EC-Council

Top Out Human Capital

CEH（認定ホワイトハッカー）ご紹介資料

セキュリティエンジニア養成講座＆国際認定資格

C|EH™
Certified Ethical Hacker

Top Out Human Capital 株式会社

CEHトレーニングコースの特長

1

学習効率重視：講習とハンズオン演習を組合わせたカリキュラム

① 講義＋演習形式で、短期間で一気に知識ベースを作り上げる
② 実際の攻撃をすぐに演習環境で実施体験

2

網羅的かつ体系的に、現実の攻撃テクニックを学べる

セキュリティエンジニアやホワイトハッカーになるために大変なのは、

IT分野の広い知識と経験： ITシステム運用全般の理解＋セキュリティ＋考え方

3

記憶が定着する！手が動く！コース終了後も半年間

オンライン演習環境iLabsが使用可能：教わった事をすぐに試せる
様々な環境、いろいろなシナリオが体験でき、多面的な理解に直結

CEH v10コースモジュール概要(1)

20モジュール で トレーニングが構成

1. ホワイトハッキングの紹介
サイバー攻撃の動向やインターネット環境の概況について。また攻撃者が狙うポイントとは？ハッキングとは？ハッカーとは？そのテクニックの全体像とは？といった基本概念を学びます。

2. フットプリンティングと調査
ハッカーが標的を狙う際、下調べとして攻撃対象に関する弱点を探るため個人や企業・団体などの情報（フットプリント）を収集します。その内容や具体的なテクニックについて学びます。

3. ネットワークの診断
ハッカーは標的の調査として、さらにネットワークの状況を調べます。オペレーティングシステム・システムアーキテクチャや稼働しているホスト、実行されているサービスまたその脆弱性などを検索するテクニックを学びます。

4. 列挙（Enumeration）
侵入した攻撃者は、次にシステムからユーザ名、マシン名、ネットワークリソース、共有、およびサービスを抜き取り、さらに深い攻撃プロセスに移ります。ここでは攻撃者がLDAPなどの様々なサービスに問い合わせを実行して、攻撃に使用できる有効なユーザー名、アドレスなどの情報を収集するテクニックを学びます。

5. 脆弱性解析
今までの調査や列挙の手法をさらに推し進め、脆弱性を悪用するための調査手法を学びます。脆弱性の調査だけでなく、評価・分析の手法、役立つソリューションやツールを通じて、脆弱性を管理する側、悪用して攻撃する側、それぞれの考え方を理解し体得します。

6.システムハッキング
今までの調査や列挙により、システムハッキングに必要な情報は集まりました。ここからは遂にシステム本体に致命的な攻撃を行います。認証突破から権限昇格攻撃、主力マルウェア（攻撃アプリケーション）の実行、ファイルの隠蔽や証拠の隠滅等、ハッキングコアとなるテクニックを学びます。

7. マルウェアの脅威
マルウェアの種類や利用方法や挙動、隠蔽のためのラッピング手法や、検体からのリバースエンジニアリング、どうやって伝播させるか？といった流布テクニックまで、ハッキングの主力武器となるマルウェアを詳細に紹介します。

8. スニッフィング
盗聴器をしかけるようにスニッフィングツールを使用して、ネットワークを通過するデータパケットを監視し、キャプチャすることでトラフィックを分析できます。スニッフィングに脆弱なプロトコルや分析手法を学びます。

9. ソーシャルエンジニアリング
あらゆる物理的・人間的・詐欺的な技術を用いて秘密情報を開示するよう人々を操る方法について学びます。ソーシャルエンジニアリングでよく狙われるターゲットとしては、ヘルプデスク担当者、技術サポートエグゼクティブ、システム管理者などが挙げられます。標的が自分の貴重な情報について意識していない、またその保護への注意が足りないという事実につけ込むテクニックです。

10. サービス拒否（DoS）
サービス拒否/不全を起こさせるDoS/DDoSのテクニックを学びます。DoSの概念や各種ツールだけでなく、ボットネットを利用した攻撃方法についても学びます。

11. セッションハイジャック
難易度の高い攻撃ですが、パケットの流れを監視する事でTCPのセッションを乗っ取り、情報の抽出やコマンドインジェクション、ソーシャルエンジニアリング（詐欺）などの危険な攻撃を実行できます。攻撃者が使うこれらのテクニックについて学びます。

V10からの新モジュール

CEH v10コースモジュール概要(2)

20モジュール で トレーニングが構成

12.ファイアウォール、IDS、ハニーポットの回避
境界防御として実装されているファイアウォールやIDS、ハニーポット等の防御システムを回避し、進入する方法について学びます。様々な種類のファイヤウォールの動作やハニーポットの原理を理解し、どのように突破するか？を理解します。

13. Webサーバのハッキング
Webサーバはインターネット上に公開され、どこからでも攻撃が可能で、さらに膨大な脆弱性が存在するため防御が難しく、攻撃側からは絶好のターゲットとなります。これらWebサーバに対しての様々な攻撃手法を学びます。

