Vendor: ISC2

Exam Code: SSCP

Exam Name: Systems Security Certified Practitioner

Version: DEMO

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 at11:59 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

Answer: D

QUESTION 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 7
_____ is the authoritative entity which lists port assignments

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

Answer: A

QUESTION 8
Cable modems are less secure than DSL connections because cable modems are shared with other subscribers?

A. True
B. False

Answer: B

QUESTION 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 10
Trend Analysis involves analyzing historical _____ files in order to look for patterns of abuse or misuse.

Answer: Log files

QUESTION 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 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 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 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 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: ABC

QUESTION 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 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 18
_____ is a major component of an overall risk management program.

A.
B.
C.
D.

Answer: Risk assessment

QUESTION 19
An attempt to break an encryption algorithm is called _____.

Answer: Cryptanalysis

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: BDNT2014