / Honeynet
 - 2.2.10 Steganography
 - 2.2.11 Command line tools: Unix/Linux and Windows
- 2.3 Given a scenario, troubleshoot common security issues
 - 2.3.1 Personnel
 - 2.3.2 Asset Management / Misconfigured devices
 - 2.3.3 Identity, Access, Authentication, Authorization and Audit (IAAAA)
 - 2.3.4 Encryption
- 2.4 Given a scenario, analyze and interpret output from security technologies
 - 2.4.1 Network security technologies
 - 2.4.2 Host security technologies
 - 2.4.3 Data security technologies
- 2.5 Given a scenario, deploy mobile devices securely
 - 2.5.1 Connection methods
 - 2.5.2 Mobile device management concepts
 - 2.5.3 Enforcement and monitoring
 - 2.5.4 Deployment models
- 2.6 Given a scenario, implement secure protocols
 - 2.6.1 Protocols
 - 2.6.2 Use cases

Domain 3.0 Architecture and Design

- 3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides
 - 3.1.1 Industry-standard frameworks and reference architectures
 - 3.1.2 Benchmarks/secure configuration guides
 - 3.1.3 Defense-in-depth/layered security
- 3.2 Given a scenario, implement secure network architecture concepts.
 - 3.2.1 Zones/topologies
 - 3.2.2 Segregation/segmentation/isolation
 - 3.2.3 VPN / Tunneling
 - 3.2.4 Security device/technology placement
 - 3.2.5 Software Defined Networks (SDN)
- 3.3 Given a scenario, implement secure systems design
 - 3.3.1 Hardware/firmware security
 - 3.3.2 Operating System Security
 - 3.3.3 Peripherals
- 3.4 Explain the importance of secure staging deployment concepts.
 - 3.4.1 Secure baseline
 - 3.4.2 Sandboxing
 - 3.4.3 Environment
 - 3.4.4 Integrity measurement
- 3.5 Explain the security implications of embedded systems.
 - 3.5.1 ICS / SCADA
 - 3.5.2 IoT / Smart Devices
 - 3.5.3 Printers / MFDs
 - 3.5.4 Camera systems
 - 3.5.5 Special purpose
- 3.6 Summarize secure application development and deployment concepts.
 - 3.6.1 Development life-cycle models
 - 3.6.2 Secure DevOps / SecDevOps
 - 3.6.3 Version control and change management
 - 3.6.4 Provisioning and deprovisioning
 - 3.6.5 Secure coding techniques
 - 3.6.6 Code quality and testing
- 3.7 Summarize cloud and virtualization concepts.
 - 3.7.1 Hypervisor
 - 3.7.2 Virtual Machine (VM)
 - 3.7.3 Cloud computing
 - 3.7.3.1 Deployment models
 - 3.7.3.2 Storage
 - 3.7.3.3 Access

- 3.8 Explain how resiliency and automation strategies reduce risk.
 - 3.8.1 Automation/scripting
 - 3.8.2 Master image
 - 3.8.3 Non-persistence
 - 3.8.4 Forms and functions
- 3.9 Explain the importance of physical security controls.

Domain 4.0 Identity and Access Management

- 4.1 Compare and contrast identity and access management concepts.
 - 4.1.1 Identification, authentication, authorization and accounting (AAA)
 - 4.1.2 Multifactor authentication
 - 4.1.3 Single Sign-On (SSO) / Federation
- 4.2 Given a scenario, install and configure identity and access services.
- 4.3 Given a scenario, implement identity and access management controls.
 - 4.3.1 Access Control Models
 - 4.3.2 Physical Access Control
 - 4.3.3 Biometrics
 - 4.3.4 Tokens
 - 4.3.5 Certificate-based authentication
 - 4.3.6 Authorization: file-system and database
- 4.4 Given a scenario, differentiate common account management practices.
 - 4.4.1 General concepts
 - 4.4.2 Account types
 - 4.4.3 Account policy enforcement

Domain 5.0 Risk Management

- 5.1 Explain the importance of policies, plans and procedures related to organizational security.
 - 5.1.1 Standard operating procedures
 - 5.1.2 Agreement types
 - 5.1.3 Personnel management
 - 5.1.4 General security policies
- 5.2 Summarize business impact analysis concepts.
- 5.3 Explain risk management processes and concepts.
 - 5.3.1 Threat assessment
 - 5.3.2 Risk assessment
 - 5.3.3 Change management
- 5.4 Given a scenario, follow incident response procedures.
 - 5.4.1 Incident response plan

