CompTIA PenTest+ 認定資格 試験出題範囲

試験番号：**PT0-002**

CompTIA

試験について

CompTIA PenTest+認定資格試験では、以下に記載した事項に必要な知識とスキルを保持しているかを確認します：

- ペネトレーションテスト実施の計画とスコープ
- 法的要件およびコンプライアンス要件の理解
- 適切なツールとテクニックを使用して脆弱性スキャンとペネトレーションテストを実行し、その結果を分析する
- 提案された修復の手法を含むレポートを作成し、経営層に結果を効率的に伝え、実用的な推奨事項を提示する

CompTIA PenTest+は、セキュリティコンサルタントまたはペネトレーションテスターとしての3〜4年の実務経験に相当するスキルを評価します。

出題範囲に掲載された項目は、認定資格試験の目的を明確にするためのものであり、試験の出題内容を完全に網羅したものではありません。

資格の認証

CompTIA PenTest+ (PT0-002)は、国際標準化機構(ISO) 17024標準への準拠を国家規格協会(ANSI)よりに認定されており、定期的な出題範囲の見直しおよびアップデートを行っています。

試験開発

CompTIAの認定資格試験は、ITプロフェッショナルに必要とされるスキルと知識に関して検討する、専門分野のエキスパートによるワークショップ、および業界全体へのアンケートの調査結果に基づいて策定されています。

CompTIA認定教材の使用に関するポリシー

CompTIA Certifications, LLCは、無許可の第三者トレーニングサイト（通称「ブレインダンプ」）とは提携関係がなく、これらが提供するいかなるコンテンツも公認・推薦・容認しません。CompTIAの認定資格試験の受験準備にこのような教材を使用した個人は、CompTIA受験者同意書の規定に基づいて資格認定を取り消され、その後の受験資格を停止されます。CompTIAでは、無許可教材の使用に関する試験実施ポリシーをよりよく理解していただくための取り組みを進めています。認定資格試験を受験される方は、**CompTIA**認定資格試験実施ポリシーをご一読ください。CompTIAの認定資格試験を受験するための学習を始める前には、必ずCompTIAが定めるすべてのポリシーをご確認ください。受験者には、**CompTIA**受験者同意書の規定を遵守することが求められています。個々の教材が無許可扱いになるかどうかを確認するには、CompTIA (**examsecurity@comptia.org**)までメールにてご確認ください。

注意事項

箇条書きで挙げられた項目は、すべての試験内容を網羅するものではありません。この出題範囲に掲載がない場合でも、各分野に関連する技術、プロセス、あるいはタスクを含む問題が出題される可能性があります。CompTIAでは、提供している認定資格試験の内容に現在必要とされているスキルを反映するため、また試験問題の信頼性維持のため、継続的な試験内容の検討と問題の改訂を行っています。必要な場合、現在の出題範囲を基に試験を改訂する場合があります。この場合、現在の試験に関連する資料・教材等は、継続的にご利用いただくことが可能です。

試験情報

試験	PT0-002
問題数	最大85問
出題形式	単一/複数選択、パフォーマンスベーステスト
試験時間	165分
推奨経験	ペネトレーションテスト、脆弱性の評価、コード分析での3〜4年の実務経験
合格スコア	750（100-900のスコア形式）

試験の出題範囲（試験分野）

下表は、この試験における試験分野（ドメイン）と出題比率の一覧です。

試験分野	出題比率
1.0 計画とスコープ	14%
2.0 情報収集と脆弱性のスキャン	22%
3.0 攻撃とエクスプロイト	30%
4.0 報告とコミュニケーション	18%
5.0 ツールとコード分析	16%
計	**100%**

1.0 計画とスコープ

1.1 ガバナンス、リスク、コンプライアンスの概念を比較対照することができる。

- 規制コンプライアンスの考慮事項
  - Payment Card Industry データセキュリティ基準(PCI DSS)
  - 一般データ保護規則(GDPR: General Data Protection Regulation)
- ロケーション制限
  - 国ごとの制限
  - ツールの制限
  - 現地の法律
  - 現地行政当局の要件
    - プライバシー要件
- 法的概念
  - サービスレベルアグリーメント(SLA)
  - 機密性
  - 作業範囲記述書
  - 秘密保持契約(NDA)
  - マスターサービス契約書
- 攻撃許可

