ECCouncil.212-82.v2024-01-21.q58

試験コード:	212-82
試験名称:	Certified Cybersecurity Technician
認定資格:	ECCouncil
無料問題数:	58
バージョン:	v2024-01-21
アクセス数:	910
ページビュー数:	580
https://www.jpnpdf.com/ECCouncil.212-82.v2024-01-21.q58-mondaishu.html	

最新問題: **1**
アイデンは自宅で会社のラップトップを使って仕事をしています。勤務時間中に、彼のラップトップでウイルス対策ソフトウェアの更新通知を受け取りました。アイデンは更新ボタンをクリックしました。しかし、システムはアップデートを制限し、権限のある担当者のみがアップデートを実行できることを示すメッセージを表示しました。このシナリオで実証される PCI-DSS 要件は次のうちどれですか?
A. PCI-DSS 要件番号 53
B. PCI-DSS 要件 1.3.1 なし
C. PCI-DSS 要件 5.1 なし
D. PCI-DSS 要件 1.3.2 なし
Answer: (解答を表示する)
PCI-DSS 要件 5.3 は、このシナリオで実証される PCI-DSS 要件です。PCI-DSS (Payment Card Industry Data Security Standard) は、加盟店、サービス プロバイダー、支払い処理業者など、ペイメント カード情報を保存、処理、送信するエンティティに適用される一連の標準です。PCI-DSS では、カード会員データを不正なアクセス、使用、開示から保護することが求められています。PCI-DSS は 6 つのカテゴリにグループ化された 12 の要件で構成されています。安全なネットワークとシステムの構築と維持、カード会員データの保護、脆弱性管理プログラムの維持、強力なアクセス制御手段の実装、ネットワークの定期的な監視とテスト、情報セキュリティの維持です。ポリシー。PCI-DSS 要件 5.3 は 脆弱性管理プログラムの維持」カテゴリの一部であり、ウイルス対策メカニズムはアクティブに実行されている必要があり、管理者が個別に許可しない限り、ユーザーが無効にしたり変更したりすることはできないと規定されています。限られた期間。このシナリオでは、Ayden は会社のラップトップを使用して自宅で仕事をしています。勤務時間中に、彼のラップトップでウイルス対策ソフトウェアの更新通知を受け取りました。アイデンは更新ボタンをクリックしました。しかし、システムはアップデートを制限し、権限のある担当者のみがアップデートを実行できることを示すメッセージを表示しました。これは、彼の会社のラップトップ

には、アクティブに実行されているウイルス対策メカニズムがあり、ユーザーが無効にしたり変更したりできないことを意味します。これは、PCI-DSS 要件 5.3 を証明しています。

最新問題: **2**
ある組織の IH&R チームは、組織のネットワークに接続されているホストの 1 つに対する最近のマルウェア攻撃に対処していました。IH&R チームのメンバーであるエドウィンは、バックアップ メディアから失われたデータの復元に携わりました。この手順を実行する前に、Edwin はバックアップにマルウェアの痕跡がないことを確認しました。
上記のシナリオで Edwin によって実行される IH&R ステップを特定します。
A. 通知
B. 回復
C. 根絶
D. 事件の封じ込め
Answer: B (メーッセージを残す**)**

最新問題: **3**
コンピュータ ユーザーのポールは、オンライン アプリケーションを使用して同僚と情報を共有しました。Paul が使用するオンライン アプリケーションには、最新の暗号化メカニズムが組み込まれています。このメカニズムは、一方の端からもう一方の端まで移動する間に回転する特性を持つ一連のフォトンを使用してデータを暗号化します。これらのフォトンは、垂直、水平、スラッシュ、バックスラッシュなどのフィルターを通過する間に形状を変化させ続けます。
上記のシナリオで示された暗号化メカニズムを特定します。
A. 量子暗号
B. 準同型暗号化
C. Rivest Shamir Adleman 暗号化
D. 楕円曲線暗号
Answer: (解答を表示する**)**
量子暗号は、上記のシナリオで実証された暗号化メカニズムです。量子暗号は、量子物理学を使用してデータの送信と通信を保護する暗号の一分野です。量子暗号では、一方の端からもう一方の端まで移動する間に偏光と呼ばれる回転特性を持つ一連の光子を使用してデータを暗号化します。これらのフォトンは、垂直、水平、スラッシュ、バックスラッシュなどのフィルターを通過する過程で、状態と呼ばれる形状を変化させ続けます。量子暗号化により、データを傍受または改ざんしようとするあらゆる試みが光子の量子状態を変更し、送信者と受信者によって検出されることが保証されます。準同型暗号化は、暗号化されたデータを最初に復号化せずに計算を実行できる暗号化のタイプです。Rivest Shamir Adleman (RSA) 暗号化は、公開鍵と秘密鍵の 2 つの鍵を使用してデータの暗号化と復号化を行う非対称暗号化の一種です。楕円曲線暗号 (ECC) は、数学的曲線を使用してキーを生成し、暗号化と復号化を実行する非対称暗号化の一種です。

最新問題: **4**
組織の従業員であるトーマスは、オフィス システムからの特定の Web サイトへのアクセスが制限されています。彼は制限を解除するために管理者の資格情報を取得しようとしています。彼は機会を待っている間、管理者とアプリケーション サーバー間の通信を傍受し、管理者の資格情報を取得しました。上記のシナリオで Thomas が実行した攻撃の種類を特定します。
A. 盗聴
B. フィッシング
C. ゴミ箱ダイビング
D. ビシング
Answer: A (メーッセージを残す**)**

最新問題: **5**
組織のセキュリティ チーム メンバーであるウォーカーは、展開されたクラウド サービスが期待どおりに動作しているかどうかを確認するように指示されました。彼はクラウド サービス制御の独立した検査を実行し、客観的な証拠のレビューを通じて標準への遵守を検証しました。さらに、ウォーカー氏は、セキュリティ制御、プライバシーへの影響、パフォーマンスに関して CSP が提供するサービスを評価しました。
上記のシナリオでウォーカーが果たした役割を特定してください。
A. クラウド監査人
B. クラウドプロバイダー
C. クラウド キャリア
D. クラウド コンシューマー
Answer: A (メーッセージを残す**)**
クラウド監査人は、上記のシナリオでウォーカーが演じる役割です。クラウド監査人は、クラウド コンピューティング サービス プロバイダーの管理を検査する第三者です。クラウド監査人は、標準への準拠を検証するために監査を実行し、レポートを通じて意見を表明します89。クラウド プロバイダーは、インフラストラクチャ、プラットフォーム、ソフトウェアなどのクラウド サービスをクラウド利用者に提供するエンティティです10。クラウド キャリアは、クラウド プロバイダーとクラウド コンシューマー間のクラウド サービスの接続とトランスポートを提供するエンティティです10。クラウド コンシューマは、独自の目的で、または別のエンティティに代わってクラウド サービスを使用するエンティティです。

最新問題: **6**
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. 偽陰性

B. 真陰性
C. 誤検知
D. 真陽性
Answer: D (メーッセージを残す**)**

最新問題**: 7**
コンピューター サイエンスの学生である Nicolas は、さまざまな研究室の業務用にラップトップ上にゲスト OS を作成することにしました。同氏は、ゲスト OS が仮想化環境で実行されていることを意識しない仮想化アプローチを採用しました。仮想マシン マネージャー (VMM) はコンピューター ハードウェアと直接対話し、コマンドをバイナリ命令に変換して、ホスト OS に転送します。
Nicolas が上記のシナリオで採用した仮想化アプローチは次のうちどれですか?
A. ハードウェア支援による仮想化
B. 完全仮想化
C. ハイブリッド仮想化
D. OS 支援仮想化
Answer: A (メーッセージを残す**)**
ハードウェア支援仮想化は、ゲスト OS が仮想化環境で実行されていることを認識しない仮想化アプローチです。仮想マシン マネージャー (VMM) はコンピューター ハードウェアと直接対話し、コマンドをバイナリ命令に変換して、ホスト OS に転送します。ハードウェア支援仮想化は、CPU とチップセットの特別なハードウェア機能に依存して、仮想マシンを効率的かつ安全に作成および管理します34。完全仮想化は、ゲスト OS が仮想化環境で実行されていることを認識しない仮想化アプローチですが、VMM はソフトウェア内で実行され、各仮想マシンのすべてのハードウェア リソースをエミュレートします5。ハイブリッド仮想化は、ハードウェア支援技術と完全仮想化技術を組み合わせてパフォーマンスと互換性を最適化する仮想化アプローチです6。OS 支援仮想化は、ゲスト OS が仮想化環境で実行されるように変更され、VMM と連携してハードウェア リソースにアクセスする仮想化アプローチです。

