CompTIA PenTest+
認定資格
試験出題範囲

試験番号：PT0-001

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：

- **評価の計画とスコープ**
- **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する**
- **結果を分析する**

また、CompTIA PenTest+を取得いただくことで、以下のような業務を行うことを可能とします。

- **提案された改善テクニックを含む文書を作成する**
- **結果を経営層に効果的に伝える**
- **実用的な推奨事項を提示する**

試験開発

CompTIAの認定資格試験は、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、全員**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。必要に応じて、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	PT0-001
問題数	最大80問
出題形式	単一/複数選択、パフォーマンスベースドテスト
試験時間	165分
推奨される経験	3〜4年間のペネトレーションテスト、脆弱性評価、脆弱性管理の実務経験で得られる知識とスキルを目安に設計されています
合格ライン	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	15%
2.0 情報収集と脆弱性の識別	22%
3.0 攻撃とエクスプロイト	30%
4.0 ペネトレーションテストツール	17%
5.0 報告とコミュニケーション	16%
計	**100%**

1.0 計画とスコープ

1.1 エンゲージメントを計画することの重要性を説明することができる。

- **ターゲットオーディエンスの理解**
- **活動規約（Rules of engagement）**
- **コミュニケーション・エスカレーションパス**
- **リソースと要件**
  - 調査結果の機密性
  - 既知と未知
- **予算**
- **影響分析と改善のタイムライン**
- **免責事項**
  - 基準時点アセスメント（Point-in-timeアセスメント）
  - 包括性
- **技術的制約**
- **サポートリソース**
  - WSDL/WADL
  - SOAPプロジェクトファイル
  - SDKのドキュメント
  - Swaggerドキュメント
  - XSD
  - サンプルアプリケーションリクエスト
  - アーキテクト図

1.2 主要な法的概念を説明することができる。

- **契約**
  - SOW
  - MSA
  - NDA
- **環境の違い**
  - 輸出規制
  - 地方自治体および政府の規制
  - 企業ポリシー
- **書面による承認**
  - 適切な機関から署名を取得する
  - 必要に応じた第三者プロバイダの承認

1.3 エンゲージメントに対する適切なスコープの重要性を説明することができる。

- **評価のタイプ**
  - 目標ベース/目的ベース
  - コンプライアンスベース
  - レッドチーム
- **特別なスコープの考慮事項**
  - 合併
  - サプライチェーン
- **ターゲット選択**
  - ターゲット
    - 内部
      - オンサイトとオフサイト
    - 外部
    - 当事者でのホストと第三者でのホスト
    - 物理的
  - ユーザー
  - SSID
  - アプリケーション
  - 考慮事項
    - ホワイトリストとブラックリスト
    - セキュリティの例外
      - IPS/WAFホワイトリスト
      - NAC
      - 証明書のピンニング
      - 会社のポリシー
- **戦略**
  - ブラックボックス、ホワイトボックス、グレーボックス
- **リスク受容**
- **インパクト耐性**
- **スケジューリング**
- **スコープクリープ**
- **脅威アクター**
  - 敵対者層
    - APT
    - スクリプトキディ
    - ハクティビスト
    - インサイダー脅威
  - 能力
  - 攻撃者の意図
  - 脅威モデル

1.4 コンプライアンスに基づく評価の重要な側面について説明することができる。

- **コンプライアンスに基づく評価、制限や注意事項**
  - 評価を完了するためのルール
  - パスワードポリシー
  - データの分離
  - 鍵管理
  - 制限事項
    - ネットワークアクセスの制限
    - ストレージアクセスの制限
- **規制に基づいた明確な目標**

