福井工業高等専門学校	開講年度	令和04年度 (2022年度)	授業科目	情報ネットワーク

科目基礎情報

科目番号	0091	科目区分	専門 / 必修
授業形態	講義	単位の種別と単位数	学修単位: 1
開設学科	電子情報工学科	対象学年	5
開設期	前期	週時間数	前期:2
教科書/教材	コロナ社　面和成　入門サイバーセキュリティ理論と実験		
担当教員	波多 浩昭		

到達目標

ネットワークセキュリティ，サイバーセキュリティに焦点をあて，インターネットとサーバー空間の脅威，攻撃手法，について概念と仕組みを理解する.

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
評価項目1　脅威	サイバー空間における脅威について網羅的に説明できる	サイバー空間の脅威に関する与えられた語句について説明できる	サイバー空間の脅威を理解していない
評価項目2　攻撃手法	攻撃手法についていくつかは自分で実践して，その仕組みを説明できる.	攻撃手法に関する与えられた語句について説明できる	攻撃手法について説明できない

学科の到達目標項目との関係

学習・教育到達度目標 RB2
JABEE JB3

教育方法等

概要	インターネットセキュリティ，サイバー空間セキュリティについて，脅威の種類及び攻撃手法について論述する. 尚、全体を通して企業での情報通信業務の実務経験者が指導を行う。
授業の進め方・方法	授業形式をとるが，パソコンを持参して実際に攻撃のいくつかの自分のパソコンで実践しながら学ぶ体験型授業とする.
注意点	この科目は学修単位科目「B」です。授業外学修の時間を含めます。 毎回、授業外学修のための課題を課します。 本科(準学士課程)の学習教育目標：RB2(◎) 環境生産システム工学プログラムの学習教育目標：JB3（◎） 関連科目：オペレーティングシステム（本科3年）,計算機構成論Ⅱ(本科4年),通信システム(本科5年) ,情報理論Ⅱ（本科5年) 学習教育目標の達成度評価方法：2回の試験の平均を総合評価とする. 但し、総合得点50点以上60点に満たないものは、10点満点の課題もしくは再試を課す. 学習教育目標の達成度評価基準：総合評価60点以上を合格とする.

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

授業計画

		週	授業内容	週ごとの到達目標
前期	1stQ	1週	セキュリティ概論　ネットワークサイバー空間の脅威	シラバス説明，ネットワークおよびサイバー空間の脅威の種類について理解する　マルウェア，Botnet，フィッシング，DDoS，DNSポゾニング，システム侵入，パスワードクラック，スタックオーバフロー，特権奪取，盗聴，改ざん
		2週	暗号１　共通鍵暗号　モード　ハッシュ　MAC	共通鍵暗号と公開会暗号の差異，共通鍵暗号の用途，共通鍵暗号の種類，DESの脆弱性，AES，暗号モード，ハッシュ関数，MAC（メッセージ認証）について説明できる
		3週	暗号２　公開鍵暗号　RSA　楕円　数学基盤	公開鍵暗号の種類，初等整数論，DHのアルゴリズム，RSAのアルゴリズム，楕円暗号のアルゴリズムなど技術的要素について説明できる
		4週	暗号３　公開鍵暗号　署名　証明書　PKI	公開鍵暗号の用途，署名，証明書，PKIなど公開鍵暗号のアプリケーションについて説明できる
		5週	TLS プロコル　サーバ認証　openssl実習	TLSプロトコル，サーバ認証（SAN），OCSPステープリングについて説明できる．opensslでX509証明書を作成できる．その証明書をWebサーバにインストルしてChromeブラウザでアクセスしてみる.
		6週	認証　パスワード　PAP/CHAP　OTP　ID連携	認証の種類，パスワード認証におけるPAP/CHAPそれぞれの特徴，ワンタイムパスワード，ID連携の方法について説明できる.
		7週	ネットワークセキュリティ技術 Proxy FW NAT IPSec（LANブリッジ，リモートアクセス） WAF LB	ネットワークセキュリティ装置である，ファイヤーウォール，NAPT，LANブリッジ，リモートアクセス，Web Application Firewall，ロードバランサの機能について説明できる.
		8週	中間試験	
	2ndQ	9週	ネットワーク攻撃実習の準備　KaliLinux	VirtualBoxを使い，ネットワークセキュリティ関連で良く用いられるKaliLinuxのインストールと以降の授業で利用するツールについて説明する.
		10週	情報収集手法 （受動的情報収集）	Google検索演算子，サーバサイトの情報収集（Shodan/maltego），個人情報収集（Spokeo/intellius），OSINT(twittermap/twint)等の検索ツールの存在を理解する.

		11週	脆弱性検出（能動的情報収集＝受動的攻撃＝スキャン）とシステムへの侵入（能動的攻撃）	ネットワーク（アドレス）スキャン()とポートスキャン(nmap)，Webスキャン(OWASPzap)，総合スキャン(GVM)による古いバージョンOSや古いバージョンのアプリケーションのサーチすることができることを知る.
		12週	システムへの侵入特権奪取（能動的攻撃）	古いバージョンのOSの脆弱性をついた侵入(Windows1803)，古いアプリケーションの脆弱性をついた侵入などのデモ実践により，侵入経路は複数あることを知る.
		13週	システムへの侵入特権奪取後の行動（能動的攻撃）	Windows10に不正侵入後、バックドアの生成（リモートデスクトップ起動）、パスワードファイルの搾取、ログの消去、新しいアカウントの生成などを行う。これにより次回以降は不正侵入経路ではなく、正規経路より不正侵入する。
		14週	ブロックチェーン	暗号化資産、トランザクション、ブロックチェーン、マイニングなどの概念を理解する
		15週	ダークWeb	匿名化ネットワークを介した公開サーバへの匿名アクセスや、特定の人にしか存在を知られず匿名化ネットワーク経由でなければアクセスできないサーバの技術的な仕組みについて理解する。
		16週	期末試験	解答とまとめ

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
専門的能力	分野別の専門工学	情報系分野	ソフトウェア	コンピュータ内部でデータを表現する方法(データ構造)にはバリエーションがあることを説明できる。	4	
				同一の問題に対し、選択したデータ構造によってアルゴリズムが変化しうることを説明できる。	4	
				リスト構造、スタック、キュー、木構造などの基本的なデータ構造の概念と操作を説明できる。	4	
			コンピュータシステム	集中処理システムについて、それぞれの特徴と代表的な例を説明できる。	4	
				分散処理システムについて、特徴と代表的な例を説明できる。	4	
			情報通信ネットワーク	プロトコルの概念を説明できる。	4	
				プロトコルの階層化の概念や利点を説明できる。	4	
				ローカルエリアネットワークの概念を説明できる。	4	
				インターネットの概念を説明できる。	4	
				TCP/IPの4階層について、各層の役割を説明でき、各層に関係する具体的かつ標準的な規約や技術を説明できる。	4	
				主要なサーバの構築方法を説明できる。	4	
				情報通信ネットワークを利用したアプリケーションの作成方法を説明できる。	4	
				有線通信の仕組みと規格について説明できる。	4	
				基本的なルーティング技術について説明できる。	4	
				基本的なフィルタリング技術について説明できる。	4	

評価割合

	試験	レポート	合計
総合評価割合	100	0	100
基礎的能力	30	0	30
専門的能力	70	0	70
分野横断的能力	0	0	0