調査 5 モデルカリキュラムの提言 コースウェア

21. OS セキュリティに関するスキル

Ⅰ. 概要	OS のセキュリティ機能として必要な機能と、オープンソース OS としてもっとも利用が期待される Linux のセキュリティ管理に関して、実際の開発・運用の際に必要な管理知識・手法の種類と特徴、内容を学ぶ。
Ⅱ. 対象専門分野	職種共通
Ⅲ. 受講対象者、受講前提	基礎的なコンピュータ科学、セキュリティ工学基礎（ITSS レベル１程度）を習得、経験を持つレベルの知識を有すること。
Ⅳ. 学習目標	・ サーバを運用する際に必要となるシステムセキュリティおよびネットワークセキュリティ強化のための知識を、実習を行うことにより習得し、セキュリティホールのない安全なサーバを Linux により構築する。 ・ セキュリティ監査ツールを用いてシステムの脆弱性を発見できる。 ・ セキュリティホールのあるパッケージのアップデートができる。 ・ アカウントの保護のための設定ができる。 ・ syslogd の設定、及び logcheck によるログの監視ができる。 ・ Tripwire によるシステムの改ざんチェックを行うことができる。 ・ サービスの把握と不要なサービスの無効化ができる。 ・ xinetd の設定ができる。 ・ iptables コマンドを使用して、パケットフィルタリングの設定ができる。 ・ ssh の公開鍵認証方式を用いた暗号化通信、及び VPN の設定ができる。
Ⅴ. 使用教科書、教材等	『Linux サーバセキュリティ』 Michael D. Bauer 著、豊福 剛 訳
Ⅵ. 習得スキルの評価方法	講義終了後の受講レポート、定量アンケート、知識確認ミニテスト、演習問題の取り組み状況を総合的に判断して評価を行う。
Ⅶ. カリキュラムの構成	レベル 1 第 1 回～第 8 回 レベル 2 第 9 回～第 15 回

講座内容

第 1 回　OS のセキュリティ機能（講義　90 分）

OSのセキュリティの基本概念と必要な機能、その発展の歴史、必然性、利点などを理解する。

(1)インターネットセキュリティの概要

1. 不正アクセスの手口
2. セキュリティ対策の概要
3. 各種クラッキングツールを使用しての root 権限取得

(2)リスクの構成要素の識別と評価

1. システム資源の認識
2. セキュリティ目標の設定
   - 脅威の識別
   - 動機
   - 脆弱性に対する攻撃
3. 防御施策立案
   - システム資産価値低減
   - 脆弱性緩和
   - 攻撃緩和

第 2 回　Linux サーバのローカルセキュリティ対策（講義＋ワークショップ　90 分）

Linux サーバのローカルセキュリティ対策の基本項目の内容と設定内容を実習で理解する。

(1)基本的な行動

1. ファイルのパーミッション
2. ログの管理と監視
3. ブート時のセキュリティ
4. root アカウントの保護
5. ログイン制限
6. パスワード管理

(2)改ざんチェック

1. パスワード
2. ファイル
3. システムログ
4. その他のリソース

第 3 回　Linux のネットワークセキュリティ対策（講義＋ワークショップ　90 分）

Linux サーバのネットワークセキュリティ管理の基本設定、パッケージの導入などの方法とその作業内容を実習で理解する。

(1)ネットワークセキュリティの基本設定

1. パケットフィルタリング（Netfilter、iptables によるルールの設定の概要）
2. xinetd サービス
3. xinetd 設定ファイル
4. telnet サーバの構成
5. xinetd のセキュリティ

(2)盗聴対策

1. 通信の暗号化
2. サーバ通信の監視

第 4 回　Linux によるファイアウォール構築（講義＋ワークショップ　90 分）

Linux サーバによるファイアウォール設計、基本設定、導入などの方法とその作業内容を実習で理解する。

(1)ファイアウォールと DMZ アーキテクチャの種類

1. 内部と外部のアーキテクチャ
2. サーバファイアウォールによる DMZ アーキテクチャ
3. DMZ へのサーバ配置の決定
4. セキュリティ機能配置の決定