2.0 情報収集と脆弱性の識別

2.1 与えられたシナリオに基づき、適切な手法を用いて情報収集を行うことができる。

- **スキャン**
- **列挙**
  - ホスト
  - ネットワーク
  - ドメイン
  - ユーザー
  - グループ
  - ネットワーク共有
  - ウェブページ
  - アプリケーション
  - サービス
  - トークン
  - ソーシャルネットワーキングサイト
- **パケットの作成**
- **パケットの検査**
- **フィンガープリンティング**
- **暗号手法**
  - Certificate inspection
- **盗聴**
  - RF通信の監視
  - スニッフィング
    - 有線
    - ワイヤレス
- **デコンパイル**
- **デバッグ**
- **オープンソース情報収集**
  - リサーチのソース
    - CERT
    - NIST
    - JPCERT/CC
    - CAPEC
    - Full disclosure
    - CVE
    - CWE

2.2 与えられたシナリオに基づき、脆弱性スキャンを実行することができる。

- **クレデンシャルとノンクレデンシャルの違い**
- **スキャンの種類**
  - ディスカバリースキャン
  - フルスキャン
  - ステルススキャン
  - コンプライアンススキャン
- **コンテナのセキュリティ**
- **アプリケーションスキャン**
  - 動的分析と静的分析
- **脆弱性スキャンの考慮事項**
  - スキャンを実行する時間
  - 使用されたプロトコル
  - 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
  - 脆弱なシステム/非伝統的資産

2.3 与えられたシナリオに基づき、脆弱性スキャン結果を分析することができる。

- **アセットの分類**
- **判断**
  - フォールス・ポジティブ
- **脆弱性の優先順位付け**
- **共通テーマ**
  - 脆弱性
  - 観察
  - ベストプラクティスの欠如

2.4 エクスプロイトの準備に情報を活用するプロセスを説明することができる。

- **潜在的なエクスプロイトに脆弱性をマッピングする**
- **ペネトレーションテストのための準備活動の優先順位付け**
- **攻撃を完了するための共通テクニックを説明する**
  - クロスコンパイルコード
  - エクスプロイトの修正
  - エクスプロイトの連鎖
  - Proof-of-concept開発（エクスプロイト開発）
  - ソーシャルエンジニアリング
  - クレデンシャル総当たり
  - 辞書攻撃
  - レインボーテーブル
  - デセプション

2.5 特化したシステムに関連する弱点を説明することができる。

- **ICS**
- **SCADA**
- **モバイル**
- **IoT**
- **組み込み**
- **POSシステム**
- **生体認証**
- **アプリケーションコンテナ**
- **RTOS**

3.0 攻撃とエクスプロイト

3.1 ソーシャルエンジニアリング攻撃を比較対照することができる。

- **フィッシング**
  - スピアフィッシング
  - SMSフィッシング
  - ボイスフィッシング
  - ホエーリング
- **誘導質問**
  - ビジネスメール詐欺
- **尋問**
- **なりすまし**
- **ショルダーサーフィン**
- USB**キードロップ**
- **モチベーションテクニック**
  - 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)

3.2 与えられたシナリオに基づき、ネットワークベースの脆弱性を利用することができる。

- **名前解決のエクスプロイト**
  - NETBIOSネームサービス
  - LLMNR
- **SMBエクスプロイト**
- **SNMPエクスプロイト**
- **SMTPエクスプロイト**
- **FTPエクスプロイト**
- **DNSキャッシュポイズニング**
- **Pass-the-hash攻撃**
- **中間者攻撃**
  - ARPスプーフィング
  - リプレイ攻撃
  - リレー
  - SSLストリッピング
  - ダウングレード攻撃
- **DoS /ストレステスト**
- **NACバイパス**
- **VLANホッピング**

3.3 与えられたシナリオに基づき、ワイヤレスとRFベースの脆弱性を利用することができる。

- **エビルツイン**
  - Karma攻撃
  - ダウングレード攻撃
- **認証解除攻撃**
- **フラグメンテーション攻撃**
- **クレデンシャルハーベスティング**
- **WPS実行の弱点**
- **ブルージャッキング**
- **ブルースナーフィング**
- **RFIDクローニング**
- **ジャミング**
- **繰り返し**

