CompTIA PenTest+ CERTIFICATION Plus Series

CompTIA PenTest+ 認定資格試験 出題範囲

試験番号：PT0-003

CompTIA PenTest+ PT0-003認定資格試験：試験出題範囲バージョン3.0
Copyright © 2023 CompTIA, Inc.無断転載禁止。

CompTIA

試験について

CompTIA PenTest+認定資格試験は、以下の必要な知識とスキルを持っていることを証明します。

- ペネトレーションテストの一環として、情報収集の計画立案と範囲設定を行い、実行する。
- 法的要件とコンプライアンス要件に沿い、その要件を満たす攻撃を実行する。
- ペネトレーションテストの各フェーズを、適切なツールを使用および修正して実行し、適切な戦術、手法、手順を使用する。
- ペネトレーションテストの各フェーズの結果を分析し、レポート文書を作成するとともに、発見事項をステークホルダーに対して効果的に伝え、実用的な推奨事項を提供する。

認定資格試験の認証
CompTIA PenTest+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、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」）とは提携関係になく、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に、認定資格試験を受験される全員の方にCompTIA認定資格試験実施ポリシーをご一読いただくようご案内しております。CompTIAの認定資格試験を受験するための学習を始める前に、必ずCompTIAが定めるすべてのポリシーをご確認ください。受験者はCompTIA受験者合意書を遵守することが求められます。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されていない場合でも、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。

Copyright © 2023 CompTIA, Inc.無断転載禁止。

試験情報

試験番号	PT0-003
問題数	最大90問
出題形式	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ターとして3〜4年の業務経験
合格スコア	750

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	エンゲージメント管理	13%
2.0	偵察と列挙	21%
3.0	脆弱性の検出と分析	17%
4.0	攻撃とエクスプロイト	35%
5.0	エクスプロイト後の活動とラテラルムーブメント	14%
計		**100%**

Copyright © 2023 CompTIA, Inc.無断転載禁止。

1.0 エンゲージメント管理

1.1 エンゲージメント前のアクティビティを要約することができる。

- **範囲の定義**
  - 規制、フレームワーク、および標準
    - プライバシー
    - セキュリティ
  - 活動規約
    - 除外事項
    - テストケース
    - エスカレーションプロセス
    - テスト期間
  - 契約書のタイプ
    - 秘密保持契約書（NDA）
    - マスターサービス契約書（MSA）
    - 作業明細書（SoW）
    - サービス利用規約（ToS）
  - ターゲット選択
    - Classless Inter-domain Routing（CIDR）範囲
    - ドメイン
    - インターネットプロトコル（IP）アドレス
    - Uniform Resource Locator（URL）
  - 評価のタイプ
    - Web
    - ネットワーク
    - モバイル
    - クラウド
    - アプリケーションプログラミングインターフェース（API）
    - アプリケーション
    - ワイヤレス
- **責任共有モデル**
  - ホスティングプロバイダーの責任
  - 顧客の責任
  - ペネトレーションテスターの責任
  - サードパーティの責任
- **法務と倫理に関する検討事項**
  - 委任状
  - レポートの必須事項に関する要件
  - ペネトレーションテスターへのリスク

1.2 共同作業とコミュニケーションのアクティビティについて説明することができる。

- **ピアレビュー**
- **ステークホルダーの調整**
- **根本原因分析**
- **エスカレーションパス**
- **セキュアな配布**
- **リスク、重大度、影響の明確化**
- **目標の再設定**
- **ビジネス影響度分析**
- **クライアントの承認**

1.3 テストのフレームワークと手法を比較対照することができる。

- Open Source Security Testing Methodology Manual（OSSTMM）
- Council of Registered Ethical Security Testers（CREST）
- Penetration Testing Execution Standard（PTES）
- MITRE ATT&CK
- Open Worldwide Application Security Project（OWASP）Top 10
- OWASP Mobile Application Security Verification Standard（MASVS）
- Purdueモデル
- **脅威モデリングのフレームワーク**
  - 潜在的損害、再現性、攻撃利用可能性、影響を受けるユーザー、発見可能性（DREAD）
  - スプーフィング、改ざん、否認、情報漏洩、Dos攻撃、特権昇格（STRIDE）
  - 運用上重要な脅威、資産、脆弱性評価（OCTAVE）