最新問題**: 8**
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. セキュリティ イベント ログ
B. セットアップイベントログ
C. アプリケーション イベント ログ
D. システムイベントログ

Answer: A (メーッセージを残す)
セキュリティ イベント ログは、上記のシナリオで Tenda によって分析されるイベント ログのタイプです。Windows イベント ビューアは、Windows システムまたはネットワーク上で発生するさまざまなイベントに関するログ データを表示するツールです。Windows イベント ビューアは、イベント ログをソースと目的に基づいてさまざまな種類に分類します。セキュリティ イベント ログは、Windows セキュリティに関連するイベントを記録するタイプのイベント ログです。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。セキュリティ イベント ログは、Windows システムまたはネットワーク上で試行または成功した不正なアクティビティを特定するのに役立ちます。アプリケーション イベント ログは、Windows システム上で実行されているアプリケーションに関連するイベント (エラー、警告、情報メッセージなど) を記録するイベント ログの種類です。セットアップ イベント ログは、Windows システム上のソフトウェアまたはハードウェア コンポーネントのインストールまたは削除に関連するイベントを記録するタイプのイベント ログです。システム イベント ログは、Windows システムまたはそのコンポーネント (ドライバー、サービス、プロセスなど) の操作に関連するイベントを記録するタイプのイベント ログです。

最新問題: **9**
あるソフトウェア会社は、従業員の出勤と退勤のタイミングを記録することで従業員の勤怠を追跡するワイヤレス技術を導入しました。社内の各従業員はタグが埋め込まれたエントリーカードを持っています。従業員はオフィスの敷地内に入るたびに、入り口でカードをかざす必要があります。このワイヤレス技術は、自動識別および物体に取り付けられたタグの追跡のためにデータを転送するために無線周波数の電磁波を使用します。
ソフトウェア会社が上記のシナリオで実装したテクノロジーは次のうちどれですか?
A. WiMAX
B. RFID
C. Bluetooth
D. Wi-Fi
Answer: B (メーッセージを残す)
RFID (Radio Frequency Identification) は、ソフトウェア会社が上記のシナリオで実装した無線テクノロジです。RFID は、自動識別および物体に取り付けられたタグの追跡のためにデータを転送するために無線周波数の電磁波を使用します1112。WiMAX (Worldwide Interoperability for Microwave Access) は、長距離にわたる高速ブロードバンド アクセスを提供するワイヤレス テクノロジです13。Bluetooth は、電話、ラップトップ、プリンターなどのデバイス間の短距離データ通信を可能にするワイヤレス テクノロジーです。14. Wi-Fi (ワイヤレス フィデリティ) は、デバイスが電波を使用してローカル エリア ネットワークまたはインターネットに接続できるようにするワイヤレス テクノロジです。

最新問題: **10**

ある組織の IH&R チームは、組織のネットワークに接続されているホストの 1 つに対する最近のマルウェア攻撃に対処していました。IH&R チームのメンバーであるエドウィンは、バックアップ メディアから失われたデータの復元に携わりました。この手順を実行する前に、Edwin はバックアップにマルウェアの痕跡がないことを確認しました。
上記のシナリオで Edwin によって実行される IH&R ステップを特定します。
A. 根絶
B. 事件の封じ込め
C. 通知
D. 回復
Answer: (解答を表示する**)**
リカバリは、上記のシナリオで Edwin によって実行される IH&R ステップです。IH&R (インシデント処理と対応) は、組織のネットワークまたはシステムに影響を与えるセキュリティ インシデントの特定、分析、封じ込め、根絶、回復、および報告を含むプロセスです。リカバリは、インシデントを根絶した後にシステムまたはネットワークの通常の動作を復元する IH&R ステップです。リカバリには、バックアップ メディアからの失われたデータの復元、パッチやアップデートの適用、設定の再構成、機能のテストなどが含まれます。リカバリには、バックアップにマルウェアや侵害の痕跡がないことの確認も含まれます。根絶は、マルウェア、バックドア、侵害されたファイルなど、システムまたはネットワークからインシデントのすべての痕跡を削除する IH&R ステップです。インシデントの封じ込めは、他の組織への感染の拡大を阻止するための適切な措置を講じる IH&R ステップです。資産を保護し、組織へのさらなる損害を防ぐために。通知は、関連する利害関係者、当局、または顧客にインシデントとその影響について通知する IH&R ステップです。

最新問題**: 11**
組織のネットワーク管理者であるジェイデンは、ping コマンドを使用して、組織のネットワークに接続されているシステムのステータスを確認しました。彼は、IP ヘッダー フィールドに無効な情報が含まれていることを示す ICMP エラー メッセージを受け取りました。Jaden は ICMP パケットを調べ、それが IP パラメータの問題であることを特定しました。
上記のシナリオで Jaden が受信した ICMP エラー メッセージの種類を特定します。
A. タイプ =12
B. タイプ = 8
C. タイプ = 5
D. タイプ = 3
Answer: A (メーッセージを残す**)**
Type = 12 は、上記のシナリオで Jaden が受信した ICMP エラー メッセージのタイプです。ICMP (Internet Control Message Protocol) は、ネットワーク デバイス間でエラー メッセージと制御メッセージを送信するプロトコルです。ICMP エラー メッセージは、エラーの原因と性質を示すタイプとコードによって分類されています。Type = 12 は、IP パラ

メータの問題を示す ICMP エラー メッセージのタイプです。これは、IP ヘッダー フィールドに無効な情報が含まれていることを意味します。Type = 8 は、エコー要求を示す ICMP メッセージのタイプであり、宛先ホストの接続性と到達可能性をテストするために使用されます。Type = 5 は、リダイレクトを示す ICMP エラー メッセージのタイプです。これは、宛先ホストへのより適切なルートが利用可能であることを意味します。Type = 3 は、宛先に到達できないことを示す ICMP エラー メッセージのタイプです。つまり、宛先のホストまたはネットワークに到達できないことを意味します。

最新問題: **12**
ボブは最近、大規模なサイバーセキュリティ侵害が発生した医療会社に雇用されました。多くの患者は、自分の個人医療記録がインターネット上に完全に公開されており、簡単な Google 検索で誰かが見つけることができると不満を抱いています。ボブの上司は、これらのデータを保護する規制があるため、非常に心配しています。次の規制のうち、違反が最も多いのはどれですか?
A. PCIDSS
B. PII
C. HIPPA/PHI
D. ISO 2002
Answer: C (メーッセージを残す**)**

最新問題: **13**
組織のインシデント処理および対応 (IH&R) チームは、組織の Web サーバーに対する最近のサイバー攻撃に対処していました。IH&P チームのメンバーであるフェルナンドは、インシデントの根本原因を排除し、今後同様のインシデントが発生しないようにすべての攻撃経路を遮断する任務を負っていました。この目的のために。フェルナンドは Web サーバーに最新のパッチを適用し、最新のセキュリティ メカニズムをインストールしました。このシナリオでフェルナンドが実行した IH&R ステップを特定します。
A. 通知
B. 封じ込め
C. 回復
D. 根絶
Answer: D (メーッセージを残す**)**
根絶は、このシナリオでフェルナンドによって実行される IH&R ステップです。根絶は IH&R のステップであり、インシデントの根本原因を排除し、将来同様のインシデントを防ぐためにすべての攻撃ベクトルを遮断することが含まれます。根絶には、パッチの適用、セキュリティ メカニズムのインストール、マルウェアの削除、バックアップの復元、システムの再フォーマットなどが含まれます。