1.2 スコープ、組織/顧客要件の重要性を説明することができる。

- 標準および手法
  - MITRE ATT&CK
  - Open Web Application Security Project (OWASP)
  - National Institute of Standards and Technology and Technology (NIST)
  - Open-source Security Testing Methodology Manual (OSSTMM)
  - Penetration Testing Execution Standard (PTES)
  - Information Systems Security Assessment Framework (ISSAF)
- エンゲージメント・ルール
  - 時間帯
  - 許可/禁止されているテストのタイプ
  - その他の制限
- 環境に関する考慮事項
  - ネットワーク
  - アプリケーション
  - クラウド
- 対象リスト/スコープ内のアセット
  - ワイヤレスネットワーク
  - インターネットプロトコル(IP) スキーム
  - ドメイン
  - アプリケーションプログラミングインタフェース(API)
  - 物理的な場所
  - ドメインネームシステム(DNS)
  - 外部ターゲットと内部ターゲット
  - 当事者でのホストと第三者でのホスト
- エンゲージメントスコープの検証
  - クライアントへの質問/契約の見直し
  - 時間管理
  - 戦略
    - 未知の環境と既知の環境のテスト

1.3 与えられたシナリオに基づいて、プロフェッショナリズムと完全性を維持することによって、倫理的ハッキングマインドセットを実証することができる。

- ペネトレーションテストチームのバックグラウンドチェック
- 特定の活動範囲を遵守
- 犯罪行為の特定
- 侵害/犯罪行為の迅速な報告
- 特定の活動に対するツールの使用制限
- 対象範囲に基づいて侵入を制限
- データ/情報の機密性を維持
- 専門家へのリスク
  - 料金/罰金
  - 刑事告発

2.0 情報収集と脆弱性のスキャン

2.1 与えられたシナリオに基づいて、パッシブな偵察を実施することができる。

- **DNS**検索
- 技術担当者の特定
- 管理者の連絡先
- クラウドとセルフホスト
- ソーシャルメディアスクレイピング
  - 主要な連絡先/職責
  - 求人情報/技術スタック
- 暗号に関連する欠陥
  - Secure Sockets Layer (SSL)認定書
  - 失効
- 企業の評判/セキュリティ態勢
- データ
  - パスワードダンプ
  - ファイルのメタデータ
  - 戦略的サーチエンジン分析/列挙
  - Webサイトアーカイブ/キャッシング
  - パブリックソースコードのリポジトリ
- オープンソースインテリジェンス**(OSINT)**
  - ツール
    - Shodan
    - Recon-NG
  - ソース
    - 共通脆弱性タイプ一覧(CWE)
    - 共通脆弱性識別子(CVE)

2.2 与えられたシナリオに基づいて、アクティブな偵察を実施することができる。

- 列挙
  - ホスト
  - サービス
  - ドメイン
  - ユーザー
  - Uniform resource locators (URL)
- **Web**サイトの偵察
  - Webサイトのクローリング
  - ウェブサイトのスクレイピング
  - ウェブリンクの手動検査
    - robots.txt
- パケットの作成
  - Scapy
- 防御検出
  - ロードバランサーの検出
  - Webアプリケーションファイアウォール(WAF)検出
  - アンチウイルス
  - ファイアウォール
- トークン
  - スコープ
  - 発行
  - 失効
- ウォードライビング
- ネットワークトラフィック
  - APIリクエストおよび応答をキャプチャ
  - スニッフィング
- クラウドアセットディスカバリー
- サードパーティーがホストするサービス
- 検出回避

2.3 与えられたシナリオに基づいて、偵察の結果を分析することができる。

- フィンガープリンティング
  - オペレーティングシステム(OS)
  - ネットワーク
  - ネットワーク機器
  - ソフトウェア
- 以下により入手した情報の分析：
  - DNS検索
  - Webサイトのクローリング
  - ネットワークトラフィック
  - アドレス解決プロトコル (ARP)トラフィック
  - Nmapスキャン
  - Webログ

