ECCouncil.212-82.v2024-01-17.q21

試験コード:	212-82
試験名称:	Certified Cybersecurity Technician
認定資格:	ECCouncil
無料問題数:	21
バージョン:	v2024-01-17
アクセス数:	816
ページビュー数:	210
https://www.jpnpdf.com/ECCouncil.212-82.v2024-01-17.q21-mondaishu.html	

最新問題: **1**
セキュリティ専門家のナンシーは、Linux マシンの予期しないシャットダウンと再起動に関連する問題を特定するように指示されました。インシデントの原因を特定するために、Nancy は Linux システム上のディレクトリに移動し、ログ ファイルにアクセスして、不適切なシャットダウンや計画外の再起動に関連する問題のトラブルシューティングを行いました。
上記のシナリオで Nancy がアクセスした Linux ログ ファイルを特定します。
A. /var/log/lighttpd/
B. /var/log/boot.log
C. /var/log/kern.log
D. /var/log/secure
Answer: (解答を表示する)

最新問題: **2**
Web アプリケーション www.movieabc.com が SQL インジェクション攻撃を受けやすいことが判明しました。Web アプリケーションを悪用してユーザーの資格情報を取得するタスクが与えられます。データベーステーブルでユーザー john にマップされている UID を選択します。
ノート：
ユーザー名: サム
合格: テスト
A. 2
B. 5
C. 3
D. 4
Answer: D (メーッセージを残す)

最新問題: **3**
ケイデンはある組織の最終面接を無事突破しました。数日後、彼は会社の公式電子メールアドレスを通じて内定通知を受け取りました。電子メールには、選択された候補者が指定された時間内に応答する必要があると記載されていました。ケイデンはその機会を受け入れ、オファーレターに電子署名を記入し、同じ電子メールアドレスに返信しました。同社は電子署名を検証し、彼の詳細をデータベースに追加しました。ここで、ケイデンは会社のメッセージを拒否できず、会社もケイデンの署名を拒否できませんでした。
上記のシナリオで説明された情報セキュリティ要素は次のうちどれですか?
A. 否認防止
B. 可用性
C. 誠実さ
D. 機密保持
Answer: (解答を表示する**)**

最新問題: **4**
プロのハッカーであるミゲルは、重要な情報に不正にアクセスするために組織を標的にしました。彼は、ターゲット アプリケーションのデータを漏洩する可能性があるエンドポイント通信の欠陥を特定しました。
上記のシナリオのアプリケーションで満たされなかった安全なアプリケーション設計原則は次のうちどれですか?
A. ユーザー入力を信頼しません
B. フォールトトレランス
C. 最も弱いリンクを確保する
D. 例外処理
Answer: D (メーッセージを残す**)**

最新問題: **5**
Richards は、組織のセキュリティ専門家であり、IDS システムを監視していました。監視中に、突然、組織のネットワーク上で進行中の侵入の試みに関する警告を受け取りました。彼は直ちに必要な措置を講じて悪意のある行為を回避しました。
上記のシナリオで IDS システムによって生成されたアラートのタイプを特定します。
A. 真陽性
B. 偽陰性
C. 真陰性
D. 偽陽性
Answer: A (メーッセージを残す**)**

最新問題: **6**
レオは食料品を買うために最寄りのスーパーマーケットまで歩いて行きました。請求部門では、請求責任者が各製品の機械読み取り可能なタグを読み取り可能な機械に照らしてス

キャンし、読み取り可能な機械が製品の詳細を自動的に読み取り、個々の製品の価格をコンピューターに表示し、スキャンした商品の合計を計算しました。すべての製品のスキャンが完了したら、レオは請求書を支払わなければなりません。
上記のシナリオで請求担当者が使用した短距離無線通信テクノロジの種類を特定します。
A. クイック
B. 無線周波数識別 (RFID)
C. QRコード、バーコード
D. 近距離無線通信（NFC）
Answer: B (メーッセージを残す**)**

最新問題**: 7**
犯罪捜査官のルーベンは、元のファイルに影響を与えることなく、疑わしいメディア内の削除されたファイルとフォルダーをすべて取得したいと考えています。この目的のために、彼はメディア全体のクローンコピーを作成し、元のメディアの汚染を防ぐ方法を使用しました。
上記のシナリオで Ruben が使用した手法を特定します。
A. スパース取得
B. 論理取得
C. ドライブの復号化
D. ビットストリームイメージング
Answer: D (メーッセージを残す**)**