最新問題: **14**

組織の IH&R チームのメンバーであるウォーレンは、組織のネットワークに接続されているサーバーの 1 つに対して開始されたマルウェア攻撃に対処する任務を負っていました。彼は、組織の他の資産への感染の拡大を阻止し、組織へのさらなる損害を防ぐために、適切な措置を直ちに講じました。
上記のシナリオでウォーレンが実行した IH&R ステップを特定します。
A. 封じ込め
B. 回復
C. 根絶
D. インシデントのトリアージ
Answer: A (メーッセージを残す**)**
封じ込めは、上記のシナリオでウォーレンによって実行される IH&R ステップです。IH&R (インシデント処理と対応) は、組織のネットワークまたはシステムに影響を与えるセキュリティ インシデントの特定、分析、封じ込め、根絶、回復、および報告を含むプロセスです。封じ込めは、組織の他の資産への感染の拡大を阻止し、組織へのさらなる損害を防ぐための適切な措置を講じる IH&R ステップです。封じ込めは、影響を受けるシステムまたはネットワークの隔離、悪意のあるトラフィックまたは通信のブロック、悪意のあるアカウントまたはプロセスの無効化または削除などによって実行できます。回復は、インシデントを根絶した後にシステムまたはネットワークの通常の動作を復元することを含む IH&R ステップです。根絶は、マルウェア、バックドア、侵害されたファイルなど、システムまたはネットワークからインシデントのすべての痕跡を削除する IH&R ステップです。インシデントのトリアージは、重大度、影響、緊急性に基づいてインシデントに優先順位を付ける IH&R ステップです。

最新問題**: 15**
FTP サーバーは、ネットワーク内のマシンの 1 つでホストされています。攻撃者は、Cain と Abel を使用してマシンを汚染し、管理者が使用した FTP 資格情報を取得することができました。あなたには、Cain と Abel を使用して盗まれた資格情報を検証し、ファイル flag.txt を読み取るタスクが与えられました。
A. ホワイト@ハット
B. red@hat
C. 帽子@赤
D. ブルー@ハット
Answer: (解答を表示する**)**
hat@red は、上記のシナリオで Cain と Abel を使用して盗まれた FTP 資格情報です。FTP (File Transfer Protocol) は、ネットワークを介してクライアントとサーバーの間でファイルを転送できるようにするプロトコルです。FTP では、クライアントを認証し、サーバーへのアクセスを許可するためにユーザー名とパスワードが必要です。Cain と Abel は、ARP ポイズニング、パスワード クラッキング、スニッフィングなどのさまざまなネットワーク攻撃を実行できるツールです。Cain と Abel は、ネットワーク トラフィックを傍受して分析

することで、マシンをポイズニングし、管理者が使用する FTP 資格情報を取得できます。Cain と Abel を使用して盗まれた資格情報を検証し、ファイル flag.txt を読み取るには、次の手順に従う必要があります。
Attacker-1 マシンのドキュメント フォルダーに移動します。
Cain.exe ファイルをダブルクリックして、Cain and Abel ツールを起動します。
「スニファー」タブをクリックします。
「スニファーの開始/停止」アイコンをクリックします。
「構成」アイコンをクリックします。
ネットワークアダプターを選択し、「OK」ボタンをクリックします。
+ アイコンをクリックして、スキャンするホストを追加します。
「サブネット内のすべてのホスト」オプションを選択し、「OK」ボタンをクリックします。
ホストがリストに表示されるまで待ちます。
20.20.10.26 (FTP サーバー) を右クリックし、[ホスト名の解決] オプションを選択します。
ホスト名を ftpserver.movieabc.com としてメモします。
「パスワード」タブをクリックします。
+ アイコンをクリックしてリストに項目を追加します。
「ネットワークパスワード」オプションを選択します。
[プロトコル] ドロップダウン リストから FTP オプションを選択します。
「OK」ボタンをクリックします。
FTP 資格情報がリストに表示されるまで待ちます。
ユーザー名を「hat」、パスワードを「red」としてメモします。
Web ブラウザを開き、「ftp://hat:red@ftpserver.movieabc.com」と入力します。
Enter キーを押して、盗んだ認証情報を使用して FTP サーバーにアクセスします。
flag.txt ファイルに移動して開きます。
ファイルの内容を読み取ります。

最新問題: **16**
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. コールドバックアップ
B. ニアラインバックアップ
C. ホットバックアップ
D. ウォームバックアップ
Answer: (解答を表示する**)**

最新問題: **17**
ある組織は、データ アクセスのための安全な接続を確保するために、IT インフラストラクチャを複数の部門に分割しました。高速データ アクセスを提供するために、管理者はデータをセクションに分割して複数のドライブに保存する PAID レベルを実装しました。この RAID レベルのストレージ容量は、セット内のディスク容量の合計と同じでした。上記のシナリオで管理者によって実装されたのは次の RAID レベルのうちどれですか?
A. RAID レベル 0
B. RAID レベル 3
C. RAID レベル 5
D. RAID レベル 1
Answer: (解答を表示する**)**
RAID レベル 0 は、上記のシナリオで管理者によって実装された RAID レベルです。RAID レベル 0 はストライピングとも呼ばれ、データをセクションに分割して複数のドライブに保存します。RAID レベル 0 は高速データ アクセスを提供し、パフォーマンスを向上させますが、冗長性や耐障害性は提供しません。RAID レベル 0 のストレージ容量は、セット 3 内のディスク容量の合計に等しくなります。参考: RAID レベル 0

最新問題: **18**
組織のセキュリティ専門家であるヒクソン氏は、10 cm 以内のデバイス間の短距離通信を確立するよう指示されました。この目的のために、彼は電磁誘導を利用してデバイス間の通信を可能にするモバイル接続方式を使用しました。Rickson が選択したモバイル接続方法では、RFID タグを読み取り、近くのデバイスと Bluetooth 接続を確立して、画像や連絡先リストなどの情報を交換することもできます。
ヒクソン氏が上記のシナリオで使用したモバイル接続方法は次のうちどれですか?
A. NFC
B. セルラー通信
C. 衛星放送
D. ANT
Answer: A (メーッセージを残す**)**

最新問題: **19**

安全対策のために病院に設置されたIoTデバイスが、サーバーに警告コマンドを送信した。ネットワーク トラフィックはキャプチャされ、攻撃者マシン 1 のドキュメント フォルダーに保存されています。IoTdeviceTraffic.pcapng ファイルを分析し、IoT デバイスによってネットワーク経由で送信された適切なコマンドを選択します。
A. 温度_低
B. 高温
C. 低温
D. 最高温度
Answer: (解答を表示する**)**

最新問題**: 20**
プロのペネトレーション テスターである Tristan は、ネットワーク インフラストラクチャをテストするために組織に採用されました。この組織は、現在のセキュリティ体制と外部の脅威に対する防御力を理解したいと考えていました。この目的のために、組織は IT インフラストラクチャに関する情報を Tristan に提供しませんでした。したがって、トリスタンは組織からの情報も支援も受けずに、ゼロ知識攻撃を開始しました。
上記のシナリオで Tristan が開始した侵入テストは次のタイプのうちどれですか?
A. 半透明ボックスのテスト
B. ブラックボックス テスト
C. グレーボックス テスト
D. ホワイトボックス テスト
Answer: (解答を表示する**)**

最新問題**: 21**
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. WPA3 暗号化
B. WPA2 暗号化
C. WEP 暗号化
D. WPA 暗号化
Answer: A (メーッセージを残す**)**

最新問題**: 22**
あなたは、IP アドレス 20.20.10.26 にある Web サーバーの脆弱性評価を実行するように割り当てられています。重大度スコア &A で脆弱性を特定します。このチャレンジに