2.4 与えられたシナリオに基づいて、脆弱性スキャンを実行することができる。

- 脆弱性スキャンの考慮事項
  - スキャンを実行する時間
  - プロトコル
  - ネットワークトポロジー
  - 帯域幅の限界
  - クエリスロットリング
  - フラジールシステム
  - 非従来型アセット
- 特定したターゲットの脆弱性をスキャン
- 検出回避のためのスキャン設定を設定
- スキャン方法
  - ステルススキャン
  - Transmission Control Protocol (TCP)接続スキャン
  - クレデンシャルとノンクレデンシャル
- **Nmap**
  - Nmap Scripting Engine (NSE)スクリプト
  - 共通オプション
    - -A
    - -sV
    - -sT
    - -Pn
    - -O
    - -sU
    - -sS
    - -T 1-5
    - -script=vuln
    - -p
- 自動化を促進する脆弱性テストツール

3.0 攻撃とエクスプロイト

3.1 与えられたシナリオに基づいて、攻撃ベクターを調査し、ネットワーク攻撃を実施することができる。

- 可用性の負荷テスト
- エクスプロイトのリソース
  - エクスプロイトデータベース(Exploit-DB)
  - パケットストーム
- 攻撃
  - ARPポイズニング
  - エクスプロイトの連鎖
  - パスワード攻撃
    - パスワードスプレー
    - ハッシュの解読
    - ブルートフォース攻撃
    - 辞書攻撃
  - On-Path攻撃（旧称：中間者攻撃）
  - Kerberoasting
  - DNSキャッシュポイズニング
  - 仮想ローカルエリアネットワーク(VLAN)
  - ネットワークアクセスコントロール(NAC)バイパス
  - メディアアクセスコントロール(MAC)スプーフィング
  - リンクローカルマルチキャスト名前解決(LLMNR)/NetBIOSネームサービス(NBT-NS)ポイズニング
  - New Technology LAN Manager (NTLM)リレー攻撃
- ツール
  - Metasploit
  - Netcat
  - Nmap

3.2 与えられたシナリオに基づいて、攻撃ベクターを調査し、ワイヤレス攻撃を実施することができる。

- 攻撃方法
  - スニッフィング
  - データの変更
  - データの破損
  - リレー攻撃
  - スプーフィング
  - 認証解除
  - ジャミング
  - ハンドシェイクのキャプチャ
  - On-Path
- 攻撃
  - エビルツイン
  - キャプティブポータル
  - ブルージャッキング
  - ブルースナーフィング
  - Radio-frequency identification (RFID)クローニング
  - Bluetooth Low Energy (BLE)攻撃
  - アンプ攻撃[近距離無線通信(NFC)]
  - WiFi protected setup (WPS) PIN攻撃
- ツール
  - Aircrack-ngスイート
  - 増幅アンテナ

3.3 与えられたシナリオに基づいて、攻撃ベクターを調査し、アプリケーションベース攻撃を実行することができる。

- **OWASP**トップ**10**
- サーバーサイドリクエストフォージェリ
- ビジネスロジックフロー
- インジェクション攻撃
  - ストラクチャードクエリランゲージ(SQL)インジェクション
    - ブラインドSQL
    - Boolean SQL
    - スタックドクエリ
  - コマンドインジェクション
  - クロスサイトスクリプティング
    - APT攻撃
    - リフレクション
  - Lightweight Directory Access Protocol (LDAP)インジェクション
- アプリケーションの脆弱性
  - 競合状態
  - エラー処理の欠如
  - コード署名の欠如
  - セキュアでないデータ転送
  - セッション攻撃
    - セッションハイジャック
    - クロスサイトリクエストフォージェリ(CSRF)
    - 特権エスカレーション
    - セッションリプレイ攻撃
    - セッションフィクセーション攻撃
- **API**攻撃
  - RESTful
  - Extensible Markup Language-Remote Procedure Call (XML-RPC)
  - Soap
- ディレクトリトラバーサル
- ツール
  - Webプロキシ
    - OWASP Zed Attack Proxy (ZAP)
    - Burp Suite community edition
  - SQLmap
  - DirBuster
- リソース
  - ワードリスト

