



SSCP

(System Security Certified Practitioner)

Total Questions: 254

Last Updated: Nov 09, 2008

Document version: 8.27.11

Thanks for purchasing techXams' Study Guide,

techXams' SSCP study guide is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this guide. An average of approximately 10 to 20 hours should be spent to study this guide and you will surely pass your exam. It's our guarantee.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Guarantee

If you study this guide properly and still unable to pass the exam, please send us a scanned copy of your official score at: refund@techeXams.ws. We will happily reimburse the cost of this study guide or send you an exchange of study guide of your choice free of cost.

Feedback

If you find any possible improvement, then please do let us know. We are always interested in improving the quality of this product. Feedback can be send at: feedback@techeXams.ws

Copyright

techXams holds the copyright of this material. techXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Question: 1.

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

- A. True
- B. False

Answer: B

Question: 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: 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: 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: 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

2

Answer: D

Question: 6.

What security principle is designed to prevent fraud?

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

is designed to

SSCP Demo Exam

Answer: B

Question: 7.

_____ is the authority for the .com domain.

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

Answer: A

Question: 8.

Cable modems are leased to subscribers and are shared with other subscribers.

- A. True
- B. False

are shared

Answer: B

Question: 9.

_____ is a file system protocol that is vulnerable to numerous security flaws.

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

Answer: D

Question: 10.

Trend Analysis involves the analysis of logs to look for patterns of abuse or misuse.

to look for patterns

Answer: Log files

Question: 11.

HTTP, FTP, SMTP rely on 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: 12.

Layer 4 in the DoD model is equivalent to which layer(s) in the OSI model?

?

- A. Layer 7 - Application
- B. Layers 2, 3, & 4
- C. Layer 3 - Network
- D. Layers 5, 6, & 7

Answer: D

Question: 13.

A Security Reference Model (SRM) is used to define the security requirements for a system. Which of the following is NOT a component of an SRM?

- B. Security Objectives
- C. D1
- D. L2TP
- E. None of the items listed

Answer: B

SSCP Demo Exam

Question: 14.

The ability to identify and document evidence is known as _____.

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

Answer: D

Question: 15.

There are 5 classes of IP addresses. Which three are most common use today, identify the three:

- A. Class A: 1-126
- B. Class B: 128-191
- C. Class C: 192-223
- D. Class D: 224-239
- E. Class E: 0.0.0.0-255.255.255.255

Answer: A, B, C

Question: 16.

The ultimate goal of digital forensics is to _____.

- A. Testify in court
- B. Preserve electronic evidence
- C. Protect the confidentiality of data
- D. Investigate the cause of a security incident

Answer: B

SSCP Demo Exam