木更津工業高等専門学校	開講年度	令和02年度 (2020年度)	授業科目	情報セキュリティⅡ

科目基礎情報

科目番号	0185	科目区分	専門 / 必修
授業形態	授業	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	後期	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の重要スキルである、
1．アクセスログ、通信ログの解析による、攻撃の検出
2．攻撃シナリオにおける検出から防御までの総合的な実践力
の習得をシステム構築演習を通じて目指す。

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
情報システム構築	情報システムを構成する要素を十分に理解し、十分な構築ができる。	情報システムを構成する要素を理解し、構築ができる。	情報システムを構成する要素を理解できず、構築ができない。
ログ解析・各種通信解析	Webサーバ、IDS/IPS、Proxyサーバによる通信解析を十分に理解できる。	Webサーバ、IDS/IPS、Proxyサーバによる通信解析を理解できる。	Webサーバ、IDS/IPS、Proxyサーバによる通信解析を理解できない。
検出から防御までの総合力	攻撃シナリオにおける各種ステップを十分に実践できる。	攻撃シナリオにおける各種ステップを実践できる。	攻撃シナリオにおける各種ステップを実践できない。

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の重要スキルである、 1．アクセスログ、通信ログの解析による、攻撃の検出 2．攻撃シナリオにおける検出から防御までの総合的な実践力 の習得をシステム構築演習を通じて目指す。
授業の進め方・方法	演習を中心に進める。 演習の効果を高めるための予習・復習も大切になる。
注意点	ツールの使い方など、ある程度の正解と考えることができる標準的な使い方が存在する。しかしながら、正しい・正し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、自身を吟味できる状態に持っていくことが期待される。

授業計画

		週	授業内容	週ごとの到達目標
後期	3rdQ	1週	Webサーバの構築とログ解析１	Webサーバの構築手法、Webサーバにおける不審なログを見極める観点を理解できる。
		2週	Webサーバの構築とログ解析２	Webサーバの構築手法、Webサーバにおける不審なログを見極める観点を理解できる。
		3週	Webサーバの構築とログ解析３	Webサーバの構築手法、Webサーバにおける不審なログを見極める観点を理解できる。
		4週	Webサーバの構築とログ解析４	Webサーバの構築手法、Webサーバにおける不審なログを見極める観点を理解できる。
		5週	Webサーバの構築とログ解析５	Webサーバの構築手法、Webサーバにおける不審なログを見極める観点を理解できる。
		6週	IDS/IPSの構築とIDS/IPSによる通信の解析とIDS/IPSの特性１	IDS/IPSの構築手法、シグネチャ作成手法、IDS/IPSの対応範囲、不審なログを見極める観点を理解できる。
		7週	IDS/IPSの構築とIDS/IPSによる通信の解析とIDS/IPSの特性２	IDS/IPSの構築手法、シグネチャ作成手法、IDS/IPSの対応範囲、不審なログを見極める観点を理解できる。
		8週	IDS/IPSの構築とIDS/IPSによる通信の解析とIDS/IPSの特性３	IDS/IPSの構築手法、シグネチャ作成手法、IDS/IPSの対応範囲、不審なログを見極める観点を理解できる。
	4thQ	9週	IDS/IPSの構築とIDS/IPSによる通信の解析とIDS/IPSの特性４	IDS/IPSの構築手法、シグネチャ作成手法、IDS/IPSの対応範囲、不審なログを見極める観点を理解できる。
		10週	Proxyサーバのログ解析のための演習環境構築とログ解析１	Proxyサーバのログ解析のための演習環境の要素と構築手法、Proxyサーバにおける不審なログを見極める観点を理解できる。
		11週	Proxyサーバのログ解析のための演習環境構築とログ解析２	Proxyサーバのログ解析のための演習環境の要素と構築手法、Proxyサーバにおける不審なログを見極める観点を理解できる。
		12週	Proxyサーバのログ解析のための演習環境構築とログ解析３	Proxyサーバのログ解析のための演習環境の要素と構築手法、Proxyサーバにおける不審なログを見極める観点を理解できる。
		13週	総合演習１	攻撃シナリオにおける検出から防御までを総合的に理解できる。
		14週	総合演習２	攻撃シナリオにおける検出から防御までを総合的に理解できる。
		15週	総合演習３	攻撃シナリオにおける検出から防御までを総合的に理解できる。
		16週	総復習	毎回の課題について必要に応じて再考する。

評価割合				
	構築	ログ解析	総合実践力	合計
総合評価割合	40	30	30	100
基礎的能力	30	20	20	70
専門的能力	10	10	10	30