ONLY HUMANS CAN COUNTER HUMAN-DRIVEN THREATS

TRAINING AND EXERCISE

CyberDefense

新型コロナウイルス感染症への対策について

サイバーディフェンス研究所は、受講者様、社員の安全と、感染拡大防止のために、下記の対策を実施致します。

- 講師のマスクの着用
- 会場入室時の検温
- 消毒液の配置
- アクリル板の設置
- お席の除菌作業
- ソーシャルディスタンスの確保
（通常2名でご利用頂くテーブルを1名様でご利用頂きます。）

トレーニングにご参加頂く受講者様におかれましては下記取組みにご協力をお願い致します。

- マスクの着用をお願いいたします。
- 休憩時に手洗い/うがいの徹底をお願いします。
- 入室時に発熱、風邪症状などの体調不良が見られる場合、入室をお断りすることがございます。

ご協力のほど、何卒よろしくお願い申し上げます。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

護る力をその手に。

ハッキング、フォレンジック、マルウェア解析をハンズオンで学ぶ。
セキュリティエキスパートの育成を目的とした、実戦的なトレーニングコース。

コース紹介

■ ハッキング

攻撃者の視点、思考を学ぶハンズオンセミナーです。Webアプリケーションやネットワークに対して実際の攻撃を体験することによって、攻撃の仕組みを深く理解します。

- **コースラインナップ**
  Webアプリケーション｜ネットワーク｜
  Binary Exploit Fundamentals ｜ハードウェアハッキング
- **対象者**
  セキュリティ技術者｜サイバー犯罪捜査官など

■ セキュリティ診断（オンライン開催）

セキュリティ診断実施に必要診断スコープの策定、診断方法、レポートの書き方まで、診断の実施に必要な知識と技術を網羅的に習得することができます。

- **コースラインナップ**
  Webアプリケーション診断｜ネットワーク診断
- **対象者**
  セキュリティ技術者｜脆弱性診断担当者など

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

トレーニング概要（2）

■ フォレンジック

本コースは、法執行機関のフォレンジック担当者やサイバー犯罪捜査官向けに最適化されており、コースマテリアルの一部はインターポールの教育にも活用されています。

- **コースラインナップ**
  メモリフォレンジック｜
  犯罪捜査とアクター分析のためのOSINT｜
  Oxygen Forensic Detectiveによるデータ解析
- **対象者**
  法執行機関のフォレンジック担当者など

■ プログラム解析

検体の収集方法から解析手法までを学ぶマルウェア解析コース、アセンブリ言語に対する理解を深めることにより高度なマルウェア解析やプログラム解析技術を身に付けることを目的としたコースなどをご用意しています。

- **コースラインナップ**
  マルウェア解析I｜マルウェア解析II
- **対象者**
  インシデントレスポンス担当者｜サイバー犯罪捜査官など

開催形式とスケジュール

随時オープンコースを開催しています。スケジュールは弊社のWebサイトを御確認下さい。また、１社限定のプライベートコースの開催や内容のカスタマイズも承りますのでお気軽にご相談下さい。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

Hands-on

■ コース概要

SQLインジェクション、クロスサイトスクリプティング、ファイルインクルージョン、デフォルト設定の弱点等を実際に発見し攻撃を体験することで、ハッカーの視点からWebに対するセキュリティへの理解を深めます。

昨今多発するWebを介した情報漏洩や不正アクセスに対する実戦的な対処能力を身につけることを目的としたトレーニングプログラムです。

■ 履修対象者

サイバー犯罪捜査官｜Webアプリケーション開発者｜システム管理者
ネットワーク管理者｜セキュリティスペシャリスト など

■ 必要なスキル

Windows / Linuxのコマンドを使用します。

■ セミナー情報

期間：2日間｜10:00 – 18:00
（プライベート開催も可能です。お問い合わせ下さい。）
定員：１１名（最小開講人数：５名）
教材：日本語
価格：209,000円（税込）
会場：サイバーディフェンス研究所トレーニングラボ

