セキュリティ演習環境の自動構築システムに関する研究

22G353 石塚 美伶　(最所研究室)

1. はじめに

サイバー攻撃の増加に伴い, セキュリティ演習による人材育成が求められている. 特に実践的な技術力を身につけられるセキュリティ演習が注目されており, 国や大企業で実施されている. 香川大学においては企業の協力を得てセキュリティ演習が実施されているが, 多くの中小企業や教育機関の教育者にとって演習環境を構築するのは難しく支援が望まれる.

2. セキュリティ演習における環境構築の課題

著者らは, 演習環境の一例として隔離環境を試作した経験から, 構築経験のない教育者が演習環境を構築する際の課題を明らかにした.

課題① 考慮すべき点の多さによる手間と時間の増大

演習環境を構築するためには, ネットワーク構成や様々なソフトウェアの設定をしなければならない. さらに, サイバー攻撃の再現には, 攻撃手法に対応した脆弱性を持つ状態の環境が必要である. このような環境は, 安全に構築・演習できる必要がある.

課題② 環境構築に必要な専門技術の習得

OS やネットワーク等のインフラ技術や環境構築に関するノウハウが不十分な者にとって, 一から演習環境を構築・運用する負荷は大きい. 特に, 仮想化ソフトウェアやコマンドなどのツールの使い方も習得する必要がある.

課題③ 受講者数分の演習環境の構築

セキュリティ演習に費用を割けない組織にとって, 高価な計算機資源を揃えるのは困難である. 安価に用意できる計算機や既存の計算機資源を流用するなど, できる限り必要な費用を抑える必要がある.

3. 演習環境の自動構築システムの提案

教育者の演習環境構築における負担軽減を目指し, 実環境を模した演習環境を GUI 操作だけで仮想空間上に構築できる自動構築システムを提案する. これにより, 専門的な技術を持っていない教育者でも, 簡単に演習環境を構築できる. 2 章で述べた課題解決のために, 本システムは以下の要件を持つ.

要件① 最小限の入力項目 (課題①の解決)

演習内容に影響しない部分を自動的に補完し設定する. これにより, 演習環境を構築する際の教育者が考慮する点を削減することができる.

要件② 演習環境の自動構築 (課題②の解決)

登録済みの設定から演習環境を構築するためのスクリプトを自動的に作成し実行する. これにより, 教育者は専門的な技術を習得する必要なくボタン 1 つで演習環境を構築できる.

要件③ 軽量な仮想マシン (課題③の解決)

軽量の仮想マシンである“Firecracker”を用いる. これにより, メモリや二次記憶を効率的に使用でき, 性能の低い計算機でも複数の演習環境を構築できる. また, 仮想マシン間の通信は仮想ネットワークを用いて実現する.

4. 演習環境の自動構築システムの実装

本システムは, 演習環境の設定情報を格納するデータベース(DB), 環境構築の土台となる環境構築サーバ, 演習環境の設定や起動停止を管理する環境管理サーバ, 教育者の GUI 操作を実現する Web サーバで構成される(図 1). 本論では, 環境管理サーバおよび環境構築サーバにおける API とその内部処理, Web サーバにおける GUI を実装した.

① API の実装

API は, Web サーバから受け取った入力項目を元にデータベースの操作と演習環境の操作を行う. この API により, 演習環境の一覧や演習環境の詳細, 仮想マシンイメージの一覧などの情報の取得, 演習環境の保存, 任意の演習環境の起動停止が可能である.

演習環境の保存では, 演習環境自体の情報の他, 演習環境を構成する仮想マシンと仮想ネットワーク, それぞれの情報を受け取りテーブルに挿入する. 演習環境の環境 ID, 仮想マシン ID, 仮想ネットワーク ID は重複を防ぐため, データベースにレコードを挿入する際に”AUTO INCREMENT”を使用し自動的に割り当てており, 演習環境データを作成する段階では定められない. そのため, ID は負の値で仮置きしたものを使用し, 内容が合致するように置換している.

② GUI の実装

GUI は, ホーム画面(図 2)と編集環境演習環境の編集画面(図 3)から成る. ホーム画面では, 登録されている演習環境の一覧が表示され, 演習環境を新規作成するか, 任意の演習環境を選択して編集するかを選ぶことができる, また, ボタン 1 つで起動停止ができる. 編集画面では, ネットワークマップ上に仮想マシンと仮想ネットワークがオブジェクトとして表示される.

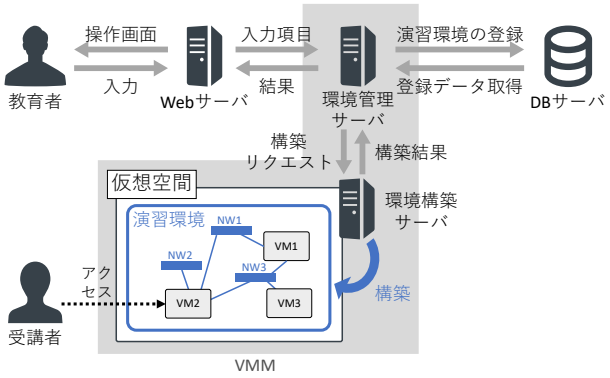

図 1 システム構成

追加ボタンを押すと，仮想マシンのイメージを選択して仮想マシン追加したり，仮想ネットワークを追加したりすることができる．また，ネットワークマップ上の任意のオブジェクトを選択すると，その仮想マシンもしくは仮想ネットワークの詳細設定ができる．

5. 評価

本システムを使用して，期待する演習環境を実現できるのか機能評価にて確認した．構築する演習環境は，3 台の仮想マシン(Web サーバ，DB サーバ，メールサーバ)と 1 つの仮想ネットワークで構成する．

