Comptia Security+ Certification Exam (SY0-501 Japanese Version)

1. ファラデーケージの正しい使い方は次のうちどれですか？

A. フォレンジック調査中にハードディスクをアクセスから保護するため

B. 携帯電話を消去するために送信される電気信号をブロックするには

C. 攻撃中にハニーポットに送信されたパケットをキャプチャする

D. 建物へのアクセスを制限して、一度に1人だけが入ることを許可する

Answer(s): B

---

2. 組織には、次の書面によるポリシーがあります。

A. ユーザーのマシンがマルウェアに感染している組織のインシデント対応を実装する

B. マシンにソフトウェアをインストールしたユーザーは、書面によるポリシーを実施するための技術的管理を実装します

C. 管理者は信頼できないリポジトリからソフトウェアをダウンロードしました。すべてのソフトウェアの整合性チェックを要求するポリシーを追加します

D. 暗号通貨ソフトウェアは誤認され、承認されています。組織の承認済みリストにソフトウェアを追加します

Answer(s): B

---

3. 従業員は、毎年初めに会社の人事部門から福利厚生登録メールを受け取ります。何人かのユーザーが電子メールの受信を報告しましたが、ユーザー名とパスワードでWebサイトにログインできません。人事サイトのURLを入力したユーザーは問題なくログインできます。次のセキュリティ問題のどれが発生していますか？

A. 複数のユーザーのコンピューターがHTTPSを使用してWebサイトにアクセスするように構成されていませんでした。

B. 内部DNSサーバーが侵害され、ユーザーをハッカーのサーバーに誘導しました。

C. ユーザーはソーシャルエンジニアリングの電子メールを受信し、外部のWebサイトに誘導されました。

D. 人事サーバーが多数のリクエストを受信した結果、DoSが発生しました

Answer(s): C

---

4. セキュリティ管理者は、コンピューターが奇妙なネットワーク関連の停止を示しているユーザーレポートを分析しています。ただし、管理者には疑わしいプロセスの実行は表示されません。前の技術者のメモは、マシンが2回修復されたことを示していますが、システムは依然として奇妙な動作を示しています。ファイルは最近システムから削除されました。

A. 論理爆弾

B. 暗号マルウェア

C. セッションハイジャック

D. ルートキット

Answer(s): D

---

5. ペネトレーションテスターは、企業の内部ネットワークに接続し、テスト期間中、気付かれることなくスキャンと段階的な攻撃を実行することができました。 SIEMは、ネットワーク上に侵入テスターのデバイスが存在することをセキュリティチームに警告しませんでした。次のうち、セキュリティチームにタイムリーに通知を提供するのはどれですか。

A. IPSでトリガーを作成し、ログインに失敗したときにセキュリティチームに警告します。

B. SIEMのアラートの相関しきい値を下げます。

C. 不正なシステムの検出とセンサーを実装します。

D. 資格情報付きの脆弱性スキャンを実行します

Answer(s): C

---

6. ネットワークエンジニアは、倉庫内のいくつかのワイヤレスバーコードスキャナーとワイヤレスコンピューターが配送サーバーに断続的に接続する理由を調査するように依頼されました。バーコードスキャナーとコンピューターはすべてフォークリフトに搭載されており、通常の使用中は倉庫内を移動します。問題を特定するためにエンジニアが行うべきことは次のうちどれですか？（2つ選択）

A. サイト調査を実行します。

B. セキュリティプロトコルをアップグレードします。

C. キャプティブポータルをインストールする

D. ヒートマップを作成します。

E. 不正アクセスポイントをスキャンします。

F. FTKイメージャーを配備します。

Answer(s): A,E

---

7. 組織は、認証スキームの一部として2つの別個の要素を必要とします。それらの要因の1つはパスワードです。次のうち、他の要素の要件を最もよく満たすのはどれですか？

A. OTP

B. PIN

C. セキュリティの質問

D. パスフレーズ

Answer(s): A

---

8. 技術者は、ユーザーActiveDirectoryグループメンバーシップに基づく動的VLAN割り当てを使用して8021Xを実装しています。次の構成のどれがVLAN定義をサポートしていますか？

A. LDAPパス

B. Shibboleth IdP

C. SAMLタグ

D. RADIUS属性

Answer(s): C

---

9. データベースにPIIがない場合でも、開発環境で本番環境に存在するのと同じデータベースサーバーの安全なベースラインが必要な理由を説明しているのは次のうちどれですか。

A. 攻撃者は、本番データベースと同じくらい簡単に、開発環境の低いデータベースから機密性の高い個人情報を抽出できます。

B. 開発と本番の両方で同じ構成がないと、開発で行われた変更が本番で同じ効果をもたらすという保証はありません。

C. データベースは、攻撃される頻度が高いため、すべての環境に安全な構成を適用する必要があるという点で独特です。

D. 法律では、個人情報を保存する機能を備えたデータベースは、環境に関係なく、または実際にPIIがあるかどうかに関係なく保護する必要があると規定されています。

Answer(s): A

---

10. 大企業のインシデントレスポンスアナリストがプロキシログデータを確認しています。アナリストは、マルウェア感染が発生した可能性があると考えています。さらに分析すると、アナリストは、疑わしいネットワークトラフィックを担当するコンピューターが最高経営責任者（CEO）によって使用されていると判断します。アナリストが取るべき最善の次のステップは次のうちどれですか。