- 5.4.2 Incident response process
- 5.5 Summarize basic concepts of forensics.
 - 5.5.1 Data acquisition
 - 5.5.2 Preservation / Order of volatility
 - 5.5.3 Chain of custody
 - 5.5.4 Legal hold
 - 5.5.5 Recovery
- 5.6 Explain disaster recovery and continuity of operations concepts.
 - 5.6.1 Backup concepts
 - 5.6.2 Geographic considerations
 - 5.6.3 Continuity of operations planning
 - 5.6.4 Recovery sites
 - 5.6.5 Order of restoration
- 5.7 Compare and contrast various types of controls.
 - 5.7.1 Administrative
 - 5.7.2 Technical
 - 5.7.3 Physical
 - 5.7.4 Corrective
 - 5.7.5 Preventive
 - 5.7.6 Detective
 - 5.7.7 Deterrent
 - 5.7.8 Compensating
- 5.8 Given a scenario, carry out data security and privacy practices
 - 5.8.1 Data sensitivity labeling and handling
 - 5.8.2 Data roles
 - 5.8.3 Data destruction and media sanitization
 - 5.8.4 Legal and compliance

Domain 6.0 Cryptography and PKI

- 6.1 Compare and contrast basic concepts of cryptography.
 - 6.1.1 Symmetric algorithms
 - 6.1.2 Asymmetric algorithms
 - 6.1.3 Hashing
 - 6.1.4 Keys and key exchange
 - 6.1.5 Digital signatures
 - 6.1.6 Common use cases
- 6.2 Explain cryptography algorithms and their basic characteristics.
 - 6.2.1 Symmetric algorithms
 - 6.2.2 Cipher modes
 - 6.2.3 Asymmetric algorithms

- 6.2.4 Hashing algorithms
- 6.3 Given a scenario, install and configure wireless security settings.
 - 6.3.1 Cryptographic protocols
 - 6.3.2 Authentication protocols
 - 6.3.3 Methods
- 6.4 Given a scenario, implement public key infrastructure.
 - 6.4.1 Components
 - 6.4.2 Concepts
 - 6.4.3 Types of certificates
 - 6.4.4 Certificate formats

Domain 1.0 Threats, Attacks and Vulnerabilities

Domain 1 Introduction

This domain explains the ability for security professionals to identify different sources of threats, vulnerabilities, types of attacks and indicators of compromise.

1.1 Indicators of compromise and types of malware



Sample Questions:

In your role as a security administrator, a user contacts you suspecting that his computer is infected. Yesterday he loaded a freeware program to help him perform a valid job function. What type of malicious software is most likely the cause of the infection?

- A. Rootkit
- B. Ransomware
- C. Trojan
- D. Worm

What type of malicious software is deliberately installed by an authorized user and sits dormant until some event invokes its malicious payload?

- A. Logic bomb
- B. Spyware
- C. Trojan horse
- D. Armored virus

1.2 Types of attacks



Sample Questions:

A user contacts you suspecting that his computer is infected. Yesterday he opened an email that looked like it was from a colleague. When he later talked to that person, she said she never sent an email. What type of attack is the most likely the cause of the infection?

A. Phishing

- B. Trojan
- C. Spear phishing
- D. Whaling

You observe a delivery person entering your building by following an employee through a locked door into a secure facility. Which term best describes this type of attack:

- A. Shoulder surfing
- B. Reciprocity
- C. Tailgating
- D. Whaling

During a breach investigation, you notice that the attacker entered the database through a web front end application by manipulating the database code to exploit a vulnerability. What is the most likely name for this type of attack?

- A. SQL parsing
- B. Database injection
- C. SQL injection
- D. Session hijacking

Which of the following type of attack is the result of software vulnerabilities and is caused by supplying more data than is expected in an input field?

- A. Buffer overflow attack
- B. Cross site scripting
- C. Denial-of-Service (DoS) attack
- D. App overloading

Which form of attack uses special programs that attempt all possible character combinations to determine passwords?

- A. brute-force attack
- B. dictionary attack
- C. password guessing
- D. birthday attack

Of the below terms, which one best describes the type of attack that captures portions of a session to play back later to convince a host that it continues to communicate with the original system?