3.4 与えられたシナリオに基づいて、攻撃ベクターを調査し、クラウド技術での攻撃を実施することができる。

- 攻撃
  - クレデンシャルハーベスティング
  - 特権エスカレーション
  - アカウントの乗っ取り
  - メタデータサービス攻撃
  - クラウドアセットの設定ミス
    - Identity and access management (IAM)
    - フェデレーション構成ミス
    - オブジェクトストレージ
    - コンテナ化技術
  - リソースの枯渇
  - クラウドマルウェアインジェクション攻撃
  - DoS攻撃
  - サイドチャネル攻撃
  - Direct-to-origin攻撃
- ツール
  - ソフトウェア開発キット(SDK)

3.5 特化したシステムに対する共通攻撃と脆弱性を説明することができる。

- モバイル
  - 攻撃
    - リバースエンジニアリング
    - サンドボックス分析
    - スパム
  - 脆弱性
    - セキュアでないストレージ
    - パスコードの脆弱性
    - 証明書のピンニング
    - 既知の脆弱なコンポーネントの使用
      (i) 依存関係の脆弱性
      (ii) パッチの断片化
    - ルートを使ったアクティビティの実行
    - アクセス許可のオーバーリーチ
    - 生体認証の統合
    - ビジネスロジックの脆弱性
  - ツール
    - Burp Suite
    - Drozer
    - モバイルセキュリティフレームワーク(MobSF)
    - Postman
    - Ettercap
    - Frida
    - Objection
    - Android SDKツール
    - ApkX
    - APK Studio
- モノのインターネット**(IoT)**デバイス
  - BLE攻撃
  - 特別な考慮事項
    - 脆弱な環境
    - 可用性に関する懸念
    - データ破損
    - データ流出
  - 脆弱性
    - セキュアでないデフォルト
    - クリアテキスト通信
    - ハードコーディングされた構成
    - 古いファームウェア/ハードウェア
    - データ漏洩
    - セキュアでないまたは古いコンポーネントの使用
- データストレージシステムの脆弱性
  - 設定ミス—オンプレミスとクラウドベース
    - ユーザー名/パスワードがデフォルト/ブランクの状態
    - ネットワーク露出
  - ユーザー入力のサニタイゼーションの欠如
  - ソフトウェアの根本的な脆弱性
  - エラーメッセージとデバッグへの対応
  - インジェクションの脆弱性
    - シングルクォーテーションの方法
- 管理インタフェースの脆弱性
  - Intelligent platform management interface (IPMI)
- 監視制御およびデータ取得**(SCADA)**/産業分野におけるモノのインターネット**(IIoT)**/産業制御システム**(ICS)**
- 仮想環境に関連した脆弱性
  - 仮想マシン(VM)エスケープ
  - ハイパーバイザーの脆弱性
  - VMリポジトリの脆弱性
- コンテナ化されたワークロードに関連する脆弱性

3.6 与えられたシナリオに基づいて、ソーシャルエンジニアリングまたは物理攻撃を実行することができる。

- アプローチのプリテキスティング
- ソーシャルエンジニアリング攻撃
  - メールフィッシング
    - ホエーリング
    - スピアフィッシング
  - ビッシング
  - ショートメッセージサービス(SMS)フィッシング
  - ユニバーサルシリアルバス(USB)ドロップキー
  - 水飲み場型攻撃
- 物理攻撃
  - テールゲート
  - ゴミあさり（ダンプスターダイビング）
  - ショルダーサーフィン
  - バッジクローニング
- なりすまし
- ツール
  - ブラウザエクスプロイトフレームワーク(BeEF)
  - ソーシャルエンジニアリングツールキット
  - なりすまし電話ツール
- 影響力を活用する方法
  - 権威(Authority)
  - 希少性(Scarcity)
  - 社会的証明(Social proof)
  - 緊急性(Urgency)
  - 類似性(Likeness)
  - 恐れ(Fear)