本システムにより，演習環境の新規登録(仮想ネットワーク・仮想マシンの追加と詳細設定)と，登録した演習環境の起動停止が可能であることを確認した．また，起動した 3 台の仮想マシンへ SSH 接続し，Web サーバにはブラウザを用いてアクセスしサービスが稼働していることを確認した．

6. 考察

実験結果より，本システムの要件は概ね満たすことができたと考える．要件①に関して，設定ファイルの記述フォーマットなどを気にせずに，仮想マシンや仮想ネットワークの設定を完了することができるようになった．要件②に関して，ボタン 1 つ押すだけで，設定済みの演習環境の構築作業を終えることができるようになった．要件③に関しては，軽量な仮想マシンである”Firecracker”を用いることで必要な計算機資源を抑えている．さらに演習環境について調査し，必要な構成やメモリを洗い出し，どの程度の規模の演習環境を作成できるか明らかにする必要がある．

また，視覚的にネットワーク構成をわかりやすくするためにコネクタを使用する，IP アドレスの入力ミスやネットワーク範囲の重複を防ぐための支援を検討するなど，改善点があることを示した．

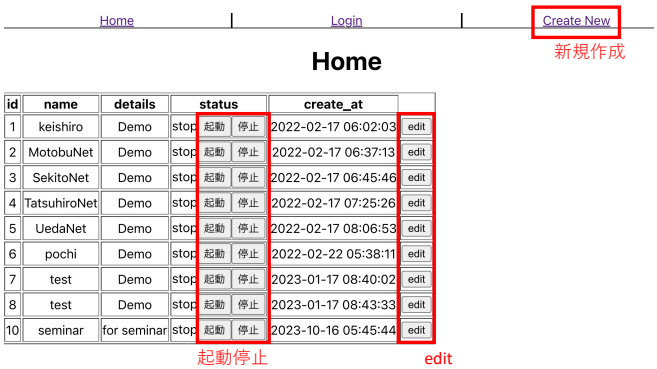

図 2 ホーム画面

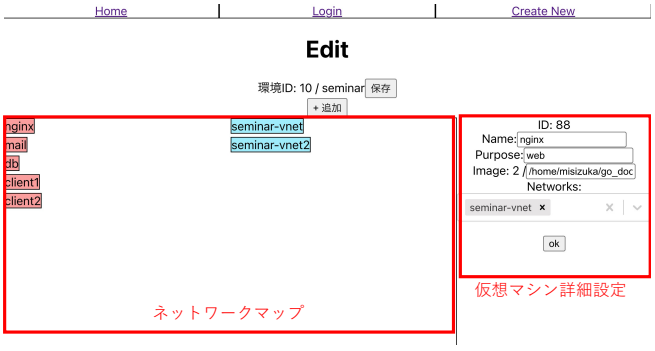

図 3 編集画面

7. 関連研究

Cuong Pham らは，セキュリティ演習のための仮想空間を構築するシステム”CyRIS(Cyber Range Instantiation System)”を開発している[1]．当論文では，YAML を記述することで演習環境を定義しており，Syntax エラーの修正など，演習環境の構築の本質とは異なる箇所に時間を割かねばならない．自身の経験上からネットワークを用いたマシン間の接続などは GUI を用いた方がわかりやすいため，GUI による演習環境の定義を目指す(課題①)．また，当論文では高性能な CPU やメモリを持つ大規模な設備を用いて仮想マシン 60 台に対して評価している．このような設備の使用が難しい地方大学においても，演習の受講生は 50 人を超えている．このことから，当論文よりも低性能な機器を用いて同規模の台数での演習を行える必要がある．自身の研究では，軽量な仮想マシン(microVM)を用いることでの実現を目指す(課題③)．

広川らは，演習環境を Docker コンテナ化することで，授業担当教員が個別の演習環境を提供する取り組みを行っている[2]．当論文では，教員の多くは演習環境を作成するためにコンテナ作成のレシピを作成することが不慣れである，という課題に対し Web UI を用いることでコンテナ作成を容易にした．ベースイメージに対し，OS が提供する任意のパッケージを追加できる．教員が演習環境を作成する際は，演習に必要なパッケージを Web UI に入力するのみで良く，自動的に演習環境として学生に提供される．しかし，セキュリティ演習では，OS などが提供しているパッケージ以外にもソースコードからビルドする必要があるソフトウェアがある場合や，ソフトウェアとは関係ない箇所で初期状態から OS の状態を大きく変更する必要がある場合がある．そのため自身の研究では，当論文を参考に，セキュリティ演習に耐えうる演習環境を作成できる GUI と構築機能を開発する(課題②)．

8. おわりに

本研究は，あらゆる組織においてセキュリティ演習が実施できるようになることが最終目標である．教育者の演習環境を構築する際の負担を軽減することを目指し，セキュリティ演習における環境構築の自動化システムを提案した． API と教育者が操作するための GUI を実装し，機能評価を行った．要件を概ね満たす実装ができた．しかし，実現化を目指すには，課題の洗い出しや機能・設計の見直しを繰り返す必要があると考える．

参考文献

[1] Cuong Pham, Dat Tang, Ken-ichi Chinen, and Razvan Beuran. Cyris: A cyber range instantiation system for facilitating security training. In Proceedings of the Seventh Symposium on Information and Communication Technology, SoICT'16, p.251–258, New York, NY, USA, 2016. Association for Computing Machinery.

[2] 佐藤悠，萩原威志ほか. Docker を用いたコンピュータ演習室向け linux 端末システムの設計. 研究報告セキュリティ心理学とトラスト (SPT), Vol. 2017, No.10, pp.1–6, 2017.