コースコード：CG-PTT2D
税込価格：550,000円 (税抜価格：500,000円)
日数：2日間

トレーニング内容

脆弱性診断やペネトレーションテストを行う際に必要不可欠となる知識やテクニックを習得します。具体的には、脆弱性やマルウェアに関する網羅的な知識をベースに、ペネトレーションテストを実施するために必要なサイバーセキュリティの実践的なスキルを習得することを目標とします。
本トレーニングでは、イスラエルのセキュリティエンジニア率いるレッドチームと連携し、仮想化技術で隔離され、安全に演習が実施できる環境下で、ペネトレーションテスト演習を行います。

ここに注目!!

『人材開発支援助成金事業展開等リスキリング支援コース』対象講座（受講費の最大75%以上が助成されます）

ワンポイントアドバイス

＜こんな方にオススメ＞
・社内セキュリティ担当部門として、ペネトレーションテスト・脆弱性診断の実践的なスキルを習得したい方
・社内システム開発担当としてセキュリティの品質管理に携わる方
・プログラミングの実務経験があり、セキュリティの知見を身に付けたい方

受講対象者

このコースの受講対象者は次の通りです。

IT担当者・情報セキュリティ担当者・SOCアナリスト・脆弱性診断士

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。

・セキュリティ業務部門で３年以上従事経験のある
・システム開発業務部門で３年以上従事経験のある
・インフラ構築業務部門で３年以上従事経験のある
・サイバージムの「Cyber-Threats and Defense Essentials」受講者または同等以上
・ネットワークおよび各種プロトコルの知識
・DBのしくみおよび、SQL文の知識
・Webアプリケーションのしくみおよび開発スキル
・Linuxの知識（コンソールによるコマンド入力操作は必須）

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。

的確な脆弱性やマルウェアに関する網羅的な知識をベースとしてペネトレーションテストを実施するための様々なツールや手法について習得します。
＜習得できるスキル＞
・ペネトレーションテストの計画から報告までの手法
・脆弱性に関する情報収集手法
・ツールを使用したペネトレーションテストの実施

アウトライン

下記PROGRAMのうち、★マークはオンデマンド（ビデオ）で事前に受講いただきます。
オンデマンド受講方法の詳細に関しましては、下記の『受講者向けガイドライン』をご参照ください。

受講者向けガイドライン

●オープニングセッション
・トレーニングの概要とスケジュール説明
●侵入テストの概要★
・侵入テストの背後にある動機
・ペンテスターとハッカーの違い
・情報収集プロセスの説明
・PTレポートを作成する方法論
・PT作業計画書を作成する方法論
・ペネトレーションテストの各種方法
●ネットワーク情報収集 ★
●ネットワーク情報収集 演習
●Web情報収集 ★
・Web情報収集による攻撃ポイント調査
●Web情報収集 演習
●Kali Linux ★
・ハッキングやサイバー攻撃に特化した Linux ディストリビューションの概要
●Kali Linux 演習
・Kali Linux の特別なハッキングツールを使用した実践的な経験
●Metasploit ★
・Metasploitの概要等
●Metasploit 演習
・Metasploitプラットフォームの特別なハッキングツールを使用した実践的な経験
●Webアプリケーションの脆弱性 ★
・最も一般的な攻撃
・Web アプリケーション ツール
・Web アプリケーション攻撃
●Web アプリケーション等の脆弱性 - PT 演習
・Web アプリケーションの脆弱性の特別なハッキング ツールを使用した実践的な経験
●クロージングセッション
・講習全体の総括と質疑応答

＜証書の発行＞
講座修了時に、受講者全員に受講証を発行いたします
修了試験において、正答率7割以上を達成された方に修了証を発行いたします

※トレーニングプログラムは一部変更になることがあります
※単独開催の場合には、お客様に応じてカスタマイズも承っております