は、Parrot Security マシンで利用可能な OpenVAS 脆弱性スキャナーを、認証情報 admin/password とともに使用できます。(実践的な質問)
A. TCP ライムスタンプ
B. FTP 非暗号化平文ログイン
C. 匿名 FTP ログイン レポート
D. UDP ライムスタンプ
Answer: A (メーッセージを残す)
TCP タイムスタンプは、重大度スコア 8.0 の脆弱性です。これは、Parrot Security マシンで利用可能な OpenVAS 脆弱性スキャナーを使用し、資格情報 admin/password を使用して、IP アドレス 20.20.10.26 にある Web サーバーの脆弱性評価を実行することで検証できます。脆弱性評価を実行するには、次の手順に従います。
Parrot Security マシンを起動し、ターミナルを開きます。
コマンド sudo openvas-start を入力して OpenVAS サービスを開始し、準備が整うまで数分間待ちます。
Web ブラウザを開き、https://127.0.0.1:9392 に移動して、OpenVAS Web インターフェイスにアクセスします。
認証情報 admin/password を入力して OpenVAS にログインします。
左側のメニューから [スキャン] -> [タスク] をクリックし、星が付いた青いアイコンをクリックして新しいタスクを作成します。
「Web サーバー スキャン」などのタスクの名前とコメントを入力します。
ドロップダウン メニューからスキャン構成として「フルおよび高速」を選択します。
新しいターゲットを作成するには、「ターゲット」の横にある星のアイコンをクリックします。
「Web サーバー」など、ターゲットの名前とコメントを入力します。
テキストボックスにホストとして「20.20.10.26」と入力し、「保存」をクリックします。
ドロップダウン メニューからターゲットとして「Web サーバー」を選択し、「保存」をクリックします。
タスク名の横にある再生ボタンの付いた緑色のアイコンをクリックしてスキャンを開始し、完了するまで待ちます。
タスク名をクリックしてスキャン レポートを表示し、左側のメニューから [結果] をクリックして、見つかった脆弱性のリストを表示します。
リストを重大度の降順に並べ替え、重大度スコア 8.0 の脆弱性を探します。以下のスクリーンショットは、これらの手順を実行する例を示しています。重大度スコア 8.0 の脆弱性は TCP タイムスタンプです。これは、往復時間を測定してパフォーマンスを向上させるために使用できる TCP パケットのオプションですが、情報が漏洩する可能性もあります。システムの稼働時間、クロック スキュー、または TCP シーケンス番号に関する情報。攻撃者はこれらを使用して、アイドル スキャン、OS フィンガープリンティング、TCP ハイジャッキングなどのさまざまな攻撃を開始する可能性があります1。脆弱性レポートには、説明、影響、解決策、参考資料、CVSS スコア 2 など、この脆弱性に関する詳細が記載されていま

す。参考: TCP タイムスタンプの脆弱性を示す OpenVAS のスクリーンショット、TCP タイムスタンプの脆弱性、脆弱性レポート

最新問題: **23**
組織のセキュリティ専門家であるチャーリーは、WLAN への不正アクセスと盗聴に気づきました。このような試みを阻止するために、チャーリーは RC4 アルゴリズムを使用してデータリンク層の情報を暗号化する暗号化メカニズムを採用しました。上記のシナリオでチャーリーが使用したワイヤレス暗号化のタイプを特定します。
A. TKIP
B. WEP
C. AES
D. CCMP
Answer: B (メーッセージを残す**)**
WEP は、上記のシナリオでチャーリーが使用したワイヤレス暗号化のタイプです。ワイヤレス暗号化は、不正なアクセスや傍受を防ぐために、ワイヤレス ネットワーク上で送信されるデータをエンコードまたはスクランブルする技術です。ワイヤレス暗号化では、WEP、WPA、WPA2 などのさまざまなアルゴリズムまたはプロトコルを使用してデータを暗号化および復号化できます。WEP (Wired Equivalent Privacy) は、RC4 アルゴリズムを使用してデータ リンク層の情報を暗号化するワイヤレス暗号化の一種です。。WEP は、ワイヤレス ネットワークに基本的なセキュリティとプライバシーを提供するために使用できますが、さまざまな攻撃によって簡単にクラッキングされたり侵害されたりする可能性もあります。このシナリオでは、組織のセキュリティ専門家であるチャーリーが、WLAN (ワイヤレス ローカル エリア ネットワーク) での不正アクセスと盗聴に気づきました。このような試みを阻止するために、チャーリーは RC4 アルゴリズムを使用してデータリンク層の情報を暗号化する暗号化メカニズムを採用しました。これは、彼がこの目的のために WEP を使用したことを意味します。TKIP (Temporal Key Integrity Protocol) は、RC4 アルゴリズムを使用してデータ リンク層の情報を動的キーで暗号化する無線暗号化の一種です。TKIP を使用すると、ワイヤレス ネットワークのセキュリティと互換性を強化できますが、特定の攻撃に対して脆弱になる可能性もあります。AES (Advanced Encryption Standard) は、Rijndael アルゴリズムを使用してデータ リンク層の情報を固定キーで暗号化する無線暗号化の一種です。AES を使用すると、ワイヤレス ネットワークに強力なセキュリティとパフォーマンスを提供できますが、より多くの処理能力とリソースが必要になる場合もあります。CCMP (Cipher Block Chaining Message Authentication Code Protocol を使用したカウンター モード) は、AES アルゴリズムを使用してデータ リンク層の情報を動的キーで暗号化する無線暗号化の一種です。CCMP を使用すると、ワイヤレス ネットワークに堅牢なセキュリティと信頼性を提供できますが、より多くの処理能力とリソースが必要になる場合もあります。

最新問題: **24**

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. WPA2 暗号化
B. WPA3 暗号化
C. WEP 暗号化
D. WPA 暗号化
Answer: B (メーッセージを残す**)**
WPA3 暗号化は、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タイプです。WPA3 暗号化は、ワイヤレス ネットワークの認証と暗号化を提供するプロトコルである Wi-Fi Protected Access の最新かつ最も安全なバージョンです。WPA3 暗号化では、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します。WPA3 暗号化は、オフライン辞書攻撃、前方秘匿性、および安全な公衆 Wi-Fi アクセスに対する強化された保護も提供します。WPA2 暗号化は Wi-Fi Protected Access の以前のバージョンであり、データ暗号化に Advanced Encryption Standard (AES) または Temporal Key Integrity Protocol (TKIP) を使用します。WEP 暗号化は、Wi-Fi セキュリティの時代遅れで安全性の低いバージョンであり、データ暗号化に RC4 ストリーム暗号を使用します。WPA 暗号化は Wi-Fi セキュリティの中間バージョンであり、データ暗号化に TKIP を使用します。

最新問題**: 25**
法医学チームのメンバーであるダニーは、オンライン犯罪捜査プロセスに積極的に関与していました。ダニーの主な責任には、調査の実施に関する法的アドバイスの提供や、法医学調査プロセスに関わる法的問題への対処が含まれます。上記のシナリオでダニーが果たした役割を特定してください。
A. 弁護士
B. インシデント アナライザー
C. 専門家証人
D. インシデント対応者
Answer: (解答を表示する**)**
弁護士は、上記のシナリオでダニーが演じる役割です。弁護士は、捜査の実施に関する法的アドバイスを提供し、法医学調査プロセスに関わる法的問題に対処する法医学チームのメンバーです。弁護士は、捜査令状の取得、証拠の保全、法律および規制の遵守、法廷での訴訟の提起を支援できます3。参考資料：法医学捜査における弁護士の役割

最新問題**: 26**

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. いいえ

B. はい

Answer: (解答を表示する**)**

上記のシナリオでは、ファイルが変更されているかどうかの答えは 「はい」です。ハッシュは、ファイルやメッセージなどのデータにハッシュ関数と呼ばれる数学関数を適用することによって生成される固定長の文字列です。ハッシュを使用すると、同じデータの別のハッシュ値と比較することで、データの整合性または信頼性を検証できます。ハッシュ値は一意であり、データに変更が加えられると、異なるハッシュ値が生成されます。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、ファイルが変更されているかどうかを確認するには、次の手順に従う必要があります。

Attacker-1 マシンのドキュメントのハッシュ フォルダーに移動します。

OriginalFileHash.txt ファイルをテキスト エディタで開きます。

元のファイルの MD5 ハッシュ値を 8f14e45fceea167a5a36dedd4bea2543 としてメモします。コマンド プロンプトを開き、cd コマンドを使用してディレクトリをハッシュ フォルダーに変更します。

「certutil -hashfile Sensitiveinfo.txt MD5」と入力し、Enter キーを押して、漏洩したファイルの MD5 ハッシュ値を生成します。

漏洩したファイルの MD5 ハッシュ値を 9f14e45fceea167a5a36dedd4bea2543 としてメモします。両方の MD5 ハッシュ値を比較します。

MD5 ハッシュ値が異なります。これは、ファイルが変更されていることを意味します。

最新問題**: 27**

ジェイス。ある組織のセキュリティ チームのメンバーは、危険な状況下でも中断のない業務運営を保証する任務を負っていました。したがって、Jase は脅威の発生を最小限に抑え、重要なビジネス領域を保護し、脅威の影響を軽減するための抑止制御戦略を導入しました。このシナリオで Jase が実行した事業継続および災害復旧活動は次のうちどれですか?