14. Webアプリケーションのハッキング
Webサーバ上に実装されるWebアプリケーションは、脆弱性スタックによりWebサーバ単独よりもさらに攻撃ポイントが増えています。構成ミス、インジェクションの欠陥、クロスサイトスクリプティング等、弱点となるポイントや攻撃テクニックから、Webアプリ全体のハッキングメソッドまでを学びます。

15. SQLインジェクション
Webアプリケーションに対する攻撃の中でも代表的かつ、多くの攻撃方法を持つSQLインジェクションをさらに深く理解するため、その概念から全体図、詳細なテクニックまでを学びます。

16.ワイヤレスネットワークのハッキング
既に一般的になっているワイヤレスネットワークに対しての攻撃手法を学びます。認証方法や暗号化方法、WEPだけでなくWPAに対するハッキング手法や、Bluetoothへのハッキングも学びます。

17.モバイルプラットフォームのハッキング
iOSやAndroid、WindowsPhone等への攻撃手法を学びます。マルウェアやルート化だけでなく、WiFi/Bluetoothを使った攻撃やアプリケーションのサンドボックス化回避、アプリストアを利用した攻撃手法など、トレンドに沿った内容を理解します。

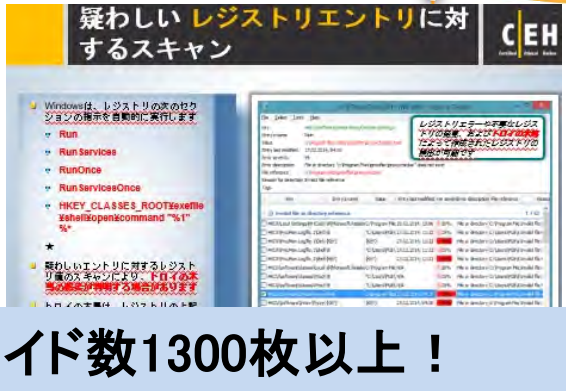
18. IoTハッキング
IoTデバイスは今や重要インフラの一部となっています。設定ミスや脆弱性があった場合、IoTは個人データやプライバシーだけでなく、身体的な安全性にとって今までにない重大なリスクをもたらします。Webカメラ、自動車、工業機器、ドアロックなど、インターネットに接続されているスマートデバイスを侵害するためにIoTの技術を理解し、そのハッキング方法について学びます。

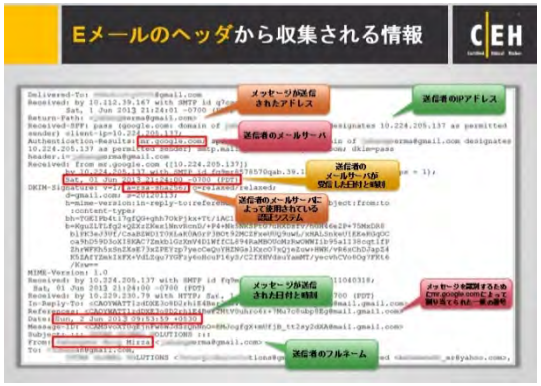
19.クラウドコンピューティング
利用が拡大するクラウド環境において、攻撃も激化しています。クラウドの構成モデルやアーキテクチャを理解し、仮想化技術がどのように使われ、どのような弱点を持つかを学びます。Webアプリのモジュールで学んだように、常時インターネットに接続され、複数のサプライチェーンが組み合わさるクラウド環境では、Webアプリの脆弱性スタックよりさらに大きなスタックとなり、脅威の種類は膨大になります。

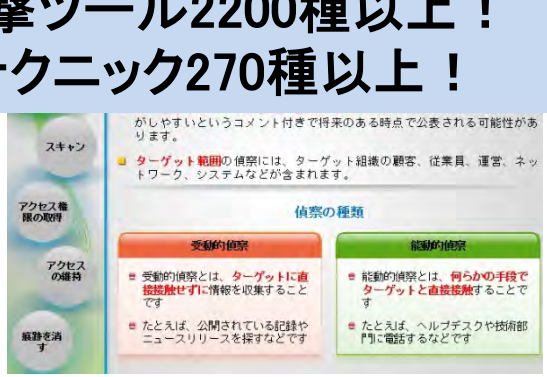
20.暗号技術
様々存在する暗号化技術の中から、攻撃対象に使われる技術について学びます。それぞれ暗号を解読するツールやテクニックを使いながら、攻撃者は暗号解読に際し、基本的な考え方として「暗号解読者が暗号化された情報にアクセスする」という仮定に基づいて攻撃を行うという事を理解します。