- A. IP hijacking
- B. Jamming
- C. Trojan
- D. Replay

You have a user call you from a hotel saying there's an issue with your organization's web site and that it looks like it's been compromised. You check it from your work at it appears fine. What is a likely cause associated with the user at the hotel?

- A. Logic bomb
- **B.** DNS Poisoning
- C. Trojan horse
- D. Evil twin

1.3 Threat actor types and attributes



Slides: Security+501 Domai

Sample Question:

Your company's website has been defaced by an organization that doesn't agree with your corporate policies. What type of treat actor typically does this?

- A. Script kiddies
- B. Hacktivist
- C. Organized crime
- D. Insiders

1.4 Penetration testing concepts



Cybrary Slides: Security+501 Domai

Sample Questions:

Of the following types of testing steps, which focuses on directly scanning a system, using techniques such as port scans, network mapping, ICMP scans to identify potential weaknesses?

- A. Operational reconnaissance
- B. Active reconnaissance
- C. Passive reconnaissance
- D. Initial exploitation

In initially conducting a penetration test, you find vulnerabilities on a separate, less secure server on the same network as the one you're investigating. You use access to that server to then attack the target servers. This type of exploit is known as:

- A. Escalation of privileges
- **B.** Pivoting
- C. Active reconnaissance
- D. Persistence

1.5 Vulnerability scanning concepts



Sample Question:

You've been asked to conduct an internal vulnerability assessment for your organization. Which of the following steps should you avoid in determining system or network weaknesses to minimize risk?

- A. Non-intrusive reconnaissance
- B. Exploiting unpatched applications
- C. Review of system control configuration settings
- D. Scanning for unpatched systems

1.6 Impact of vulnerabilities



Sample Question:

In this type of vulnerability, accounts have greater privileges than is needed to perform a function and is solved by Least Privilege?

- A. Improperly configured accounts
- B. Resource exhaustion
- C. Improper input handling
- D. Race condition

Domain 2.0 Technologies and Tools

Domain 2 Introduction

The second domain focuses on technologies and tools used with security. You'll learn about the practical use and management of applications to protect, detect, and respond to threats, attacks and vulnerabilities you learned about in Domain 1.

Many of the objectives for Security+ SY0-502 are based on 'given a scenario' to simulate real-live experiences of a security professional. This requires you to understand how to use appropriate software tools, such as network mappers and scanners, network security technologies, vulnerability assessment applications, penetration testing tools, and exploitation frameworks. For Security+, you'll need to be able to assess the security posture of an organization, troubleshoot common security issues, and analyze and interpret output from security technologies.

There are many labs associated with this domain that will help you better understand the concepts. The more practice you get with technology, the more prepared you'll be for both real-world situations and the Security+ exam.

2.1 Network components supporting security



Sample Questions:

This condition exists when data units can travel from a first LAN segment to a second LAN segment through more than one path and is solved by STP?

- A. Logic bomb
- B. Flooding
- C. MAC spoofing
- D. Looping

Which of the following tunneling configurations is the process of allowing a remote VPN user to access a public network (the Internet) at the same time that the user is allowed to access organizational resources?

- A. Split-tunneling
- B. Inline access
- C. Always-on VPN
- D. IPSec VPN

This type of firewall passes or blocks traffic to specific ports or IP addresses based on predetermined rules?

A. Stateful inspection

- B. Proxy
- C. Packet-filtering
- D. Unified Threat Management

Which international standard is used for Network Access Control?

- A. IEEE 802.1X
- B. IEEE 802.11
- C. ISO 27001
- D. GDPR

Security+ Labs:

- Firewall Rule Based Management
- Configuring IDS and Honeypots

2.2 Security assessment tools



Slides: Security+501 Domai

Sample Questions:

Also known as packet sniffers, these tools help you troubleshoot network issues by gathering packet-level information across the network?

- A. Vulnerability scanners
- B. Exploitation frameworks
- C. Configuration compliance
- D. Protocol analyzers

Alex is conduct forensics of a phishing email. She knows the IP address of the originating email server. What command would show Alex the compete path to that IP address?

