コースコード：EC-CPENT
税込価格：687,500円 (税抜価格：625,000円)
日数：5日間

トレーニング内容

このトレーニングでは、IoTシステム、OTシステムのペンテスト、独自のエクスプロイトの作成、ツールの構築、高度なバイナリエクスプロイト、隠しネットワークへのダブルピボットなど、様々な技術を習得することができます。
従来のペンテストのトレーニングとは異なり、複雑なネットワークに対して効果的な侵入テストを行う方法を学ぶことができる厳格なペンテスト・プログラムです。

・このトレーニングは、株式会社Armor Tech Labの開催となります
・受講後30日間視聴可能なプレイバック動画のZoom URLを提供いたします
・テキストは、オフラインでも閲覧可能な電子テキストと、印刷テキストを提供します
・コース初日の7営業前後に Armor Tech Lab社より、印刷テキスト送付先住所の確認メールが届きます
・受講料の中に受験料 (1回分) が含まれています。受験は後日、各自で申込みとなります
・コースの受講登録には、会社名、氏名（漢字およびローマ字）、E-mailアドレスが必要です。これらの登録情報は、EC-Council日本総代理店であるGSX社に提供いたします

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
PowerShellを使用して、シルバーとゴールドチケットとケロベロスティングを実行します。ここで高いスコアを得るにはPowerShellバイパス技術やその他の高度な方法を使用する必要があります。

・IoTシステムの攻撃
CPENTは世界で唯一のIoT攻撃を教える資格です。ネットワークに接続したら、IOT デバイスのファームウェアを識別し、それを抽出してリバースエンジニアリングする必要があります。

・フィルタ処理されたネットワークのバイパス
ほとんどの認定資格がトレーニングを行うフラットネットワークとは異なり、フィルタ処理されたネットワークを特定し、 Webアプリケーションにアクセスし、データを抽出します。

・運用技術(OT)のペンテスト
CPENTは、Modbus通信プロトコルを傍受し、PLCとそのスレーブノード間で通信することを可能にする世界初のペンテスト認証です。

・エクスプロイトを書く: 高度なバイナリ搾取
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が必要とするスキルです。複雑なタスクをこなし、欠陥のあるバイナリを見つけてリバースエンジニアリングし、プログラムの実行を制御するエクスプロイトを作成します。CPENTには32ビットおよび64ビットのコードチャレンジが含まれています。

・ピボットを使用した非表示のネットワークへのアクセス

横移動と、フィルタされたネットワークを通じてピボットする意味について説明します。ファイアウォールとフィルタリングルールを特定してから直接ネットワークに侵入する際には、単一のピボット方法を使用して隠しネットワークにピボットを試みる必要があります。

・ダブルピボット
CPENTは、ダブルピボットを使用して隠されたネットワークにアクセスする必要がある世界初の認証です。

・特権エスカレーション
特権エスカレーション手法をマスターして、ルート・アクセスを獲得します。

・防御メカニズムの回避
防御メカニズムによる保護をバイパスする方法を教えます。

・スクリプトによる攻撃の自動化
Ruby、Python、PowerShell、Perl、BASH、ファジー、およびメタスプロイトを使用した、7つの自己研究付録を使用して、高度な侵入テスト技術とスクリプト作成の準備をします。

・エクスプロイトを武器にする
自身のスキルをカスタマイズし、専門知識を活用し、課題に挑戦しましょう。

・プロフェッショナルレポートを作成する
クライアントにインパクトを与えるレポートの書き方を教えます。

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。

・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
・システムアドミニストレーター
・リスクアセスメントプロフェッショナル
・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
・セキュリティエンジニア
・SOCアナリスト

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。

・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。

・ペンテスターのプロフェッショナルとなる
・CPENT試験で70%以上の正解をし CPENT ホルダーとなる

・CPENT試験で90%以上の正解をし LPT (Licenced Penetration Tester) ホルダーとなる

【LPT (Licensed Penetration Tester)】
CPENTライブレンジ試験で90%を超えるスコアを獲得すると、CPENT認定を取得するだけでなく、ライセンス侵入テスター (LPT) マスター資格も取得できます。
LPT (マスター) とは、ネットワーク・ピボットの助けを借りて、エクスプロイト・コードを自分に有利に働かせたり、Bash、Python、Perl、Rubyスクリプトを書いたりして、多重防護ネットワーク・セキュリティ・モデルの鎧の隙間を見つけることができることを意味します。
CPENT試験は、自身の頭で考えることによる創造的なアプローチの実施により、従来の技術に依存しないことが要求されます。

【LPT (マスター) 認定プロフェッショナルの特徴】
・ペネトレーションテストに対する再現性と測定可能なアプローチの実証
・高度な手法と攻撃の実行による、WebアプリケーションのSQLインジェクション、クロスサイトスクリプティング(XSS)、LFI、RFIの脆弱性の特定
・専門的かつ業界で認められたレポートを提出し管理者と技術者の賛同を取得する
・EC-Council独自のペネトレーションテスト手法へのアクセス
・脆弱なシステム・アプリケーションにアクセスするためのエクスプロイトコードの作成
・Windows、Linuxなどのオペレーティングシステムの脆弱性の悪用
・権限エスカレーション実行による、システムへのルートアクセスの取得
・「既成概念にとらわれない」思考と「横方向」の思考
・完全にオンラインのリモート監督付き認定試験によるテストの完全性と価値の確保

アウトライン

ペネトレーションテストと手法の紹介

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

ネットワーク侵入テストー外部

ネットワーク侵入テストー内部

ネットワーク侵入テストー周辺機器

Webアプリケーションのペネトレーションテスト

ワイアレスペネトレーションテスト

IoTペネトレーションテスト

OT/SCADAペネトレーションテスト

クラウドペネトレーションテスト

バイナリ解析と活用

レポートの作成とテスト後のアクション