Copyright © 2023 CompTIA, Inc.無断転載禁止。

1.4 ペネトレーションテストレポートの構成要素を説明することができる。

- **フォーマットの調整**
- **文書の仕様**
- **リスクスコア**
- **定義**
- **レポートの構成要素**
  - エグゼクティブサマリー
  - 手法
  - 発見事項の詳細
  - 攻撃の説明
  - 推奨事項
    - 改善策のガイダンス
- **テストの制限と仮定**
- **レポートの検討事項**
  - 法務
  - 倫理
  - 品質管理（QC）
  - 人工知能（AI）

1.5 与えられたシナリオに基づいて、発見事項を分析し、レポート内で適切な改善策を推奨することができる。

- **技術的制御**
  - システムのセキュリティ強化
  - 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
  - 暗号化
  - プロセスレベルの改善策
  - パッチ管理
  - キーローテーション
  - 証明書管理
  - シークレット管理ソリューション
  - ネットワークセグメンテーション
  - インフラストラクチャセキュリティ管理
- **管理的制御**
  - 役割/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
- **運用的制御**
  - 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**
  - アクセス制限ホール
  - 生体認証制御
  - ビデオによる監視

Copyright © 2023 CompTIA, Inc.無断転載禁止。

2.0 偵察と列挙

2.1 与えられたシナリオに基づいて、情報収集手法を適用することができる。

- **アクティブ偵察とパッシブ偵察**
- **オープンソースインテリジェンス（OSINT）**
  - ソーシャルメディア
  - 求人掲示板
  - スキャンコードリポジトリ
  - ドメイン名システム（DNS）
    - DNS検索
    - リバースDNS検索
  - キャッシュされたページ
  - 暗号に関連する欠陥
  - パスワードダンプ
- **ネットワーク偵察**
- **プロトコルスキャン**
  - 伝送制御プロトコル（TCP）/User Datagram Protocol（UDP）スキャン
- **証明書の透明性ログ**
- **情報漏洩**
- **検索エンジン分析/列挙**
- **ネットワークスニッフィング**
  - モノのインターネット（IoT）およびオペレーショナルテクノロジー（OT）プロトコル
- **バナーグラビング**
- **ハイパーテキストマークアップ言語（HTML）スクレイピング**

2.2 与えられたシナリオに基づいて、列挙手法を適用することができる。

- **オペレーティングシステム（OS）フィンガープリンティング**
- **サービスディスカバリー**
- **プロトコル列挙**
- **DNS列挙**
- **ディレクトリ列挙**
- **ホストディスカバリー**
- **共有列挙**
- **ローカルユーザー列挙**
- **メールアカウント列挙**
- **ワイヤレス列挙**
- **許可列挙**
- **シークレット列挙**
  - クラウドアクセスキー
  - パスワード
  - APIキー
  - セッショントークン
- **攻撃パスのマッピング**
- **Webアプリケーションファイアウォール（WAF）列挙**
  - オリジンアドレス
- **Webクローリング**
- **マニュアル列挙**
  - robots.txt
  - サイトマップ
  - プラットフォームのプラグイン

2.3 与えられたシナリオに基づいて、偵察と列挙のためのスクリプトを修正することができる。

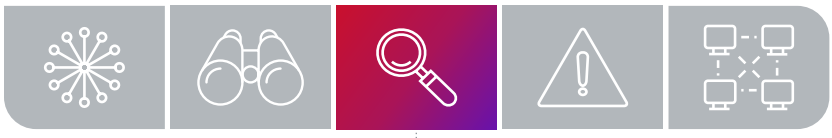
- **情報収集**
- **データ操作**
- **スクリプティング言語**
  - Bash
  - Python
  - PowerShell
- **論理構成**
  - ループ
  - 条件文
  - ブール演算子
  - 文字列演算子
  - 算術演算子
- **ライブラリ、関数、クラスの使用**