- A. ping
- B. tracert
- C. netstat
- D. nslookup

Security+ Labs:

- Network Vulnerabilities, Part 1
- Password Cracking Tools
- Scanning and Remediating Vulnerabilities with OpenVAS

Page | 19 Cybrary - Ron Woerner

2.3 Common security issues



Sample Questions:

For this common security issue, the first item to check as you begin the troubleshooting process is that the correct username and password have been entered.

- A. Baseline deviation
- B. Unauthorized software
- C. Authentication errors
- D. Clear-text credentials

2.4 Output from security technologies



Sample Questions:

This security tool is best for checking to see if specific system files have been changed and report on those changes.

- A. File integrity checker
- B. HIDS / HIPS
- C. Application whitelisting
- D. DLP

You are working as a security analyst and receive a call from an end user saying he received a warning about a virus. Which of the following is <u>not</u> a step you should take to resolve the issue?

- A. Detach the infected system from the network
- B. Manually delete virus files
- C. Run an additional anti-virus scan
- D. Review system log files

Security+ Labs:

- Application Data Establish Host Security
- Implement Patching with WSUS

2.5 Mobile device security



Sample Questions:

This form of wireless communications has three modes of operation peer-to-peer mode, read/write mode, and card emulation:

- A. Wi-Fi
- B. Bluetooth
- C. Near-Field Communication (NFC)
- D. Biometrics

This form of Mobile Device Management is used to control access to the file storage and sharing capabilities of services.

- A. Mobile Content Management
- B. Mobile Application Management
- C. Containerization
- D. Push notification services

2.6 Secure protocols



Sample Questions:

With this protocol, each managed device has a software agent reporting configuration settings and alerts (traps) to a central Management Server.

- A. SNMPv3
- B. SMTP
- C. SSL/TLS
- D. LDAPS

This is a client-based protocol used for securing email. The most common use case for this protocol is securing internal client messages.

- A. IMAPS
- B. S/MIME
- C. SFTP
- D. DNS

Domain 3.0 Architecture and Design

Domain 3 Introduction

The Security+ 501 third domain concentrates on security architecture and design, which is often based on known frameworks, best practices, and secure configuration guides. These fall into different categories: Industry-specific frameworks, reference architectures, and regulatory and non-regulatory requirements. Security professionals need to understand how these fit within their organization's security and IT infrastructure.

In addition to understanding frameworks, you must be able to demonstrate the ability to implement secure network and system architecture concepts. This includes assessing, developing and managing a secure network topology based on business and compliance requirements. You will also need to have a base of knowledge in securing applications (AppSec) and development operations (DevOps). The more you can automate for consistent resiliency, the better. Lastly, you can't forget about physical security, which is another threat vector impact cybersecurity.

3.1 Frameworks, best practice and secure configuration guides



Sample Questions:

This standard gives guidelines for information security controls applicable to the provision and use of cloud services.

- A. NIST SP800-12
- B. ISO/IEC 27002:2017
- C. ISO/IEC 27017:2015
- D. NERC Cloud Information Protection (CIP)

According to the CompTIA Security+ blueprint, which of the following is not a consideration for defense-in-depth or layered security?

- A. Vendor diversity
- **B.** Security benchmarks
- C. Control diversity
- D. User training

3.2 Secure network architecture concepts



Sample Questions:

Alice is a CISO for a financial institution. She wants to use a device that is intentionally broken to catch and log potential attacks?

- A. Honeypot
- B. SIEM
- C. VLAN
- D. Proxy firewall

Alice hired you as her network architect. She wants a file transfer server in an area that's accessible from both the Internet and to internal users. What's your best approach?

- A. Place the server on a guest wireless segment
- B. Place the server in a honeynet
- C. Place the server on a virtual LAN
- D. Place the server in a DMZ

Security+ Labs:

- Firewall Rule Based Management
- Firewalls and Evasion
- Configurating IDS and Honeypots
- Implementing a Network Policy Server

3.3 Secure systems design



Sample Question:

Alice is a CISO for a financial institution. She wants to make sure all laptop's hard drives are automatically encrypted. What tool can she use?

- A. UEFI
- B. Root of Trust
- C. Bitlocker
- D. RSA Encryption

Security+ Lab:

Data Encryption

3.4 Secure staging and deployment



Sample Questions:

Alice is a CISO for a financial institution. She is looking for an environment used for testing that is completely off of their network. Which do you recommend?

- A. Sandbox
- B. Test network
- C. Production
- D. Development

3.5 Embedded systems security



3.6 Secure application development



Sample Questions:

Which of the following would be the most secure way to deploy a legacy application that requires a legacy operating system?

