仮想マシンを活用した不正アクセス対策学習支援システムへの Web サイト攻撃対策学習機能の実装

Learning Function for Countermeasure against Web Site Attack in Learning Support System for Countermeasure against Unauthorized Access using Virtual Machine

福山 和生[*1]，井口 信和[*2]
Kazuki FUKUYAMA[*1], Nobukazu IGUCHI[*2]
[*1] 近畿大学大学院総合理工学研究科
[*1]Graduate School of Science and Technology, Kindai University
[*2] 近畿大学理工学部情報学科
[*2]School of Science and Engineering, Kindai University
Email: iguchi@info.kindai.ac.jp

あらまし：インターネットの普及に伴い，SQL インジェクションなどの Web サイトの脆弱性を狙った攻撃が増加している．また，セキュリティ学習に実環境を用いることは，現状のシステムに影響を及ぼすため危険である．そこで本研究では，仮想ネットワーク上に不正アクセス対策機器である WAF を動作させ，Web サイト攻撃のフィルタリングやログの収集・解析を実施する．これにより，利用者は仮想環境を用いて安全に Web サイト攻撃の対策学習を実施できる．
キーワード：**セキュリティ学習**，不正アクセス ，SQL インジェクション，WAF，仮想ネットワーク

1. 序論

インターネットの普及に伴い，不正アクセスによる被害が多発している．中でも，Web サイトの脆弱性を狙った攻撃が問題となっている．Web サイトへの不正アクセス事件で大きく報道される項目のうち，約 8 割が SQL インジェクションによって引き起こされている(1)．SQL インジェクションとは，Web アプリケーションへの入力を介して Web アプリケーションと連動するデータベースに不正な SQL 命令を実行させる攻撃である．この攻撃の対策方法の一つとして Web アプリケーションファイアウォール(以下，WAF)などの対策機器の導入が有効である．ところが警察庁の調査により，不正アクセス対策を実施し，システムの脆弱性を検証している組織は，5 分の 1 程度であることが分かった(2)．その理由として，不正アクセス対策に必要な知識を有したエンジニアの不足や，外部委託するための予算がないといった問題が指摘されている．そのため，各組織は独自で不正アクセス対策の教育を実施する場合がある．しかし，エンジニアの教育に実環境を用いることは，現状のシステムに影響を及ぼすため危険である．

そこで本研究では，これまで開発してきた『仮想マシンを活用した不正アクセス対策学習支援システム(3)』を基に，WAF を導入した Web サーバを仮想ネットワーク上で動作させることで，Web 攻撃対策の学習ができる機能(以下，本機能)を開発した．これにより，学習者は実環境に影響を与えず，仮想ネットワーク上で安全に Web 攻撃対策の学習を実施できる．

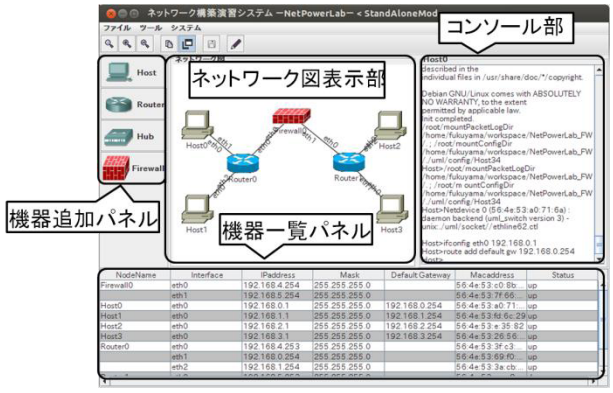

図 1 ネットワーク構築支援 GUI

2. 仮想マシンを活用した不正アクセス対策学習支援システム

このシステムでは，User Mode Linux を用いて作成した仮想マシンを，仮想的なネットワーク機器として動作させる．そして，ホストやルータなどのネットワーク機器同士を相互に接続することで，1 台の PC 上で実機を用いた場合と同様のネットワークの構築演習が可能となる．

2.1 システム概要

構築したネットワーク上で仮想的なファイアウォールを動作させる．これにより，ネットワーク上を流れるパケットのフィルタリングやログの収集，フィルタリングのテストができる．

