コースコード：VER-IOTHACK
税込価格：396,000円 (税抜価格：360,000円)
日数：3日間

トレーニング内容

初級～中級者向けの、IoTデバイスに対するハンズオン中心のセキュリティトレーニングです。

これまで100を超えるIoTデバイスの調査・テスト実績を有するエンジニアが、そのノウハウをもとに、Wi-Fiルーターを通じてソフトウェア／ハードウェア解析をはじめとした基礎的なIoTハッキング手法を受講者が体験することで、機器の脆弱性について理解を深められるトレーニングを提供します。
また、車載ECUを模擬したソフトウェアを通じて基礎的なCANのハッキング手法を体験することで、ECUの脆弱性についても理解できます。

3日間のトレーニングで「組込みデバイスへのハッキング」、「ファームウェアに対するリバースエンジニアリング」、「バイナリエクスプロイト」、「CANプロトコルへのハッキング」など多くのトピックを学べます。

ここに注目!!

ワンポイントアドバイス

本トレーニングの受講にPCが必要となります。当日はPCをご持参ください。
受講に必要なPCの詳細スペックは下記をご参照ください。
PCをご準備いただくことが難しい方向けに、当社にてレンタルPC（有償）のご提供が可能です。
お申し込み時にお知らせください。（レンタル費用1台11,000円（税込））

【受講に必要なPC環境】
・OS Windowsのみ（Windows11を推奨）
・メモリ 最低8GB（16GB以上を推奨）
・HDD 50GB以上の空き容量
・OSの管理者権限があるユーザでログインできること
・USBメモリの読み込みができること
・USBポートが2つ以上
・ウィルス対策ソフトウェアを管理者権限で停止、解除ができること
・無線LANアダプタ（会場の無線LANに接続可能なこと）※無線規格：IEEE802.11a/b/g/n/ac
・VMwareもしくはVirtualBoxをインストール可能であること。
※VMwareもしくはVirtualBoxが、快適に動作可能な環境が必要であること。

受講対象者

このコースの受講対象者は次の通りです。

・IoTデバイスおよびIoTシステムのセキュリティについて学びたいとお考えの方

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。

・一般的なOS、コンピュータ・アーキテクチャ、ネットワーキングに関わる基本的な知識
・IoTに関する基本的な知識
・Linuxの基本操作のご経験がある方

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。

・デバイスファームウェアの抽出と分析
・バイナリのデバッグと逆アセンブル
・UART、SPI、JTAGの悪用、JTAGのデバッグとそれを用いたエクスプロイト
・ファームウェアのダンプ、ハードウェアとソフトウェアのデバッグ
・IoTデバイスのクラウドやモバイル機能への攻撃
・スニッフィング、リプレイ、MITM、無線通信による攻撃、BLEによるエクスプロイト
・ARMとMIPSのリバースエンジニアリング、従来型攻撃と非従来型攻撃の手法
・プラットフォームへの攻撃、 など

アウトライン

主な講座内容
1日目
IoTセキュリティの基礎を説明した後に、実際のIoTデバイスに対して、既知脆弱性を使用したサイバー攻撃に関する基本的なテクニックを学びます。
・IoTセキュリティアーキテクチャーの内部概念
・既知のIoTデバイスの脆弱性（ケーススタディ）
・IoTデバイスのファームウェア取得とリバースエンジニアリング

2日目
実際のIoTデバイスを分解して、回路基板の持つコンポーネントを理解し、基板のサイバー攻撃に関する基本的なテクニックを学びます。また、車載ネットワークの基礎を説明いたします。
・回路基板のコンポーネントとデバイスルートの取得
・UARTのエクスプロイト
・車載ネットワークの内部概念

3日目
車載を模擬したシミュレーション環境にて、車載ネットワークのサイバー攻撃に関する基本的なテクニックを学びます。
・CANバスの盗聴および再送攻撃
・UDSプロトコルを用いた攻撃

主な習得内容
・IoTデバイスへ基礎的な攻撃
・デバイスファームウェアの抽出と分析
・バイナリのデバッグと逆アセンブル
・ファームウェアのダンプ、ハードウェアとソフトウェアのデバッグ
・IoTデバイスの通信機能への攻撃
・車載ネットワークの基礎知識
・CANバスの盗聴、再送攻撃

・UDSプロトコルを用いた攻撃の一例 その他

※ 当日の進行状況により、内容変更の可能性がございます。