SEC504: Hacker Tools, Techniques, and Incident Handling

GCIH Incident Handler giac.org/gcih

6日間 プログラム | 38 CPEs | ラップトップが必要になります

SEC504で習得する事項

- インシデントレスポンスにダイナミックなアプローチを適用する方法
- ホスト、ネットワーク、ログの分析による脅威の特定方法
- 効果的なクラウドインシデントレスポンスのためのベストプラクティス
- ライブ解析、ネットワークインサイト、メモリーフォレンジックを用いたサイバー調査プロセス
- 重要資産を守るための防御スポット戦略
- エンドポイント検出ツールを回避するための攻撃者のテクニック
- 複雑なクラウドの脆弱性を悪用する攻撃者の手法
- 最初の侵害後に横展開するための内部情報を発見するプロセス
- システムのアクセス制御を回避するための最も効果的な攻撃方法
- 攻撃者が使う巧妙なテクニックと、それを阻止する方法

GCIH Incident Handler giac.org/gcih

GIAC Certified Incident Handler

GIACインシデントハンドラ認定 は、幅広い重要なセキュリティスキルを使用して、コンピュータセキュリティインシデントを検出、対応、および解決する実務家の能力を検証します。GCIH認証保有者は、一般的な攻撃手法、ベクター、ツールを理解することにより、セキュリティインシデントを管理するために必要な知識を持っているだけでなく、そのような攻撃が発生した場合に防御し、対応します。

- インシデント対応とコンピュータ犯罪の調査
- コンピュータ/ネットワークハッカーの悪用
- ハッカーツール(Nmap、Nessus、Metasploit、Netcat)

最近のクラウドやオンプレミスのシステムでは、侵害を防ぐことが目標とされていますが、実際には検知と対応が重要となります。組織を侵害から遠ざけるには、企業の損失を最小限に抑えるためのインシデント対応をいかにうまく処理するかにかかっています。

SEC504では、インシデント対応にダイナミックなアプローチを適用する方法を学びます。侵害の指標を用いて、Windows、Linux、クラウド・プラットフォームに影響を与える侵害に効果的に対応するための手順を学習します。このコースで得たスキルと実践的な経験を現場に持ち帰り、すぐに適用することが可能です。

インシデントレスポンスを効果的に行うための手順を理解することは、方程式の一部に過ぎません。初期の侵害から内部ネットワークの横展開まで、攻撃者が組織に対して取る行動を完全に把握するためには、攻撃者のツールとテクニックを理解する必要があります。SEC504のハンズオン環境では、攻撃者自身が使用するツールを用いて、その方法や攻撃者が残したアーティファクトを理解することができます。攻撃者の考え方を理解することで、攻撃者がどのように組織に対して取引を行うのかを知ることができ、攻撃者の動きを予測し、より優れた防御策を構築することができます。

コース開発者より

攻撃者のツールとテクニックが変わったので、それに合わせてインシデントレスポンスのテクニックも変える必要があります。2019年にSEC504の著者を引き継いでからは、インシデントレスポンスで成功するために必要なスキルを身につけられるよう、コース全体を書き換えました。攻撃がWindowsを中心としたものであれ、重要なデータベースプラットフォームへの攻撃やクラウドの脆弱性の悪用であれ、攻撃を効果的に特定し、影響を最小限に抑え、効率的に対応するための準備ができます。ハッカーツールやテクニックの知識を持ち、セキュリティを飛躍的に向上させる防御スキルを駆使することで、今日のサイバー脅威に対応するために組織が必要とするサブジェクト・マター・エキスパートとなる準備が整います。

—Joshua Wright

「SEC504 は全てにおいて優れていて、ペンテスターやディフェンダーの方々には最適なコースです。攻撃者がどのように考え、どのように情報を収集し、どのようにシステムを制御してそれを維持するかを理解するのに非常に役立ちました」

—Evan Brunk, Acuity Insurance

「素晴らしい内容です！ 開発者として、エクスプロイトを理解することは非常に有益で、より良いコーディングプラクティスがセキュリティポジションにどのように役立つかを理解することは非常に役立ちます」

—Alex Colclough, Clayton Homes

コース詳細

SECTION 1: インシデントレスポンスとサイバー調査

SEC504の最初のセクションでは、DAIR（Dynamic Approach to Incident Response）を適用して、組織内でインシデント対応プロセスを開発・構築し、脅威を効果的に検証、範囲、封じ込め、評価、修正する方法を学びます。このプロセスは、実際に発生した脅威を題材にした実習や例を用いて詳しく説明していきます。

主なトピック: インシデントレスポンス、デジタル調査、ライブレスポンス、ネットワーク調査、メモリ解析、マルウェア解析、クラウド調査、ブートキャンプLinuxオリンピック

