2020年度　日本工学院八王子専門学校

ＩＴスペシャリスト科　　(ｾｷｭﾘﾃｨ専攻)

セキュリティ実習２

対象	４年次	開講期	前期	区分	必	種別	実習	時間数	60	単位	2
担当教員	坂部			実務経験	無	職種					

授業概要

シスコシステムズのルータやスイッチを用いたセキュリティ実習を行います。

到達目標

セキュリティエンジニアとして最低限な知識と技能（CCNA CyberOpsに合格できるレベル）を有することを目標とする。攻撃対象となりうるOS（WindowsやLinux）のシステム管理法の習得から始め、ネットワークを流れるパケット（正常時と擬似的な攻撃を行った場合）の収集・解析を行い攻撃か否かを判断できるようになる。攻撃を回避するための安全な通信技術を適用する方法を習得する。

授業方法

CCNA CyberOpsに準じた実習を行う。個人で行う実習が中心となる。実習内容はセキュリティに関わるOSの仕組みを確認し、OS標準のコマンドの使い方を使ったシステムの管理などを行う。ネットワークを流れるパケットを監視し、ネットワークの動作を再確認する。サーバへの攻撃を体験し、攻撃の痕跡をログ(記録)から読み取る。更にサーバを攻撃から守るために必要な技術を実装し、セキュリティ技術を習得していく。

成績評価方法

試験と課題、理解度確認の小テストを総合的に評価する。授業参加度、授業態度も評価に含まれる。

履修上の注意

セキュリティの基本的な知識を学習していることが前提となる。理由のない遅刻や欠席は認めない。授業時数の４分の３以上出席しない者は定期試験を受験することができない。

教科書教材

資料を配布する

回数	授業計画
第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）
第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）
第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）

2020年度　日本工学院八王子専門学校	
ＩＴスペシャリスト科　　(ｾｷｭﾘﾃｨ専攻)	
セキュリティ実習２	
第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）
第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）
第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）
第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）
第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）
第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）
第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）
第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）
第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）
第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）
第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）
第１５回	通信データから脅威の原因を特定（HTTPとDNSのデータから脅威の特定法を理解し、実際に操作できる）