System Security Certified Practitioner (SSCP Japanese Version)

1. 光ファイバーは ISO/OSI のどの層で機能しますか?

A. ネットワーク層

B. トランスポート層

C. データリンク層

D. 物理層

Answer(s): A

---

2. 低速シリアル インターフェイスを介した TCP/IP ネットワーキングをサポートするために開発されたテクノロジは次のうちどれですか?

A. ISDN

B. スリップ

C. xDSL

D. T1

Answer(s): C

---

3. 次のうち、署名ベースの侵入検知システムの問題はどれですか?

A. 以前に識別された攻撃シグネチャのみが検出されます。

B. 署名データベースは、推論要素で補強する必要があります。

C. Windows オペレーティング システムでのみ動作します。

D. ハッカーは署名の評価を回避できます。

Answer(s): B

---

4. システム開発ライフサイクルの方法論が不適切な場合に最も重大なリスクとなるのは、次のうちどれですか?

A. プロジェクトの完了が遅れます。

B. プロジェクトはコスト見積もりを超えます。

C. プロジェクトは既存のシステムと互換性がありません。

D. プロジェクトは、ビジネスおよびユーザーのニーズを満たすことができません。

Answer(s): D

---

5. アクセス制御の目的をサポートする「ソフト」メカニズムに重点を置いているのは、次の制御の組み合わせのうちどれですか?

A. 予防/技術ペアリング

B. 予防/管理ペアリング

C. 予防的/物理的なペアリング

D. 探偵/管理のペアリング

Answer(s): B

---

6. Web ブラウザからエンド ユーザーのマシン上で実行される命令またはコードは、

A. JavaScript

B. アクティブ X

C. モバイル

D. マルウェア

E. Windows スクリプト

Answer(s): A

---

7. 国際標準化機構 / オープン システム相互接続 (ISO/OSI) レイヤーに、次の特徴のどれがありませんか?

A. ネットワーク通信のスタンダードモデル

B. ネットワーク機器から受信パケット数やルーティングテーブルなどの情報を取得するために使用

C. 異なるネットワークが通信できるようにします

D. 7 つのプロトコル層 (別名プロトコル スタック) を定義します。

Answer(s): B

---

8. サブジェクトのセキュリティ クリアランスが必要なアクセス制御モデルは次のうちどれですか?

A. ID ベースのアクセス制御

B. ロールベースのアクセス制御

C. 任意アクセス制御

D. 強制アクセス制御

Answer(s): D

---

9. ルート CA 証明書の更新の主な問題は何ですか?

A. すべてのユーザーから古いルート CA 証明書を収集する必要があります。

B. 新しいルート CA 証明書をすべての PKI 参加者に確実に配布する必要があります。

C. 新しいルート CA 証明書の発行が必要です。

D. すべてのエンド ユーザー キーのキー リカバリが必要です。

Answer(s): D

---

10. 次のうち、電子メール メッセージの認証と機密性を提供するために使用されるものはどれですか?

A. デジタル署名

B. PGP

C. IPSEC ああ

D. MD4

Answer(s): B

---

11. 情報セキュリティに関連して、送信されたメッセージが受信されたメッセージであり、メッセージが意図的または意図せずに変更されていないという保証は、次のうちどれの例ですか?

A. 完全性

B. 守秘義務

C. 在庫状況

D. ID

Answer(s): A

12. コンピューティング能力の向上により、nst 暗号化キー

A. 優れたキー ジェネレーターの使用。

B. セッション キーの使用。

C. ブルート フォースの暗号キー攻撃に対して防御できるものは何もありません。

D. ブルート フォース キー攻撃の影響を受けないアルゴリズム。

Answer(s): B

---

13. ハニーポットを設定する主な目的は何ですか?

A. ハッカーを誘惑して未使用のシステムを攻撃する

B. 潜在的なハッカーを罠にかけ、追跡するため

C. ネットワーク上に生け贄の子羊を設定するには

D. 特定の種類の攻撃がいつ進行しているかを知り、ネットワークを強化するための攻撃手法について学習します。

Answer(s): D

---

14. コンピュータで生成された証拠は、次のように考慮されます。

A. 最良の証拠

B. 中古証拠

C. 実証的証拠

D. 直接証拠

Answer(s): C

15. Triple DES で暗号化するときに使用できる異なるキーの最大数は?

A. 1

B. 2

C. 3

D. 4

Answer(s): C

---

16. 侵入テストには 3 つのステップが含まれます。以下の 3 つのステップを特定します:
(3 つ選択してください)

A. システム制御

B. ネットワークスキャン

C. 戦争運転

D. ネットワーク侵入

E. ネットワーク偵察

F. システムサービスの拒否

Answer(s): A,D,E

---

17. 組織は、災害復旧を次のどれと見なすべきではありませんか?

A. 確定費用。

B. 任意費用。

C. 法規の施行。

D. 規制の遵守。

Answer(s): D

---

18. 送信者が電子送信を送信したことを否定できない場合、この概念は_____ として知られています。

A. 検証

B. PKI

C. 公開鍵

D. 否認防止

E. 取り消し不能な信頼

Answer(s): D

---

19. インシデント対応の主な目標は何ですか?

A. 起訴に使用できるすべての証拠の回収に成功する

B. 脅威や災害に備える企業の能力を向上させる

C. 会社の災害復旧計画を改善する

D. イベントによって引き起こされた損傷を封じ込め、修復します。

Answer(s): C

---

20. スプーフィングは、信頼できる送信元アドレスからの IP パケットを偽造することによって、あるコンピュータを別のコンピュータに対して認証する高度な技術です (True / False)。

A. 真

B. 偽

Answer(s): A