コースコード：GX-CSTN
税込価格：220,000円 (税抜価格：200,000円)
日数：2日間

ここに注目!!

本トレーニングの目的や概要を以下から動画でご覧いただけます。
SecuriST「脆弱性診断士」ご紹介 (グローバルセキュリティエキスパート社YouTubeチャンネル)
※動画投稿時からアップデートがある可能性がございます。トレーニングの最新情報は本ページ記載内容をご参照ください。

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。

・脆弱性診断の技術を身につけたいが、何から初めて良いか分からないといった悩みを持っている企業や組織の方
・脆弱性診断の内製化に取り組みたい開発会社、脆弱性診断の要員を育成したい開発会社やセキュリティ関連サービス会社の方
・イントラネット／インターネット向けのネットワークシステムに関わる方
・ネットワークシステムのセキュリティ要件の定義を行う方、ネットワークシステムの評価を行う方
・ネットワークシステムの構築担当者、テスト担当者、品質管理の担当者

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。

・Windows 、Linuxなど OSのインストール経験のある方
・ホームルーターなど簡単なネットワーク機器の設定を行った事がある方

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。

・ネットワークシステムの脆弱性に関する知識を習得する
・「どの範囲まで」「どのレベルまで」、脆弱性を探せば適切なのか?判るようになる
・脆弱性を発見するための手段やツールに関する知識を習得する
・発見した脆弱性がどの程度のリスクなのか 、判別することができる

アウトライン

ネットワーク脆弱性診断の基礎知識

診断対象となるシステムについて

診断で得られる情報

診断についての推奨事項

診断実行者の役割と責任

フットプリンティング／OSINT

公開された情報のチェック

OSINT (Open Source Intelligence)

IPアドレスの登録情報

DNS、WHOIS、命名規則

検索エンジン、GHDB

公式Webサイト

DNS環境のチェック

ポートスキャン／ネットワークスキャン

ポートスキャン／ネットワークスキャンの目的

スキャン実行後の対応

診断対象リストの作成

スキャンの実行

スキャンとファイアウォール

アカウントの検査

アカウント名の列挙

認証強度の確認

デフォルトアカウント・パスワード

パスワードクラッカー

セキュリティスキャナー

- セキュリティスキャナーの機能
- セキュリティスキャナーの問題点
- セキュリティスキャナーの使い方
- 発見した脆弱性の存在を確認

レポート

- 診断報告書に関する要件
- 報告書の内容
- 脆弱性情報の情報源
- 脆弱性の深刻度の評価