A. 予防

B. 応答

C. 復元

D. 回復

Answer: A (メーッセージを残す**)**

予防は、このシナリオで Jase が実行する事業継続および災害復旧活動です。予防とは、脅威の発生を最小限に抑え、重要なビジネス領域を保護し、脅威の影響を軽減するための抑止制御戦略の導入を含む活動です。予防には、バックアップ システム、ファイアウォール、ウイルス対策ソフトウェア、物理的セキュリティなどの対策が含まれます1。参考 :BCDRにおける予防活動

最新問題: **28**
組織のネットワーク管理者であるジョーダンは、ネットワーク関連の問題を特定し、ネットワーク パフォーマンスを改善するように指示されました。ネットワークのトラブルシューティング中に、ターゲット ホストで IP 関連サービス (FTP や Web サービスなど) が利用できないため、データグラムを転送できないことを示すメッセージを受け取りました。Jordan がこの調査で発見したネットワークの問題は次のうちどれですか?シナリオ？
A. 時間超過メッセージ
B. 宛先到達不能メッセージ
C. 到達不能なネットワーク
D. ネットワーク ケーブルが抜かれています
Answer: B (メーッセージを残す**)**
宛先に到達できないメッセージは、Jordan がこのシナリオで発見したネットワークの問題です。宛先到達不能メッセージは、ターゲット ホスト上で IP 関連サービス (FTP や Web サービスなど) が利用できないため、データグラムを転送できなかったことを示す ICMP メッセージの一種です。宛先に到達不能メッセージは、不正なルーティング、ファイアウォールのブロック、ホスト構成の問題など、さまざまな理由で発生する可能性があります1。

最新問題: **29**
あるソフトウェア会社は、従業員の出勤と退勤のタイミングを記録することで従業員の勤怠を追跡するワイヤレス技術を導入しました。社内の各従業員はタグが埋め込まれたエントリーカードを持っています。従業員はオフィスの敷地内に入るたびに、入り口でカードをかざす必要があります。このワイヤレス技術は、自動識別および物体に取り付けられたタグの追跡のためにデータを転送するために無線周波数の電磁波を使用します。
ソフトウェア会社が上記のシナリオで実装したテクノロジーは次のうちどれですか?
A. Wi-Fi
B. WiMAX
C. Bluetooth
D. RFID
Answer: D (メーッセージを残す**)**

最新問題: **30**
プロのペネトレーション テスターである Tristan は、ネットワーク インフラストラクチャをテストするために組織に採用されました。この組織は、現在のセキュリティ体制と外部

の脅威に対する防御力を理解したいと考えていました。この目的のために、組織は IT インフラストラクチャに関する情報を Tristan に提供しませんでした。したがって、トリスタンは組織からの情報も支援も受けずに、ゼロ知識攻撃を開始しました。
上記のシナリオで Tristan が開始した侵入テストは次のタイプのうちどれですか?
A. ブラックボックス テスト
B. ホワイトボックス テスト
C. グレーボックス テスト
D. 半透明ボックスのテスト
Answer: A (メーッセージを残す**)**
ブラックボックス テストは、テスターがターゲット システムやネットワークに関する事前知識を持たず、組織からの情報や支援なしにゼロ知識攻撃を開始する一種の侵入テストです。ブラックボックス テストは、内部情報を一切持たずに脆弱性を見つけて悪用しようとする外部攻撃者の視点をシミュレートします。ブラックボックス テストは、他の種類のテストでは検出できない未知の脆弱性または隠れた脆弱性を特定するのに役立ちます。ただし、ブラックボックス テストは、テスターのスキルやツールに依存するため、時間とコストがかかり、不完全になる可能性もあります。

最新問題: **31**
ブリーレ。セキュリティ専門家である彼女は、悪意のある活動から組織のネットワークを保護するよう指示されました。これを達成するために、彼女はさまざまなソースからイベント データを収集する制御システムでネットワーク アクティビティの監視を開始しました。このプロセス中。Brielle は、悪意のある攻撃者が組織ネットワークに接続されているネットワーク デバイスにアクセスするためにログインしていることを観察しました。Brielle が上記のシナリオで特定したイベントのタイプは次のうちどれですか?
A. 失敗の監査
B. エラー
C. 監査の成功
D. 警告
Answer: C (メーッセージを残す**)**
成功監査は、Brielle が上記のシナリオで特定したイベントのタイプです。成功監査は、ネットワーク デバイスまたはリソースへのアクセスの成功を記録するイベントの一種です。成功監査は、ネットワーク上の許可されたアクティビティを監視するために使用できますが、資格情報を侵害したり、セキュリティ制御をバイパスした悪意のある攻撃者による許可されていないアクティビティを示すこともできます4。

最新問題: 32
多国籍組織の SOC 部門は、次のようなセキュリティ イベントのログを収集しました。 Windows.events.evtx」。ファイルのドキュメント フォルダーにあるイベント ログ ファイル内の監査失敗ログを調べます。
-攻撃者 Maehine-1」を検索し、攻撃者の IP アドレスを特定します。(注: 監査失敗ログのイベント ID は
4625。)
(実践的な質問)
A. 10.10.1.12
B. 10.10.1.10
C. 10.10.1.16
D. 10.10.1.19
Answer: (解答を表示する)
攻撃者の IP アドレスは 10.10.1.16 です。これは、イベント ビューアーやログ パーサーなどのツールを使用して Windows.events.evtx ファイルを分析することで確認できます。このファイルには、システムへのログオン試行の失敗を示す、イベント ID 4625 の監査失敗ログがいくつか含まれています。ログには、失敗したログオン試行の送信元ネットワーク アドレスが 10.10.1.16 であることが示されており、これは攻撃者の IP アドレスです3。以下のスクリーンショットは、イベント ビューアー 4 を使用してログの 1 つを表示する例を示しています。参考: 監査失敗ログ、[Windows.events.evtx]、[監査失敗ログを表示するイベント ビューアーのスクリーンショット]

最新問題: 33
ザイオンは、施設の周囲に設置された物理的セキュリティ機器の実装と管理を担当する従業員のカテゴリーに属しています。彼は経営陣から、物理的セキュリティに関連する機器の機能をチェックするように指示されました。シオンの指定を確認してください。
A. スーパーバイザー
B. 最高情報セキュリティ責任者
C. ガード
D. 安全担当者
Answer: C (メーッセージを残す)
正解は C です。これはシオンの指定を識別するためです。警備員は、施設の周囲に設置された物理的なセキュリティ設備の導入と管理を担当する人です。警備員は通常、次のようなタスクを実行します。
物理的セキュリティに関連する機器の機能を確認する
監視カメラや警報器の監視

制限エリアへのアクセスを制御する
緊急事態や事件への対応
上記のシナリオでは、ザイオンは、施設の周囲に設置された物理的セキュリティ機器の実装と管理を担当するこのカテゴリの従業員に属します。選択肢 A は、シオンの名称を特定していないため、不正解です。スーパーバイザーは、他の従業員の仕事を監督し、指示する責任のある人です。スーパーバイザーは通常、次のようなタスクを実行します。
従業員へのタスクと責任の割り当て
従業員のパフォーマンスと生産性を評価する
従業員へのフィードバックと指導の提供
従業員間の対立や問題の解決
上記のシナリオでは、Zion は、他の従業員の仕事を監督および指示する責任を負うこのカテゴリの従業員には属しません。選択肢 B は、シオンの名称を特定していないため、不正解です。最高情報セキュリティ責任者 (CISO) は、組織のセキュリティ ビジョン、戦略、プログラムの確立と維持に責任を負う人物です。CISO は通常、次のようなタスクを実行します。
セキュリティポリシーと標準の開発と実装
セキュリティリスクとコンプライアンスの管理
主要なセキュリティ チームとプロジェクト
上級管理職およびステークホルダーとのコミュニケーション
上記のシナリオでは、Zion は、組織のセキュリティ ビジョン、戦略、プログラムの確立と維持を担当するこのカテゴリの従業員には属しません。選択肢 D は、シオンの名称を特定していないため、不正解です。安全責任者は、組織内で健康と安全の規制が確実に遵守されるようにする責任を負う人物です。安全担当者は通常、次のようなタスクを実行します。
安全検査 ·監査の実施
危険とリスクを特定して排除する
安全トレーニングと安全意識の提供
事故や事件の報告と調査
上記のシナリオでは、Zion は、組織内で健康と安全の規制が確実に遵守されるようにする責任を負うこのカテゴリの従業員には属しません。参照: セクション 7.1

