木更津工業高等専門学校	開講年度	令和04年度 (2022年度)	授業科目	情報セキュリティ I

科目基礎情報

科目番号	0106	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: 2
開設学科	情報工学科	対象学年	4
開設期	前期	週時間数	2
教科書/教材			
担当教員	米村 恵一		

到達目標

セキュリティアナリストに要求される知識・スキルの習得の準備段階としての
1．Webサーバへのアクセスログとその通信ログにおける分析・解析の基礎に必要な観点への理解
2．Webサーバへの攻撃とその対策方法の基礎への理解
3．攻撃シナリオの実際とその考え方への理解
を深める

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
ログ分析・解析の基礎の理解	分析・解析に必要な観点を十分に理解できる	分析・解析に必要な観点を理解できる	分析・解析に必要な観点を理解できない
攻撃手法の基礎の理解	攻撃手法の基礎を十分に理解できる	攻撃手法の基礎を理解できる	攻撃手法の基礎を理解できない
防御手法の基礎の理解	防御手法の基礎を十分に理解できる	防御手法の基礎を理解できる	防御手法の基礎を理解できない
攻撃シナリオとその考え方の理解	攻撃シナリオとその考え方を十分に理解できる	攻撃シナリオとその考え方を理解できる	攻撃シナリオとその考え方を理解できない

学科の到達目標項目との関係

教育方法等

概要	セキュリティアナリストに要求される知識・スキルの習得の準備段階としての 1．Webサーバへのアクセスログとその通信ログにおける分析・解析の基礎に必要な観点への理解 2．Webサーバへの攻撃とその対策方法の基礎への理解 3．攻撃シナリオの実際とその考え方への理解 を、座学・演習・自学自習による課題の遂行、により深める
授業の進め方・方法	座学と実機を使用した演習をバランスよく実施する 実際に手を動かす演習が重要になってくるが，その演習の効果を高めるための座学と予習・復習も非常に大切になる 自学自習による課題の遂行が、理解を深めることを助け、同時に、次の回への予習としての位置づけにもなっている
注意点	各設問、演習問題、課題、実機演習における進め方、には，概ね正解と考えることができる基本的な回答や考え方、手法が存在する しかしながら，それに近い・近くないにこだわらず，考えられるあらゆる可能性を吟味することに意義があり，そのためには，日ごろの努力によって、自身を吟味できる状態に持っていくことが期待される

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	SOCオペレータとは？ ネットワークの基礎知識の復習１ パケットキャプチャと通信ログ１	SOCオペレータとそのスキルを理解する ネットワークの基本コマンドを確認する パケットキャプチャにより見えるものを理解する 通信ログに記載されている内容を理解する
		2週	ネットワークの基礎知識の復習２ パケットキャプチャと通信ログ２ 偵察の実行	ネットワークの基本コマンドを確認する パケットキャプチャにより見えるものを理解する 通信ログに記載されている内容をさらに理解する 偵察を理解する
		3週	偵察の実行と結果から考える 情報提示についての考え方 ログの持つ様々な情報 ディレクトリトラバーサルとログ解析	偵察の実行とその結果を理解する 情報提示についての考え方を理解する ログの持つ様々な情報を活用する考え方を理解する ディレクトリトラバーサルとそのログを理解する
		4週	ディレクトリトラバーサルの防御方法 各種ファイルの場所 HTTPメッセージ	ディレクトリトラバーサルの防御方法を理解する 狙われやすいファイルがなぜ狙われるのかを理解する HTTPメッセージへの理解を深め、ログを見るための知識を増やす
		5週	XSS（クロスサイトスクリプティング） パーセントエンコーディング サイバー攻撃に対する様々な考え方	XSS（クロスサイトスクリプティング）の基本を理解する ログを読む知識を増やすためパーセントエンコーディングを理解する サイバー攻撃に対する様々な考え方を理解する
		6週	XSS（クロスサイトスクリプティング）の防御方法 SQLインジェクションとログ解析 ファイヤーウォール、サーバ設定	XSS（クロスサイトスクリプティング）の防御方法を理解する SQLインジェクションの基本を理解しそのログを理解する ファイヤーウォール、サーバ設定を考え、守るための方法への理解を深める
		7週	SQLインジェクションの防御方法 OSコマンドインジェクションとログ解析 SQLインジェクションの別の形 エラーログを読む	SQLインジェクションの防御方法を理解する OSコマンドインジェクションの基本を理解しそのログを理解する SQLインジェクションの別の形を理解する エラーログから攻撃を推測する考え方への理解を深める

		8週	SQLインジェクションの別の形に対して攻撃側から見る SQLインジェクションの防御方法２ 遠隔操作の基本的な攻撃手法 OSコマンドインジェクションの防御方法	SQLインジェクション攻撃のエラーログと攻撃側の行動の比較から考え理解を深める SQLインジェクションの防御方法の理解を深める 遠隔操作の基本的な攻撃手法を理解する OSコマンドインジェクションの防御方法を理解する
	2ndQ	9週	実機演習１（これまで学んだ攻撃手法により、ターゲットサーバへ侵入する）	これまで学んだ攻撃手法を実践し理解を深める
		10週	実機演習２（ターゲットサーバへの侵入において、パスワードクラックを実践する）	これまで学んだ攻撃手法を実践し理解を深める パスワードクラックへの（対策も含め）理解を深める
		11週	実機演習３（ターゲットサーバの脆弱性に対策を施すことで、これまでに学んだ防御手法を実践する）	これまで学んだ攻撃手法を実践し理解を深める パスワードクラックへの（対策も含め）理解を深める これまで学んだ防御方法を実践し理解を深める
		12週	Windowsへの攻撃の実際の基礎１	Windowsへの攻撃の実際を、攻撃ツールMimikatzの活用を通して、理解を深める
		13週	Windowsへの攻撃の実際の基礎２	Windowsへの攻撃の実際を、エクセルマクロの実行によるエクスプロイトを通して、理解を深める
		14週	実機演習４（ターゲットサーバの脆弱性に対策を施すことで、これまでに学んだ防御手法を実践する２、Windowsへの攻撃の実際を実践する１、守る観点からのフォレンジックを実践する１）	これまで学んだ防御方法を実践し理解を深める Windowsへの攻撃の実際を実践し理解を深め、守る立場からフォレンジックについても理解を深める
		15週	実機演習５（Windowsへの攻撃の実際を実践する２、守る観点からのフォレンジックを実践する２）	Windowsへの攻撃の実際を実践し理解を深め、守る立場からフォレンジックについても理解を深める
		16週	情報セキュリティに触れて自身で感じたことを学習する（最終報告書として提出）	情報セキュリティに触れて自身で感じたことを学習し、これまでの内容への総合的な理解へつなげる

評価割合

	各回の課題	期末報告書	合計
総合評価割合	60	40	100
ログ分析・解析の基礎の理解	15	10	25
攻撃手法の基礎の理解	15	10	25
防御手法の基礎の理解	15	10	25
攻撃シナリオとその考え方の理解	15	10	25