一関工業高等専門学校	開講年度	令和04年度 (2022年度)	授業科目	情報セキュリティ特論

科目基礎情報

科目番号	0034	科目区分	専門 / 選択
授業形態	講義	単位の種別と単位数	履修単位: 1
開設学科	未来創造工学科（情報・ソフトウェア系）	対象学年	5
開設期	後期	週時間数	2
教科書/教材	参考書籍、参考URLは授業において適宜紹介		
担当教員	宇梶 郁,千田 栄幸		

到達目標

1. ログ解析の必要性と重要性を理解する
2. サーバ監視の具体的な手法を理解し実施できる
3. 実務科教員（副業先生）によるペネトレーションテスト演習
4. 実務科教員（副業先生）による情報セキュリティインシデントハンドリング演習
5. 情報セキュリティ対策の重要性を理解し未知の攻撃に備えることができる

【教育目標】D

ルーブリック

	理想的な到達レベルの目安	標準的な到達レベルの目安	未到達レベルの目安
1. ログ解析の必要性と重要性を理解する	インターネットで調べることなくログファイルの保存場所を確認して各種ログファイルを閲覧できる	インターネットで情報収集しながらログファイルの保存場所を確認して各種ログファイルを閲覧できる	左記のいずれもできない
2. サーバ監視の具体的な手法を理解し実施できる	要求に応じたログデータの正規化、抽出、リアルタイム監視ができる	ログデータの正規化、抽出、リアルタイム監視の３つのうち２つができる	左記3項目のうちひとつしかできない又はひとつもできない
3. 実務科教員（副業先生）によるペネトレーションテスト演習	ペネトレーションテスト結果を分析し、脆弱性についての考察ができる	ペネトレーションテストを実施し、実施結果を収集できる	左記のいずれもできない
4. 実務科教員（副業先生）による情報セキュリティインシデントハンドリング演習	情報セキュリティインシデント発生時に適切に他部門との連携や事後対応ができる	情報セキュリティインシデント発生時に適切な初動対応ができる	左記のいずれもできない
5. 情報セキュリティ対策の重要性を理解し未知の攻撃に備えることができる	自発的に情報セキュリティ対策案を提示できる	他者の情報セキュリティ対策案を一緒に検討できる	情報セキュリティ対策案について議論できない

学科の到達目標項目との関係

教育方法等

概要	サイバー攻撃と情報セキュリティの重要性を十分に理解し、ログ解析用スクリプトを作成できるようになることと実務科教員（副業先生）によるインシデントハンドリングを体験することを主な目標とする。また、各種情報セキュリティ対策手法を通して、未知の攻撃にどう対自していくかを議論できる能力を養う。
授業の進め方・方法	第1週、第15週は講義（座学）、第６週、第７週、第13週、第14週はセキュリティ実務科教員（副業先生）による演習、講義、机上訓練等を予定しています。他については、20-30分程度内容説明後の演習を予定。プログラミング言語はスクリプト言語を使用予定。Bash / Perl / Pythonのうち自分が得意な言語いずれでも可。 Linuxの演習環境へのsshログイン環境必須。 基本的なUNIXコマンドを使用できることが望ましい。 座学、演習説明にはスライドを使用。
注意点	演習課題、レポート等は演習用Linuxサーバの指定場所、指定形式での保存による提出必須。

授業の属性・履修上の区分

□ アクティブラーニング	☑ ICT 利用	□ 遠隔授業対応	☑ 実務経験のある教員による授業

必履修

授業計画

		週	授業内容	週ごとの到達目標
後期	3rdQ	1週	サイバー攻撃と情報セキュリティ	サイバー攻撃の種類や情報セキュリティに関する概要と演習環境の使い方についての理解
		2週	コマンドとシェル環境の活用	Linuxの演習環境の基本操作
		3週	ログ解析に有効なツールとコマンドの活用	ログ解析によく利用される代表的なコマンドとそのオプションの活用できる
		4週	各種ログファルとフォーマット①	Linuxの演習環境を通して、代表的なログファイルの保存場所を確認し内容を閲覧できる。また、コマンドラインからログデータを正規化できる
		5週	ログ解析プログラミング	Linuxの演習環境で動作するシェルスクリプト（Bash/Perl/Python等）またはコマンドラインを使用してログ解析ができる
		6週	Webサーバのペネトレーションテスト演習①	ペネトレーションテストの重要性と実習の進め方について説明後、対象サーバに対するペネとレーションテストの実施。
		7週	Webサーバのペネトレーションテスト演習②	テスト後にまとめた結果を発表。副業先生から講評をいただき完了とする。（第６週、第７週は連続して実施するのが望ましい）
		8週	リアルタイムサーバ監視	サーバのリアルタイム監視の必要性とそのために必要なコマンドとその活用方法を理解する
	4thQ	9週	サーバ監視の可視化	スクリプトによるリアルタイム監視と典型的な監視ツールによるログの可視化手順を理解する
		10週	バイナリファイル調査	Linuxコマンドを使ってバイナリファイルの内容を調査できる

		11週	ネットワークプログラミング	スクリプトによるネットワークプログラミングができる
		12週	セキュリティ診断	サイバー攻撃を受けている時のサーバの状態を確認できる
		13週	情報セキュリティインシデントハンドリング演習①	事前講義を通してインシデント発生時の対応手順等を理解する
		14週	情報セキュリティインシデントハンドリング演習②	机上訓練を通してインシデント発生時の対応手順を体験する（第１３週、第１４週は連続して実施するのが望ましい）
		15週	未知の攻撃への備え	未知の攻撃に備えて何ができるかを考えることができる
		16週		

モデルコアカリキュラムの学習内容と到達目標

分類	分野	学習内容	学習内容の到達目標	到達レベル	授業週

評価割合

	課題（レポート）	発表	相互評価	態度	合計
総合評価割合	100	0	0	0	100
基礎的能力	30	0	0	0	30
専門的能力	30	0	0	0	30
分野横断的能力	40	0	0	0	40