CEHv12 の特徴

新しい技術を追加

CEHv11 から 12 にバージョンアップを行い、新しい技術が追加されています。

- MITRE ATT&CK フレームワーク
- 侵入解析のダイヤモンドモデル
- 永続性を確立する技術
- NAC とエンドポイントセキュリティの回避
- フォグコンピューティング
- エッジコンピューティング
- グリッドコンピューティング

1　NICE 2.0 にマッピング

CEH は NICE 2.0 フレームワークファイナルバージョンに準拠したトレーニング・資格であり、セキュリティエンジニアとしてキャリアを構成するのに役立ちます。

2　新たな攻撃ベクトル

OWASP トップ 10、IoT ハッキング、脆弱性分析、APT、ファイルレスマルウェア、WebAPI 脅威、Webhooks、Web Shell、OT 攻撃、クラウド攻撃、AI、ML など 18 の攻撃ベクトルに重点を置いた内容となっています。

3　現代のエクスプロイト技術

初級レベルから既存および新規の脆弱性について学習することにより、エクスプロイト開発の改善が期待できます。OT テクノロジー、コンテナテクノロジーなど、最新のテクノロジーに触れることができます。

4　ハンズオンハッキングの課題

“Break-The-Code チャレンジ”を使用すると、4 つの複雑なレベルにまたがる 24 の究極のハッキングチャレンジを試すことができます。最先端のトリックを体験できます。

5　　最新のケーススタディと現在の傾向

TTP と攻撃の範囲を理解するのに役立つ模範的なケーススタディを学習します。潜在的なサイバー攻撃を、事前に保護、検出、分析するために、現代の実際に起こった事件と傾向から学習することができます。

6　　マルウェア分析の強化されたフォーカス

ランサムウェア、銀行および金融マルウェア、IoT ボットネット、OT マルウェア分析、Android マルウェアなど、最新のマルウェア分析技術に役立つ学習をすることができます。

7　　ライブ・サイバーレンジ

新しいオンライン演習環境は、Certified Ethical Hacker Training プログラムに 100%マッピングされています。

8　　オンライン演習環境

新しいオンライン演習環境は、Certified Ethical Hacker Training プログラムに 100%マッピングされています。

9　　多数の高度なハッキングテクニック、トリック、ツールを使用

CEH は、ファイルレスマルウェア、高度なソーシャルエンジニアリング手法など、最新のハッキング手法を紹介するための環境やサービスを提供し続けます。最先端のハッキングツールの使い方を学習することができます。

CEH v12 のモジュール

CEH v12 は CEH v11 と同一タイトルの 20 モジュールで構成されていますが、内容は最新の状況に更新されています。

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ー名、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。

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。

13 Web サーバへのハッキング

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 アプリケーションへのハッキング

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へのハッキング

iOS や Android 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/OT へのハッキング

IoT デバイスは今や重要インフラの一部となっています。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の 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。また、製造業、電力などの止まってはならない生産ラインの OT ハッキングの概念とハッキング方法学びます。

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。

BSI Professional Services Japan 株式会社 へのお問い合わせ先：

BSI.PSJ@bsigroup.com

お急ぎの方は、下記弊社営業担当へのご連絡も受け付けております。

弊社主催有料研修担当：

◆三森　優（Yu, Mitsumori）070-1640-8511