

# Comptia PenTest+ Certification (PT0-002, Japanese Version)

1. さまざまな種類の画像ファイルのデータを隠すために使用するのに最適なツールは次のうちどれですか？

A. キスメット

B. 雪

C. レスポンダ

D. メタスプロイト

**Answer(s): B**

---

2. 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 テストに固有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。次のドキュメントのうち、侵入テスターにこのアクションの責任を負わせることができるのはどれですか？

A. SLA

B. NDA

C. ROE

D. MSA

**Answer(s): B**

---

3. 侵入テスターは、サーバーから MD5 ハッシュを収集し、レインボー テーブルを使用して簡単にハッシュを解読することができました。

A. アルゴリズム要件の強化

B. ユーザーパスワードの暗号化

C. パッチ管理プログラム

D. サーバー上のアクセス制御

**Answer(s): A**

---

4. ペネトレーション テスターが、明示的な許可なしに、内部クライアント アプリケーションで見つかった新しい脆弱性に対して CVE 番号を割り当てるよう要求しました。ペネトレーション テスターが違反した可能性が最も高いのは次のうちどれですか？

A. SLA

B. NDA

C. ROE

D. SOW

**Answer(s): C**

---

5. API で HTTP 応答をインターセプトし、その内容を変更し、元のモバイル デバイスに転送するために使用するのに最適なツールは次のどれですか？

A. Drozer

B. Burp Suite

C. Android SDK Tools

D. MobSF

**Answer(s): B**

---

6. ペネトレーションテスターが 192.168.1.112 の評価を実施しています。次の出力があるとし  
ます。

A. ポートスキャン

B. ブルートフォース

C. 資格情報のスタッフィング

D. DoS 攻撃

**Answer(s): B**

---

7. 侵入テスターは、バッファ オーバーフローの脆弱性について独自のアプリケーションをテ  
ストするために契約されました。次のツールのうち、このタスクに最も適しているのはどれで  
すか？

A. GDB

B. バーススイート

C. 検索スプリット

D. ネットキャット

**Answer(s): A**

---

8. 次の評価方法のうち、ICS 環境に害を及ぼす可能性が最も高いのはどれですか？

A. Ping スweep

B. パケット解析

C. プロトコルリバース

D. アクティブスキャン

**Answer(s): D**

---

9. ペネトレーションテスターは最終報告書に次のコメントを書いた：「テストされたシステムの85% がインターネットからの不正アクセスを受けやすいことが判明した。」このメッセージは次のどの読者を対象としていますか？

A. システム管理者

B. 経営幹部

C. データプライバシーオプズマン

D. 規制当局者

**Answer(s): B**

---

10. システムに侵入した後、ペネトレーションテスターは、次にどのようなアクションを実行するかを決定するために、より多くの情報を必要とします。テスターは次のコマンドを実行しません。

A. メタデータ サービス攻撃

B. コンテナ脱出テクニック

C. 資格情報の収集

D. リソース枯渇

**Answer(s): A**

---

11. 侵入テスト中に、認証要件のない Web コンポーネントが見つかりました。Web コンポーネントではファイルのアップロードも可能で、ターゲットのパブリック Web の 1 つでホストされています。ペネトレーション テスターは次に次のアクションを実行する必要がありますか？

A. 評価を続行し、結果を重大としてマークします。

B. 問題を一時的に修正しようとしています。

C. すぐに主連絡先に通知します。

D. 評価が完了するまで Web サーバーをシャットダウンします。

**Answer(s): C**

---

12. ペネトレーションテスターが営業時間外にテストを実施していたところ、重要なシステムがダウンしていることに気づきました。次の連絡先のうち、最初に通知する必要があるのはどれですか？

A. セカンダリ

B. 緊急事態

C. 技術的

D. プライマリ

**Answer(s): D**

---

13. 次の状況のうち、侵入テスターが緊急連絡先に通知する必要があるのはどれですか？

A. チームは、組織内の重要なサーバーを悪用します。

B. チームは、ネットワーク上のシステムで別のアクターを発見しました。

C. チームはリモートでネットワークにアクセスできなくなります。

D. チームは組織から PII またはクレジットカード データを盗み出します。

**Answer(s): B**

---

14. 侵入テストのスキャン段階の実行中に、侵入テスターは次のコマンドを実行します。

A. -su

B. -pn

C. -sn

D. -ss

**Answer(s): B**

---

15. 次の概念のうち、侵入テスト中に実行される特定の一連の手順とアプローチを定義するものはどれですか？

A. 方法論

B. 所見

C. 作業明細書

D. スコープの詳細

**Answer(s): A**

---

16. 以前のシステムへのアクセスを取得した後、ペネトレーション テスターはネットワークに対して Nmap スキャンを実行し、次の結果を得ます。

A. コマンドには -port 135 オプションが必要です。

B. テスターが間違った IP アドレスを入力しました。

C. PowerShell には管理者権限が必要です。

D. RDP のアカウントがサーバーに存在しません。

**Answer(s): D**

---

17. セキュリティ コンサルタントは、読みやすいレポートを簡単に生成できるアプリケーションを使用して脆弱性評価を実行したいと考えています。攻撃者は次のどれを使用すべきでしょう

か。

A. ブレーキマン

B. ネッサス

C. メタスプロイト

D. 最高司令官

**Answer(s): B**

---

18. Web サイトの欠陥を調査するために、ペネトレーション テスターが雇われました。テストの時間帯の 1 つで、ネットワーク エンジニアは、Web サーバーへの GET 要求が殺到し、Web サイトの応答時間が 80% 短縮されていることに気付きました。ネットワーク エンジニアは、侵入テスターに連絡して、これらの GET 要求がテストの一部であるかどうかを判断します。次のうち、ペネトレーションテスターでチェックする目的を最もよく表しているのはどれですか？

A. 状況認識

B. 再スケジュール

C. DDoS 防御

D. 対立解消

**Answer(s): D**

---

19. 侵入テスターは、Windows サーバーで次のコマンドを実行しました。

A. svaccount 権限をダウングレードします。

B. スケジュールされたバッチ ジョブを削除します。

C. テスターが作成した資格情報を削除します。

D. 逆シェル接続を閉じます。

**Answer(s): C**

---

20. 侵入テスターは、アクティブなシステムを迅速に識別するためにクラス C ネットワークを調査しています。侵入テスターは次のコマンドのどれを使用する必要がありますか？

A. nmap sn 192.168.0.1 192.168.0.1.254

B. nmap sn 192.168.0.1/16

C. nmap sN 192.168.0.0/24

D. nmap sn 192.168.0.1-254

**Answer(s): D**

---