3.7 与えられたシナリオに基づき、エクスプロイト後のテクニックを実行することができる。

- ポストエクスプロイトツール
  - Empire
  - Mimikatz
  - BloodHound
- ラテラルムーブメント
  - パスザハッシュ攻撃
- ネットワークのセグメンテーションテスト
- 特権エスカレーション
  - 水平
  - 垂直
- シェル制限のアップグレード
- 足掛かり/持続性の構築
  - トロイの木馬
  - バックドア
    - バインドシェル
    - リバースシェル
  - デーモン
  - スケジュールされたタスク
- 検出回避
  - 環境寄生型手法/ファイルレスマルウェア
    - PsExec
    - Windows Management Instrumentation (WMI)
    - PowerShell (PS)リモート処理/Windowsリモート管理(WinRM)
  - データ流出
  - 痕跡を削除する
  - ステガノグラフィー
  - 隠れチャネルの確立
- 列挙
  - ユーザー
  - グループ
  - フォレスト
  - 機密データ
  - 暗号化されていないファイル

4.0 報告とコミュニケーション

4.1 レポートの重要な要素を比較対照することができる。

- 報告対象者
  - 経営幹部
  - 第三者の関係者
  - 技術者
  - 開発者
- レポートの内容（**特定の順番ではない）
  - エグゼクティブサマリー
  - スコープの詳細
  - 方法論
    - 攻撃ナラティブ
  - 発見事項
    - リスク評価（参照フレームワーク）
    - リスクの優先順位付け
    - ビジネス影響度分析
  - 指標と対策
  - 修復
  - 終了時
  - 補遺
- レポートの保存時間
- セキュアな配布
- メモを取る
  - テスト中の継続的な記録作成
  - スクリーンショット
- 共通テーマ/根本原因
  - 脆弱性
  - 観察
  - ベストプラクティスの欠如

4.2 与えられたシナリオに基づいて、発見事項を分析し、レポート内の適切な修復を推奨することができる。

- 技術的制御
  - システムの強化
  - ユーザー入力のサニタイズ/クエリのパラメータ化
  - 多要素認証を実装する
  - パスワードの暗号化
  - 処理レベルの修復
  - パッチ管理
  - キーローテーション
  - 証明書管理
  - 秘密管理ソリューション
  - ネットワークのセグメンテーション
- 管理
  - ロールベースアクセス制御
  - セキュアなソフトウェア開発ライフサイクル
  - パスワードの最小要件
  - ポリシーと手順
- 運用管理
  - ジョブローテーション
  - 時間帯制限
  - 強制的な休暇
  - ユーザートレーニング
- 物理的制御
  - アクセスコントロールの入口
  - 生体認証制御
  - ビデオ監視

4.3 ペネトレーションテストのプロセスにおけるコミュニケーションの重要性を説明することができる。

- コミュニケーションパス
  - 担当者
  - 技術担当者
  - 緊急時の連絡先
- コミュニケーションのきっかけ
  - 重要な発見
  - 状況報告
  - 過去の侵害を示す指標
- コミュニケーションの理由
  - 状況認識
  - エスカレーションの解消
  - 衝突回避
  - フォールスポジティブの特定
  - 犯罪行為
- 目標の再設定
- 発見事項の提示

4.4 レポート後の実施アクティビティを説明することができる。

- 活動後のクリーンアップ
  - シェルの取り外し
  - テスターが作成した認証情報を削除する
  - ツールを削除する
- クライアントの承認
- 教訓の管理
- フォローアップ活動/再テスト
- 調査結果の証明
- データ破壊処理

5.0 ツールとコード分析

5.1 スクリプトとソフトウェア開発の基本概念を説明することができる。

- 論理構成
  - ループ
  - 条件付き
  - ブール演算子
  - 文字列演算子
  - 算術演算子
- データ構造
  - JavaScript Object Notation (JSON)
  - キーバリュー
  - アレイ
  - 辞書
  - カンマ区切り値(CSV)
  - リスト
  - ツリー
- ライブラリ
- クラス
- 手順
- 関数

