コースの詳細

Ultimate Hacking

Foundstone® Services トレーニングコース

TM

Ultimate Hacking コースでは、新しいモジュール、新しい悪質コード、新しいハッカー技法を使用したネットワークとアプリケーションの効率的な攻撃/防御方法を習得します。高い評価を得ている実践的な講義環境で、ステップバイステップの攻撃実行方法、侵入テストの実行方法、インターネット/イントラネットネットワークおよびホストレベルシステムでの攻撃のブロック方法を学習できます。こうしたセキュリティ技法と手法の活用方法を学ぶことにより、重要な内部/外部資産を悪質な脅威から積極的に保護できるようになります。

コースの目標

- 攻撃を特定して対応する
- 侵入テストを実施する
- 脅威から内部/外部資産を保護する

トピックの概要

- フットプリンティング
- スキャン
- 列挙
- システムハッキング（Windows）
- システムハッキング（UNIX）
- Web ハッキング

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

このコースで得られる成果を最大限に高めるには、UNIX、Windows OS、コンピュータフォレンジック、TCP/IP ネットワーキングに関する基本的な知識が必要です。

コースの概要

モジュール 1—フットプリンティング

- 概要
- 範囲の決定
- 適切な権限の取得
- 公表されている情報
- WHOIS と DNS の列挙
- DNS の問い合わせ
- ネットワーク偵察

モジュール 2—スキャニング

- ホスト検出
- サービス検出
- オペレーティングシステム—検出

モジュール 3—列挙

- バナーグラビング
- 脆弱性スキャン
- Metasploit について

モジュール 4—システムハッキング（Windows）

- ネットワーク列挙
- ホスト列挙
- 列挙の対策
- 侵入
- 拡大する影響
- 侵入の対策
- 特権エスカレーション攻撃
- 特権エスカレーションの対策
- 略奪
- 略奪の対策
- 拡大する影響の対策
- クリーンアップ（形跡の隠匿）

モジュール 5—システムハッキング（UNIX）

- UNIX/Linux の概要
- 列挙
- 列挙の対策
- 侵入の対策
- 特権エスカレーション攻撃
- 特権エスカレーションの対策
- 略奪
- 略奪の対策
- 拡大する影響
- 拡大する影響の対策
- クリーンアップ（形跡の隠匿）

モジュール 6—Web ハッキング

- e コマースアーキテクチャの概要
- HTTP/HTTPS 入門
- 検出
- 構成管理
- 承認
- セッションの処理
- データの検証
- OWASP Top

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