■ コースの内容

1. イントロダクション

Webサーバ攻略の作戦

2. Webアプリケーションの構成

Webアプリの主な要素と脆弱性 / グーグル検索

3.ブラウザのセキュリティ

Webブラウザの脆弱性

4. HTTPSのセキュリティ

HTTPSの機能と概念 / HTTPSの技術的脆弱性 / 人的要素による脆弱性

5. Webサーバのハッキング

問題ある設定のWebサーバの攻略 / 情報の露出 / Webサーバ特定の脆弱性

6. SQLインジェクション

SQLインジェクションの技術 / データベースの攻略

7. ファイルインクルージョン

ファイルインクルージョンとは / ファイルインクルージョンの実行

8. クロスサイトスクリプティング

クロスサイトスクリプティング技術 / サイトのハイジャック / セッションハイジャック / ネットワークの脆弱性への攻撃 / HTMLの概念と脆弱性

※ コース内容はカリキュラム改善の目的で予告なく変更される場合があります。予めご了承ください。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

Hands-on

■ コース概要

ブラックボックスハッキングによるミッション形式の実習により、実際のネットワークに対して、受講者が自ら攻撃対象の脆弱なポイントを見つけ出し、攻撃を試行します。

また、ソーシャルエンジニアリングを含むハッカーの思考を体験することにより、現実の攻撃にも柔軟に対応できる実戦的な対処能力を身につけることを目的としています。

■ 履修対象者

サイバー犯罪捜査官｜システム管理者ネットワーク管理者｜セキュリティスペシャリスト など

■ 必要なスキル

Windows / Linuxのコマンドを使用します。

■ セミナー情報

期間：2日間｜10:00 – 18:00

（プライベート開催も可能です。お問い合わせ下さい。）

定員：１１名（最小開講人数：５名）

教材：日本語

価格：209,000円（税込）

会場：サイバーディフェンス研究所トレーニングラボ

■ コースの内容

1. サイバー攻撃の歴史

2. 侵入手順

3. 標的の情報収集

インターネットサービス登録情報 / ドメイン名登録情報 / 命名規則 / 電子メールの利用 / 検索エンジンの利用 / Webサイトの分析

4. ソーシャル・エンジニアリング

手口と心理的な罠 / 人的ファクタ / ポリシーの重要性

5. 匿名性の確保

シェル及びプロキシのセオリ / 匿名プロキシ / シェルの第三者中継 / TOR(オニオンルータ) / I2P

6. 標的の特定

ポートスキャン / 脆弱性スキャン / 既知の脆弱性

7. 攻撃手段

Exploit/ ルートキット

8. リモートアクセス

Webリモート管理 / PRC / リモートデスクトップ

9. パスワードハッキング

ブルートフォース / 辞書攻撃、レインボーテーブル / ライブセッション

※ コース内容はカリキュラム改善の目的で予告なく変更される場合があります。予めご了承ください。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

Binary Exploit Fundamentals

Hands-on

■ コース概要

このトレーニングでは、メモリ破壊の脆弱性を利用したリモートからのシェル起動という一連のプロセスを通して攻撃者視点でのBinary Exploitationの考え方に触れていただきます。

脆弱性攻撃の古典的なシナリオの把握から、総合演習では様々な手法や考え方を組み合わせたフルスクラッチでのExploit開発を体験することができます。なお、本トレーニングではLinux環境で動作するプログラムに対する演習を実施します。

■ 履修対象者

- ●サイバー犯罪捜査官
- ●法執行機関のサイバーテロ対策担当者
- ●法執行機関のフォレンジック担当者
- ●脆弱性再現のためのPoCの解析や記述をする必要のある方
- ●Exploit開発をする必要のある方

■ 必要となるスキル

基礎的なLinux端末でのオペレーション

-Linux端末でのCUI操作

-SSH等のプロトコルを利用したリモート環境への接続

プログラミングの知識

-CやC++でのプログラムの記述（ポインタや構造体がわかる）

-PythonやRuby等の軽量言語でのスクリプトの記述

ネイティブコードのリバースエンジニアリング

-逆アセンブリの読解（CPUアーキテクチャは問わず）

-デバッガによるプログラムのデバッグ・解析経験

■ コースの内容

1. Binary Exploitationの概要

   Binary Exploitationでできること

2. Binary Exploitationの考え方

   プログラムを解析する

   Exploitの方針を立てる

   メモリ破壊を利用してメモリを読み書きする

   Buffer Overflow, Use-after-Free, Buffer Over-read, ...