(2)サーバファイアウォール設定のポリシー

(3)iptables によるセキュリティ管理

1. ルータの設定の確認
2. iptables の位置づけ
3. iptables の設定の順序と方法
4. iptables の運用

第 5 回　Linux のサーバセキュリティ設定（講義＋ワークショップ　90 分）

Linux サーバセキュリティ管理の基本設定、アプリケーションパッケージの導入などの方法とその作業内容を実習で理解する。

(1)サーバとしての管理方針と実施方法

1. インストール方針
2. サービス提供方針

(2)サーバでのセキュリティ実施方法

1. ソフトウェアを最新状態に保つ
2. 不要なユーザアカウントの削除
3. シェルアクセスの制限
4. 既知のユーザだけにアクセスを限定する
5. chroot されたファイルシステムでサービスを実行する
6. SUID=root の使用を極力なくす
7. 必要なソフトウェアだけをインストール

第 6 回　安全なリモートアクセス（講義＋ワークショップ　90 分）

Linux の管理者権限の設定、アプリケーションパッケージの導入などの方法とその作業内容を実習で理解する。

(1)セキュアシェルの基礎知識

1. SSH の動作について
2. OpenSSH の入手とインストール
3. SSH の手引き
4. sftp と scp を使って暗号化されたファイル転送を行う
5. SSH の設定を調整する
6. sshd の設定と実行

(2)SSH の応用

1. SSH での公開鍵暗号
2. RSA と DSA の認証の設定と使用法
3. SSH を使ったリモートコマンドの実行
4. SSH を使った TCP ポートフォワーディング

第 7 回　SSL によるサーバ VPN と CA（講義＋ワークショップ　90 分）

Linux サーバによる SSL によるサーバ VPN と CA の導入、設定の方法とその作業内容を実習で理解する。

(1)トンネリングの仕組みと設定

1. OpenSSL の設定
2. Stunnel の設定
3. CA を使うための手順
4. Stunnel を用いたクライアント／サーバ間のトンネリング実習

(2)IPsec による暗号化通信の導入

1. Linux2.6 における IPsec の構成
2. 鍵交換デーモン
3. x509 証明書を用いた PKI

(3)IPsec による暗号化通信ワークショップ

第 8 回 ドメインネームサービスのセキュリティ対策(講義＋ワークショップ 90 分)

Linux の DNS に関してセキュリティ設定、導入などの方法とその作業内容を実習で理解する。

(1)DNS の基本動作

(2)DNS セキュリティの原則

1. セキュリティリスク
2. アタックの種類と特徴
3. DNS が持つべきセキュリティ機能

(3)BIND におけるセキュリティ対策

1. BIND のバージョンとセキュリティ
2. セキュリティを考慮した実行環境
3. named.conf のセキュリティ対策
4. ゾーンファイルのセキュリティ
5. BIND の高度なセキュリティ:TSIG と DNSSEC

(4)djbdns

1. djbdns の概要
2. djbdns のサービス
3. djbdns のインストール
4. tinydns の実行
5. djbdns クライアントプログラムの実行
6. rsync と ssh によるゾーン転送の暗号化

第 9 回　電子メールのセキュリティ対策（講義＋ワークショップ　90 分）

Linux のメールサーバ機能に関してセキュリティ設定、導入などの方法とその作業内容を実習で理解する。
Sendmail、Postfix を使用してセキュリティメールの構築方法を理解する。

(1)MTA と SMTP セキュリティ

1. 電子メールのセキュリティアーキテクチャ
   - SMTP ゲートウェイと DMZ ネットワーク
   - SMTP セキュリティ
   - 迷惑メール
   - SMTP AUTH
   - SMTP コマンドによる検証
2. MTA にセキュリティ対策

(2)Sendmail のセキュリティ

1. Sendmail の長所と短所
2. Sendmail のセキュリティ構築
   - Sendmail の入手とインストール
   - Sendmail の設定の概要
   - Sendmail.mc の設定
   - Sendmail を chroot して実行するための設定
   - Sendmail のマップやその他のファイルの設定
   - Sendmail における SMTP AUTH の設定
   - Sendmail と STARTTLS
   - TLS を使う Sendmail の設定