Copyright © 2023 CompTIA, Inc.無断転載禁止。

2.4 与えられたシナリオに基づいて、偵察と列挙のための適切なツールを使用することができる。

- Wayback Machine
- Maltego
- Recon-ng
- Shodan
- SpiderFoot
- WHOIS
- nslookup/dig
- Censys.io
- Hunter.io
- DNSdumpster
- Amass
- Nmap
  - Nmap Scripting Engine（NSE）
- theHarvester
- WiGLE.net
- InSSIDer
- OSINTframework.com
- Wireshark/tcpdump
- Aircrack-ng

Copyright © 2023 CompTIA, Inc.無断転載禁止。



3.0 脆弱性の検出と分析

3.1 与えられたシナリオに基づいて、様々な手法を用いて脆弱性を検出することができる。

- **スキャンの種類**
  - コンテナースキャン
    - サイドカースキャン
  - アプリケーションスキャン
    - 動的アプリケーションセキュリティテスト（DAST）
    - 対話型アプリケーションセキュリティテスト（IAST）
    - ソフトウェアコンポジション解析（SCA）
    - 静的アプリケーションセキュリティテスト（SAST）
      - コードとしてのインフラストラクチャ（IaC）
      - ソースコード分析
    - モバイルスキャン
  - ネットワークスキャン
    - TCP/UDPスキャン
    - ステルススキャン
  - ホストベーススキャン
  - 認証済みスキャンと未認証スキャン
  - シークレットスキャン
  - ワイヤレス
    - サービスセット識別子（SSID）スキャン
    - チャネルスキャン
    - 信号強度スキャン
- **産業用制御システム（ICS）脆弱性評価**
  - マニュアル評価
  - ポートミラーリング
- **ツール**
  - Nikto
  - Greenbone/Open Vulnerability Assessment Scanner（OpenVAS）
  - TruffleHog
  - BloodHound
  - Tenable Nessus
  - PowerSploit
  - Grype
  - Trivy
  - Kube-hunter

3.2 与えられたシナリオに基づいて、偵察、スキャン、列挙の各フェーズで得られた出力を分析することができる。

- **スキャン、偵察、および列挙結果の検証**
  - フォールスポジティブ
  - フォールスネガティブ
  - トゥルーポジティブ
  - スキャンの完全性
  - スキャン構成のトラブルシューティング
- **公開済みエクスプロイトの選択**
- **スクリプトを使用した結果の検証**

3.3 物理的セキュリティのコンセプトを説明することができる。

- **テールゲート（共連れ）**
- **現地調査**
- **ユニバーサルシリアルバス（USB）ドロップ**
- **バッジのクローニング**
- **ロックピッキング**

Copyright © 2023 CompTIA, Inc.無断転載禁止。

4.0 攻撃とエクスプロイト

4.1 与えられたシナリオに基づいて、出力を分析して攻撃の優先順位付けを行い、攻撃に備えることができる。

- **ターゲットの優先順位付け**
  - 高価値資産の特定
  - 記述子とメトリック
    - 共通脆弱性スコアリングシステム（CVSS）ベーススコア
    - 共通脆弱性識別子（CVE）
    - 共通脆弱性タイプ一覧（CWE）
    - Exploit Prediction Scoring System（EPSS）
  - EOL（エンドオブライフ）ソフトウェア/システム
  - デフォルト構成
  - 実行中のサービス
  - 脆弱な暗号化方式
  - 防御能力
- **能力の選択**
  - ツールの選択
  - エクスプロイトの選択とカスタマイズ
    - コード分析
  - 文書化
    - 攻撃パス
    - ローレベル図表の作成
    - ストーリーボード
  - 依存性
  - 範囲に関する制限の検討
    機密性の高いシステムのラベリング

4.2 与えられたシナリオに基づいて、適切なツールを使用してネットワーク攻撃を実行することができる。

- **攻撃の種類**
  - デフォルトの認証情報
  - オンパス攻撃
  - 証明書サービス
  - 正しく設定されていないサービスのエクスプロイト
  - 仮想ローカルエリアネットワーク（VLAN）のホッピング
  - マルチホームホスト
  - リレー攻撃
  - 共有列挙
  - パケットの作成
- **ツール**
  - Metasploit
  - Netcat
  - Nmap
    - NSE
  - Impacket
  - CrackMapExec（CME）
  - Wireshark/tcpdump
  - msfvenom
  - Responder
  - Hydra