最新問題**: 8**
組織のネットワーク セキュリティ管理者である Matias は、ネットワークに安全なワイヤレス ネットワーク暗号化を実装する任務を負っていました。この目的のために、Matias は 256 ビット ガロア/カウンター モード プロトコル (GCMP-256) を使用してデータの信頼性と機密性を維持するセキュリティ ソリューションを採用しました。
上記のシナリオで Matias が採用したセキュリティ ソリューションで使用されるワイヤレス暗号化の種類を特定します。
A. WEP暗号化
B. WPA3暗号化
C. WPA暗号化
D. WPA2暗号化
Answer: B (メーッセージを残す**)**

最新問題**: 9**
セキュリティの専門家である Karter 氏は、ネットワークに侵入しようとする攻撃者をおびき寄せるために、組織のネットワークにハニーポットを導入しました。この目的のために、彼は実際の OS とターゲット ネットワークのアプリケーションおよびサービスをシミュ

レートするタイプのハニーポットを構成しました。さらに、Karter によって展開されたハニーポットは、事前設定されたコマンドにのみ応答します。
上記のシナリオで Karter によってデプロイされたハニーポットのタイプを特定します。
A. 低インタラクションのハニーポット
B. 高インタラクション ハニーポット
C. ピュアハニーポット
D. 中程度のインタラクション ハニーポット
Answer: (解答を表示する**)**

最新問題**: 10**
システム管理者である Ryleigh は、組織データの完全バックアップを定期的に実行するように指示されました。この目的のために、彼女は従業員がシステムにアクセスしていない固定日にバックアップ手法を使用しました。つまり、サービス レベルのダウンタイムが許容されるときに完全バックアップが作成されました。
上記のシナリオで Ryleigh が使用したバックアップ手法を特定します。
A. ウォームバックアップ
B. コールドバックアップ
C. ニアラインバックアップ
D. ホットバックアップ
Answer: B (メーッセージを残す**)**

最新問題**: 11**
組織のセキュリティ専門家であるレットは、進化する脅威から防御するために、企業ネットワークに IDS ソリューションを導入するよう指示されました。この目的のために、Rhett 氏は、まず考えられる侵入のモデルを作成し、次にこれらのモデルを受信イベントと比較して検出の決定を行う IDS ソリューションを選択しました。
上記のシナリオで IDS ソリューションで採用された検出方法を特定します。
A. 署名認識
B. 異常検知
C. 不使用検出
D. プロトコル異常検出
Answer: B (メーッセージを残す**)**

最新問題**: 12**
ネットワーク内で SSH が有効になっているマシンへの SSH 接続を開始します。マシンに接続したら、flag.txt ファイルを見つけて、ファイル内に隠されているコンテンツを選択します。SSH ログインの認証情報は以下に提供されます。
ヒント：
ユーザー名: サム
パスワード: admin@l23

A. bob2@sam
B. サム2@ボブ
C. ボブ@サム
D. サム@ボブ
Answer: C (メーッセージを残す**)**

最新問題**: 13**
セキュリティの専門家である Malachi は、送受信トラフィックを追跡するために組織にファイアウォールを導入しました。彼は、OSI モデルのセッション層で動作するファイアウォールを導入し、ホスト間の TCP ハンドシェイクを監視して、要求されたセッションが正当であるかどうかを判断しました。
上記のシナリオで Malachi によって実装されたファイアウォール テクノロジーを特定します。
A. 回線レベルのゲートウェイ
B. 次世代ファイアウォール (NGFW)
C. パケットフィルタリング
D. ネットワークアドレス変換(NAT)
Answer: (解答を表示する**)**

最新問題**: 14**
アシュトンは、SoftEight Tech でセキュリティ スペシャリストとして働いています。彼は経営陣からインターネット アクセス ポリシーを強化するよう指示されました。この目的のために、彼は、システムの使用でもネットワークの使用でも、すべてを禁止し、すべての会社のコンピューターに厳しい制限を課す一種のインターネット アクセス ポリシーを実装しました。
上記のシナリオでアシュトンによって実装されたインターネット アクセス ポリシーの種類を特定します。
A. 偏執的な政策
B. 慎重な方針
C. 無差別ポリシー
D. 寛容なポリシー
Answer: A (メーッセージを残す**)**