(3)Postfix

1. Postfix のアーキテクチャ
2. Postfix のセキュリティ構築
   - Postfix 入手とインストール
   - Postfix の設定

第 10 回　Web のセキュリティ対策①（講義＋ワークショップ　90 分）

Linux による Web サーバの設定、導入方法とその作業内容を実習で理解する。

(1)Web サーバのセキュリティ

1. Web の問題と対策
2. 脆弱性とセキュリティ対策のタイミング
3. Web セキュリティの原則

(2)Apache のセキュリティ構築

1. 導入と設定
   - インストールについて
   - Apache ファイル階層のセキュリティ対策
   - Apache の設定
   - Apache の設定ファイル
   - 設定オプション
2. セキュリティコンポーネント
   - 静的コンテンツ
   - 動的コンテンツ：SSI（Server-Side Includes）
   - 動的コンテンツ：CGI（Common Gateway Interface）

第 11 回　Web のセキュリティ対策②（講義＋ワークショップ　90 分）

Linux の管理者権限の設定、アプリケーションパッケージの導入などの方法とその作業内容を実習で理解する。

(1)CGI スクリプトのセキュリティ対策

1. HTTP、URL、CGI
2. フォームデータの処理
3. ファイルのインクルード
4. フォームからのファイルアップロード
5. データベースへのアクセス
6. 他のスクリプトのチェック

(2)Web サーバのセキュリティ応用機能

1. 認証
2. アクセスコントロール
3. セッションとクッキー
4. サイト管理：ファイルのアップロード
5. 新しいフレームワーク：SOAP、Web サービス、REST のセキュリティ
6. ロボットとスパイダー
7. 攻撃の検知と回避
8. キャッシュ、プロキシ、ロードバランサ

第 12 回　ファイルサービスのセキュリティ対策（講義＋ワークショップ　90 分）

Linux のファイルサービスのセキュリティ設定、導入などの方法とその作業を実習で理解する。

(1)FTP のセキュリティ

1. FTP セキュリティの原則
2. ProFTPD を使った匿名 FTP の実現
3. FTP 以外のファイル共有方式

・ SFTP と scp

(2)FTP サーバのセキュリティ設定内容と手順

1. パーミッション
2. ftp によるファイル書き込みを禁止する方法
3. welcome.msg
4. /etc/ftp* ファイル群
5. /etc/ftpaccess によるアクセス制御
6. upload の設定
7. /etc/ftpusers の設定
8. /etc/ftphosts の設定

第 13 回 システムログの管理(講義＋ワークショップ 90 分)

Linux のシステムログの管理の方法、手順、設定、作業内容を実習で理解する。

(1)syslog

1. syslog の設定
2. syslog-ng
   - syslog-ng をソースコードからインストールする
   - syslog-ng を実行する
   - syslog-ng の設定
   - 高度な設定
3. logger を使ってシステムログをテストする
4. システムログファイルの管理

(2)swatch を用いたログ監視の自動化

1. swatch の導入と運用
   - swatch のインストール
   - swatch の設定の概要
   - swatch の高度な設定
   - swatch の設定最適化

第 14 回 Linux による侵入検知の手法(講義＋ワークショップ 90 分)

Linux サーバを用いて、サーバによる侵入検知の仕組み、方法、実際の作業内容を実習で理解する。

(1)Tripwire

1. Tripwire の入手、コンパイル、インストール
2. Tripwire の設定
3. Tripwire によるチェックと更新
4. Tripwire のポリシー変更
5. その他の整合性チェックプログラム

(2)Snort

1. Snort の入手、コンパイル、インストール
2. Snort によるパケットのアナライズ
3. Snort によるパケットのロギング
4. Snort を IDS として設定

第 15 回 サーバのセキュリティ監査と設定の自動化(講義＋ワークショップ 90 分)

Linux の管理者権限の設定、アプリケーションパッケージの導入などの方法とその作業内容を実習で理解する。

(1)サーバのセキュリティ監査方針

1. ファイアウォールをスキャナで検査
2. セキュリティ機能を理解して活用
3. 要塞ホスト設定のドキュメント化

(2)監査ツール

1. サーバ監査ツール
2. ローカル監査ツール

(3)ログの設定、運用、監視

1. Bastille Linux を使った自動セキュリティ強化
2. Bastille の入手とインストール
3. Bastille の設定と実行
4. Bastille のログ

以上