情報処理安全確保支援士特定講習　講習情報

ＮＥＣマネジメントパートナー株式会社

サイバー攻撃トレーニング　－Ｒｅｄ　Ｔｅａｍ　Ｔｒａｉｎｉｎｇ－

実施機関名	ＮＥＣマネジメントパートナー株式会社		
講習名	サイバー攻撃トレーニング　－Ｒｅｄ　Ｔｅａｍ　Ｔｒａｉｎｉｎｇ－		
特定講習番号	22-004-029		
講習形態	リモート形式	定員（１回あたり）	24 名
受講日数	1 日間	受講時間	6.5 時間
受講料	88,000（円/税込み）		

対象分野 <ITSS+（セキュリティ領域）>	主な分野	脆弱性診断・ペネトレーションテスト	関連分野

講習内容	あらかじめ用意された演習用システムに対し、レッドチーム（攻撃を実践する側）である受講者がサイバー攻撃をおこなうことで、ペネトレーションテストに必要な技術を養います。また、攻撃者の着目点や攻撃手法を修得し、防御策の策定に活かします。
具体的な到達目標	以下の能力を身に付け、ペネトレーションテスト、また防御策の策定に活かせるようになる。 ・攻撃者のネットワーク探索手法を説明することができる。 ・サーバ攻略における攻撃者の着目点を説明することができる。 ・ネットワーク攻略における攻撃者の着目点を説明することができる。
修得できるスキル	・ポートスキャンスキル ・ペネトレーションテストツールの実行スキル ・Windowsネットワーク探索スキル ・脆弱性実証コードを使用した具体的な脆弱性診断スキル
講習の理解・習得のために推奨される実務経験	・組織における情報システム、ネットワーク運用管理経験があることが望ましい ・Linuxサーバ構築または運用経験があることが望ましい ・Windowsサーバ構築または運用経験があることが望ましい
講習の理解・習得のために推奨される知識・技術	・代表的な攻撃手法　（事前調査、権限取得、不正実行、感染拡大） ・ポートスキャン、攻撃に利用されるWindowsコマンドに関する知識 ・KALI Linuxに関する知識、Metasploit Flameworkの知識 ・Webアプリケーション脆弱性に関する知識
技術・知識の到達度の把握・測定方法	・実習操作状況把握のため、画面のモニタリングやヒアリングをおこなう。 ・グループワークの際は各グループを巡回（ヒアリングを含む）して状況を把握する。 ・グループワーク後の発表内容、質疑応答内容の妥当性を確認する。
修了認定の判断基準	・出席率３／４以上、かつ以下を総合的に審査し決定する。 ①グループ作業およびディスカッションへの参加度合い（発言状況、関与度） ②実習課題において行ったペネトレーション作業が正しい解釈で合理的な内容となっているか ③実習中の講師による進捗、取組み状況、課題、方針などの確認に対する回答が妥当性を有しているか
修了認定基準に満たない受講者への措置	修了と認められない場合には、受講者へ通知の上、修了の認定をおこなわない。
受講者に対するサポート体制	・常時チャット、音声による質問を受付ける。 ・講師が各グループを巡回して状況を把握し、必要に応じて追加説明・アドバイスをおこなう。 ・発表内容や質疑応答内容において理解度に不安のある場合には、詳細な解説や個別に補足説明をおこなう。
講習実施施設所在地	東京都港区芝浦
ホームページ	https://www.neclearning.jp/courseoutline/courseId/SN436/