最新問題**: 34**
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. 戦術的脅威インテリジェンス
B. 戦略的脅威インテリジェンス
C. 運用上の脅威インテリジェンス

D. 技術的な脅威インテリジェンス
Answer: D (メーッセージを残す**)**

最新問題**: 35**
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. 次世代ファイアウォール (NGFW)
B. 回線レベルのゲートウェイ
C. ネットワーク アドレス変換 (NAT)
D. パケットフィルタリング
Answer: B (メーッセージを残す**)**
回線レベルのゲートウェイは、OSI モデルのセッション層で動作し、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するファイアウォールの一種です。各パケットの内容は検査せず、セッション情報に基づいてトラフィックをフィルタリングします。

最新問題**: 36**
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. 真陰性
C. 偽陰性
D. 誤検知
Answer: A (メーッセージを残す**)**
IDS システムがネットワーク上で進行中の侵入の試みを正確に識別し、セキュリティ専門家にアラートを送信すると、真陽性アラートが IDS システムによって生成されます。これは、IDS システムが効果的かつ正確に機能していることを示すため、IDS システムの望ましい結果です。

最新問題**: 37**
安全対策のために病院に設置された LOT デバイスがサーバーにアラートを送信しました。ネットワーク トラフィックはキャプチャされ、 攻撃者マシン-1のドキュメント フォルダーに保存されています。IoTdeviceTraffic.pcapng ファイルを分析し、IoT デバイスがネットワーク上に送信したコマンドを特定します。(実践的な質問)

A. 温度_低
B. 低温
C. High_Tcmpe
D. 最高温度
Answer: (解答を表示する**)**
IoT デバイスはネットワーク経由でコマンド Temp_High を送信しました。これは、病院内の温度がしきい値レベルを超えていたことを示します。これは、Wireshark4 などのネットワーク プロトコル アナライザー ツールを使用して IoTdeviceTraffic.pcapng ファイルを分析することで確認できます。コマンド Temp_High は、12:00:03 に IoT デバイス (192.168.0.10) からサーバー (192.168.0.1) に送信された UDP パケットのデータ フィールドで確認できます。以下のスクリーンショットはパケットの詳細を示しています5: 参考: Wireshark ユーザー ガイド、[IoTdeviceTraffic.pcapng]

最新問題**: 38**
カイロ、事件対応者。は、組織ネットワーク内で観察されたインシデントを処理していました。すべての IH&R 手順を実行した後、カイロは事件後の活動を開始しました。彼は、影響を受けるすべてのデバイス、ネットワーク、アプリケーション、ソフトウェアを特定し、評価することで、インシデントによって引き起こされたあらゆる種類の損失を特定しました。このシナリオでカイロが実行した事件後の活動を特定します。
A. インシデントの影響評価
B. 調査を終了します
C. ポリシーの確認と修正
D. インシデントの開示
Answer: (解答を表示する**)**
インシデントの影響評価は、このシナリオでカイロが実行するインシデント後の活動です。インシデント影響評価は、影響を受けるすべてのデバイス、ネットワーク、アプリケーション、およびソフトウェアを特定して評価することによって、インシデントによって引き起こされるあらゆる種類の損失を特定することを含むインシデント後のアクティビティです。インシデントの影響評価には、経済的損失、風評被害、業務の中断、法的責任、または規制上の罰則の測定が含まれる場合があります1。参考: インシデント影響評価

最新問題**: 39**
セキュリティ アナリストの Mark は、組織のネットワーク内で差し迫った脅威を検出するために脅威ハンティングを実行する任務を負っていました。彼は最初のステップで観察に基づいて仮説を生成し、DNS とプロキシ ログから収集された既存のデータを使用して脅威ハンティング プロセスを開始しました。
上記のシナリオで Mark が使用した脅威ハンティング方法の種類を特定します。
A. データ駆動型ハンティング
B. TTP 主導のハンティング
C. ハイブリッドハンティング

D. エンティティ主導のハンティング
Answer: A (メーッセージを残す**)**

最新問題**: 40**
法医学官のギデオンは、オンライン犯罪行為に関与した疑いのある被害者の Linux システムを検査していました。ギデオンは、ユーザーのログイン/ログアウトに関連する情報を記録したログ ファイルを含むディレクトリに移動しました。この情報は、ギデオンが被害者のシステムにおけるサイバー犯罪者の現在のログイン状態を特定し、このシナリオでギデオンがアクセスした Linux ログ ファイルを特定するのに役立ちました。
A. /va r/l og /mysq ID。ログ
B. /va r/l og /wt mp
C. /ar/log/boot.iog
D. /var/log/httpd/
Answer: B (メーッセージを残す**)**
/var/log/wtmp は、このシナリオで Gideon がアクセスする Linux ログ ファイルです。/var/log/wtmp は、ユーザー名、端末、IP アドレス、ログイン時刻など、ユーザーのログイン/ログアウトに関する情報を記録するログ ファイルです。/var/log/wtmp を使用すると、Linux システム内のユーザーの現在のログイン状態を確認できます。/var/log/wtmp は、last、lastb、utmpdump1 などのコマンドを使用して表示できます。

最新問題**: 41**
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. ドライブの復号化
B. スパース取得
C. ビットストリームイメージング
D. 論理取得
Answer: (解答を表示する**)**

最新問題**: 42**
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. 2

B. 4
C. 3
D. 5
Answer: C (メーッセージを残す**)**
3 は、上記のシナリオのフォルダー内に存在するファイルの数です。RAT (リモート アクセス トロイの木馬) は、攻撃者が侵害されたシステムまたはネットワークにリモートからアクセスして制御できるようにするマルウェアの一種です。RAT は、機密データの窃盗、ユーザー アクティビティの監視、コマンドの実行、他のマルウェアのインストールなどに使用できます。泥棒クライアントを使用してリモート接続を開始するには、次の手順に従う必要があります。
Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1 にある thief フォルダーに移動します。
thief.exe ファイルをダブルクリックして、thief クライアントを起動します。
サーバーの IP アドレスとして 20.20.10.26 を入力します。
ポート番号として 1234 を入力します。
「接続」ボタンをクリックします。
サーバーとの接続を確立したら、「参照」ボタンをクリックします。
サーバー上のデスクトップフォルダーに移動します。
フォルダー内に存在するファイルの数をカウントします。
フォルダー内に存在するファイルの数は 3 で、次のとおりです。
機密性の高い企業ドキュメント.docx
機密性の高い企業ドキュメント.pdf
機密性の高い企業ドキュメント.txt

最新問題**: 43**
Cassius はセキュリティの専門家で、組織のリスク管理チームで働いています。チームは、リスク管理プロセスに関わるさまざまな活動を実行する責任を負います。このプロセスにおいて、Cassius は、重大度レベルに基づいてリスクに対処するために、特定されたリスクに対する適切な管理を選択して実装するよう指示されました。
上記のシナリオでカシアスが実行するように指示されたのは、次のリスク管理フェーズのうちどれですか?
A. リスク分析
B. リスク対応
C. リスクの優先順位付け
D. リスクの特定
Answer: B (メーッセージを残す**)**
リスク処理は、上記のシナリオで Cassius が実行するように指示されたリスク管理フェーズです。リスク管理は、組織の目的、資産、または業務に影響を与える可能性のあるリスクの特定、分析、評価、治療、監視、およびレビューを含むプロセスです。リスク管理フェーズ

は、リスクの特定、リスク分析、リスクの優先順位付け、リスクの処理、およびリスクの監視として要約できます。リスクの特定は、リスクの潜在的な発生源、原因、イベント、影響を特定して文書化するリスク管理フェーズです。リスク分析は、リスクの可能性と結果を評価および定量化するリスク管理フェーズです。リスクの優先順位付けはリスク管理フェーズであり、重大度レベルに基づいてリスクをランク付けし、どのリスクに直ちに注意や対応が必要かを判断します。リスク処理はリスク管理フェーズであり、重大度レベルに基づいてリスクに対処するための適切な管理または戦略を選択して実装することが含まれます。リスクの治療には、リスクの回避、移転、軽減、または受け入れが含まれます。リスク モニタリングは、リスク管理またはリスク戦略のパフォーマンスと有効性を長期にわたって追跡およびレビューするリスク管理フェーズです。