3.4 与えられたシナリオに基づき、アプリケーションベースの脆弱性を利用することができる。

- **インジェクション**
  - SQL
  - HTML
  - コマンド
  - コード
- **認証**
  - クレデンシャル総当たり
  - セッションハイジャッキング
  - リダイレクト
  - デフォルトクレデンシャル
  - 脆弱なクレデンシャル
  - Kerberosのエクスプロイト
- **認可**
  - パラメータ汚染
  - 不安定なダイレクトオブジェクトのリファレンス
- **クロスサイトスクリプティング (XSS)**
  - 保存済み/永続性
  - 反射
  - DOM
- **クロスサイトリクエストフォージェリ (CSRF/XSRF)**
- **クリックジャッキング**
- **セキュリティミスコンフィギュレーション**
  - ディレクトリトラバーサル
  - Cookieの操作
- **ファイルのインクルード**
  - ローカル
  - リモート
- **安全でないコードプラクティス**
  - ソースコード内のコメント
  - エラー処理の欠如
  - 過度に冗長なエラー処理
  - ハードコードのクレデンシャル
  - 競合状態
  - 関数/保護されていないAPIの不正使用
  - 隠れた要素
    - DOMの機密情報
  - コード署名の欠如

3.5 与えられたシナリオに基づき、ローカルホストの脆弱性を利用することができる。

- **OSの脆弱性**
  - Windows
  - Mac OS
  - Linux
  - Android
  - iOS
- **セキュアでないサービスとプロトコルの設定**
- **特権エスカレーション**
  - Linux固有
    - SUID/SGIDプログラム
    - 安全でないSUDO
    - Ret2libc
    - スティッキービット
  - Windows固有
    - Cpassword
    - LDAPのクリアテキストクレデンシャル
    - Kerberoasting
    - LSASSのクレデンシャル
    - 無人インストール
    - SAMデータベース
    - DLLハイジャック
  - エクスプロイト可能なサービス
    - 引用されていないサービスパス
    - 書き込み可能なサービス
  - セキュアでないファイル/フォルダのアクセス許可
  - キーロガー
  - スケジュールされたタスク
  - カーネルエクスプロイト
- **デフォルトのアカウント設定**
- **サンドボックスエスケープ**
  - シェルのアップグレード
  - VM
  - コンテナ
- **物理的なデバイスのセキュリティ**
  - コールドブート攻撃
  - JTAGデバッグ
  - シリアルコンソール

3.6 施設に関連する物理的なセキュリティ攻撃を要約することができる。

- **ピギーバック/テールゲート**
- **フェンスジャンプ**
- **ダンプスターダイビング**
- **ロックピッキング**
- **ロックバイパス**
- **出口センサー**
- **バッジクローン化**

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。

- **Lateral movement**
  - RPC / DCOM
    - PsExec
    - WMI
    - スケジュールされたタスク
  - PSリモーティング/ WinRM
  - SMB
  - RDP
  - Apple Remote Desktop
  - VNC
  - Xサーバ転送
  - Telnet
  - SSH
  - RSH/Rlogin
- **持続性**
  - スケジュールされたジョブ
  - スケジュールされたタスク
  - デーモン
  - バックドア
  - トロイの木馬
  - 新しいユーザー作成
- **痕跡を削除する**

4.0 ペネトレーションテストツール

4.1 与えられたシナリオに基づき、Nmapを使って情報収集演習を実施することができる。

- **SYNスキャン (-sS) と全接続スキャン (-sT)**
- **ポートの選択 (-p)**
- **サービスID (-sV)**
- **OSフィンガープリンティング (-O)**
- **pingの無効化 (-Pn)**
- **ターゲット入力ファイル (-iL)**
- **タイミング (-T)**
- **出力パラメータ**
  - -oA
  - -oN
  - -oG
  - -oX

4.2 さまざまなツールの使用例を比較対照することができる。

(**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。)