4.3 与えられたシナリオに基づいて、適切なツールを使用して認証攻撃を実行することができる。

- **攻撃の種類**
  - 多要素認証（MFA）疲労攻撃
  - Pass-the-hash攻撃
  - Pass-the-ticket攻撃
  - Pass-the-token攻撃
  - Kerberos攻撃
  - Lightweight Directory Access Protocol（LDAP）インジェクション
  - 辞書攻撃
  - ブルートフォース攻撃
  - マスク攻撃
  - パスワードスプレー攻撃
  - クレデンシャルスタッフィング
  - OpenID Connect（OIDC）攻撃
  - Security Assertion Markup Language（SAML）攻撃
- **ツール**
  - CME
  - Responder
  - hashcat
  - John the Ripper
  - Hydra
  - BloodHound
  - Medusa
  - Burp Suite

Copyright © 2023 CompTIA, Inc.無断転載禁止。

4.4 与えられたシナリオに基づいて、適切なツールを使用してホストベースの攻撃を実行することができる。

- **攻撃の種類**
  - 特権昇格
  - クレデンシャルダンピング
  - セキュリティツールの迂回
  - 正しく設定されていないエンドポイント
  - ペイロードの難読化
  - ユーザーが制御するアクセスバイパス
  - シェルエスケープ
  - キオスクエスケープ
  - ライブラリインジェクション
  - プロセスホローイングとインジェクション
  - ログの改ざん
  - 引用されていないサービスパスのインジェクション
- **ツール**
  - Mimikatz
  - Rubeus
  - Certify
  - Seatbelt
  - PowerShell/PowerShell Integrated Scripting Environment（ISE）
  - PsExec
  - Evil-WinRM
  - Living off the Land Binaries（LOLBins）

4.5 与えられたシナリオに基づいて、適切なツールを使用してWebアプリケーション攻撃を実行することができる。

- **攻撃の種類**
  - ブルートフォース攻撃
  - 衝突攻撃
  - ディレクトリトラバーサル
  - サーバーサイドリクエストフォージェリ（SSRF）
  - クロスサイトリクエストフォージェリ（CSRF）
  - デシリアライゼーション攻撃
  - インジェクション攻撃
    - Structured Query Language（SQL）インジェクション
    - 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（XSS）
    - サーバーサイドテンプレートインジェクション
  - 安全でない直接オブジェクト参照
  - セッションハイジャック
  - 任意コード実行
  - ファイルのインクルード
    - リモートファイルインクルージョン（RFI）
    - ローカルファイルインクルージョン（LFI）
    - Webシェル
  - APIの悪用
  - JSON Web Token（JWT）の不正操作
- **ツール**
  - TruffleHog
  - Burp Suite
  - Zed Attack Proxy（ZAP）
  - Postman
  - sqlmap
  - Gobuster/DirBuster
  - Wfuzz
  - WPScan

4.6 与えられたシナリオに基づいて、適切なツールを使用してクラウドベースの攻撃を実行することができる。

- **攻撃の種類**
  - メタデータサービス攻撃
  - IDおよびアクセス管理の構成ミス
  - サードパーティの統合
  - リソースの構成ミス
    - ネットワークセグメンテーション
    - ネットワーク制御
    - 認証管理とアクセス管理（IAM）認証情報
    - 流出したストレージバケット
    - サービスへのパブリックアクセス
  - ログ情報の漏洩
  - 画像と作成物の改ざん
  - サプライチェーン攻撃
  - ワークロードランタイム攻撃
  - コンテナーエスケープ
  - 信頼関係の悪用
- **ツール**
  - Pacu
  - Docker Bench
  - Kube-hunter
  - Prowler
  - ScoutSuite
  - クラウドネイティブのベンダーツール

