コースコード：RH-RH414
税抜価格：365,000円
日数：5日間

前提条件

・RHCE認定RHCSA認定または、同等のスキルレベルをお持ちであること ・適切なスキルセットの知識を持っているかどうかがわからない場合は、オンラインスキルチェックで確認してください

受講対象者

・Red Hat Enterprise Linuxシステムのセキュリティ強化方法に関する技術的なガイドを必要とする方
・Red Hat Enterprise Linux システム上に、再現性と拡張性のある方法を用いて、セキュリティポリシー要求を実装する責任を持つ方
・そのシステムがセキュリティポリシー要件を満たすことを証明しなければならない方
・セキュリティ上重要なオペレーティングシステム/ソフトウェアアップデートの管理を含む、セキュリティ要件への継続的遵守の維持管理を行う方
・RHCEレベルのスキルを持っていることを強く推奨。

コース概要

このコースでは、セキュリティ要件を遵守するためのRed Hat Enterprise Linuxシステムの保護の方法について学習する、RHCEもしくは同等のスキルを持つエンジニア向けのコースです。
多くのセキュリティポリシーや標準では、システム管理者が、特定のユーザー認証の懸念、アップデートの適用、システム監査とロギング、ファイルシステムの整合性などの課題に対処することが求められます。
このコースでは、特定のポリシーおよび設定に関する問題への対処方法について解説します。

目的

Red Hat Enterprise Linux 6を不正アクセスから保護するためのセキュリティ機能の実装について理解する

アウトライン

1.セキュリティ更新のトラッキング
Red Hat Enterprise Linux で更新を生成する方法、および YUM を使用して使用可能なエラータを特定するクエリを実行する方法の理解
2.ソフトウェア更新の管理
更新のプロパティの検証など、更新をシステムに適用するためのプロセスの開発
3.ファイルシステムの作成
高度なファイルシステムレイアウトの割り当てによる、ファイルシステム暗号化の使用
4.ファイルシステムの管理
セキュリティ関連のオプションとファイルシステム属性による、ファイルシステムのプロパティの調整
5.特殊なパーミッションの管理
set user ID (SUID)、set group ID (SGID)、および sticky (SVTX) パーミッションの使用による、これらのパーミッションを有効にしたファイルの特定
6.追加のファイルアクセス制御の管理
ファイルアクセス制御リストを使用による、ファイルとディレクトリに適用されたデフォルトのパーミッションの修正
7.ファイルシステムに対する変更の監視
マシン上のファイルの変更を監視するソフトウェアの設定
8.ユーザーアカウントの管理
ユーザーにパスワードエージングのプロパティを設定し、ユーザーアカウントを監査
9.PAM (Pluggable Authentication Module) の管理
PAM に変更内容を適用してユーザーにさまざまなタイプのルールを適用
10.コンソールアクセスのセキュリティ保護
セキュリティに基づいて設定を有効または無効にするための、さまざまなコンソールサービスのプロパティの調整
11.一元認証のインストール
Red Hat ID管理（IdM）のサーバーとクライアントのインストールと設定
12.一元認証の管理
クライアントシステムへのユーザーアクセスと、それらのシステム上のユーザーに付与される追加権限の両方を制御するための、Red Hat ID管理ルールの設定
13.システムログの設定
トランスポート層の暗号化を使用およびリモートシステムで生成された追加ログの

管理のためのリモートログの設定

14.システム監査の設定

システム監査の有効化と設定

15.ネットワークサービスへのアクセスの制御

ネットワークサービスへの接続を制限するファイアウォール規則の管理