6ZC-04

セキュリティインシデントにおける デジタルフォレンジック演習システムの開発

輿水　基秀† 福田　洋治‡ 井口　信和‡
近畿大学理工学部情報学科† 近畿大学情報学部/情報学研究所‡

1. はじめに

組織が直面するセキュリティ上の新たな脅威に対して，自らの役割に応じた能動的な対応ができるようなスキルを備えた人材で構成され，関連部署同士が緊密に連携するようなセキュリティ体制の構築が求められており，CSIRT はその 1 つである．CSIRT 人材には，初動対応で必要となる基本的な手順，操作やそこで収集したデジタル痕跡への簡易的な調査，被害拡大の防止，被害範囲の確認等でフォレンジック調査に関する知識やスキルが求められるが，それらを学ぶことができる無料の演習環境や教育コンテンツは不足している．

豊田らは，情報工学系の大学院を想定した高等教育機関や中小企業を対象に，演習プログラムの共同開発が可能なサイバー攻撃と防御演習システムを提案している[1]．VirtualBox， Docker といった仮想化技術を利用した演習環境上に，演習プログラムを実装するシステムを構築することで，高等教育機関や中小企業で導入が容易で演習プログラムが共同開発可能なエコシステムの考え方に基づくシステムである．

著者らは，特定の人や組織に対して，メールや Web など間接的な方法で，悪意ある第三者が仕掛けた罠に誘導するという誘導型攻撃に注目して， 標的型メールによる誘導型攻撃の訓練を行うための方法，これを無料のソフトウェアを組み合わせ実現する方法を与えている[2]．VirtualBox，Vagrant を用いた仮想環境上に攻撃メールを用いた Web を介した誘導型攻撃のインシデントの訓練シナリオを用意し，Java 言語によりシナリオ作成部，訓練内容提示部と操作・状況提示部を部分的に試作し，動作確認を行っている．

本研究では，情報系の初学者を対象にマルウェア感染，不正アクセス，DoS・DDoS 攻撃，記憶媒体等の紛失・盗難，メールの誤送信などのセキュリティインシデントにおけるフォレンジック調査の過程の知識やスキルを学ぶための VirtualBox，Vagrant などの無料の仮想化技術に基づく学習者の PC 上で動作させる演習システムを開発する．

A Digital Forensics Training System on Security Incident
†Motohide Koshimizu, Department of Informatics, Faculty of Science and Engineering, Kindai University
‡Youji Fukuta, Nobukazu Iguchi, Faculty of Infomatics, Kindai University / Cyber Informatics Research Institute, Kindai University

著者らの演習システムでは，閉じた仮想ネットワーク上に標的ホスト，攻撃ホスト等を配置し，これらのホスト上で攻撃ツールやコマンドを実行し，セキュリティインシデントを発生させ，適切なロガーの配置，その設定を検討する演習や，実際にロガーを配置，設定した上でのエビデンスの収集，保存，保護，解析の演習を想定している．攻撃の体験だけでなく，攻撃の活動を観測，記録し，その記録から攻撃が行われた痕跡を抽出するフォレンジック調査を学ぶ目的で，演習資料，VirtualBox，Vagrant に基づく演習環境のファイルセットの作成，演習システムに求められる機能の試作を行っている．

2. デジタルフォレンジック演習システム

本研究では，セキュリティインシデントにおけるフォレンジック調査の過程の知識やスキルを学ぶための VirtualBox，Docker などの無料の仮想化技術に基づく学習者の PC 上で動作させる演習システムを開発する．

演習システムの要件は，以下のとおりである．

要件 1 ・・・ ロガーの配置と設定の後，攻撃を体験する．次に取得したログに対してフォレンジック調査を行い，調査内容をフォレンジックレポートにまとめるという一連の過程をエミュレータ上で体験、演習ができる．

要件 2 ・・・ 学習者のノート PC でいつでも、どこでも、多種多様な攻撃に対するフォレンジック調査のシナリオの演習が無料で実施できる．

要件 3 ・・・ 学習者は演習環境（仮想環境）の使用，設定と管理等の複雑なコマンドや GUI の操作を必要としない．

要件 4 ・・・ 学習者のノート PC 上の演習環境（仮想環境）で起こった個々の事象について，学習者に説明やヒント，コメントが提示できること．

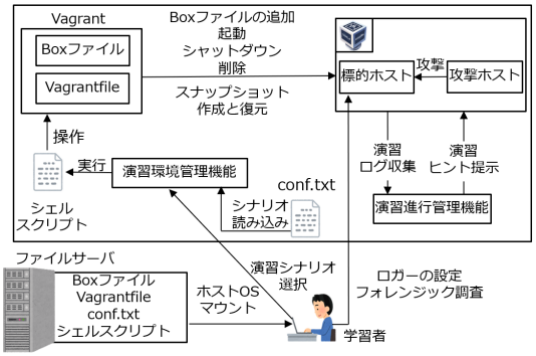

図 1 システムの構成と動作

上記の要件 1～4 を満たすように演習システムを考案した．本演習の構成と動作を図 1 に示す．

学習者は，演習シナリオに従って，標的ホストと攻撃ホストを操作し，ロガーの配置や設定をした後，攻撃を体験，取得したログに対して，フォレンジック調査するところまで，仮想化技術に基づきエミュレートするため，要件 1 に対応する．