   プログラムの制御を奪う

   リターンアドレスの上書き, GOT Overwrite, ...

   保護機構による影響とそのバイパスを考える

   DEP, SSP, ASLR, PIE, ...

   目的とする操作を行う

3. 総合演習

■ セミナー情報

期間：3日間｜10:00 – 18:00

費用：412,500円/（税込）

定員：10名（最小開講人数：５名）

会場：サイバーディフェンス研究所トレーニングラボ

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

ハードウェアハッキングトレーニング

Hands-on

■ コース概要

本コースは、ハードウェアハッキングに必要となる基礎的な知識とテクニックを習得するためのハンズオントレーニングコースです。

ハッキング対象のハードウェアの技術仕様に関する情報収集から、ロジック・アナライザ等を用いた通信の盗聴・解析、ファームウェアのダンプ、取得したファームウェアの解析まで一連の技術を習得することを目的としており、チップオフやはんだ付けなども体験することができます。

制御システムを始め、様々なIoTのサイバーセキュリティに関与する技術者、防衛装備品などの特殊なデバイスのセキュリティに関与する技術者、法執行機関のフォレンジック担当者にとって有用な知識とスキルの獲得が可能なトレーニングコースです。

■ 履修対象者

サイバー犯罪捜査官｜法執行機関のフォレンジック担当者｜重要インフラのシステム管理者｜セキュリティスペシャリスト

■ セミナー情報

期間：2日間｜10:00 – 18:00

（プライベート開催も可能です。お問い合わせ下さい。）

定員：１０名（最小開講人数：5名）

教材：日本語

価格： 550,000円（税込）

会場：サイバーディフェンス研究所トレーニングラボ

■ コースの内容

1. ハードウェアデバイスへの攻撃に関する基礎知識

   組込みシステムの構成

   組込みシステムでよく使用されるプロトコル

2. 対象デバイスに関する情報収集

   デバイスの回路構成の推定

   攻撃起点の見極め

3. UART通信の概要

   UARTのタッピングと解析

4. JTAGを用いたファームウェアの動的解析

5. ファームウェアの奪取

   SPIフラッシュの取り外しと読み出し

   eMMCの取り外しと読み出し

   読み出したファームウェアの解析

■ 前提知識

・Linux端末でのCUI操作（Windowsは使用しません。LinuxのCUI使用経験の無い方の参加はご遠慮ください）

■ 推奨スキル

・はんだ付け（趣味の電子工作レベルで問題ありません）

※ コース内容はカリキュラム改善の目的で予告なく変更される場合があります。予めご了承ください。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

Hands-on

■ コース概要

本コースは、組織内でWebアプリケーションの脆弱性診断に取り組むために必要な攻撃技術の知識、診断技術や脆弱性判定の基準などを身につけることを目的としています。

セキュアなWebシステム／Webアプリケーション構築に必要な脆弱性診断技術、実施方法やツールの使い方、レポートの書き方などを、実践・実習を通して具体的に学んで頂きます。また、脆弱性診断を身につけてもらうために理解が必要な、昨今のWebに対する脅威や攻撃の具体例なども学んで頂きます。

■ 履修対象者

脆弱性診断のノウハウを身につけたい方｜Webアプリケーション開発者
セキュリティスペシャリスト など

■ セミナー情報

期間：2日間｜10:00 – 18:00
（プライベート開催も可能です。お問い合わせ下さい。）
定員：２０名（最小開講人数：５名）
教材：日本語
価格：209,000円（税込）
会場：オンライン開催（Zoom使用）

■ コースの内容

1. Webアプリケーションの脅威とその攻撃手法
2. Webサイトへの攻撃とその特徴
3. Webアプリケーションへの攻撃手法

   クロスサイトスクリプティング（XSS） / クロスサイトトレーシング（XST） / SQLインジェクション / ディレクトリトラバーサル / OSコマンドインジェクション / HTTPヘッダインジェクション / セッションハイジャック / クロスサイトリクエストフォージェリー（CSRF） / パスワード攻撃 / 強制ブラウズ / その他の攻撃手法について