- A. Sandboxing
- B. Input validation
- C. Code Signing
- D. In transit encryption

Alice wants to reduce the probability of SQL injection attacks against the company's web server. What secure development measure would work best?

- A. Stress testing
- **B.** Input validation
- C. IPS
- D. Agile programming

3.7 Cloud and virtualization security



Sample Questions:

This cloud computing model provides not only virtualized deployment, but also a value-added solution stack and an application development environment.

- A. Security as a Service
- B. Application as a Service
- C. Platform as a Service
- D. Hybrid Cloud

Which term describes a cloud feature involving dynamically allocating resources as needed?

- A. Multitenancy
- B. Elasticity
- C. Partitioning
- D. Sandboxing

Security+ Lab:

Managing Local Storage and Virtual Hard Disks

3.8 Resiliency and automation strategies



Sample Question:

Which risk mitigation technique uses a standard disk image for system restoration upon breach or failure.

- A. Master image
- B. Platform as a Service
- C. Nonpersistence
- D. High Availability

3.9 Physical security controls



Sample Question:

Which of the following is an intermediate access mechanism used in a high-security installation that requires visual inspection and authentication to gain access?

- A. Proximity reader
- B. Shielding
- C. Turnstiles
- D. Mantrap

Domain 4.0 Identity and Access Management

Domain 4 Introduction

Identity and access management (IAM) is the focus of the fourth domain of Security+ 501. IAM is the security principle that defines the proper authentication, authorization, and access to resources for users. It's a framework that uses Identity Management (IdM) tools to enables the right individuals to access the right resources at the right times and for the right reasons.

This domain covers four main principles of identity and access management: identity and access management concepts, selecting the appropriate identity and access service solution, implementing identity and access management controls, and following account management best practices.

4.1 Identity and access management concepts



Slides: Security+501 Domai

Sample Question:

Which of the following is a term used whenever two or more parties authenticate each other?

- A. SSO
- **B.** Mutual Authentication
- C. Transitive Trust
- D. Federation

Security+ Lab:

• Implementing AD Federation Services

4.2 Install and configure identity and access services



Slides: Security+501 Domai

Sample Questions:

This access control protocol for use on networks uses UDP transport to sent authentication information to a central server?

- A. CHAP
- B. Kerberos

- C. OpenIDv2
- D. RADIUS

This protocol uses a key distribution center (KDC) to orchestrate the authentication process.?

- A. RADIUS
- B. Federated identity
- C. Kerberos
- D. LDAP

Security+ Lab:

• Configuring RADIUS

4.3 Implement identity and access management controls



Sample Questions:

Which of the following authentication methods provides credentials that are only valid during a single session?

- A. Tokens
- B. Kerberos
- C. Certificates
- D. Smartcards

You are looking to implement a new access control mechanism that takes into account the entire environment and requested actions for access. What model does this best describe?

- A. ABAC Attribute-Based Access Control
- B. Federated identity
- C. RBAC Role-Based Access Control
- D. DAC Discretionary Access Control

Security+ Lab:

Managing Certificates

4.4 Common account management practices



Sample Questions:

Juan is a database administrator for his organization. He's setting up a new MS SQL server system and needs to establish an account for it. Which of the following would be the best type of account for this use?

- A. Service account
- B. Domain admin account
- C. User account
- D. Group account

What is the name of the annual auditing process whereby you determine if given accounts continue to require a set of privileges?

- A. Offboarding
- B. Federated identity
- C. Recertification
- D. Account maintenance

Domain 5.0 Risk Management

Domain 5 Introduction

Security is all about managing risk – the likelihood of an unexpected event that will impact the organization. The fifth Security+ domain covers Risk Management concepts. This includes how to assess business impacts, manage corporate policies, identify and analyze potential risks, and enable appropriate business decisions. This domain also explores incident response and forensics, disaster recovery and business continuity of operations as the effects of risks. Lastly, it looks at various types of security controls and methods for carrying out data security and privacy practices.

5.1 Security policies, plans and procedures



lidos Security + 501 Domai

Sample Questions:

Which of the following policies describes how the employees in an organization can use corporate resources?

