



EC-Council



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



Top Out Human Capital 株式会社

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

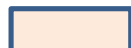
あらゆる物理的・人間的・詐欺的な技術を用いて秘密情報を開示するよう人々を操る方法について学びます。ソーシャルエンジニアリングでよく狙われるターゲットとしては、ヘルプデスク担当者、技術サポートエグゼクティブ、システム管理者などが挙げられます。標的が自分の貴重な情報について意識していない、またその保護への注意が足りないという事実につけ込むテクニックです。

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ア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。

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。

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つた場合、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。

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。

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。

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。

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。

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。

20. 暗号技術

様々な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



ソーシャルネットワーキングサイトで 入手できる情報

The diagram illustrates the types of information that can be obtained from social networking sites, categorized by the user type and the platform used.

Attacker (攻撃者) - Information Obtainable (取得できる情報):

- 連絡先情報、住所など (Contact information, address, etc.)
- 友達のリスト、友達の情報など (List of friends, information about friends, etc.)
- 所属組織の特定 (Identification of the affiliated organization)
- 興味対象 (Interests)
- アクティビティ (Activities)

User (ユーザー) - Actions (行動):

- プロフィールの管理 (Profile management)
- 友達とつながる、チャット (Connect with friends, chat)
- 写真とビデオの共有 (Sharing photos and videos)
- ゲームで遊ぶ、グループに参加する (Playing games, joining groups)
- イベントの作成 (Event creation)

Organization (組織) - Actions (行動):

- ユーザーの認識 (User recognition)
- 製品の販促 (Product promotion)
- ユーザーサポート (User support)
- 人事採用 (Recruitment)
- 従業員の任用のための背景調査 (Background check for employee hiring)

Attacker (攻撃者) - Information Obtainable (取得できる情報):

- ビジネス戦略 (Business strategy)
- 製品プロフィール (Product profile)
- ソーシャルエンジニアリング (Social engineering)
- プラットフォーム/テクノロジー情報 (Platform/technology information)
- ビジネスのタイプ (Business type)

Platforms (Social Networking Sites):

- Facebook (f)
- LinkedIn (in)
- Weibo (weibo)
- Twitter (t)
- Google+ (g+)

アイデンティティの盗み方


元のアイデンティティ・スティーブン・チャールズ
住所: San Diego CA 92130

Steven Charles Den
5 DD A3D456789

スティーブン・チャールズ

注: ここに示すイラストは、典型的なアイデンティティ盗犯のまよっては、これが当てはまる場合と当てはまらない場合がありま

疑わしいレジストリエントリに対 するスキャン




Windowsは、レジストリの次のセクションの表示を自動的に実行します

- Run
- Run Services
- RunOnce
- RunServicesOnce

HKEY_CLASSES_ROOT\System\AlternateShell\opencommand "%1" %*

★ 疑わしいエントリに属するレジストリ値の読み込みや実行により、ドメインのセキュリティを侵害する可能性があります



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！

[illegible][illegible]

The diagram is divided into two main sections. The top section, titled '情報収集の手段' (Methods of Information Gathering), contains three overlapping circles: 'スキャン' (Scan) in blue, 'アクセス権限の取得' (Acquisition of Access Rights) in green, and 'アクセスの維持' (Maintenance of Access) in red. The bottom section, titled '偵察の種類' (Types of Reconnaissance), contains two boxes: '受動的偵察' (Passive Reconnaissance) in orange and '能動的偵察' (Active Reconnaissance) in green. The orange box lists two points: ① 受動的偵察とは、ターゲットに直接接触せずに情報を収集することです (Passive reconnaissance is the collection of information without direct contact with the target) and ② たとえば、公開されている記録やニュースリリースを探すなどです (For example, searching for publicly available records or news releases). The green box lists two points: ① 能動的偵察とは、何らかの手段でターゲットと直接接触することです (Active reconnaissance is direct contact with the target by some means) and ② たとえば、ヘルプデスクや技術部門に電話するなどです (For example, calling the help desk or technical department).


情報収集の手段

- スキャン
- アクセス権限の取得
- アクセスの維持
- 痕跡を消す

偵察の種類

- 受動的偵察**
 - ① 受動的偵察とは、ターゲットに直接接触せずに情報を収集することです
 - ② たとえば、公開されている記録やニュースリリースを探すなどです
- 能動的偵察**
 - ① 能動的偵察とは、何らかの手段でターゲットと直接接触することです
 - ② たとえば、ヘルプデスクや技術部門に電話するなどです

webインフラのフットプリント： サービス検出



1

Web サーバが提供するサービスに依存している既知のポートを照会するためにソケット web サービスをスキャンします。


2






サービス検出に依存されるツール：
1. Nmap 2. NetSec Tools Pro 3. Nessus/ナラサ

3

既知サービスは、web アプケーションのフットプリントの検出の基盤と見なします。

ポート	サービス (IANA/IANA)
80	ハイパーテキスト転送プロトコル
81	代用 WWW
8080	Kerberos
443	SSL (HTTPS)
9000	Microsoft 管理用クライアント
2381	Compaq iManager Manager
2321	Compaq iManager Manager over SSL
4242	Microsoft アダプティブセンターポート管理
7002	BEA WebLogic
7003	BEA WebLogic over SSL
7070	Sun Java Web Server over SSL
8000	HTTP 代理サーバー、または Nmap のポート
8001	HTTP 代理サーバー、または Nmap のポート
8006	Apache Tomcat
9090	Sun Java Web Server 管理用クライアント
10000	Nessus/ナラサ管理用クライアント



