コースの詳細

Ultimate Hacking: Expert

Foundstone® Services トレーニングコース

TM

この高度なコースは、従来とは異なる方法で現在のスキルをテストし、発展させていく機会を経験豊富なセキュリティ担当者に提供します。このクラスでは、高度な攻撃から組織を保護するために必要な最新の知識と防御を伝授するとともに、組織の最も重要な情報資産を保護する方法を説明します。業界有数のコンサルタントグループが講師を務めるこのコースは、現在使用可能な侵入テスト活用して最高レベルのトレーニングを提供します。

コースの目標

- 攻撃を特定して対応する
- カスタム脆弱性検出を作成する
- 高度な侵入テストを実施する
- 手動での Web アプリケーション評価手法
- 悪質なコードを理解し、作成する

トピックの概要

- ネットワーク監視
- 不正な監視
- ネットワーク偵察
- Metasploit の攻撃コードを使用した侵入テスト
- 高度な Web ハッキング
- データベースのハッキング
- Windows ルートキットとメモリ分析
- コードベースの脆弱性

対象者

- このコースは、マルウェアアウトブレークやネットワーク調査を担当するネットワーク管理者、企業セキュリティ担当者、監査担当者、警察官、コンサルタントを対象としています。

intel Security

コースの詳細

推奨する事前作業

受講者は、UNIX、Windows OS、コンピュータフォレンジック、TCP/IP ネットワーキングの高度な知識を習得している必要があります。また、弊社の「Ultimate Hacking」コースをすでに受講している方が対象になります。

コースの概要

モジュール 1—ネットワーク監視

- 監視と検出の事例
- ネットワーク監視ツールの高度な用法
- 完全なコンテンツとセッションデータの分析
- 侵入検知システム（IDS）の実装
- Snort の高度な機能と分析

モジュール 2—不正な監視

- ARP の理解
- スイッチドネットワークのスニッフィング
- 中間者（MITM）手法
- 一般的なツールと手法
- 一般的なプロトコルのインターセプトと修正
- カスタム中間者（MITM）攻撃の作成
- 対策

モジュール 3—ネットワーク偵察

- 最も一般的なツールの悪用と理解
- スキャンの手法
- 高度な OS とサービスの識別
- 高度なポートスキャンの手法
- カスタム偵察スクリプトの作成
- 効率的なスキャン
- 対策

モジュール 4—Metasploit の攻撃コードを使用した侵入テスト

- 検知の回避
- 進捗の追跡
- 列挙
- ブルートフォース攻撃
- ペイロードと攻撃後の処理
- Metasploit の高度な機能
- Metasploit の拡張
- 対策

モジュール 5—高度な Web ハッキング

- SQL インジェクションの概要
- SQL インジェクションの高度なトピック
- クロスサイトスクリプティング（XSS）の概要
- XXS の高度なトピック
- XSS フレームワーク
- クロスサイトリクエストフォージェリ（CSRF）
- 対策

モジュール 6—データベースハッキング

- データベースの検出とサービスの列挙
- 一般的な構成ミス
- データベースのコンテンツの列挙
- MSSQL ストアド（および Extended ストアド）プロシージャ
- データベースを通じた OS とのやりとり（シェルショベリング）
- 対策

コースの詳細

モジュール 7—Windows ルートキットとメモリ分析

- ルートキットの概要
- Windows ルートキットの使用
- Windows メモリ分析
- Windows ルートキットの検出と削除
- 対策

モジュール 8—コードベースの脆弱性

- コンピュータアーキテクチャ、メモリ、データ構造の基礎知識
- 静的コード解析
- デバッガを使用した潜在的な脆弱性の発見
- バッファオーバーフロー攻撃の作成
- その他のタイプのコードベースの脆弱性の理解
- 対策

To order, or for further information, please call 1 888 847 8766 or email SecurityEducation@intel.com.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com