5.2 与えられたシナリオに基づいて、ペネトレーションテストで使用するスクリプトまたはコードのサンプルを分析することができる。

- **Shell**
  - Bash
  - PS
- プログラミング言語
  - Python
  - Ruby
  - Perl
  - JavaScript
- 次の場合のエクスプロイトコードを分析:
  - ファイルのダウンロード
  - リモートアクセスの開始
  - ユーザーの列挙
  - アセットの列挙
- 自動化の機会
  - ペネトレーションテストのプロセスを自動化
    - ポートスキャンを実行し、結果に基づいて次のステップを自動化
    - 構成を確認し、レポートを作成
  - テスト中のIPアドレスを変更するためのスクリプトの記述
  - 暗号列挙およびレポート作成のためのNmapスクリプトの記述

5.3 ペネトレーションテストのフェーズにおいて次のツールの用途を説明することができる。

（**この出題範囲は、特定ベンダーの機能をテストすることではありません。）

- スキャナー
  - Nikto
  - Open vulnerability assessment scanner (Open VAS)
  - SQLmap
  - Nessus
  - Open Security Content Automation Protocol (SCAP)
  - Wapiti
  - WPScan
  - Brakeman
  - Scout Suite
- クレデンシャルテストツール
  - Hashcat
  - Medusa
  - Hydra
  - CeWL
  - John the Ripper
  - Cain
  - Mimikatz
  - Patator
  - DirBuster
- デバッガ
  - OllyDbg
  - 免疫デバッガ
  - GNUデバッガ(GDB)
  - WinDbg
  - Interactive Disassembler (IDA)
  - Covenant
  - SearchSploit
- **OSINT**
  - WHOIS
  - Nslookup
  - Fingerprinting Organization with Collected Archives (FOCA)
  - theHarvester
  - Shodan
  - Maltego
  - Recon-NG
  - Censys
- 無線
  - Aircrack-ngスイート
  - Kismet
  - Wifite2
  - 不正なアクセスポイント
  - EAPHammer
  - mdk4
  - Spooftooph
  - Reaver
  - Wireless Geographic Logging Engine (WiGLE)
  - Fern
- ウェブアプリケーションツール
  - OWASP ZAP
  - Burp Suite
  - Gobuster
  - w3af
- ソーシャルエンジニアリングツール
  - ソーシャルエンジニアリングツールキット(SET)
  - BeEF
- リモートアクセスツール
  - Secure Shell (SSH)
  - Ncat
  - Netcat
  - ProxyChains
- ネットワーキングツール
  - Wireshark
  - Hping
- **MISC**
  - SearchSploit
  - Responder
  - Impacket
  - Empire
  - Metasploit
  - mitm6
  - CrackMapExec
  - TruffleHog
  - Censys
- ステガノグラフィツール
  - Openstego
  - Steghide
  - Snow
  - Coagula
  - Sonic Visualiser
  - TinEye
- クラウドツール
  - Scout Suite
  - CloudBrute
  - Pacu
  - Cloud Custodian

CompTIA PenTest+ (PT0-002)略語リスト

下記はCompTIA PenTest+認定資格試験で使用される略語の一覧です。包括的な試験準備プログラムの一環として、リストを復習し、知識の習得に努めてください。

略語	詳細説明
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AS2	Applicability Statement 2
BeEF	Browser Exploitation Framework
BLE	Bluetooth Low Energy
BSSID	Basic Service Set Identifier
CA	Certificate Authority
CAPEC	Common Attack Pattern Enumeration and Classification
CLI	Command -Line Interface
CSRF	Cross-Site Request Forgery
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DB	Database
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EAP	Extensible Authentication Protocol
FOCA	Fingerprinting Organization with Collected Archives
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GDB	GNU Debugger
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

略語	詳細説明
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDA	Interactive Disassembler
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSAF	Information Systems Security Assessment Framework
JSON	JavaScript Object Notation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLMNR	Link-Local Multicast Name Resolution
LSASS	Local Security Authority Subsystem Service
MAC	Media Access Control
MDM	Mobile Device Management
MobSF	Mobile Security Framework
MOU	Memorandum of Understanding
MSA	Master Service Agreement
MX	Mail Exchange
NAC	Network Access Control
NBT-NS	NetBIOS Name Service
NDA	Non-disclosure Agreement
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NS	Name Server
NSE	Nmap Scripting Engine
NTLM	New Technology LAN Manager