4. 脆弱性診断の基準

   Webアプリケーション脆弱性診断概要 / 脆弱性診断の診断方法と脆弱性の有無の判定方法 / 脆弱性診断の診断対象の選び方 / 脆弱性診断のレポートの記載方法とポイント

5. 脆弱性診断の実施

   診断ツールの使い方 / 各脆弱性に対応した診断方法 / 実際の診断業務を想定した実習

※ コース内容はカリキュラム改善の目的で予告なく変更される場合があります。予めご了承ください。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

セキュリティ診断｜ネットワークコース（オンライン開催）

Hands-on

■ コース概要

ネットワークシステムのセキュリティ上の弱点を発見するには、セキュリティスキャナーなどのツールによる診断は効果的な方法の1つです。しかし、セキュリティスキャナーで発見できる問題は全体の一部だけです。実際の攻撃者はもっと多くの情報を収集し、あなたのシステムを攻撃しようとします。

本コースでは、セキュアなネットワークシステム構築に必要な脆弱性診断技術、実施方法やツールの使い方、リスクの算出方法などを、実践や実習を通して具体的に学んで頂きます。

■ 履修対象者

脆弱性診断のノウハウを身につけたい方｜システム管理者｜ネットワーク管理者｜ネットワークの構築に関わる方｜セキュリティスペシャリスト など

■ セミナー情報

期間：2日間｜10:00 – 18:00
（プライベート開催も可能です。お問い合わせ下さい。）
定員：２０名（最小開講人数：５名）
教材：日本語
価格： 209,000円（税込）
会場：オンライン開催（Zoom使用）

■ コースの内容

1. ネットワーク脆弱診断の基礎知識
2. フットプリンティング
   公開された情報のチェック / DNS環境のチェック
3. ポートスキャン
   ポートスキャナーの使用方法 / ポートスキャンによる検査
4. アカウントの検査
   ユーザアカウントの列挙 / 認証強度の確認
5. セキュリティスキャナー
   セキュリティスキャナーによる既知の脆弱性診断 / 攻撃実現可能性のチェック / Webアプリケーションセキュリティスキャナーによる簡易診断
6. レポート
   発見した脆弱性について

※ コース内容はカリキュラム改善の目的で予告なく変更される場合があります。予めご了承ください。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

フォレンジック｜メモリフォレンジック

Hands - on

■ コース概要

サイバー攻撃やサイバー犯罪の発展、増加に伴い、コンピュータに搭載されているディスクだけでなく、メモリを適切に保全し、解析することが求められています。

メモリフォレンジックのための環境は整ってきており、実際の調査でも活用出来る状況です。一方でOSのアップデートに伴いメモリ管理の構造が変更されるなどの理由により、解析者がメモリや解析ツールの仕組み、動作を理解して複数の手法やツールを使いこなす必要があります。

本コースでは、メモリフォレンジック分野の現状やメモリ関連の基礎/原理を学びつつ、ハンズオンを通して実践的なスキルを身につけていきます。

主にオープンソースおよびフリーツールを用い、Windowsのメモリを対象とします。

■ 履修対象者

サイバー犯罪捜査官｜サイバーテロ対策担当者｜組織のCSIRTメンバー
ネットワーク管理者｜システム管理者｜インシデントレスポンス担当者 など

■ セミナー情報

期間：2日間｜10:00 – 18:00
（プライベート開催も可能です。お問い合わせ下さい。）
定員：１０名（最小開講人数：５名）
教材：日本語
価格：209,000円（税込）
会場：サイバーディフェンス研究所トレーニングラボ

■ コースの内容

フォレンジック

1. メモリ基礎
2. メモリ保全（基礎）
3. カービングベースの解析
4. メモリイメージ解析ツール
5. メモリイメージ変換
6. Windows システム基礎 / 解析
7. Windows アーティファクト解析
8. パスワード / 暗号解析

マルウェア解析

1. マルウェア解析におけるメモリ解析
2. Windowsマルウェア解析
3. 高度なマルウェア検知

■ 前提知識

・フォレンジック調査やインシデント対応の経験またはノウハウがある
・コマンドプログラムの利用/操作が出来る
・VirtualBoxの操作が出来る

※ コース内容はカリキュラム改善の目的で予告なく変更される場合があります。予めご了承ください。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

