6.8 包括的サイバーセキュリティ演習

[開講科目名]

(授業科目)高度サイバーセキュリティ PBL Ⅰ／(enPiT-Pro)包括的サイバーセキュリティ演習

[開講科目名(英)]

Comprehensive Cyber Security Training

[単位数] 1 単位

[開講日]

(調整中)

[担当教員]

高野 祐輝(大阪大学), 明石 邦夫(情報通信研究機構), 宮地 充子(大阪大学)

[授業の目的・概要]

一般的に, サイバー攻撃は, 探索活動, 侵入・感染, 侵入・感染時攻撃, 侵入・感染後攻撃と言うように, いくつかの段階を踏んで行われる事が多い.

そのため, サイバー攻撃に適切に対処するためには, マルウェア解析や暗号技術といった要素技術の習得のみではなく, サイバー攻撃の各段階における手法と防御技術を系として捉え, 包括的に理解し, 適切なネットワーク設計をする必要がある.

そこで, 本 PBL では, 仮想エンタープライズネットワークを用いて, サイバー攻撃における各段階の手法を学習するとともに, ネットワークレベルでの対策手法とネットワーク設計の演習を行う.

[学習目標]

本 PBL では攻撃手法学習, ネットワークレベル防御演習, 検疫ネットワーク設計演習の 3 つを行い, さまざまな攻撃とその対策手法について習得する.

(1) 攻撃手法学習

攻撃学習では, SYN スキャンなどの各種スキャン方法, 辞書攻撃, リフレクション攻撃などの攻撃手法について学ぶ.

(2) ネットワークレベル防御演習

ネットワークレベル防御演習では, OpenBSD の PF 等に代表されるパケットフィルタリング機構を利用し, 上記攻撃手法学習で学んだ攻撃手法に対するネットワークレベルでの対策手法を習得する.

(3) 検疫ネットワーク設計演習

検疫ネットワークの設計を行うことで, セキュアなネットワーク設計を行う方法を習得する.

[成績評価]

レポートによる評価を行い, 評価基準は以下の通りとする.

最優:ファイアウォール技術とペネトレーションテストを組み合わせて, 検疫ネットワークの設計と構築を行うことができる

優:ファイアウォール技術で DeMilitarized Zone のあるネットワーク設計と構築を行うことができる

良:ファイアウォール技術で適切なネットワークアクセスコントロールができる

可：各種サイバー攻撃手法と防御手法について論じることができる