略語	詳細説明
NTP	Network Time Protocol
OS	Operating System
OSINT	Open-source Intelligence
OSSTMM	Open-source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
PBKDF2	Password-Based Key Deviation Function 2
PCI DSS	Payment Card Industry Data Security Standard
PHP	PHP: Hypertext Preprocessor
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PS	PowerShell
PSK	Pre-Shared Key
PTES	Penetration Testing Execution Standard
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFC	Request for Comment
RFID	Radio-Frequency Identification
ROE	Rules of Engagement
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDR	Software-defined Radio
SET	Social Engineering Toolkit
SGID	Set Group ID
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service-level Agreement
SMB	Server Message Block
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SOW	Statement of Work
SQL	Structured Query Language
SSD	Solid-State Drive
SSH	Secure Shell
SSHD	Solid-State Hybrid Drive
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
SUID	Set User ID
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time to Live
TTP	Tactics, Techniques and Procedures
UDP	User Datagram Protocol
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
USB	Universal Serial Bus
UTF	Unicode Transformation Format
VAS	Vulnerability Assessment Scanner
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VPS	Virtual Private Server
WAF	Web Application Firewall
WEP	Wired Equivalent Privacy
WiGLE	Wireless Geographic Logging Engine
WinRM	Windows Remote Management
WMI	Windows Management Instrumentation
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
XML-RPC	Extensible Markup Language-Remote Procedure Call
XSS	Cross-Site Scripting
ZAP	Zed Attack Proxy

CompTIA PenTest+のハードウェアとソフトウェア一覧

本リストは、PenTest+の受験準備として役立てていただくためのハードウェアとソフトウェアのリストです。トレーニングを実施している企業でも、トレーニングの提供に必要なラボコンポーネントを作成したい場合に役立ちます。各トピックに箇条書きで挙げられた項目は例であり、すべてを網羅するものではありません。

機器

- ラップトップ
- ワイヤレスアクセスポイント
- サーバー
- Graphics Processing Unit (GPU)
- スイッチ
- ケーブル接続
- モニター
- ファイアウォール
- HID/ドアアクセスコントロール
- パケットを注入できるワイヤレスアダプタ
- 指向性アンテナ
- モバイルデバイス
- IoT機器（カメラ、Raspberry Pi、スマートTVなど）
- Bluetoothアダプタ
- クラウド環境へのアクセス
  - コマンドラインインターフェイス(CLI)アクセス
  - 管理コンソールアクセス
  - クラウドサービスのインスタンス
- 多機能プリンター（有効な有線/無線）
- ドメイン参加プリンター
- RFIDリーダー
- 生体認証機器
- プログラマブルコントローラ
  - ソフトウェア無線(SDR)キット
- USBフラッシュドライブ
  - 兵器化されたUSBドライブ

予備のハードウェア

- ケーブル
- キーボード
- マウス
- 電源
- ドングル/アダプタ

予備のパーツ

- HDMIケーブル
- 予備のハードドライブ
- 予備のモニター

ツール

- 鍵開錠キット
- バッジ複製キット
- 指紋採取キット
- ネイルポリッシュ（指紋を覆うため）

ソフトウェア

- OSライセンス
- オープンソースOS
- ペネトレーションテストフレームワーク
- VMソフトウェア
- スキャンツール
- クレデンシャルテストツール
  - スプレーツール
  - パスワードクラッカー
- デバッガ
- ファジングツール
- ソフトウェア保証ツール
- ワイヤレステストツール
- ウェブプロキシツール
- ソーシャルエンジニアリングツール
- リモートアクセスツール
- ネットワークツール
- モビリティテストツール
- セキュリティ情報およびイベントマネジメント(SIEM)/侵入検知システム(IDS)/侵入防止システム(IPS)
- コマンドツールおよびコントロールツール
- 検出ツールおよび回避ツール

CompTIA