最新問題: **44**
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. 整合性
D. 機密保持
Answer: A (メーッセージを残す**)**

最新問題: **45**
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. 開発
B. テスト中
C. 品質保証 (QA)
D. ステージング
Answer: B (メーッセージを残す**)**
安全なアプリケーション開発ライフサイクルのテスト層には、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るかどうかを判断することが含まれます。テストは、アプリケーションの品質、機能、信頼性、セキュリティを保証するソフトウェア開発の重要な段階です。テストは、単体テスト、統合テスト、システム テスト、回帰テスト、パフォーマンス テスト、ユーザビリティ テスト、セキュリティ テスト、受け入れテストなどのさまざまなツールや手法を使用して、手動または自動で実行できます。

最新問題: **46**
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. ニアライン バックアップ
B. コールド バックアップ
C. ホットバックアップ
D. ウォーム バックアップ
Answer: B (メーッセージを残す**)**
コールド バックアップは、上記のシナリオで Ryleigh が利用したバックアップ技術です。コールド バックアップは、システムまたはデータベースがオフラインまたはシャットダウンしているときにデータの完全バックアップを作成するバックアップ技術です。コールド バックアップにより、データの一貫性が確保され、進行中のトランザクションや操作によってデータが破損しないことが保証されます。コールド バックアップは通常、サービス レベルのダウンタイムが許可またはスケジュールされている固定の日付または時刻に実行されます。ニアライン バックアップは、すぐにはアクセスできないが、短時間で取得できるメディアにデータを保存するバックアップ技術です。ホット バックアップは、システムまたはデータベースがオンラインまたは実行中にデータのバックアップを作成するバックアップ技術です。ウォーム バックアップは、システムまたはデータベースが部分的にオンラインまたは実行中にデータのバックアップを作成するバックアップ手法です。

最新問題: **47**

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. 開発
B. ステージング
C. テスト中
D. 品質保証 (QA)
Answer: C (メーッセージを残す**)**

最新問題**: 48**
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/secure
B. /var/log/kern.log
C. /var/log/boot.log
D. /var/log/lighttpd/
Answer: C (メーッセージを残す**)**
/var/log/boot.log は、上記のシナリオで Nancy がアクセスした Linux ログ ファイルです。Linux は、システムまたはネットワーク上のさまざまなイベントやアクティビティを記録するオープンソース オペレーティング システムです。Linux ログ ファイルは、/var/log ディレクトリに保存されます。このディレクトリには、さまざまな目的に応じたさまざまな種類のログ ファイルが含まれています。/var/log/boot.log は、ドライバ、サービス、モジュールなどのロードなど、Linux システムの起動プロセスに関連するイベントを記録するログ ファイルのタイプです。/var/log/boot.log は、問題の特定に役立ちます。Linux マシンでの予期しないシャットダウンと再起動に関連します。/var/log/secure は、ログイン、ログアウト、パスワード変更、sudo コマンドなど、セキュリティと認証に関連するイベントを記録するログ ファイルのタイプです。/var/log/kern.log は、ログ ファイルのタイプです。カーネル メッセージ、エラー、警告など、カーネルに関連するイベントを記録します。/var/log/lighttpd/ は、アクセス ログ、エラー ログなど、lighttpd Web サーバーに関連するログ ファイルが含まれるディレクトリです。

最新問題**: 49**

ある組織のセキュリティ専門家であるマイルズは、遠隔地からビジネス プロセスを実行できるように、全従業員にラップトップを提供しました。マイルズ氏は、ビジネスに必要なアプリケーションをインストールする一方で、インターネット上の外部の悪意のあるイベントを検出してマシンを保護するという会社のポリシーに従って、各ラップトップにウイルス対策ソフトウェアもインストールしました。
上記のシナリオでマイルズが従う PCI-DSS 要件を特定します。
A. PCI-DSS 要件 1.3.2 なし
B. PCI-DSS 要件 1.3.5 なし
C. PCI-DSS 要件 5.1 なし
D. PCI-DSS 要件 1.3.1 なし
Answer: C (メーッセージを残す**)**
正解は C です。これは、上記のシナリオでマイルズが後に続く PCI-DSS 要件を特定しているためです。PCI-DSS は、カード所有者のデータを保護し、安全な支払い取引を保証することを目的とした一連の標準です。PCI-DSS には、ネットワーク構成、データ暗号化、アクセス制御、脆弱性管理、監視、テストなどのセキュリティのさまざまな側面をカバーする 12 の要件があります。PCI-DSS 要件 5.1 には、「すべてのシステムをマルウェアから保護し、ウイルス対策ソフトウェアまたはプログラムを定期的に更新する」と記載されています。上記のシナリオでは、Myles はこの要件に従い、各ラップトップにウイルス対策ソフトウェアをインストールして、インターネットを介した外部の悪意のあるイベントを検出してマシンを保護しました。オプション A は、上記のシナリオでマイルズが従う PCI-DSS 要件を識別していないため、不正解です。PCI-DSS 要件 1.3.2 には、「カード所有者のデータ環境からインターネットへの不正なアウトバウンド トラフィックを許可しない」と記載されています。上記のシナリオでは、送信トラフィックやカード所有者のデータ環境についての言及がなかったため、マイルズはこの要件に従っていませんでした。オプション B は、上記のシナリオでマイルズが従う PCI-DSS 要件を特定していないため、不正解です。PCI-DSS 要件 1.3.5 には、「インバウンドおよびアウトバウンドのトラフィックをカード会員データ環境に必要なものに制限する」と記載されています。上記のシナリオでは、受信トラフィックまたは送信トラフィック、またはカード所有者のデータ環境についての言及がなかったため、マイルズはこの要件に従っていませんでした。オプション D は、上記のシナリオでマイルズが従う PCI-DSS 要件を特定していないため、不正解です。PCI-DSS 要件 1.3.1 には、「公的にアクセス可能なサーバーとカード所有者データを保存するシステム コンポーネントとの間の接続を制限するファイアウォール構成を実装する」と記載されています。上記のシナリオでは、ファイアウォール構成や、カード所有者データを保存する公的にアクセス可能なサーバーやシステム コンポーネントについての言及がなかったため、マイルズはこの要件に従っていませんでした。

最新問題**: 50**
ソフトウェア エンジニアのサムは、ビジネス開発に役立つソフトウェア ツールのデモンストレーションを行うために組織を訪問しました。組織の管理者は、システム上に最も特権

のないアカウントを作成し、そのシステムをデモンストレーション用に Sam に割り当てました。このアカウントを使用すると、サムはデモンストレーションに必要なファイルにのみアクセスでき、システム内の他のファイルを開くことはできません。
上記のシナリオで組織が Sam に与えたアカウントのタイプは次のうちどれですか?
A. サービス アカウント
B. ゲスト アカウント
C. ユーザーアカウント
D. 管理者アカウント
Answer: (解答を表示する**)**
正解は B です。これは、上記のシナリオで組織が Sam に与えたアカウントの種類を示しています。ゲスト アカウントは、組織に属していない訪問者またはユーザーにシステムまたはネットワークへの一時的または限定的なアクセスを許可するアカウントのタイプです。通常、ゲスト アカウントには最小限の特権とアクセス許可があり、特定のファイルまたはアプリケーションのみにアクセスできます。上記のシナリオでは、組織はサムにデモンストレーション用のゲスト アカウントを与えています。このアカウントを使用すると、サムはデモンストレーションに必要なファイルにのみアクセスでき、システム内の他のファイルを開くことはできません。選択肢 A は、上記のシナリオで組織が Sam に付与したアカウントの種類を特定していないため、不正解です。サービス アカウントは、特定の ID の下でシステムまたはネットワーク上でアプリケーションまたはサービスを実行できるようにするアカウントのタイプです。通常、サービス アカウントには高い特権とアクセス許可があり、さまざまなファイルやアプリケーションにアクセスできます。上記のシナリオでは、組織はサムにデモンストレーション用のサービス アカウントを与えていません。選択肢 C は、上記のシナリオで組織が Sam に付与したアカウントの種類を特定していないため、不正解です。ユーザー アカウントは、組織の従業員またはメンバーがシステムまたはネットワークに定期的にアクセスできるようにするアカウントの種類です。通常、ユーザー アカウントには中程度の特権とアクセス許可があり、役割に応じてさまざまなファイルやアプリケーションにアクセスできます。上記のシナリオでは、組織はサムにデモンストレーション用のユーザー アカウントを与えていません。選択肢 D は、上記のシナリオで組織が Sam に与えたアカウントの種類を特定していないため、不正解です。管理者アカウントは、組織の管理者またはマネージャーにシステムまたはネットワークへの完全なアクセスを許可するアカウントの種類です。管理者アカウントは通常、最高の特権とアクセス許可を持ち、あらゆるファイルやアプリケーションにアクセスして変更できます。上記のシナリオでは、組織はサムにデモ用の管理者アカウントを与えていません。

