2022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

ネットワークセキュリティ実習１

| 対象 | 3年次 | 開講期 | 後期 | 区分 | 選 | 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

（セキュリティ専攻）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機能を実習で確認する。

到達目標

この実習の到達目標はネットワークセキュリティ演習1で学習するシステムのセキュリティに向上に関わる知識や技術の習得である。WindowsやLinuxの管理に必要なコマンドを使ったシステム管理の方法、ネットワークの各種プロトコルの動作とその取得とその内容の分析、通信の暗号化・復号化とログ解析の技術津を習得する。

授業方法

この実習はシスコネットワーキングアカデミーのCCNACybersetuciryOprationsに準じた実習を各自のノートPCを使って個人ごとに実習する。Linuxやネットワークの実習は仮想環境を利用するため実機としてネットワーク機器を利用することはない。それぞれの実習終了後、まとめのレポートを提出する。

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、コンピュータの基本的な仕組みと操作をできることが前提となる。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。実習機材は他のクラスと共用するので丁寧に扱うこと。

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で紹介する。

| 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） |

| 2022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 | |
| ネットワークセキュリティ実習１ | |
| 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、TCP3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のデータから脅威を特定法を理解し、実際に操作できる。） |