IT-Prüfungen.de
Prüfungsvorbereitung Online

-Echte und Originale Prüfungsfragen und
 Antworten aus Testcenter
-Machen Sie sich fit für Ihre berufliche Zukunft!

Prüfungsnummer :   SSCP

Prüfungsname : System Security Certified

Practitioner (SSCP)

Version :   Demo

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

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

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

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

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: A, B, C

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

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

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

Answer: Risk assessment

9.An attempt to break an encryption algorithm is called _____.

Answer: Cryptanalysis

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

11.If Big Texastelephone company suddenly started billing you for caller ID and call forwarding without your permission, this practice is referred to as _____.

Answer: Cramming

12.When an employee leaves the company, their network access account should be _____?

Answer: Disable

13.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

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

A. SSL

B. OPSEC

C. IPSEC

D. Kerberos

E. All of the above

Answer: C

15. What are some of the major differences of Qualitative vs. Quantitative
methods of performing risk analysis? (Choose all that apply)

A. Quantitative analysis uses numeric values

B. Qualitative analysis uses numeric values

C. Quantitative analysis is more time consuming

D. Qualitative analysis is more time consuming

E. Quantitative analysis is based on Annualized Loss Expectancy (ALE)
formulas

F. Qualitative analysis is based on Annualized Loss Expectancy (ALE)
formulas

Answer: A, C, E

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

to break.

A. True

B. False

Answer: B

17.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

18.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

19.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

20.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

21.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

22._____ is the authoritative entity which lists port assignments

A. IANA

B. ISSA

C. Network Solutions

D. Register.com

E. InterNIC

Answer: A

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

A. True

B. False

Answer: B

24._____ 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

25.Is the person who is attempting to log on really who they say they are?

What form of access control does this questions stem from?

A. Authorization

B. Authentication

C. Kerberos

D. Mandatory Access Control

Answer: B