Vendor: ISC

Exam Code: SSCP

Exam Name: System Security Certified Practitioner (SSCP)

Version: Demo

QUESTION 1
DES - Data Encryption standard has a 128 bit key and is very difficult to break.

A. True
B. False

Correct 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

Correct 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

Correct 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

Correct 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

Correct 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

Correct Answer: B

QUESTION 7
_____ is the authoritative entity which lists port assignments.

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

Correct Answer: A

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

A. True
B. False

Correct 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

Correct Answer: D

QUESTION 10

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

Correct 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

Correct 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

Correct 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

Correct 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

Correct 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

Correct 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

Correct 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

Correct Answer: A

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

Correct Answer: Risk assessment

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

Correct Answer: Cryptanalysis

QUESTION 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)

Correct Answer: C

QUESTION 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 _____.

Correct Answer: Cramming

QUESTION 22
When an employee leaves the company, their network access account should be _____?

Correct Answer: Disable

QUESTION 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.

Correct Answer: 90

QUESTION 24
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

Correct Answer: C

QUESTION 25
Wiretapping is an example of a passive network attack?

A. True
B. False

Correct Answer: A

QUESTION 26
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

Correct Answer: ACE

QUESTION 27
Which of the concepts best describes Availability in relation to computer resources?

A. Users can gain access to any resource upon request (assuming they have proper permissions)
B. Users can make authorized changes to data
C. Users can be assured that the data content has not been altered
D. None of the concepts describes Availability properly

Correct Answer: A

QUESTION 28
Which form of media is handled at the Physical Layer (Layer 1) of the OSI Reference Model?

A. MAC
B. L2TP
C. SSL
D. HTTP
E. Ethernet

Correct Answer: E

QUESTION 29
Instructions or code that executes on an end user's machine from a web browser is known as _____ code.

A. Active X
B. JavaScript
C. Malware
D. Windows Scripting
E. Mobile

Correct Answer: E

QUESTION 30
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

Correct Answer: B

EnsurePass.com Members Features:

1. Verified Answers researched by industry experts.
2. Q&As are downloadable in PDF and VCE format.
3. 98% success Guarantee and **Money Back** Guarantee.
4. Free updates for **180** Days.
5. **Instant Access to download the Items**

View list of All Exam provided:
http://www.ensurepass.com/certfications?index=A

To purchase Lifetime Full Access Membership click here:
http://www.ensurepass.com/user/register

Valid Discount Code for 2015: JREH-G1A8-XHC6

To purchase the HOT Exams:

Cisco		CompTIA		Oracle	VMWare	IBM
100-101	640-554	220-801	LX0-101	1Z0-051	VCAD510	C2170-011
200-120	200-101	220-802	N10-005	1Z0-052	VCP510	C2180-319
300-206	640-911	BR0-002	SG0-001	1Z0-053	VCP550	C4030-670
300-207	640-916	CAS-001	SG1-001	1Z0-060	VCAC510	C4040-221
300-208	640-864	CLO-001	SK0-003	1Z0-474	VCP5-DCV	RedHat
350-018	642-467	ISS-001	SY0-301	1Z0-482	VCP510PSE	EX200
352-001	642-813	JK0-010	SY0-401	1Z0-485		EX300
400-101	642-832	JK0-801	PK0-003	1Z0-580		
640-461	642-902			1Z0-820		