Copyright © 2023 CompTIA, Inc.無断転載禁止。

4.7 与えられたシナリオに基づいて、適切なツールを使用してワイヤレス攻撃を実行することができる。

- **攻撃**
  - ウォードライビング
  - エビルツイン攻撃
  - 信号のジャミング
  - プロトコルのファジング
  - パケットの作成
  - 認証解除
  - キャプティブポータル
  - Wi-Fi Protected Setup（WPS）Personal Identification Number（PIN）攻撃
- **ツール**
  - WPAD
  - WiFi-Pumpkin
  - Aircrack-ng
  - WiGLE.net
  - InSSIDer
  - Kismet

4.8 与えられたシナリオに基づいて、適切なツールを使用してソーシャルエンジニアリング攻撃を実行することができる。

- **攻撃の種類**
  - フィッシング
  - ビッシング
  - ホエーリング
  - スピアフィッシング
  - スミッシング
  - ゴミ箱あさり
  - サーベイランス
  - ショルダーサーフィン
  - テールゲート（共連れ）
  - 盗聴
  - 水飲み場型攻撃
  - なりすまし
  - クレデンシャルハーベスティング
- **ツール**
  - ソーシャルエンジニアリングツールキット（SET）
  - Gophish
  - Evilginx
  - theHarvester
  - Maltego
  - Recon-ng
  - Browser Exploitation Framework（BeEF）

4.9 専用システムに対する一般的な攻撃を説明することができる。

- **攻撃の種類**
  - モバイル攻撃
    - 情報漏洩
    - 脱獄/root化
    - 許可の悪用
  - AI攻撃
    - プロンプトインジェクション
    - モデルの不正操作
  - OT
    - レジスタの不正操作
    - CAN bus攻撃
    - Modbus攻撃
    - プレーンテキスト攻撃
    - リプレイ攻撃
  - 近距離無線通信（NFC）
  - ブルージャッキング
  - Radio-Frequency Identification（RFID）
  - Bluetoothスパミング
- **ツール**
  - Scapy
  - tcprelay
  - Wireshark/tcpdump
  - MobSF
  - Frida
  - Drozer
  - Android Debug Bridge（ADB）
  - Bluestrike

4.10 与えられたシナリオに基づいて、スクリプトを使用して攻撃を自動化することができる。

- **PowerShell**
  - PowerSploit
  - PowerView
  - PowerUpSQL
  - AD search
- **Bash**
  - 入力/出力管理
  - データ操作
- **Python**
  - Impacket
  - Scapy
- **Breach and Attack Simulation（BAS）**
  - Caldera
  - Infection Monkey
  - Atomic Red Team

Copyright © 2023 CompTIA, Inc.無断転載禁止。

5.0 エクスプロイト後の活動とラテラルムーブメント

5.1 与えられたシナリオに基づいて、永続性を確立して維持するためのタスクを実行することができる。

- **スケジュールされているタスク/cronジョブ**
- **サービス作成**
- **リバースシェル**
- **バインドシェル**
- **新規アカウントの追加**
- **有効なアカウント認証情報の取得**
- **レジストリキー**
- **コマンド&コントロール（C2）フレームワーク**
- **バックドア**
  - Webシェル
  - トロイの木馬
- **ルートキット**
- **ブラウザの拡張機能**
- **セキュリティ管理の改ざん**

