Check Point Certified Security Principles Associate (CCSPA)

1. Which of the following is NOT a restriction, for partners accessing internal corporate resources through an extranet?

A. Preventing modification of restricted information

B. Using restricted programs, to access databases and other information resources

C. Allowing access from any location

D. Preventing access to any network resource, other than those explicitly permitted

E. Viewing inventory levels for partner products only

Answer(s): C

---

2. Which type of Business Continuity Plan (BCP) test involves practicing aspects of the BCP, without actually interrupting operations or bringing an alternate site on-line?

A. Structured walkthrough

B. Checklist

C. Simulation

D. Full interruption

E. Parallel

Answer(s): C

---

3. Which of the following equations results in the Single Loss Expectancy for an asset?

A. Asset Value x % Of Loss From Realized Exposure

B. Asset Value x % Of Loss From Realized Threat

C. Annualized Rate of Occurrence / Annualized Loss Expectancy

D. Asset Value x % Of Loss From Realized Vulnerability

E. Annualized Rate of Occurrence x Annualized Loss Expectancy

Answer(s): B

---

4. Which of the following is an integrity requirement for Remote Offices/Branch Offices (ROBOs)?

A. Private data must remain internal to an organization.

B. Data must be consistent between ROBO sites and headquarters.

C. Users must be educated about appropriate security policies.

D. Improvised solutions must provide the level of protection required.

E. Data must remain available to all remote offices.

Answer(s): B

---

5. Operating-svstem fingerprinting uses all of the following, EXCEPT _____, to identify a target operating system.

A. Sequence Verifier

B. Initial sequence number

C. Address spoofing

D. Time to Live

E. IP ID field

Answer(s): C

---

6. Internal intrusions are loosely divided into which categories? (Choose TWO.)

- [ ] A. Attempts by insiders to perform appropriate acts, on information assets to which they have been given rights or permissions.
- [ ] B. Attempts by insiders to access resources, without proper access rights
- [ ] C. Attempts by insiders to access external resources, without proper access rights.
- [ ] D. Attempts by insiders to perform inappropriate acts, on external information assets to which they have been given rights or permissions.
- [ ] E. Attempts by insiders to perform inappropriate acts, on information assets to which they have been given rights or permissions.

Answer(s): B E

---

7. _____ occurs when an individual or process acquires a higher level of privilege. Or access, than originally intended.

A. Security Triad

B. Privilege aggregation

C. Need-to-know

D. Privilege escalation

E. Least privilege

Answer(s): D

---

8. Which encryption algorithm has the highest bit strength?

A. AES

B. Blowfish

C. DES

D. CAST

E. Triple DES

Answer(s): A

---

9. How is bogus information disseminated?

A. Adversaries sort through trash to find information.

B. Adversaries use anomalous traffic patterns as indicators of unusual activity. They will employ other methods, such as social engineering, to discover the cause of the noise.

C. Adversaries use movement patterns as indicators of activity.

D. Adversaries take advantage of a person's trust and goodwill.

E. Seemingly, unimportant pieces of data may yield enough information to an adversary, for him to disseminate incorrect information and sound authoritative,

Answer(s): E

---

10. Which type of Business Continuity Plan (BCP) test involves shutting down z on-line, and moving all operations to the alternate site?

A. Parallel

B. Full interruption

C. Checklist

D. Structured walkthrough

E. Simulation

Answer(s): B

---

11. What must system administrators do when they cannot access a complete i testing?

A. Extrapolate results from a limited subset.

B. Eliminate the testing phase of change control.

C. Request additional hardware and software.

D. Refuse to implement change requests.

E. Deploy directly to the production environment.

Answer(s): A

---

12. To protect its information assets, ABC Company purchases a safeguard that costs $60,000. The annual cost to maintain the safeguard is estimated to be $40,000. The aggregate Annualized Loss Expectancy for the risks the safeguard is expected to mitigate is $50,000.
At this rate of return, how long will it take ABC Company to recoup the cost of the safeguard?

A. ABC Company will never recoup the cost of this safeguard.

B. Less than 7 years

C. Less than 3 years

D. Less than 1 year

E. Less than 5 years

Answer(s): B

---

13. Which of the following is NOT an auditing function that should be performed regularly?

A. Reviewing IDS alerts

B. Reviewing performance logs

C. Reviewing IDS logs

D. Reviewing audit logs

E. Reviewing system logs

Answer(s): B

---

14. Which TWO of the following items should be accomplished, when interviewing candidates for a position within an organization?

- [ ] A. Hire an investigation agency to run background checks.
- [ ] B. Verify all dates of previous employment.
- [ ] C. question candidates, using polygraphs, n
- [ ] D. Contact personal and professional references.
- [ ] E. Run criminal-background checks.

Answer(s): B D

---

15. Which of these metrics measure how a biometric device performs, when attempting to authenticate subjects? (Choose THREE.)

- [ ] A. False Rejection Rate

- [ ] B. User Acceptance Rate
- [ ] C. Crossover Error Rate
- [ ] D. False Acceptance Rate
- [ ] E. Enrollment Failure Rate

Answer(s): A C D

---

16. A new U.S. Federal Information Processing Standard specifies a cryptographic algorithm. This algorithm is used by U.S. government organizations to protect sensitive, but unclassified, information. What is the name of this Standard?

A. Triple DES

B. Blowfish

C. AES

D. CAST

E. RSA

Answer(s): C

---

17. Which of the following is likely in a small-business environment?

A. Most small businesses employ a full-time information-technology staff.

B. Resources are available as needed.

C. Small businesses have security personnel on staff.

D. Most employees have experience with information security.

E. Security budgets are very small.

Answer(s): E

---

18. When attempting to identify OPSEC indicators, information-security professionals must: (Choose THREE.)

- [ ] A. Discover the information daily activities yield.
- [ ] B. Meet with adversaries.
- [ ] C. Perform business impact analysis surveys.
- [ ] D. Scrutinize their organizations' daily activities.
- [ ] E. Analyze indicators, to determine the information an adversary can glean? Both from routine and nonroutine activities.

Answer(s): A D E

---

19. Why should each system user and administrator have individual accounts? (Choose TWO.)

- [ ] A. Using generic user names and passwords increases system security and reliability.
- [ ] B. Using separate accounts for each user reduces resource consumption, particularly disk space.
- [ ] C. By using individual login names and passwords, user actions can be traced.
- [ ] D. If users do not have individual login names, processes can automatically run with root/administrator access.
- [ ] E. A generic user name and password for users and security administrators provides anonymity, which prevents useful logging and auditing.

Answer(s): C E

---

20. Organizations_____ risk, when they convince another entity to assume the risk for them.

A. Elevate

B. Assume

C. Deny

D. Transfer

E. Mitigate

Answer(s): D