	アンチウイルス技術の回避	CEH
01	トロイの木馬ファイルを複数の断片に分割し、1つのファイルとして圧縮処理します	
02	常に自分自身のトロイの木馬を書き込み、アプリケーションに組み込みます	
03	トロイの木馬の情文を変更します <ul style="list-style-type: none"> EXEを可逆圧縮ソフトに変換する EXE圧縮ソフトは DOC、EXE、PPT、EXE、または PDF、EXE に変換する (3つのソフトの組合せ、Windows は「既知の既読子」を登録表にためるため、DOC、PPT、および PDF のみが登録されます) 	
04	<u>バイナリエディタを使用してトロイの木馬のコンテンツを変更し、さらにチェックサムを変更してから、ファイルを再編成します</u>	
05	web からダウンロードしたトロイの木馬を決して使用しません (これらのファイルはアンチウイルスによって簡単に検出されてしまうからです)	

webサービス攻撃



- webサービスの進化やビジネスでのwebサービス使用の増加は、アプリケーションフレームワークに新たな攻撃ベクトルを提供しています。
- webサービスは、接続ポイントを記述するためのWeb Services Definition Language (WSDL)、webサービスの記述および発見のためのUniversal Description, Discovery, and Integration (UDDI)、そしてさまざまなウェブアプリケーションの身元に対して脆弱なwebサービス間の通信のためのSimple Object Access Protocol (SOAP) に基づいています。



プロセッシング層

XML, AJAX, Portal, その他

セキュリティ層

WS-Security

ディレクトリ層

UDDI, WSDL

アクセス層

SOAP, REST

トランスマンション層

HTTP, HTTPS, JMS, その他

パラメータの改ざん、WSDLのプロキシ、SQL注入、DoSなどのMITM、フィッシング、クロスサイトスクリプティング、マルウェアインジェクション、ブルートフォース、データ漏えい等。コンテンツ管理システム、セッション管理など、文字列の改ざん、偽造も注意。

コードリーク、アクセス可能なAPIを公開するエラーページ、誤ったログが漏洩する危険性。

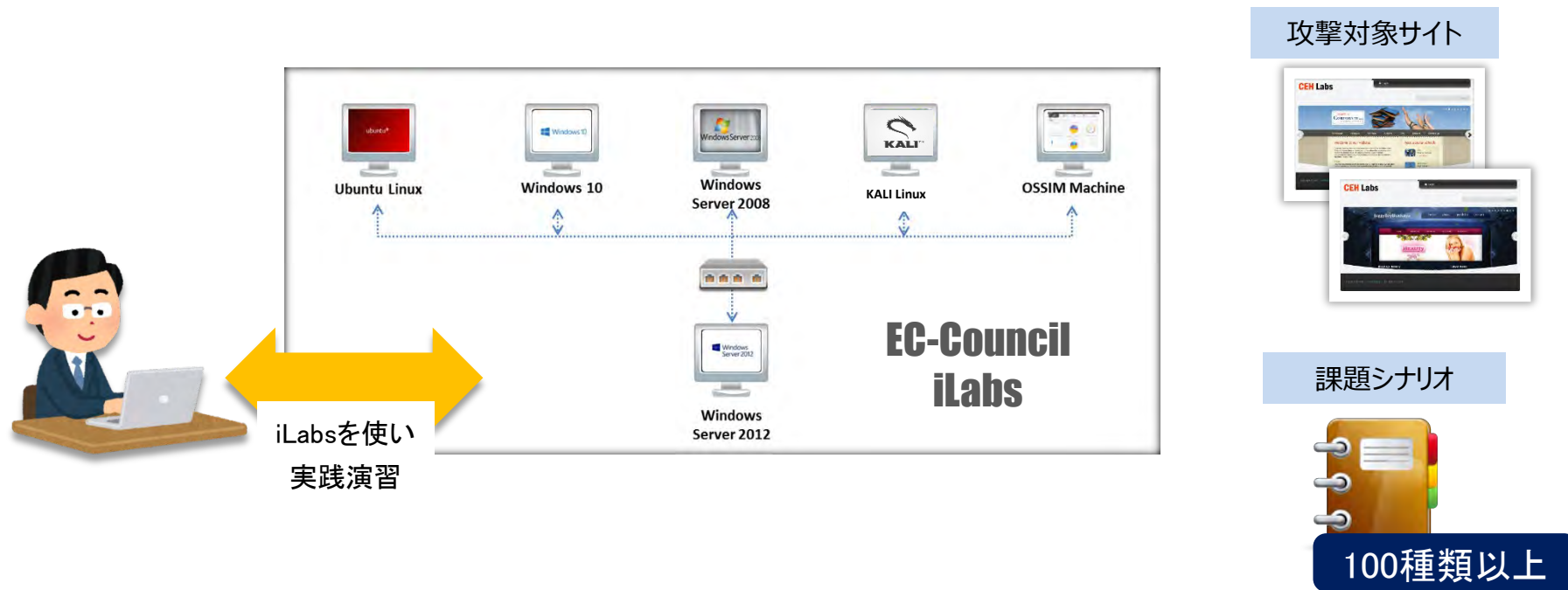
パフォーマンステストフレーム、XML攻撃、スレームの攻撃、標準またはカスタムXMLスキーマ、DoS、未知なゼロデイロッド。

スピアフィッシング、なりすまし、WS-Routing、サブプロセス、サービスタグging。

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。



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ティング
- ・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みです。(※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