SECTION 2: 情報収集、スキャン、情報列挙

このコースセクションでは、攻撃者が攻撃前のステップとして偵察を行うためのテクニックを見ていきます。これには、オープンソースインテリジェンス、ネットワークスキャン、ターゲットの列挙攻撃を使用して、ネットワークセキュリティのギャップを見つける方法が含まれます。攻撃者のテクニックを使って、ターゲットネットワークのセキュリティを評価し、Windows、Linux、クラウドのターゲットの一般的なプロトコルやエンドポイントを評価します。攻撃を行った後は、これらの攻撃によって残っているログデータや証拠を調査し、攻撃が行われたことを確認します。

主なトピック: MITRE ATT&CK Frameworkの解説、オープンソースインテリジェンス、DNS Interrogation、Webサイトの偵察、Nmapによるネットワークとホストのスキャン、クラウドスキャン、シャドークラウドのターゲット列挙、Server Message Block (SMB) セッション、DeepBlueCLI

SECTION 3: パスワード攻撃と不正アクセス攻撃

パスワード攻撃は、攻撃者が防御を回避して組織の資産にアクセスするための最も確実なメカニズムです。このコースセクションでは、パスワードや多要素認証の弱点を突いて得られたアクセスを使って、他のネットワークターゲットにアクセスする複雑な攻撃を調査します。

主なトピック: パスワード攻撃、パスワードハッシュの理解、パスワードクラッキング、Domain Password Audit Tool (DPAT)、安全でないストレージ、多目的Netcat

SECTION 4: 公開システムに対する攻撃とDrive-By攻撃

このセクションでは、公開サーバの脆弱性やクライアント側の脆弱性を利用した標的搾取フレームワークを紹介します。公開されているWebサイトの暗黙の信頼性を利用して、ブラウザの脆弱性を突いたり、Microsoft Officeドキュメントでコードを実行したり、脆弱なWebアプリケーションに関連する多くの脆弱性を悪用するために、攻撃者のツールやテクニックを適用していきます。

主なトピック: Metasploit Framework、Drive-By Attacks、システムリソース利用量モニタ、コマンドインジェクション、クロスサイトスクリプティング（XSS）、SQLインジェクション、SSRFとIMDS攻撃

SECTION 5: 回避手法と侵入後の攻撃

SEC504の最初のセクションでは、DAIR（Dynamic Approach to Incident Response）を適用して、組織内でインシデント対応プロセスを開発・構築し、脅威を効果的に検証、範囲、封じ込め、評価、修正する方法を学びます。このプロセスは、実際に発生した脅威を題材にした実習や例を用いて詳しく説明していきます。

主なトピック: インシデントレスポンス、デジタル調査、ライブレスポンス、ネットワーク調査、メモリ解析、マルウェア解析、クラウド調査、ブートキャンプLinuxオリンピック

SECTION 6: Capture-the-Flagイベント

このCapture-the-Flagイベントは、最近不正アクセスを受けた架空の企業であるISS Playlistのコンサルタントとして、実践的な活動を終日行います。このCTFでは、攻撃者が現代の高度なネットワーク環境を侵害するために使用しているのと同じ技術を用いて、クラスで学んだすべてのスキルを適用します。チームまたは個人で、Windows、Linux、Internet of Thingsデバイス、クラウドのターゲットなどのターゲットシステムに対して、スキャン、エクスプロイト、エクスプロイト後のタスクを行います。この実践的な課題は、プレーヤーがスキルを実践し、コースを通して学んだコンセプトを強化できるように設計されています。このイベントでは、成功に必要なオンデマンドのガイダンスを提供する統合ヒントシステムにより、ターゲットシステムの侵害、エンドポイントプロテクションプラットフォームのバイパス、内部ネットワークの高価値ホストへのピボット、企業データの流出を成功させるためのステップをガイドします。

主なトピック: ターゲットの発見と統合、オープンソースインテリジェンス・偵察・情報収集の適用、公開資産の侵害、Eメールの侵害、Windows Active Directoryへの攻撃、パスワードスプレー・推測・認証情報への攻撃、侵入後のピボットと横展開、エクスプロイトの選択・設定・デリバリー、内部攻撃者による侵害の属性

受講対象者

- インシデントハンドリングチームに属する方
- インシデントハンドリングチームリーダー
- システムの防御と攻撃への対応の最前線にいるシステム管理者
- システムが攻撃を受けた時に最初に対応するセキュリティ担当者
- 攻撃を防止、検知、対応するために、システムを設計、構築、運用したい一般的なセキュリティ関係者およびセキュリティアーキテクト

「SEC504は、私が今まで受講した中で最高のコースです。このコースで、受講生はセキュリティの幅広い内容を理解できるようになります」

—Joshua Nielson, Microsoft

「インシデントレスポンスは、規模の小さな企業では最も活用されていない側面です。SEC504は、経営陣がその価値を理解するのを助ける能力を私たちに与えてくれます」

—David Freedman, Nationwide Payment Solutions