日本工学院専門学校	開講年度	2020年度（令和2年度）	科目名	ネットワークセキュリティ演習１

科目基礎情報

開設学科	ITスペシャリスト科	コース名	セキュリティ専攻	開設期	後期
対象年次	3年次	科目区分	選択	時間数	60時間
単位数	4単位	開講時間		授業形態	実習
教科書/教材	実習資料は毎回配布する。関連する資料等についてはそれぞれの実習内意で紹介する。				

担当教員情報

担当教員	中西真也・兒玉奉恵	実務経験の有無・職種	有・システムエンジニア

学習目的

安全な企業ネットワークの構築と管理に必要となるルータやスイッチの設定などを学習します。

到達目標

この演習の到達目標はシステムのセキュリティの向上に必要な知識と関連する技術を習得することである。セキュリティの知識としてOSとその上で動作するプログラムとネットワークの関係、ネットワークを流れるパケットを取得し、通信内容の分析方法、通信の暗号化と復号化に必要な技術、システムに残されたアクセスログなどの情報を元に脅威を特定する方法を習得することである。

教育方法等

授業概要	この授業はシスコネットワーキングアカデミーのCCNA Cybersecurity Opationsの内容に準じた座学を実施する。OS、サーバ、ネットワークと多岐にわたり、内容によっては各自のノートPCを使っての検証を行うこともある。また、参考資料の閲覧、情報検索でも各自のノートPCを利用する。
注意点	コンピュータやネットワークに関する基礎知識、基本的な操作を習得していることを前提としている。ノートPCを使用することもあるので持参すること。出席は授業時間開始時にのみ取る。遅刻は授業開始10分までを認め、それ以降は欠席となる。授業時間の3/4以上出席しない者は定期試験を受験できない。

評価方法	種別	割合	備考
	試験・課題	50%	試験と課題内容で評価する。
	小テスト	40%	実習内容の理解度を確認する。
	レポート	0%	
	成果発表（口頭・実技）	0%	
	平常点	10%	授業参加度、授業態度を評価する。

授業計画（1回～15回） 1回（ 4 ）時間 ※45分を1時間とする

回	授業内容	各回の到達目標
1回	サイバーセキュリティの攻撃と防御	攻撃側、防御側の行動、思考法について理解し、それを実行できる
2回	Windowsのシステム管理その1	プロセスとTCP/UDPのつながり、レジストリの調査、ユーザ作成などの操作できる
3回	Windowsのシステム管理その2	PowerShell、タスクマネージャ、システムリソースの監視と管理などの操作ができる
4回	Liinuxのシステム管理	テキストエディタ、CLI、シェルコマンドを使いLinuxシステムの管理ができる
5回	Liinuxのシステム管理	サーバ、ログファイル、ファイルシステムとパーミッションを理解し、それらを操作できる
6回	フレーム、パケット、セグメント	WiresharkでEthernetフレーム、TCP 3ウェイハンドシェイクの確認方などを理解し、操作できる
7回	アプリケーションプロトコルの確認	WiresharkでDNS、HTTP、HTTPSのキャプチャでき、それらを分析できる
8回	DNSトラフィック	DNSの要求と応答パケットの探索ができ、分析できる
9回	MySQLデータベースの攻撃	攻撃への対策法を理解し、攻撃への対処ができる
10回	サーバログを読む	ログの読み方を理解し、ログを分析できる
11回	暗号化と復号化	OpenSSLとハッカーツールで暗号化と復号化の方法を理解し、それらを操作できる
12回	TelnetとSSH、ハッシュ	WiresharkでTelnetとSSHのパケットをキャプチャでき、それらを分析できる
13回	Snortとファイアウォール	設定と状態の確認法を理解し、設定・検証できる
14回	ログファイルの変換と実行ファイルの抽出	ログの変換、特定の情報の抽出する方法を理解し、実際に操作できる
15回	通信データから脅威の原因を特定	HTTPとDNSのデータから脅威を特定法を理解し、実際に操作できる