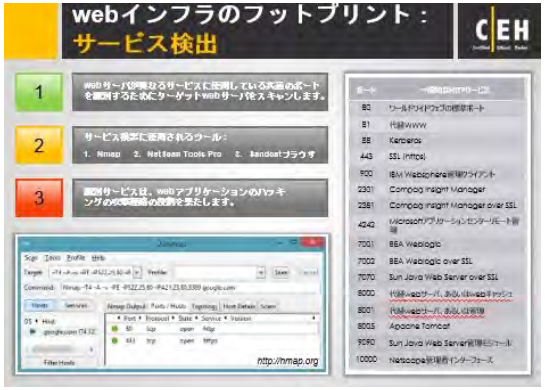
V10からの新モジュール

テキストサンプル







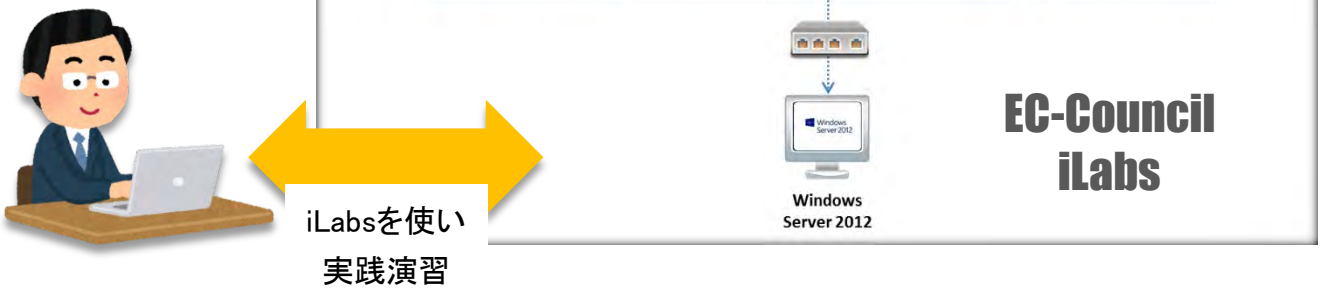


スライド数1300枚以上！
登場攻撃ツール2200種以上！
攻撃テクニック270種以上！

演習環境【 iLabs 】（アイラボ）

様々な環境を想定した、独自のトレーニングシステムです。

利用者毎に完全に分離された、**手軽で安全な攻撃できる演習環境**を提供いたします。



攻撃対象サイト

課題シナリオ

100種類以上

iLabsには、各種OS環境・ネットワーク環境ならびに、有償・無償の攻撃/解析ツールなどが使用でき、また演習頂くための多数の課題シナリオを有しています。

面倒な検証環境の準備やセットアップが不要で、インターネットに繋がっていればオフィスや自宅から**いつでも、どこからでもご利用頂けます。**

CEHトレーニングコース対象者の要件

知識・スキルレベルについて

■下記の内容が理解できれば問題ありません(予習推奨)

1. CCNAレベルのネットワークに関する内容
2. LPIC Level1程度のLinuxに関する内容
3. 企業で導入されているFirewallなどネットワーク・セキュリティ機器の構成に関する内容
4. 下記ツールの使い方
   - Wireshark や tcpdump
   - nmap
   - ローカルプロキシ（Burp Suite、Owasp Zed Attack Proxy、Fiddler）

■下記の様な実務経験があると講座内容がより理解しやすくなります

- プログラミング(C/Perl/Java/PHP)
- ネットワーク構築
- ネットワークトラブルシュート
- パケット解析
- ペネトレーションテスト

日本人講師/日本語テキストですので、英語力は不要です。

費用および資格取得までの流れ

5日間：9:30 - 17:30
専用日本語テキスト（CEHv10）
演習用仮想空間（i-Labs）6ヶ月間利用権
EC-Council 認定試験1回（コース受講後 約1年有効）
【受講費用(税抜)】¥498,000- / 1人

５日間の受講

５日間、CEHコースを受講頂きます。

受講後トレーニング

ご自宅やお客様オフィスからインターネット接続にてiLabsにアクセス頂き、課題トレーニングをして頂きます。

試験　1年以内に受験が必要

トップアウトヒューマンキャピタル東京会場にて受験頂きます。試験時間は4時間、Webで4択問題にご回答を頂きます。
試験は月1回程度実施。残念ながら合格できなかった場合には、再受験可能（再試験代80,000円）

資格の維持　合格後

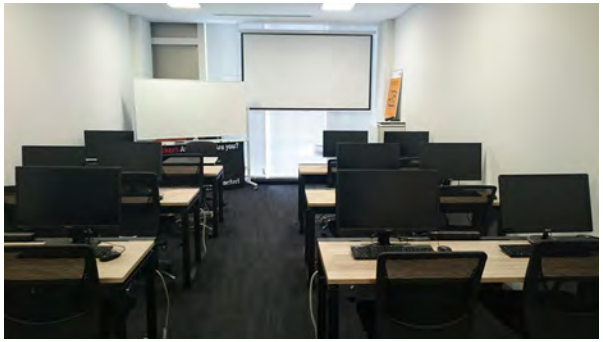
資格の有効期間は合格後3年間です。情報セキュリティに関する活動を報告することで、資格維持延長が可能となるプログラム「ECE Scheme」がございます。3年間で120ポイント以上で承認、さらに3年間資格が維持延長される仕組です。（※EC-Councilメンバーシップへの加入は年会費$80-）

トレーニング＆試験会場(東京開催の場合)

※近隣の別会場開催の場合もあります

〒108-0014
東京都港区芝5丁目29番20号
クロスオフィス三田

アクセス
- 都営地下鉄 三田線/浅草線
  三田駅 A3出口から徒歩3分
- JR田町駅から徒歩5分




Top Out
Human Capital