フォレンジック｜Oxygen Forensicによるスマートフォン解析コース

Hands-on

■ コース概要

本コースは、Oxygen Forensics社製のOxygen Forensic Detectiveをお使いのユーザ、もしくはこれから導入を検討しているユーザを対象としたトレーニングコースです。

スマートフォンのデータ抽出から解析までフォレンジック調査を行う上で必要な同製品の基本的な知識を2日で学ぶコースとなります。

■ 履修対象者

法執行機関の捜査官やフォレンジック担当者

※本コースは官公庁限定コースです。官公庁職員の方以外は受講いただけません。

■ セミナー情報

期間：2日間｜10:00 – 18:00
（プライベート開催も可能です。お問い合わせ下さい。）

定員：１１名（最小開講人数：５名）

教材：日本語

価格：受講費用　209,000円（税込）
Oxygen Forensic Detectiveとのセット割引もご用意しています。

会場：サイバーディフェンス研究所トレーニングラボ

■ **コース内容**

1. スマートフォンにおける初動対応
2. スマートフォンにおけるフォレンジック
3. Oxygenの概要と基本操作
4. Oxygen Forensicによるデータ解析

解析例

- ◆ デバイス所有者が使用するアカウントを知りたい
- ◆ デバイス所有者のWeb閲覧履歴や検索履歴を知りたい
- ◆ デバイス所有者が送受信したメッセージ内容を知りたい
- ◆ デバイス所有者の行動履歴を知りたい
- ◆ デバイス所有者が撮影/収集した画像や動画を検索したい
- ◆ とにかく事件に関係するキーワードが証拠品に記録されていないか探したい
- ◆ 共犯者や犯罪グループとの繋がりを解明したい

5. その他の機能（Cloud Extractorなど）
6. SQLite3データベース
7. Androidデバイスからの証拠保全
8. iOSデバイスからの証拠保全

OXYGEN FORENSIC

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

犯罪捜査とアクター分析のためのOSINT（官公庁限定コース）

Hands-on

■ コース概要

サイバースペースにおいて安全なOSINT（Open Source Intelligence：公開情報に基づく調査）を行う知識とテクニックを体系的に学ぶトレーニングコースです。

本コースは、法執行機関の犯罪捜査官、インテリジェンス組織や防衛組織のリサーチャー、ダークウェブやアンダーグラウンドコミュニティと接触する必要のある方を主な対象者として想定しています。

OSINTを行うための環境構築から、業務を遂行するときに必要となるセキュリティ対策、自己匿名化などOSINT業務の担当者自身の情報を相手に提供しないための対策を意識しながら安全にリサーチを行うテクニック、ディープウェブ、ダークウェブを含むアンダーグラウンドコミュニティとの関わり方、流出データや仮想通貨の分析、脅威アクター特定のためのリサーチ手法をハンズオンで学びます。

本コースを受講することによって、情報分析、犯罪捜査とアトリビューションに有効かつ安全なOSINTテクニックを習得することができます。さらに副次的な効果として犯罪者が自分自身の秘匿化のために利用しうる技術を把握することができます。

■ セミナー情報

期間：2日間｜10:00 – 18:00

（プライベート開催も可能です。お問い合わせ下さい。）

定員：１０名（最小開講人数：５名）

教材：日本語

価格：209,000円（税込）

会場：サイバーディフェンス研究所トレーニングラボ

■ 前提知識

・コンピュータ（OS）やネットワークの基本を理解している

・基本情報技術者試験の取り扱い内容の知識を備えている

・Linuxの基本操作経験がありコマンド入力に抵抗がない

■ 履修対象者

法執行機関の犯罪捜査官｜インテリジェンス組織のアナリスト｜防衛組織のリサーチャー｜官公庁の脅威分析担当者｜官公庁でダークウェブやアンダーグラウンドと接触する方

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

犯罪捜査とアクター分析のためのOSINT（官公庁限定コース）

Hands-on

■ コースの内容

1．秘匿化・匿名化の基本

自己秘匿化・匿名化とは / アイデンティティの作り方 / サーチを行う場所 / False Flag(偽陽性)