- A. Internet Use Policy
- B. Service Level Agreement (SLA)
- C. Acceptable Use Policy (AUP)
- D. Separation of duties policy

According to the CompTIA Security+ blueprint, this is the personnel management practice of rotating administrative users between roles to ensure that fraudulent activity cannot be sustained?

- A. Job rotation
- B. Separation of duties
- C. Job shadowing
- D. Role-based awareness training

5.2 Business impact analysis (BIA)



Slides: Security+501 Domai

Sample Questions:

In the context of a business impact assessment, this term represents how long a product can reasonably be expected to perform, based on specific testing?

- A. Recovery Time Objective
- B. MTTF
- C. MTTR
- D. Single Point of Failure (SPF)

5.3 Risk management concepts and processes



Slides: Security+501 Domai

Sample Questions:

Chose the best term for the risk strategy accomplished any time you take steps to reduce risk.

- A. Risk management
- B. Risk avoidance
- C. Qualitative risk analysis
- D. Risk mitigation

In conducting a risk analysis, if you calculate the SLE to be \$5,000 and it's known there will be 5 occurrences a year, then the annual loss expectancy is:

- A. \$25,000
- B. \$5,000
- C. \$12,500
- D. Cannot be determined with the information

Answer: \$25,000. ALE=SLE X ARO = \$5000 X 5

5.4 Incident response procedures



Slides: Security+501 Domai

Sample Questions:

According to NIST, which is not a listed step in the Incident Response Process?

- A. Preparation
- **B.** Documentation
- C. Eradication

D. Detection

The following is NISTs definition of what term?

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.

- A. Incident Response
- B. Disaster
- C. Risk
- D. Incident

5.5 Digital forensics



Sample Questions:

Which of the following is the process used during data acquisition for the preservation of all forms of relevant information when litigation is reasonable anticipated?

- A. Legal Hold
- B. Chain of Custody
- C. Order of Volatility
- D. Capturing Images

What hardware or software tool should be used whenever you are capturing a system image to preserve the integrity of the original media?

- A. Read-Only Media
- B. Linux dd command
- C. System hashes
- D. Write blocker

Security+ Lab:

Introduction to Digital Forensics

5.6 Disaster recovery and business continuity



Sample Question:

This is the step where you prioritize the systems and services to be recovered in a disaster event with the most critical systems coming online first?

- A. Order of restoration
- B. System restore planning
- C. Differential backups
- D. Server redundancy

5.7 Types of security controls



Sample Question:

Security cameras, motion sensors, and audits are a form of which type of security controls?

- A. Deterrent
- B. Technical
- C. Corrective
- D. Detective

5.8 Data security and privacy



Sample Questions:

This method of data destruction is a cost-effective method to reduce the size of objects with the intent of making them no longer usable?

- A. Shredding
- B. Pulping
- C. Degaussing
- D. Pulverizing

Domain 6.0 Cryptography and PKI

Domain 6 Introduction

Domain 6 of Security+ 501 reviews how cryptography is used in our modern computing systems. Cryptography is an ancient concept dating back to the ancient Assyrians and Egyptians. In the beginning, the systems of cryptography were manually performed. During the twentieth century, machines and mechanical cryptography were born. Today, cryptography is a primary security control.

As a security professional, you need to have sufficient knowledge of the concepts of cryptography, the different encryption methods and how they're applied across applications, systems and networks. In studying the fundamental cryptography concepts, you will begin to understand how it works as a tool to protect and authenticate all types of information, including how this protection applies to systems with no prior contact residing in separate geographical locations. While cryptography is mathematically-based, you don't need to be a math expert to survive this section on the Security+ exam.

6.1 Basic concepts of cryptography



Slides: Security+501 Domai

Sample Questions:

You are using asymmetric encryption and want to sign a file to prove you sent it and it hasn't been altered. Which key do you use?

- A. Your public key
- B. Your private key
- C. The recipients public key
- D. The recipients private key

Which type of cipher encrypts data in fixed length group of bits?

- A. Quantum cryptography
- B. Block cipher
- C. Asymmetric ciphers
- D. Streaming cipher

6.2 Cryptographic algorithms



Sample Questions:

This block cipher uses a "key bundle" that comprises three different DES keys, each of 56 bits?

- A. DES
- B. AES
- C. RSA
- D. 3DES

This cryptographic algorithm works by generating a keystream block by encrypting sequential values of some counter and is used to convert a block cipher into a stream cipher.