最新問題**: 15**
組織のネットワーク スペシャリストである Tenda は、Windows イベント ビューアを使用してログ データを調査し、試みられた、または成功した不正なアクティビティを特定していました。Tenda によって分析されたログには、Windows セキュリティに関連するイベントが含まれています。具体的には、ログオン/ログオフ アクティビティ、リソース アクセス、および Windows システムの監査ポリシーに基づく情報です。
上記のシナリオで Tenda によって分析されたイベント ログのタイプを特定します。

A. システムイベントログ
B. イベントログの設定
C. アプリケーションイベントログ
D. セキュリティイベントログ
Answer: (解答を表示する**)**

最新問題**: 16**
あるソフトウェア会社は、安全なアプリケーション開発のベスト プラクティスに従って新しいソフトウェア製品を開発しています。ソフトウェア アナリストの Dawson は、クライアントのネットワーク上のアプリケーションのパフォーマンスをチェックして、エンドユーザーがアプリケーションにアクセスする際に問題が発生していないかどうかを判断しています。
安全なアプリケーション開発ライフサイクルの次の層のうち、アプリケーションのパフォーマンスのチェックが含まれるのはどれですか?
A. 品質保証 (QA)
B. ステージング
C. 開発
D. テスト中
Answer: D (メーッセージを残す**)**

最新問題**: 17**
多国籍企業のセキュリティ専門家である Lorenzo は、リモート アクセス サーバーの一元的な認証、認可、およびアカウンティングを確立するよう指示されました。この目的のために、彼はクライアントサーバーモデルに基づき、OSI モデルのトランスポート層で動作するプロトコルを実装しました。
上記のシナリオで Lorenzo が使用したリモート認証プロトコルを特定します。
A. 半径
B. IMAPS
C. POP3S
D. SNMPv3
Answer: A (メーッセージを残す**)**

最新問題: **18**
RAT は、サーバーのデスクトップにある企業の重要な機密文書を盗むために、ネットワークに接続されているマシンの 1 つにセットアップされており、さらなる調査により、サーバーの IP アドレス 20.20.10.26 が判明しました。Thief クライアントを使用してリモート接続を開始し、フォルダー内に存在するファイルの数を確認します。
ヒント: Thief フォルダは、Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1 にあります。
A. 4
B. 3
C. 5
D. 2
Answer: B (メーッセージを残す**)**

最新問題: **19**
ある組織は、IT インフラストラクチャを外部攻撃から保護するためにネットワーク オペレーション センター (NOC) チームを雇用しました。この組織は、進化する脅威からリソースを保護するために、一種の脅威インテリジェンスを利用しました。脅威インテリジェンスは、NOC チームが、攻撃者がどのように組織に対して攻撃を実行することが予想されるかを理解し、情報漏洩を特定し、攻撃目標と攻撃ベクトルを決定するのに役立ちました。
上記のシナリオで組織が利用する脅威インテリジェンスの種類を特定します。
A. 運用上の脅威インテリジェンス
B. 技術的脅威インテリジェンス
C. 戦略的脅威インテリジェンス
D. 戦術的脅威インテリジェンス
Answer: B (メーッセージを残す**)**

最新問題: **20**
組織に関する機密情報を含むテキスト ファイルが漏洩し、組織の評判を落とすために変更されました。安全対策として、組織には元のファイルの MD5 ハッシュが含まれていました。流出したファイルは整合性を調べるために保存される。 Sensitiveinfo.txt」という名前のファイルは、OriginalFileHash.txt とともに、攻撃者マシン 1 のドキュメント内の Hash という名前のフォルダーに保存されています。元のファイルのハッシュ値と漏洩したファイルを比較し、「はい」または「いいえ」を選択してファイルが変更されているかどうかを示します。
A. はい
B. いいえ
Answer: A (メーッセージを残す**)**

最新問題: **21**

あなたは、クライアント xyz の従業員のユーザー認識をテストするペネトレーション テスターです。あなたは、いくつかの公的ソースから 2 人の従業員の電子メールを収集し、それを電子メールで従業員に送信するためのクライアント側のバックドアを作成しています。あなたはサイバーキルチェーンのどの段階にいますか?

A. 偵察
B. 武器化
C. 搾取
D. コマンドアンドコントロール
Answer: B (メーッセージを残す**)**