2．環境構築

自己匿名化のための環境構築

3．秘匿化・匿名化に便利なサービス

VPNサービスの選び方 / メールサービスの選び方（end to end 暗号化メール） / その他の通信経路

4．連絡手段

メッセンジャーの選び方 / メッセンジャーの使い分け / XMPP / PGP / メッセンジャーの利用

5．仮想通貨

ウォレットのセットアップ / 入手方法 / 匿名化

6．アンダーグラウンドコミュニティ

ダークウェブ・アンダーグラウンド概要 / ダークウェブの探索 / ディープウェブの探索

7．リサーチの実践

アンダーグラウンドコミュニティ分析 / 流出データ分析 / 仮想通貨の分析 / アクター分析

※ コース内容はカリキュラム改善の目的で予告なく変更される場合があります。予めご了承ください。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

マルウェア解析 I

Hands-on

■ コース概要

本コースは、マルウェア感染が疑われるインシデントが発生した際の実践的な対処方法を身につけることを目的としたトレーニングコースです。

マルウェアの解析に必要な知識を基礎から学び、ハンズオンでの検体解析をとおして、実戦的なマルウェア解析技術を習得することを目的とします。

■ 履修対象者

サイバー犯罪捜査官｜法執行機関のフォレンジック担当者｜インシデントレスポンス担当者｜セキュリティスペシャリスト

■ 必要なスキル

基本情報処理技術者試験合格相当の知識

システム/ネットワークの運用経験

プログラミング経験

■ セミナー情報

期間：2日間｜10:00 – 18:00

（プライベート開催も可能です。お問い合わせ下さい。）

定員：１０名（最小開講人数：５名）

教材：日本語

価格： 209,000円（税込）

会場：サイバーディフェンス研究所トレーニングラボ

■ コースの内容

1. マルウェア概論

   マルウェアの種類 / マルウェアの挙動 / 侵入経路 / 昨今のマルウェア

2. マルウェア解析概論

   解析環境 / 解析手法 / 解析観点 / 耐解析機能

3. マルウェア解析

   解析手法 / 解析ツール / 挙動の確認（プロセス・ファイル・レジストリ・ネットワーク）/ 動的解析

4. 悪性文書ファイル解析

   解析手法 / 解析ツール / 難読化されたスクリプトの解析 / 動的解析

5. 最終演習

   実際のインシデントを想定したマルウェアの解析

※ コース内容はカリキュラム改善の目的で予告なく変更される場合があります。予めご了承ください。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

マルウェア解析 II

Hands-on

■ コース概要

本トレーニングでは、ハンズオン形式によるマルウェア解析を通じて、マルウェアの解析の際に必要となる基本的なリバースエンジニアリング技術について学びます。

モニタツールによる動的解析では解析できないような、マルウェアが潜在的に有する機能や通信プロトコルを解析できるようになることを目的としています。

■ 履修対象者

サイバー犯罪捜査官｜法執行機関のフォレンジック担当者｜インシデントレスポンス担当者｜セキュリティスペシャリスト

■ 必要なスキル

Windows OSの基本的な知識

C言語についての基本的な知識およびプログラミング経験

■ セミナー情報

期間：2日間｜10:00 – 18:00

（プライベート開催も可能です。お問い合わせ下さい。）

定員：１０名（最小開講人数：５名）

教材：日本語

価格： 209,000円（税込）

会場：サイバーディフェンス研究所トレーニングラボ

■ コースの内容

1.リバースエンジニアリングの基礎

静的解析と動的解析の特徴／コンパイラの挙動

2.アセンブリ言語基礎

命令のフォーマット／レジスタ／メモリ／スタック／数値の表現

3.IDAの使用法

IDAの各ウインドウの特徴・使用法

4.x86命令解説

主要な命令の解説

5.リバースエンジニアリングのためのC言語

C言語とアセンブリ言語の関係性／各構文との対応

6.Windows API基礎

ファイル操作／レジストリ操作／コマンド実行・プロセス関連／メモリ管理・コードインジェクション／ソケット通信／HTTP通信

7.演習

※ コース内容はカリキュラム改善の目的で予告なく変更される場合があります。予めご了承ください。

 Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

Contact Information

サイバーディフェンス研究所
事業推進部
TEL : 03-5843-9015｜FAX : 03-5843-9016
email : sales@cyberdefense.jp