- A. GCM
- B. CTR (counter mode)
- C. AES
- D. Twofish

This hashing algorithm, now considered compromised, produces a 16-byte hash value, usually expressed as a 32 digit hexadecimal number?

- A. SHA-1
- B. Rainbow tables
- C. MD5
- D. HMAC

Alice and Bob want to shared a file over the Internet. They plan on using AES-256 for file encryption, but need to share a secret key between them. Which algorithm is best for this use?

- A. Diffie-Hellman
- B. RSA
- C. SHA-1
- D. ECB

Security+ Lab:

Encryption and Hashing

6.3 Wireless security



Sample Questions:

Also known as WPA-Personal, this is a security mechanism used to authenticate and validate users on a wireless LAN (WLAN) or Wi-Fi connection?

- A. WPA-PSK
- B. PEAP
- C. WPA-TKIP
- D. WPA-CCMP

This network authentication protocol uses digital certificate-based mutual authentication, which occurs automatically with no intervention by the user.

- A. PEAP
- B. EAP-FAST
- C. EAP-TLS
- D. EAP-TTLS

6.4 Public key infrastructure (PKI)



Slides: Security+501 Domai

Sample Questions:

The job of this service is to issue certificates, verify the holder of a digital certificate, and ensure that holders of certificates are who they claim to be.

- A. Certificate Authority
- B. Registration Authority
- C. Root Certificate
- D. Key Escrow

Which of the following is NOT contained in a standard X.509 certificate?

- A. Serial number
- B. Issuer name
- C. Subject's private key
- D. Subject's public key

Security+ Labs:

- Understanding PKI Concepts
- Manage Certificates

Test Taking Tips

Taking a certification exam can be intimidating, even to the most seasoned professional.

In this section, I'll share some tips and tricks in preparing for and taking standard certification exams. Here are a variety of ideas to help you before and during the exam. Some of these may help you and some may not, depending on who you are and the type of exam you are taking.

This tutorial is focus on standardized certification exams with multiple choice questions. These are based on resources and my personal insights. Normal caveats apply: use at your own risk and your mileage may vary.

General Strategies

- Take as many sample tests as you can
- Try to replicate the testing environment as much as possible
 - No phones, Internet, or distractions
 - Take an entire test exam in one sitting
 - No cheating / looking up answers Give your best guess and move on
- Know your strengths and weaknesses
 - Subject areas you know well and those you don't
 - Work on your weaker areas
- Use positive self-talk
 - You may never, truly be totally ready for it.
 - Great can be the enemy of good-enough

Before you begin

- Review your certification program's testing policies and methods
- Know:
 - The number of questions
 - o Time allotted
 - Type of test
 - Traditional
 - Computer Aided Testing
 - Type of questions
- Scheduling your test Make the time
- Familiarize yourself with the look, feel and navigation of a computer-based test.

Test Day

- Get a good night sleep and eat a light snack
- Know what you should and should not bring to the exam
 - Should: Identification
 - Should not: Cell phone (leave in your car or with a trusted person)
 - Should not: Study guides and prep materials
- Know where your test center is (map it) and parking –
 Get to your test center early

- Read all instructions and rules carefully (twice!) don't rush
- Know how much time you have per question pace yourself
- Breathe and think positively

Taking the exam – Questions

- Read the entire question carefully (twice)
 - o Don't skim or skip
- Reword the question
 - Look for hints in the question
 - Focus on key words
 - Key words: *not, sometimes, always,* and *never*
 - Adjectives: *most,* least likely, *best,* etc.
 - Remove distractors
- Single right answer or multiple answers?

Taking the exam – Multiple Choice Answers

- Answer question in your mind before looking at the answers
- Read each answer
- Eliminate wrong answers
- Use the process of elimination
- Pick the best (most appropriate) answer
- Make an educated guess
- It's usually best to stick with your first choice -- but not always

Taking the exam – Answer Strategies

- Look for similar words in the question and answer
- Look for the longest and most specific answer
- Watch for negatives and extreme wording (not, all, always)
- Try the "True or False" technique
- "None of the above" is seldom correct.
- "All of the above" is often correct if the answers are very specific or two are correct

Handling Panic Attacks

- Take a time-out & deep breath
- Positive thoughts / Envision success
- Create your study space in your mind
 - "Go to the place where the answers are."
- Do you best on the question and move on / Don't dwell