コースコード：CO-PENTESTPLUS
税込価格：231,000円 (税抜価格：210,000円)
日数：3日間

トレーニング内容

CompTIA PenTest+は、システムの脆弱性を特定し、リスクを軽減し、これらを報告するスキルを評価します。クラウド、Webアプリ、API、IoTといった攻撃対象領域におけるペネトレーションテストの全段階を網羅し、脆弱性管理やラテラルムーブメントといった実践的なスキルを重視しています。CompTIA PenTest+は、ペネトレーションテスターやセキュリティコンサルタントとしてのキャリアアップに必要な専門知識を習得するのに役立ちます。

ここに注目!!

CompTIA PenTest+は3～4年間の ペネトレーションテスト、脆弱性評価、 および脆弱性管理の実践経験で得られる知識やスキルを目安に設計されています。サイバーセキュリティのキャリアパスにおいて、CompTIA CySA+と共に中級のスキルに位置されます。

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。

本トレーニングは、Pentest+認定の公式カリキュラム(5日間)と教材をベースに3日間に短縮しています。試験対策に特化したトレーニングではございませんのでご注意ください。

Pentest+試験の詳細については、こちらをご覧ください。

※本トレーニングでは、eBookとしてCompTIAの「CertMaster Study Pentest+ V3 (PT0-003) 日本語版」（12か月間利用可能）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、オンラインラボとしてCompTIAの「CertMaster Labs for Pentest+ 英語版」（12か月間利用可能）を使用します。
※受講された方を対象とした自主学習教材としてWeb確認問題(Let's Check)（6ヶ月間利用可能）が含まれます。
Web確認問題(Let's Check)につきまして、詳細はこちらをご覧ください。

ワンポイントアドバイス

受講対象者

このコースの受講対象者は次の通りです。

- Pentest+ 認定資格 (試験番号：PT0-003)の取得を目指す方

・3～4年の ペネトレーションテスト、脆弱性評価、
および脆弱性管理の実践経験で得られる知識やスキルと同等のレベルを証明したい方

前提条件

このコースを受講する前に受講者が習得しておく必要がある知識およびスキルは次のとおりです。

・セキュリティ関連業務の2～3年程度の経験

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 Security+ 任意、受講されていれば望ましい
CompTIA Cybersecurity Analyst (CySA+) 任意、受講されていれば望ましい

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。

・法的および倫理的な要件に準拠しながら、ペネトレーションテストの計画と範囲を策定し、是正措置の提案を含む詳細な報告書を作成して、プロジェクト管理を支援します。アクティブおよびパッシブな偵察を実施し、情報を収集し、システムを列挙して脆弱性を効果的に特定します
・脆弱性スキャンを実施し結果を分析、発見を検証してセキュリティ上の弱点を特定し、対応する
・適切なツールと技術を使用して、ネットワーク、ホストベース、ウェブアプリケーション、クラウドベースの攻撃を実行し、システム防御をテストする
・持続性を維持し、ラテラルムーブメントを実施し、発見を文書化して、ポストエクスプロイト活動中の是正措置を支援する

アウトライン

1. ペンテスト：始める前に
1.1 プロとしての行動とペンテスト
1.2 コラボレーションと対話
1.3 テストフレームワークと方法論概要
1.4 ペンテストのスクリプト入門

2. テスト活動前アクティビティの適用
2.1 範囲の定義
2.2 評価種別の比較
2.3 責任共有モデルの利用
2.4 法律的、倫理的考慮事項の特定

3. 列挙と偵察
3.1 情報収集技法
3.2 ホストとサービスの検出技法
3.3 攻撃計画のための列挙
3.4 特定資産の列挙

4. 脆弱性のスキャンと特定
4.1 脆弱性の検出技術
4.2 偵察スキャンと列挙についての分析
4.3 物理的セキュリティの概念

5. ペンテスト攻撃の実行
5.1 攻撃の準備と優先順位付け
5.2 スクリプトによる自動化

6. Webベースの攻撃
6.1 Webベースの攻撃
6.2 クラウドベースの攻撃

7. エンタープライズ攻撃
7.1 ネットワーク攻撃の実行
7.2 認証攻撃の実行
7.3 ホストベース攻撃の実行

8. 専用の攻撃
8.1 ワイヤレス攻撃
8.2 ソーシャルエンジニアリング攻撃
8.3 専用システムの攻撃

9. ペンテストタスクの実行
9.1 永続性の確立と維持
9.2 環境でのラテラルムーブメント
9.3 ステージングとデータ抽出
9.4 クリーンアップと復元

10. レポートと推奨事項
10.1 ペンテストレポートの構成要素
10.2 発見事項の分析と修復の推奨