2.2 ネットワーク構築支援 GUI

学習者が扱う GUI を図 1 に示す．『ネットワーク図表示部』は，仮想ネットワークの物理トポロジを表している．仮想マシンは，『機器追加パネル』から

画像をドラッグ＆ドロップすることで，選択した機器を生成できる．『コンソール部』は，生成した仮想マシンのターミナルと接続しており，コマンドの入力とその結果が確認できる．また,『機器一覧パネル』では，各機器の簡易的な設定情報の確認ができる．

3. 研究内容

本機能では，構築したネットワーク上で仮想的な Web サーバを動作させる．Web サーバとして用いる仮想マシンの作成には，設定に GUI を利用できる Virtual Box を使用した．この Web サーバは，図 2 に示した SQL インジェクションの実験ページを持っており，このページで学習者は，SQL インジェクションの体験や，WAF を用いた Web 攻撃のフィルタリング，ログの収集・解析ができる．以下に本機能の具体的な利用方法を示す．

3.1 ユーザ登録

学習者は，最初に実験用の新規ユーザの登録を行う．登録情報には，『ID，名前，住所，電話番号，メールアドレス，パスワード』を利用する．各項目を入力後，送信ボタンを押下することで登録が完了する．

3.2 通常ログイン

作成したユーザアカウントの ID とパスワードを，ログインページで正しく入力し，ログインボタンを押下することで通常のログインができる．

3.3 SQL インジェクション体験

ログインページで，ID には任意の文字列を入力し，パスワードに，SQL インジェクションが発生する『' OR 1='1』の文字列を入力し，ログインボタンを押下する．これにより，図 3 のように現在登録されているアカウント情報が全て表示されてしまう．

3.4 Web 攻撃フィルタリング

本機能では，Web 攻撃のフィルタリングに WAF を利用する．フィルタリング設定ページで，フィルタリングしたい Web 攻撃を選択する．選択された攻撃を WAF が検知した際，そのアクセスを拒否する．

3.5 ログ収集・解析

不正な命令が実行された際，WAF はログを収集する．また，ログの内容を解析することで，攻撃ごとにログを確認できる．

4. 動作検証

本機能の動作検証として，最初に，実験用ユーザアカウントを作成した．次に作成したアカウントを用いて，通常の方法でログインできるか確認した．確認後，ユーザ ID 入力部分には何も入力せず，パスワード入力部分に，SQL インジェクションが発生する『' OR 1='1』の文字列を入力し，ログインを試みた．これにより，現在登録済みのアカウント情報が全て表示されることを確認できた．次に，WAF を動作させ，SQL インジェクションをフィルタリング

図 2 SQL インジェクション実験用ページ

図 3 SQL インジェクション実行結果

する設定を適用した．適用後，再び SQL インジェクションを実行した．その結果，エラーメッセージ 403 番の Forbidden が表示された．これにより，SQL インジェクションのフィルタリングを確認できた．最後に SQL インジェクションを正しく検知できているか，WAF のログを確認した．ログより，Web ページが SQL インジェクションによって攻撃されているのを確認できた．以上の結果から，本システムは期待した動作をしていることが分かった．

5. 結論

本研究では，Web サイト攻撃対策の学習ができるシステムを開発した．本システムは仮想ネットワーク上で，実際に SQL インジェクションを発生させることで，攻撃手法と被害について学習できる．

今後は SQL インジェクション以外の Web 攻撃であるクロスサイトスクリプティングやバッファオーバーフローなどの対策を学習できるよう，機能の拡張を検討している．

参考文献

(1) 2013 年上半期 TokyoSOC 情報分析レポート：http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2013_h1.pdf
(2) 平成 25 年度不正アクセス行為対策等の実態調査 http://www.npa.go.jp/cyber/research/h25/h25countermeasures.pdf
(3) 福山和生，井口信和，“仮想マシンを活用した不正アクセス対策学習システム”，情報処理学会第 77 回全国大会講演論文集，pp.4-777 4-778，Mar.2014