5.2 与えられたシナリオに基づいて、環境全体でラテラルムーブメントを行うためのタスクを実行することができる。

- **ピボット**
- **リレーの作成**
- **列挙**
  - サービスディスカバリー
  - ネットワークトラフィックディスカバリー
  - 追加の認証情報のキャプチャ
  - クレデンシャルダンピング
  - 文字列検索
- **サービスディスカバリー**
  - Server Message Block（SMB）/ファイル共有
  - リモートデスクトッププロトコル（RDP）/仮想ネットワークコンピューティング（VNC）
  - Secure Shell（SSH）
  - クリアテキスト
  - LDAP
  - リモートプロシージャコール（RPC）
  - ファイル転送プロトコル（FTP）
  - Telnet
  - ハイパーテキスト転送プロトコル（HTTP）/Hypertext Transfer Protocol Secure（HTTPS）
    - Webインターフェース
  - Line Printer Daemon（LPD）
  - JetDirect
  - RPC/分散コンポーネントオブジェクトモデル（DCOM）
  - プロセスID
- **Windows Management Instrumentation（WMI）**
- **Windowsリモート管理（WinRM）**
- **ツール**
  - LOLBins
    - Netstat
    - Netコマンド
    - cmd.exe
    - explorer.exe
    - ftp.exe
    - mmc.exe
    - rundll32
    - msbuild
    - route
    - strings/findstr.exe
  - Covenant
  - CrackMapExec
  - Impacket
  - Netcat
  - sshuttle
  - Proxychains
  - PowerShell ISE
  - バッチファイル
  - Metasploit
  - PsExec
  - Mimikatz

Copyright © 2023 CompTIA, Inc.無断転載禁止。

5.3 ステージングとデータ流出に関する概念を要約することができる。

- **ファイルの暗号化と圧縮**
- **隠れチャネル**
  - ステガノグラフィー
  - DNS
  - Internet Control Message Protocol（ICMP）
  - HTTPS
- **電子メール**
- **クロスアカウントリソース**
- **クラウドストレージ**
- **代替データストリーム**
- **テキストストレージサイト**
- **仮想ドライブのマウント**

5.4 クリーンアップと修復のアクティビティを説明することができる。

- **永続性メカニズムの削除**
- **構成の変更の復元**
- **テスターが作成した認証情報の削除**
- **ツールの削除**
- **インフラストラクチャのスピンダウン**
- **作成物の保全**
- **安全なデータ破棄**

Copyright © 2023 CompTIA, Inc.無断転載禁止。

CompTIA PenTest+ PT0-003略語リスト

下記は CompTIA PenTest+ PT0-003 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、リスト全体を復習し、記載されているすべての略語の知識の習得に努めてください。

略語	正式名称
AD	Active Directory
ADB	Android Debug Bridge
AI	Artificial Intelligence
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
BAS	Breach and Attack Simulation
BeEF	Browser Exploitation Framework
BGP	Border Gateway Protocol
BIA	Business Intelligence Analytics
C2	Command and Control
CI/CD	Continuous Integration/Continuous Delivery
CIDR	Classless Inter-Domain Routing
CGI	Common Gateway Interface
CLI	Command-Line Interface
CME	CrackMapExec
CNAME	Canonical Name
COFF	Common Object File Format
CREST	Council of Registered Ethical Security Testers
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DAST	Dynamic Application Security Testing
DCOM	Distributed Component Object Model
DDoS	Distributed Denial of Service
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DoS	Denial of Service
DREAD	Damage potential, Reproducibility, Exploitability, Affected users, Discoverability
DROWN	Decrypting RSA [Rivest-Shamir-Adleman] with Obsolete and Weakened Encryption
EFSRPC	Encrypting File System Remote Protocol
ELF	Executable and Linkable Format

略語	正式名称
EPSS	Exploit Prediction Scoring System
EXIF	Exchangeable Image File Format
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GIF	Graphic Interchange Format
HID	Host-based Intrusion Detection
HSTS	HTTP Strict Transport Security
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaC	Infrastructure as Code
IAM	Identity and Access Management
IAST	Interactive Application Security Testing
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDOR	Insecure Direct Object Reference
IdP	Identity Provider
IDS	Intrusion Detection System
IGRP	Interior Gateway Routing Protocol
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrustion Prevention System
ISE	Integrated Scripting Environment
JWT	JSON Web Token
KDC	Key Distribution Center
KRBTGT	Kerberos Ticket Granting Ticket
LDAP	Lightweight Directory Access Protocol
LFI	Local File Inclusion
LLMNR	Link-Local Multicast Name Resolution
LOLBins	Living off the Land Binaries
LPD	Line Printer Daemon
LSASS	Local Security Authority Subsystem Service
MAC	Media Access Control
MASVS	Mobile Application Security Verification Standard
MFA	Multifactor Authentication
MIB	Management Information Base

