Vendor: (ISC)2

Exam Code: SSCP

Exam Name: Systems Security Certified Practitioner

Version: DEMO
QUESTION 1
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 2
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 3
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 4
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 5
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 6
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 7
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 8
______________ is a major component of an overall risk management program.

Answer: Risk assessment

QUESTION 9
An attempt to break an encryption algorithm is called ________________.

Answer: Cryptanalysis

QUESTION 10
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 11
Which of the following is a reason to use a Firewall?

A. To evaluate intrusions as they happen
B. To watch for internal attacks
C. To prevent or stop potential intrusions
D. To signal an alarm on a suspected intrusion

Answer: C

QUESTION 12
Which of the following is an attribute of polymorphic code?

A. It mutates while keeping the original algorithm intact
B. It uses encryption for all the code
C. It operates based on specific conditions
D. It is written to self replicate altering the computer configuration

Answer: A

QUESTION 13
Flooding network ports is an example of which type of attack?

A. Man-in-the-Middle
B. Brute force
C. Denial of service
D. Birthday

Answer: C

QUESTION 14
Which of the following is currently used in conjunction with most Internet-based certificates to provide continuous authentication?

A. Secure Multipurpose Internet Mail Extension (S/MIME)
B. Secure Sockets Layer (SSL)
C. Secure Shell (SSH)
D. Secure Electronic Transaction (SET)

Answer: B

QUESTION 15
Encryption ciphers that use the same key to encrypt and decrypt are called?

A. Asymmetric encryption
B. Symmetric encryption
C. Public key encryption
D. Digital signature encryption

Answer: B