

(CompTIA PenTest+)

CompTIA PenTest+は、ネットワーク上の脆弱性を特定、報告、管理するための実践的なペネトレーションテストを行うサイバーセキュリティプロフェッショナル向けの認定資格です。CompTIA CySA+が、インシデントの検出と対応による「防御」に重点を置いているのに比べ、CompTIA PenTest+は、ペネトレーションテストと脆弱性診断による「攻撃」に重点を置いています。これら2つの認定資格は、一見反するスキルのように見えますが、依存関係にあると言えます。サイバーセキュリティにおいて高いスキルを有するためには、これら2つの「防御」と「攻撃」の両方のスキルを備えている必要があります。CompTIA PenTest+試験については、[こちら](#)をご覧ください。

下記のコースを受講済み、または同等の知識を有する方

- [\(CompTIA Cybersecurity Analyst \(CySA+\)\)](#)

受講対象者

- ネットワーク上の脆弱性を特定、報告、管理するための実践的なペネトレーションテストを行うサイバーセキュリティプロフェッショナルを目指したい方。
- CompTIA PenTest+を取得したい方。

概要

効率的に作業を進めるためにフレームワークをカスタマイズし、結果を適切に報告すると共に、ITセキュリティ全般的な状態の改善を図るための戦略を提案できるスキルとベストプラクティスを育成します。

また、従来のデスクトップやサーバーに加えて、クラウドやモバイルなどの新しい環境でデバイスをテストするための実践的なスキルと知識も評価することが可能です。

本トレーニングでは、ペネトレーションテストの手法、脆弱性評価、また攻撃があった際のネットワークを回復するために必要となるスキルについて学びます。

CompTIA PenTest+に対応しています。

本トレーニングでは、The Official CompTIA PenTest+ Student Guide (Exam PTO-001) eBook (電子テキスト) を使用します。

本トレーニングでは、知識の補強および理解度向上のため、オンラインラボ (6か月間利用可能) を使用します。

目的

このコースを修了すると次のことができるようになります。

最新のペネトレーションテスト、攻撃に対するネットワークのレジリエンスを維持するために必要な脆弱性評価および管理

効率的に作業を進める上で必要な評価フレームワークをカスタマイズし、結果を適切に報告するためのスキル

セキュリティ管理上の弱点となりうる点への改善計画、実装、管理をするためのスキル

クラウドやモバイルなどの新しい環境でデバイスをテストを実施するための実践的なスキルと知識

アウトライン

Planning and Scoping Penetration Tests
Conducting Passive Reconnaissance
Performing Non-Technical Tests
Conducting Active Reconnaissance
Analyzing Vulnerabilities
Penetrating Networks
Exploiting Host-Based Vulnerabilities
Testing Applications
Completing Post-Exploit Tasks
Analyzing and Reporting Pen Test Results

各章にオンラインラボ（6ヶ月間利用可能）がついております。（コース中に全ての演習は取り扱いません）