



ISC SSCP

System Security Certified Practitioner

Q&A

DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

**QUESTION NO: 1**

**DES - Data Encryption standard has a 128 bit key and is very difficult to break.**

- A. True
- B. False

**Answer: B**

**QUESTION NO: 2**

**What is the main difference between computer abuse and computer crime?**

- A. Amount of damage
- B. Intentions of the perpetrator
- C. Method of compromise
- D. Abuse = company insider; crime = company outsider

**Answer: B**

**QUESTION NO: 3**

**A standardized list of the most common security weaknesses and exploits is the \_\_\_\_\_.**

- A. SANS Top 10
- B. CSI/FBI Computer Crime Study
- C. CVE - Common Vulnerabilities and Exposures
- D. CERT Top 10

**Answer: C**

**QUESTION NO: 4**

**A salami attack refers to what type of activity?**

- A. Embedding or hiding data inside of a legitimate communication - a picture, etc.
- B. Hijacking a session and stealing passwords
- C. Committing computer crimes in such small doses that they almost go unnoticed
- D. Setting a program to attack a website at 11:59 am on New Year's Eve

**Answer: C**

**QUESTION NO: 5**

**Multi-partite viruses perform which functions?**

- A. Infect multiple partitions
- B. Infect multiple boot sectors
- C. Infect numerous workstations
- D. Combine both boot and file virus behavior

**Answer: D**

**QUESTION NO: 6**

**What security principle is based on the division of job responsibilities - designed to prevent fraud?**

- A. Mandatory Access Control
- B. Separation of Duties
- C. Information Systems Auditing
- D. Concept of Least Privilege

**Answer: B**

**QUESTION NO: 7**

**\_\_\_\_\_ is the authoritative entity which lists port assignments**

- A. IANA
- B. ISSA
- C. Network Solutions
- D. Register.com
- E. InterNIC

**Answer: A**

**QUESTION NO: 8**

**Cable modems are less secure than DSL connections because cable modems are shared with other subscribers?**

- A. True
- B. False

**Answer: B**

**QUESTION NO: 9**

\_\_\_\_\_ is a file system that was poorly designed and has numerous security flaws.

- A. NTS
- B. RPC
- C. TCP
- D. NFS
- E. None of the above

**Answer: D**

**QUESTION NO: 10**

Trend Analysis involves analyzing historical \_\_\_\_\_ files in order to look for patterns of abuse or misuse.

**Answer: Log files**

**QUESTION NO: 11**

HTTP, FTP, SMTP reside at which layer of the OSI model?

- A. Layer 1 - Physical
- B. Layer 3 - Network
- C. Layer 4 - Transport
- D. Layer 7 - Application
- E. Layer 2 - Data Link

**Answer: D**

**QUESTION NO: 12**

Layer 4 in the DoD model overlaps with which layer(s) of the OSI model?

- A. Layer 7 - Application Layer
- B. Layers 2, 3, & 4 - Data Link, Network, and Transport Layers
- C. Layer 3 - Network Layer
- D. Layers 5, 6, & 7 - Session, Presentation, and Application Layers

**Answer: D**

**QUESTION NO: 13**

**A Security Reference Monitor relates to which DoD security standard?**

- A. LC3
- B. C2
- C. D1
- D. L2TP
- E. None of the items listed

**Answer: B**

**QUESTION NO: 14**

**The ability to identify and audit a user and his / her actions is known as \_\_\_\_\_.**

- A. Journaling
- B. Auditing
- C. Accessibility
- D. Accountability
- E. Forensics

**Answer: D**

**QUESTION NO: 15**

**There are 5 classes of IP addresses available, but only 3 classes are in common use today, identify the three: (Choose three)**

- A. Class A: 1-126
- B. Class B: 128-191
- C. Class C: 192-223
- D. Class D: 224-255
- E. Class E: 0.0.0.0 - 127.0.0.1

**Answer: A, B, C**

**QUESTION NO: 16**

**The ultimate goal of a computer forensics specialist is to \_\_\_\_\_.**

- A. Testify in court as an expert witness
- B. Preserve electronic evidence and protect it from any alteration
- C. Protect the company's reputation
- D. Investigate the computer crime

**Answer: B**

**QUESTION NO: 17**

**One method that can reduce exposure to malicious code is to run applications as generic accounts with little or no privileges.**

- A. True
- B. False

**Answer: A**

**QUESTION NO: 18**

**\_\_\_\_\_ is a major component of an overall risk management program.**

**Answer: Risk assessment**

**QUESTION NO: 19**

**An attempt to break an encryption algorithm is called \_\_\_\_\_.**

**Answer: Cryptanalysis**

**QUESTION NO: 20**

The act of intercepting the first message in a public key exchange and substituting a bogus key for the original key is an example of which style of attack?

- A. Spoofing
- B. Hijacking
- C. Man In The Middle
- D. Social Engineering
- E. Distributed Denial of Service (DDoS)

Answer: C

QUESTION NO: 21

If Big Texas telephone company suddenly started billing you for caller ID and call forwarding without your permission, this practice is referred to as \_\_\_\_\_.

Answer: Cramming

QUESTION NO: 22

When an employee leaves the company, their network access account should be \_\_\_\_\_?

Answer: Disable

QUESTION NO: 23

Passwords should be changed every \_\_\_\_\_ days at a minimum.  
90 days is the recommended minimum, but some resources will tell you that 30-60 days is ideal.

Answer: 90

QUESTION NO: 24

IKE - Internet Key Exchange is often used in conjunction with what security standard?

- A. SSL
- B. OPSEC
- C. IPSEC
- D. Kerberos