Copyright © 2023 CompTIA, Inc.無断転載禁止。

略語	正式名称
MMS	Multimedia Messaging Service
MSA	Master Services Agreement
MX	Mail Exchange
NDA	Non-Disclosure Agreement
NFC	Near-Field Communication
NSE	Nmap Scripting Engine
NTLM	New Technology LAN Manager
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OIDC	OpenID Connect
OpenVAS	Open Vulnerability Assessment Scanner
OS	Operating System
OSINT	Open-Source Intelligence
OSSTMM	Open-Source Security Testing Methodology Manual
OT	Operational Technology
OWASP	Open Worldwide Application Security Project
PTES	Penetration Testing Execution Standard
PWS	Performance Work Statement
QC	Quality Control
RCE	Remote Code Execution
RDP	Remote Desktop Protocol
RFI	Remote File Inclusion
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RPC	Remote Procedure Call
SaaS	Software as a Service
SAM	Security Account Manager
SAML	Security Assertion Markup Language
SAST	Static Application Security Testing
SCA	Software Composition Analysis
SCADA	Supervisory Control and Data Acquisition
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDR	Software-Defined Radio
SET	Social Engineering Toolkit
SIEM	Security Information and Event Management
SMB	Server Message Block
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SOC	Security Operations Center
SoW	Statement of Work
SPN	Service Principal Name
SQL	Structured Query Language
SQLi	Structured Query Language Injection
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSO	Single Sign-on
SSRF	Server-Side Request Forgery
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TCP	Transmission Control Protocol
TGS	Ticket Granting Service
TLS	Transport Layer Security
ToS	Terms of Service
TTP	Techniques, Tactics, Procedures
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VPN	Virtual Private Network
WAF	Web Application Firewall
WinRM	Windows Remote Management
WLAN	Wireless Local Area Network
WMI	Windows Management Instrumentation
WPAD	Web Proxy Auto Discovery
WPS	Wi-Fi Protected Setup
XSS	Cross-Site Scripting
ZAP	Zed Attack Proxy

Copyright © 2023 CompTIA, Inc.無断転載禁止。

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に CompTIA が用意した、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実習室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。

ハードウェア

- コンピューター
- ワイヤレスアクセスポイント
- サーバー
- スイッチ
- ケーブル接続
- ファイアウォール
- ルーター
- ホストベースの侵入検知（HID）/ドアアクセスコントロール
- パケットインジェクションが可能な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、マイクロコンピューター、スマートTVなど）
- Bluetoothアダプタ
- 多機能プリンター（有線/ワイヤレスに対応）
- NFC/RFIDクローニング機器
- 鍵開錠キット（該当する場合）
- 生体認証デバイス
- プログラマブルロジックコントローラー
  - ソフトウェア無線（SDR）キット
- USBフラッシュドライブ

ソフトウェア

- 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ース（CLI）へのアクセス
  - 管理コンソールへのアクセス
  - クラウドサービスのインスタンス
- 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
- 仮想マシンソフトウェア
- スキャンツール
  - 脆弱性スキャンツール
  - SAST
  - DAST
- 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
- アプリケーションセキュリティツール
- デバッガ
- ワイヤレステストツール
- Web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
  - プロトコルアナライザー
  - スニッフィングツール
- モビリティテストツール
- オープンソースまたは公開済みのSecurity Information and Event Management（SIEM）/侵入検知システム（IDS）/侵入防止システム（IPS）/エンドポイントセキュリティの各ツール
- C2ツール

CompTIA

© 2023 CompTIA, Inc. は CompTIA, Inc. のライセンスの下で使用。無断転載禁止。上記プログラムに関連するすべての認定プログラムおよび教育は、CompTIA, Inc. のみによって運営されています。CompTIA は、CompTIA, Inc. の米国内および全世界における登録商標です。ここに示すその他のブランド及び会社名は、CompTIA, Inc. またはその各所有者の商標またはサービスマークである場合があります。CompTIA, Inc. の書面による同意なしに複製または配布することは禁じられています。米国で印刷。10986-2023 年 12 月