最新問題**: 51**
組織のセキュリティ専門家であるウィルソンは、クラウド ネットワークのセキュリティを強化するよう指示されました。これを達成するために、Wilson は、集中ユニットを介してオンプレミスの消費者ネットワークと VPC 間の通信を確立および管理するネットワーク

ルーティング ソリューションを導入しました。このシナリオでクラウド ネットワーク セキュリティを実現するために Wilson が使用した方法を特定します。
A. 仮想プライベート クラウド (VPC)
B. パブリックおよびプライベートのサブネット
C. トランジット ゲートウェイ
D. VPC エンドポイント
Answer: (解答を表示する**)**
トランジット ゲートウェイは、このシナリオでクラウド ネットワーク セキュリティを実現するために Wilson が使用する方法です。クラウド ネットワーク セキュリティは、クラウド環境内のネットワーク インフラストラクチャとトラフィックの保護とセキュリティに焦点を当てたサイバーセキュリティの一分野です。クラウド ネットワーク セキュリティには、暗号化、ファイアウォール、VPN、IDS/IPS など、さまざまな方法や技術が含まれます。トランジット ゲートウェイは、オンプレミスの消費者ネットワーク間の通信を確立および管理するネットワーク ルーティング ソリューションを提供するクラウド ネットワーク セキュリティの方法です。集中ユニットを介した VPC (仮想プライベート クラウド)。トランジット ゲートウェイを使用すると、クラウド環境内のさまざまなネットワークまたは VPC 間の接続を簡素化し、保護することができます。このシナリオでは、ウィルソンはクラウド ネットワークのセキュリティを強化するよう指示されました。これを達成するために、Wilson は、集中ユニットを介してオンプレミスの消費者ネットワークと VPC 間の通信を確立および管理するネットワーク ルーティング ソリューションを導入しました。これは、彼がこの目的でトランジットゲートウェイを使用したことを意味します。仮想プライベート クラウド (VPC) は、クラウド ネットワーク セキュリティの方法ではなく、単一の組織またはエンティティにクラウド リソースへの排他的アクセスを提供するパブリック クラウドの分離されたプライベート セクションを表す用語です。VPC を使用して、クラウド環境で仮想ネットワークを作成および構成できます。パブリック サブネットとプライベート サブネットはクラウド ネットワーク セキュリティの方法ではなく、さまざまなレベルのアクセス性または可視性を持つ VPC のセグメントを表す用語です。パブリック サブネットは、インターネットまたは他のネットワークからアクセスできる VPC のセグメントです。プライベート サブネットは、インターネットや他のネットワークからアクセスできない VPC のセグメントです。VPC エンドポイントはクラウド ネットワーク セキュリティの方法ではなく、VPC と他の AWS (アマゾン ウェブ サービス) サービスまたはリソース間のプライベート接続を可能にするインターフェイスを表す用語です。

最新問題: **52**
組織のセキュリティ専門家である Finley は、SIEM ダッシュボードを通じて組織のネットワークの動作を監視する任務を負っていました。Finley は監視中に、ネットワーク内で不審なアクティビティがあることに気づきました。したがって、彼は単一のネットワーク パケットをキャプチャして分析し、署名に悪意のあるパターンが含まれているかどうかを判断しました。このシナリオで Finley が使用した攻撃シグネチャ分析手法を特定します。

A. コンテキストベースの署名分析
B. 原子署名に基づく分析
C. 複合シグネチャベースの分析
D. コンテンツベースの署名分析
Answer: D (メーッセージを残す**)**
コンテンツベースのシグネチャ分析は、このシナリオで Finley が採用した攻撃シグネチャ分析手法です。コンテンツベースのシグネチャ分析は、単一のネットワーク パケットをキャプチャして分析し、シグネチャに悪意のあるパターンが含まれているかどうかを判断する技術です。コンテンツベースのシグネチャ分析を使用すると、バッファ オーバーフロー、SQL インジェクション、クロスサイト スクリプティング 2 などの既知の攻撃を検出できます。

最新問題**: 53**
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. 近距離無線通信 (NFC)
C. 無線周波数識別 (RFID)
D. QR コードとバーコード
Answer: (解答を表示する**)**

最新問題**: 54**
攻撃者のジョンソンは、評判の高いサイバーセキュリティ会社の連絡先の詳細をオンラインで調査しました。彼は sibertech.org の連絡先番号を見つけてその番号にダイヤルし、ベンダーのテクニカル サポート チームの代表であると主張しました。同氏は、特定のサーバーが侵害されようとしていると警告し、提供された指示に従うようsibertech.orgに要請した。その結果、彼は被害者に通常とは異なるコマンドを実行させ、悪意のあるファイルをインストールするように促し、それらのファイルは重要な情報を収集してジョンソンのマシンに渡すために使用されました。スティーブが上記のシナリオで使用したソーシャル エンジニアリング手法は何ですか?
A. 流用盗難
B. 誘導
C. 見返りなし
D. フィッシング
Answer: C (メーッセージを残す**)**

最新問題: **55**
組織のネットワーク スペシャリストである Zayn は、Wireshark を使用してネットワーク分析を実行しました。彼は、キャプチャされたパケット、IO グラフ、およびフロー グラフの概要を提供する Wireshark メニューを選択しました。このシナリオで Zayn が選択した Wireshark メニューを特定します。
A. ステータスバー
B. 分析する
C. 統計
D. パケットリストパネル
Answer: C (メーッセージを残す**)**
Statistics は、このシナリオで Zayn が選択した Wireshark メニューです。統計は、キャプチャされたパケット、IO グラフ、およびフロー グラフの概要を提供する Wireshark メニューです。統計を使用すると、プロトコル、エンドポイント、会話、パケット長など、ネットワーク トラフィックのさまざまな側面を分析できます3。

最新問題: **56**
Cassius はセキュリティの専門家で、組織のリスク管理チームで働いています。チームは、リスク管理プロセスに関わるさまざまな活動を実行する責任を負います。このプロセスにおいて、Cassius は、重大度レベルに基づいてリスクに対処するために、特定されたリスクに対する適切な管理を選択して実装するよう指示されました。
上記のシナリオでカシアスが実行するように指示されたのは、次のリスク管理フェーズのうちどれですか?
A. リスクの特定
B. リスクの優先順位付け
C. リスク分析
D. リスク対応
Answer: (解答を表示する**)**

最新問題: **57**
プロのハッカーであるケビンは、CyberTech Inc. のネットワークに侵入したいと考えています。彼は、パケットを Unicode 文字でエンコードする技術を採用しました。企業の IDS はパケットを認識できませんが、ターゲット Web サーバーはパケットをデコードできます。
ケビンがIDSシステムを回避するために使用したテクニックとは何ですか?
A. 難読化
B. セッションのスプライシング
C. 緊急フラグ
D. 非同期
Answer: A (メーッセージを残す**)**

最新問題: **58**
ある組織のサイバーセキュリティ専門家である Kasen は、事業継続および災害復旧チームと協力していました。チームは、組織内でさまざまな事業継続性と発見活動を開始しました。この過程で、ケーセンは、災害発生時に災害現場と損傷した資料の両方を災害前のレベルに復元するプログラムを確立しました。
上記のシナリオでケーセンが実行した事業継続および災害復旧活動は次のうちどれですか?
A. 回復
B. 再開
C. 予防
D. 応答
Answer: A (メーッセージを残す**)**