EC-Council Certified Network Defender (CND) (312-38 Japanese Version)

1. Wiresharkユーティリティを使用してネットワークトラフィックを監視していて、ネットワークで特定の地域からの大量のトラフィックが発生していることに気づきました。ネットワーク上のDoSインシデントが疑われます。ファーストレスポンダーとしての最初の反応は何ですか？

A. 恐れ、不確実性、疑いを避ける

B. インシデントを伝える

C. 初期評価を行う

D. ウイルス対策を無効にする

Answer(s): C

---

2. ユーザーが他のユーザーに代わって要求されたリソースにアクセスできるようにするのはどの承認ですか?

A. 明示的な認可

B. 分散型認可

C. 暗黙的な承認

D. 集中認証

Answer(s): C

---

3. 顧客の個人情報のプライバシーを保護するために、クラウド サービス プロバイダーは次のどの基準に準拠する必要がありますか?

A. ISO/IEC 27018

B. ISO/IEC 27019

C. ISO/IEC 27020

D. ISO/IEC 27021

Answer(s): A

---

4. 従業員のコンプライアンス問題に対する意識を高めることができるのはどのような研修ですか?

A. ソーシャル エンジニアリング意識向上トレーニング

B. セキュリティポリシー研修

C. 物理的セキュリティ意識向上トレーニング

D. データ分類に関するトレーニング

Answer(s): B

---

5. Sophieは、過去7年間、MNCでWindowsネットワーク管理者として働いています。彼女は、SMB1が有効になっているか無効になっているかを確認したいと考えています。次のコマンドのどれがソフィーにそうすることを許可しますか？

A. Get-WindowsOptionalFeatures -Online -FeatureNames SMB1Protocol

B. Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

C. Get-WindowsOptionalFeature -Online -FeatureNames SMB1Protocol

D. Get-WindowsOptionalFeatures -Online -FeatureName SMB1Protocol

Answer(s): B

---

6. ネットワーク セキュリティ エンジニアのライアンは、最近の攻撃を受けて、ユーザーが直面している攻撃の種類に関する情報を入手しようとしています。彼は、Kojoney と呼ばれる 1 つのハニーポットを運用することを決定しました。彼は、実際の脆弱性システムではなく、ネットワークの脆弱性をエミュレートして、この調査をより安全かつ柔軟にすることに興味を持っています。彼はどのタイプのハニーポットを実装しようとしているのでしょうか?

A. 研究ハニーポット

B. インタラクションの高いハニーポット

C. インタラクションの少ないハニーポット

D. 純粋なハニーポット

Answer(s): C

---

7. 企業は最近新しいオフィスに移転し、新しい近所は少し危険です。 CEOは、物理的な境界と玄関のドアを24時間監視したいと考えています。この仕事をするための最良の選択肢は何ですか？

A. 玄関ドアと通りを指すカメラ付きのCCTVを設置します

B. 玄関ドアに柵を使用する

C. すべての玄関ドアと会社の周囲に沿ってライトを使用します

D. 玄関ドアにIDSを使用し、それらのいくつかを角の近くに設置します

Answer(s): A

---

8. どのタイプのファイアウォールが3つのインターフェイスで構成されており、組織の特定のセキュリティ目標に基づいてシステムをさらに細分化できますか？

A. スクリーニングされたサブネット

B. 要塞ホスト

C. スクリーニングされていないサブネット

D. マルチホームファイアウォール

Answer(s): D

---

9. データの冗長性を提供しない RAID レベルはどれですか?

A. RAID レベル 0

B. RAID レベル 1

C. RAID レベル 50

D. RAID レベル 10

Answer(s): A

---

10. あるカスタマーエッジ（CE）から別のカスタマーエッジ（CE）へのトラフィックを保証するVPN QoSモデルはどれですか？

A. パイプモデル

B. AAAモデル

C. ハブアンドスポークVPNモデル

D. ホースモード

Answer(s): A

---

11. アルバートは、MNCでWindowsシステム管理者として働いています。彼はPowerShellロギングを使用して、ネットワーク全体の疑わしいスクリプトアクティビティを特定します。彼は、変数の初期化やコマンドの呼び出しなど、PowerShellの実行時にパイプラインの実行の詳細を記録したいと考えています。 PowerShellの実行時にパイプラインの実行の詳細を記録するPowerShellログコンポーネントはどれですか？

A. モジュールロギング

B. スクリプトブロックロギング

C. イベントログ

D. トランスクリプトロギング

Answer(s): B

---

12. ツリーネットワークで構成されるシナリオを考えてみましょう。ルートノードNは、2つのmanノードN1とN2に接続されています。

A. メインノードの障害は、メインノードに関係なく、同じレベルの他のすべての子ノードに影響します。

B. 子ノードまたはその送信に障害を引き起こしません

C. メインノードの障害は、メインノードに接続されているすべての関連する子ノードに影響します

D. ルートノードにのみ影響します

Answer(s): C

---

13. データ破壊のパージ手法に関与する手法を特定します。

A. 焼却

B. 上書き

C. 消磁

D. 拭き取り

Answer(s): B

---

14. カイルは、25台のワークステーションと4台のサーバーを管理するIT技術者です。サーバーはアプリケーションを実行し、ほとんどの場合機密データを保存します。カイルは、何も失われないように、サーバーのデータを毎日バックアップする必要があります。会社のオフィスの電源は常に信頼できるとは限りません。カイルは、サーバーがダウンしたり、電源が長時間切れたりしないようにする必要があります。カイルは、バッテリーを充電し、必要に応じて電力を供給するインバーターとコンバーターのペアを備えた無停電電源装置（UPS）を購入することにしました。カイルはどのタイプのUPSを購入しましたか？

A. カイルはフェロ共振スタンバイUPSを購入しました。

B. カイルはラインインタラクティブUPSを購入しました

C. 彼はスタンバイUPSを購入しました

D. 彼はTrue OnlineUPSを購入しました。

Answer(s): D

---

15. Blake は、会社の最新の災害および事業継続計画に取り組んでいます。計画の最後のセクションでは、コンピューターとデータの発生への対応について説明します。ブレーク氏は、計画におけるインシデントの種類ごとに重大度のレベルを概説しています。失敗したスキャンとプローブの重大度レベルはどれですか?

A. 重大度レベルが非常に高い

B. 重大度レベルが低い

C. 中程度の重大度レベル

D. 重大度レベル高

Answer(s): B

---

16. 次のうち、個々の管理者アカウントのパスワードを作成してWindows ADに保存するのはどれですか？

A. LSASS

B. SRM

C. SAM

D. LAPS

Answer(s): D

---

17. ネットワークインターフェイスカード（NIC）はどのOSI層で機能しますか？

A. 物理層

B. プレゼンテーション層

C. ネットワーク層

D. セッション層

Answer(s): A

---

18. ワイヤレスネットワークはどのIEEE標準を使用しますか？

A. 802.11

B. 802.18

C. 802.9

D. 802.10

Answer(s): A

---

19. ロスは、組織内で30人の従業員と25台のコンピューターのみを管理しています。同社が使用しているネットワークはピアツーピアです。ロスはアクセス制御手段を構成し、従業員がファイルとフォルダーに対して独自の制御手段を設定できるようにします。ロスはどのアクセス制御を実装しましたか？

A. 随意アクセス制御

B. 強制アクセス制御

C. 非任意アクセス制御

D. 役割ベースのアクセス制御

Answer(s): A

---

20. インシデント発生後に会社の詳細を伝える責任は誰にありますか?

A. PRスペシャリスト

B. IR担当者

C. IRマネージャー

D. IR管理者

Answer(s): A