- **用途**
  - 偵察
  - 列挙
  - 脆弱性スキャン
  - クレデンシャル攻撃
    - オフラインパスワードクラッキング
    - ブルートフォースサービス
  - 持続性
  - 構成の準拠
  - 回避
  - デコンパイル
  - フォレンジック
  - デバッグ
  - ソフトウェア保証
    - ファジー化
    - SAST
    - DAST
- **ツール**
  - スキャナー
    - Nikto
    - OpenVAS
    - SQLマップ
    - Nessus
  - クレデンシャルテストツール
    - Hashcat
    - Medusa
    - Hydra
    - Cewl
    - John the Ripper
    - Cain and Abel
    - Mimikatz
    - Patator
    - Dirbuster
    - W3AF
  - デバッガ
    - OLLYDBG
    - Immunity debugger
    - GDB
    - WinDBG
    - IDA
  - ソフトウェア保証
    - Findbugs/findsecbugs
    - Peach
    - AFL
    - SonarQube
    - YASCA
  - OSINT
    - Whois
    - Nslookup
    - Foca
    - Theharvester
    - Shodan
    - Maltego
    - Recon-NG
    - Censys
  - ワイヤレス
    - Aircrack-NG
    - Kismet
    - WiFite
  - Webプロキシ
    - OWASP ZAP
    - Burp Suite
  - ソーシャルエンジニアリングツール
    - SET
    - BeEF
  - リモートアクセスツール
    - SSH
    - NCAT
    - NETCAT
    - Proxychain
  - ネットワーキングツール
    - Wireshark
    - Hping
  - モバイルツール
    - Drozer
    - APKX
    - APK studio
  - MISC
    - Searchsploit
    - Powersploit
    - Responder
    - Impacket
    - Empire
    - Metasploit framework

4.3 与えられたシナリオに基づき、ペネトレーションテストに関連するツールからのアプトプットやデータを分析することができる。

- **パスワードクラッキング**
- **Pass-the-hash攻撃**
- **バインドシェルの設定**
- **リバースシェルの取得**
- **接続のプロキシ**
- **Webシェルのアップロード**
- **インジェクション**

4.4 与えられたシナリオに基づき、基本的なスクリプト（Bash、Python、Ruby、PowerShellに限る）を分析することができる。

- **ロジック**
  - ループピング
  - フローコントロール
- **I/O**
  - ファイルとターミナルとネットワーク
- **置換**
- **変数**
- **共通操作**
  - 文字列操作
  - 比較
- **エラーハンドリング**
- **配列**
- **エンコード/デコード**

5.0 報告とコミュニケーション

5.1 与えらえたシナリオに基づき、レポートの作成とベストプラクティスを使用することができる。

- **データの正規化**
- **発見と改善の報告書**
  - エグゼクティブサマリー
  - 方法論
  - 所見と改善
  - 指標と対策
    - リスク評価
  - 終了時
- **リスクアペタイト**
- **レポートの保存時間**
- **レポートの安全な取り扱いと処分**

5.2 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。

- **エンゲージメント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証明書を削除する
  - ツールを削除する
- **クライアントの受け入れ**
- **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**

5.3 与えられたシナリオに基づき、発見された脆弱性に対する軽減戦略を提案することができる。

- **ソリューション**
  - 人物
  - プロセス
  - テクノロジー
- **調査結果**
  - 共有ローカル管理者のクレデンシャル
  - パスワードの複雑さが弱い
  - プレーンテキストのパスワード
  - マルチファクタ認証なし
  - SQLインジェクション
  - 不要なオープンサービス
- **改善**
  - クレデンシャル/LAPSをランダム化する
  - 最小限のパスワード要件/パスワードフィルタ
  - パスワードを暗号化する
  - マルチファクタ認証を実装する
  - ユーザ入力のサニタイズ/クエリのパラメータ化
  - システムハードニング

5.4 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**
- **コミュニケーショントリガ**
  - 重要な発見
  - ステージ
  - 事前妥協の指標
- **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
  - 競合の解消
- **目標の再設定**