演習は，学習者の PC 上で，VirtualBox を用いた仮想環境上でエミュレートするため，要件 2 を満たす．

学習者は，演習環境管理機能の GUI からボタン操作することで，ファイルサーバから Box ファイルの追加，標的ホストと攻撃ホストの起動，標的ホストと攻撃ホストのスナップショットの作成と復元，標的ホストと攻撃ホストのシャットダウン，Box ファイルと標的ホスト，攻撃ホストの削除ができる．以上のことから，要件 3 に対応する．

演習進行管理機能は，標的ホストと攻撃ホストのログファイルを監視して分析することで，学習者が行った操作に対して，説明やヒント，コメントを提示できる機能であり，要件 4 に対応する．

3. 動作確認

VirtualBox（6.1.38）と Vagrant（2.3.4）を PC（CPU：Intel Core i7-6700K 4．0GHz，Main Memory：32GB，OS：Ubuntu 22．04．1 LTS）上に導入し，演習環境管理機能と演習進行管理機能を Java（eclipse 2022-09，java sdk 8）で試作した．

ドライブバイダウンロード攻撃（CVE-2014-6332）に対するフォレンジック調査の演習シナリオ，演習の資料，演習環境のファイルセット（標的ホスト：Windows7 32bit SP1(Internet Explorer8) と攻撃ホスト；Kali Linux v2021.2 の仮想 OS）を作成した．

ドライブバイダウンロード攻撃に対するフォレンジック調査の演習シナリオ，演習の資料，演習環境のファイルセットを用いて，試作した機能が意図した動作をすること，演習システムを使用して演習が行えることをそれぞれ確認した．

作成した演習シナリオでは，標的ホストに，ロガーとして，Windows Event Log，Tshark の設定を行った後，攻撃ホストから攻撃スクリプトを実行して作成した悪性 Web サイトにアクセスすることで，疑似マルウェアがダウンロード，実行されバックドアが設置される．

フォレンジック調査では，収集したログを用いてダウンロードされた疑似マルウェアの抽出や疑似マルウェアがダウンロードされたディレクトリの絶対パス，バックドアの設置場所などを調査，フォレンジックレポートにまとめるという演習内容である．

演習中の標的ホストと攻撃ホストの操作画面を図 2 に示す．演習環境管理機能を使用した仮想環境の構築からスナップショットの作成と復元，仮想環境のシャットダウン，仮想環境の削除，ドライブバイダウンロード攻撃シナリオが実施可能であることを確認した．演習進行管理機能について演習シナリオとは別に動作確認用のファイルを作成し，意図した動作をすることを確認した．

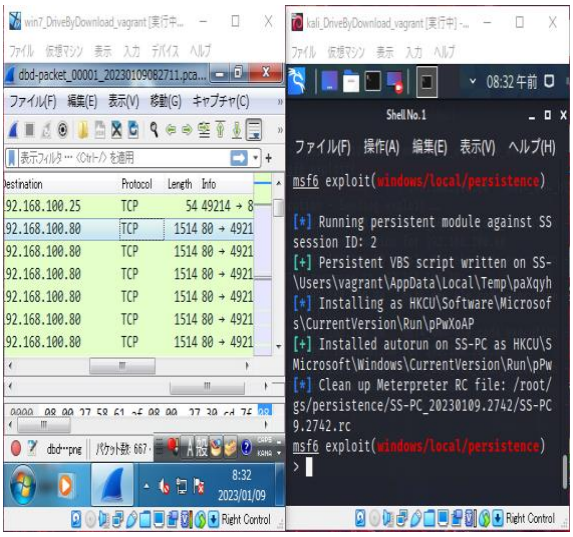

図 2 ドライブバイダウンロード攻撃シナリオの操作画面（左：標的ホスト Wireshark，右：攻撃ホスト Metasploit）

4. まとめ

著者らが考える演習システムに求められる演習環境管理機能と演習進行管理機能を試作，VirtualBox と Vagrant による仮想環境を構築，一例として，ドライブバイダウンロード攻撃に対するフォレンジック調査の演習シナリオ，演習の資料，演習環境のファイルセットを作成した．動作確認の結果，作成した演習の資料，演習環境のファイルセットを用いて，試作した機能が意図した動作をすること，演習システムを使用して演習が行えることを確認した．

今後の課題として，多種多様な攻撃に対するフォレンジック調査の演習シナリオの作成，試作中の演習進行管理機能の実装と評価，学習者に対して演習シナリオの効果などを調べる利用評価実験の実施が挙げられる．

参考文献

[1] 豊田真一，中田亮太郎，長谷川久美ほか：エコシステムで構成するサイバー攻撃と防御演習システム CyExec の提案，コンピュータセキュリティシンポジウム 2018 論文集，Vol.2018，No.2，pp.1301-1306（2018）

[2] 清時耀，福田洋治，井口信和：インシデントの仕組み学習と体験を可能とするセキュリティ訓練システムの開発-web を介した誘導型攻撃の訓練の検討-，2018 年度電気関係学会関西連合大会，pp.330-331(2018)