コースコード：EC-CPENT
税込価格：759,000円 (税抜価格：690,000円)
日数：5日間

ここに注目!!

【CPENT (認定ペネトレーションテスティングプロフェッショナル) の特徴】

・高度なWindows攻撃
ADフォレストに侵入し、PowerShellの防御機能をバイパス（回避）したうえで、シルバー/ゴールデンチケット攻撃やKerberoasting（ケルベロースティング）を実行します。

・IoTシステムの攻撃
IoTデバイスを特定し、ファームウェアを抽出してリバースエンジニアリングを行います。

・フィルタ処理されたネットワークのバイパス
セグメンテーションアーキテクチャ内に構築されたWebゾーン型の演習環境において、ネットワークの分離ルール（セグメンテーションルール）を特定し、Webゾーンへ侵入および重要なデータの抽出を実行します。

・運用技術(OT)のペンテスト
ICS/SCADAネットワークへの侵入、PLCデータの操作、ならびにModbus通信の傍受について学習します。

・高度なバイナリエクスプロイト
欠陥のあるコードを見つけることは、有能なペンテスターには不可欠なスキルです。脆弱性のあるバイナリを特定してリバースエンジニアリングし、防御機能をバイパス（回避）しながら、32ビット/64ビットプログラム向けのエクスプロイトを作成します。

・ピボットを使用した隠れたネットワークへのアクセス
フィルタリングルールを特定し、ネットワークに侵入して、フィルター越しのシングルピボッティング（単一の踏み台経由）で隠れたセグメントへとピボットします。CPENTでは、互いに異なるネットワーク間でのピボットや、フィルタリング機器のバイパス（回避）が取り上げられます。

・ダブルピボット
CPENTは、ダブルピボット（2段階の踏み台経由）を使用して隠されたネットワークにアクセスする方法についても学習します。

・権限昇格
最新の権限昇格手法について学習します。また、コードをリバースエンジニアリングして実行制御を奪い、制限されたシェル環境を突破し、root／管理者権限を取得する課題も用意されています。

・スクリプトによる攻撃の自動化
Python、PowerShell、Bash、Metasploitを用いたスクリプト作成を習得し、ペネトレーションテストの自動化を実現します。

・エクスプロイトの武器化
カスタムツールを構築し、オフェンシブセキュリティの戦略を策定します。

・プロフェッショナルレポートを作成する
ペネトレーションテストの調査結果を効果的に文書化し、クライアントに実効性の高いセキュリティ改善策を提案するレポートの書き方を学習します。

受講対象者

このトレーニングはこのような方におすすめです。

攻撃技法を用いたセキュリティ検証を行う方
・ホワイトハッカー
・ペネトレーションテスター
・セキュリティーテスター

セキュリティ分析・助言を担う方
・情報セキュリティコンサルタント
・セキュリティアナリスト
・リスク評価専門家

防御・運用を担う技術者
・セキュリティエンジニア
・システム管理者

前提条件/前提知識

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。

EC-Council の CEH (Certified Ethical Hacker) 資格、または同等のスキルを有していること

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。

・高度なペネトレーションテスト技法を体系的に理解し、検証・評価・攻撃シナリオ設計などに活用できるようになる。
・攻撃者視点や最新の攻撃トレンドを理解したうえで、現実的なリスク評価や対策提案に活かせるようになる。
・攻撃者がどこを突くのかを理解し、防御設計や運用の精度を高められる。

アウトライン

ペネトレーションテストの基本概念

ペネトレーションテストのスコープとエンゲージメント

オープンソースインテリジェンス（OSINT)

ソーシャルエンジニアリングによる侵入テスト

Webアプリケーションへのペネトレーションテスト

APIおよびJava Web Tokenへのペネトレーションテスト

境界防御回避テクニック

Windowsの悪用と権限昇格

Active Directoryペネトレーションテスト

Linuxの悪用と権限昇格

リバースエンジニアリング、ファジング、バイナリエクスプロイト

ラテラルムーブメントとピボット

IoTペネトレーション

レポートの作成とテスト後のアクション