CompTIA PenTest+略語

下記はCompTIA PenTest+認定資格試験で使用される略語の一覧です。受験者には、試験準備の一環として、これら用語を復習し、理解することをお勧めします。

略語	詳細説明
ACL	Access Control List
ADFS	Active Directory Federation Services
AP	Access Point
API	Application Programming Interface
APNS	Apple Push Notification Service
APT	Advanced Persistent Threat
ASLR	Address Space Layout Randomization
BPA	Business Partnership Agreement
CA	Certificate Authority
CAPEC	Common Attack Patterns Enumeration Classification
CERT	Computer Emergency Response Team
CGI	Common Gateway Interface
CIFS	Common Internet File System
CIRT	Computer Incident Response Team
CORS	Cross-Origin Request Scripting
COTS	Commercial Off-The-Shelf
CRL	Certificate Revocation List
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
DFD	Data Flow Diagram
DLL	Dynamic Link Library
DNS	Domain Name Service
DOM	Document Object Model
DoS	Denial of Service
DTP	Dynamic Trunking Protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
EULA	End User License Agreement
FTP	File Transfer Protocol
GPO	Group Policy Object
GPP	Generic Packetized Protocol
GRE	Generic Routing Encapsulation
HSTS	HTTP Strict Transport Security
HTML	HyperText Markup Language

略語	詳細説明
I/O	Input/Output
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDOR	Indirect Object Reference
IoT	Internet of Things
IPS	Intrusion Prevention System
IV	Initialization Vector
JPCERT	Japan Computer Emergency Response Team
JTAG	Joint Test Action Group
LAPS	Local Administrator Password Solution
LFI	Local File Inclusion
LLMNR	Link-Local Multicast Name Resolution
LSASS	Local Security Authority Subsystem Service
MDM	Mobile Device Management
MFA	Multifactor Authentication
MITM	Man-in-the-Middle
MSA	Master Service Agreement
NAC	Network Access Control
NBNS	Net Bios Name Service
NDA	Non-Disclosure Agreement
NFC	Near-Field Communication
NIST	National Institute of NStandards and Technology
NOP	No Operation
NSE	Network Service Engine
OS	Operating System
OSINT	Open Source Intelligence
OWASP	Open Web Application Security Project
PII	Personally Identifiable Information
POS	Point of Sale
PS	PowerShell
RCE	Remote Code Executionl
RDP	Remote Desktop Protocol
RFI	Remote File Inclusion
RFID	Radio Frequent ID
RFP	Request for Proposal
ROE	Rules of Engagement
RPC	Remote Procedure Call
RSH	Remote Shell

略語	詳細説明
RTOS	Real Time Operating System
SAM	Security Account Manager
SAN	Subject Alternative Name
SAST	Static Application Security Testing
SCADA	Supervisory Control and Data Acquisition
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy
SDK	Software Development Kit
SGID	Set Group ID
SID	Secure Identifier
SIEM	Security Incident Event Manager
SLA	Service Level Agreement
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOC	Security Operation Center
SOW	Statement of Work
SPN	Service Principle Name
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
SUID	Set User ID
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOTP	Time-Based One-Time Password
TPM	Trusted Platform Module
TTP	Tactics, Techniques and Procedures
UDP	User Diagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Connection
VPN	Virtual Private Network
WADL	Web Application Description Language
WAF	Web Application Firewall
WAR	Web Application Archive
WEP	Wired Equivalency Protocol
WinRM	Windows Remote Management
WMI	Windows Management Instrumentation
WPAD	Web Proxy Auto-Discovery
WPS	WiFi Protected Setup
WSDL	Web Services Description Language
XSD	XML Schema Document
XSS	Cross-Site Scripting
XST	Cross-Site Tracing
XXE	External Entity

CompTIA PenTest+のハードウェアとソフトウェアのリスト

CompTIAでは、PenTest+認定資格試験の受験準備をされる方への参考用に、下記のハードウェアとソフトウェアのサンプル一覧を提示しています。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。

機材
- ラップトップ
- 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
- 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

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

ツール
- ロックピックキット
- バッジクローナ
- 指紋リフター

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
- 仮想マシンソフトウェア
- スキャンツール
- クレデンシャルテストツール
- デバッガ
- ソフトウェア保証ツール
- 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
- モビリティテストツール

CompTIA