A. CEOに直接電話して、イベントの認識を確認する

B. CEOのワークステーションのイメージを再作成します

C. CEOのワークステーションでマルウェアスキャンを実行します

D. CEOのワークステーションをネットワークから切断します。

Answer(s): D

---

11. エンドポイントへのゼロデイ攻撃を阻止するのに最も効果的なのは次のうちどれですか？（2つ選択してください）

A. リバースプロキシのインストール

B. ユーザーから管理者権限を削除する

C. ウイルス対策およびマルウェア対策システムツールの導入

D. Webアプリケーションファイアウォールの実装

E. マルチベンダーNGFWの導入

F. アプリケーションのホワイトリストの実装

Answer(s): B,F

---

12. コンピュータフォレンジックアナリストは、500ページのテキストを含む単一のファイルを含むサムドライブを収集しました。ファイルの機密性を維持するために、アナリストは次のうちどれを使用する必要がありますか？

A. SHA

B. SLA

C. NOA

D. AES

Answer(s): D

---

13. セキュリティアナリストが大規模なワイヤレスネットワークを強化しています。主な要件は次のとおりです

A. CCMP

B. 802.1X

C. 802.3

D. LDAP

E. TKIP

F. WPA2-PSK

Answer(s): B,F

---

14. セキュリティ管理者は、BYODのリスク評価を作成しています。リスク評価の要件の1つは、以下に対処することです。

A. モバイルデバイスを強化したMDMを実装します。

B. 暗号化を実装します。

C. ウェブメールに安全な接続でVPNを実装します。

D. ハッシュを実装します。

E. ネットワークにクラウドストレージ機能を実装して許可します。

Answer(s): A,E

---

15. システム管理者は、新しいWebサイトでHTTPSの使用を強制したいと考えています。システム管理者は、CSRを生成した後、次のうちどれを実行する必要がありますか？

A. 公開鍵をパスワードで保護します。

B. サーバーに証明書をインストールします。

C. 新しいキーがCRLにないことを確認します。

D. CAに公開鍵を提供します。

Answer(s): B

---

16. ネットワークで分離された一部の産業用コンピューターにウイルス対策ソリューションを展開した後、サービスデスクチームは、コンピューターの画面に次のメッセージが表示されていることに関するトラブルチケットを受け取りました。

A. 産業用コンピューターのセット全体のフルスキャンを一元的にアクティブ化し、新しい脅威を探します

B. 検出されたファイルを検疫からただちに削除して環境を保護し、ウイルス対策コンソールからアラートをクリアします

C. ウイルス対策ベンダーのクラウドから直接手動のウイルス対策署名の更新を実行します

D. セキュリティモジュール、非互換性、およびソフトウェアのホワイトリストに関するウイルス対策ベンダーのドキュメントを確認してください。

Answer(s): D

---

17. セキュリティエンジニアは、MFAを導入することにより、ネットワーク上の機密VLANをさらに保護したいと考えています。次のうちどれがこれの最良の例ですか？

A. 秘密の質問とCAPTCHA

B. 指紋スキャナーと音声認識

C. RSAトークンとパスワード

D. PSKとPIN

Answer(s): C

---

18. 会社には、侵入テストのチームがあります。このチームは、会社のファイルサーバー上に、クリアテキストのユーザー名とそれに続くハッシュが含まれていると思われるファイルを見つけました。このファイルの内容について詳しく知るために、侵入テスト担当者は次のどのツールを使用する必要がありますか？

A. Vulnerability scanner

B. Password cracker

C. Netcat

D. Exploitation framework

Answer(s): B

---

19. セキュリティ対策として、組織はすべての外部メディアによるネットワークへのアクセスを無効にしました。一部のユーザーはネットワークに転送する必要のあるデータを持っている可能性があるため、セキュリティ管理者が内部ネットワークを安全に保ちながらデータを転送するのに最適な方法はどれですか。 ？

A. 別のVLANにデータをアップロードする

B. スタンドアロンのスキャンシステムを使用する

C. データ管理者に連絡する

D. DMZにメディアをアップロードします

Answer(s): D

---

20. 最高セキュリティ責任者（CSO）は、許可されていないユーザーに情報が流出するリスクがあるため、ハードドライブの再利用を防止するポリシーを実装しています。ワークステーションを廃止するための最も実用的なプロセスは次のうちどれですか？

A. すべてのハードドライブを取り外し、ディスクを細断処理します。

B. すべてのハードドライブを取り外してパージします。

C. すべてのハードドライブを取り外し、消磁します。

D. すべてのハードドライブを取り外し、ゴミ箱に捨てます。

Answer(s): A
