7ZF-06

仮想マシンを用いた 攻防戦型ネットワークセキュリティ学習支援システムにおける SQL インジェクション攻撃に関する演習の実装

湯川誠人† 井口信和‡

近畿大学大学院総合理工学研究科† 近畿大学理工学部情報学科‡

1. 序論

警察庁が 620 の組織を対象に実施した調査によると，不正アクセス行為に対する脆弱性調査を実施していない組織は約 58%であった [1]．その原因として，セキュリティ技術者の不足等が挙げられる．この改善には，不正アクセス対策等のネットワークセキュリティ教育を各組織が実施し，セキュリティ技術者を育成する必要がある．

さらに，ここ数年で増加しているサイバー攻撃とその複雑さ [2]から，従来の学習のみでは実際に攻撃を防ぐことが難しくなっている．その解決には，防御の視点のみでなく，攻撃の視点から攻撃の性質などを学び，それを防御に活かすことが必要である [3]．両側の視点でセキュリティを学べる演習として，攻防戦型の演習である Capture The Flag がある．しかし，このような攻防戦型の演習を実環境で実施する場合，運用しているネットワークに影響を与えるおそれがある．また，実機を新たに用意して演習を実施する場合においても，実機のソフトウェアや内部の情報に支障をきたすおそれがある．

そこで，我々はこれまでに 1 対 1 で行う攻防戦型演習を可能とする仮想マシンを用いたネットワークセキュリティ学習支援システム（以下，本システム）を開発してきた [4]．本システムは，実機の代わりに仮想マシンを用いることで，安全に攻防戦型の演習を実施できる環境の提供を可能としている．これにより，従来の学習に攻撃の視点を加えた学習が可能なセキュリティ技術者教育の支援を可能とした．

本稿では，本システムで実施できる演習をより充実させるため，SQL インジェクション攻撃に関する演習を実施できるようにした．SQL インジェクション攻撃とは，データベースと連携した Web アプリケーションに対して，不正な SQL 文を入力することで，データベースに対して不正な操作を可能とする攻撃である．IBM Security Services の報告によると，2017 年下半期に観測したセキュリティインシデントの内，約 90%がサーバで発生していた [5]．サーバに対する攻撃の内訳としては，Web アプリケーション攻撃が最も多く占めており，その中で SQL インジェクション攻撃の試みが約 75%となっている [5]．このことから，この攻撃の性質と対策方法を理解することが重要である．この攻撃に関する演習を実施することにより，攻撃側はこの攻撃方法を学習でき，それを防御に活かすことができる．防御側は，その対応方法を学習できる．

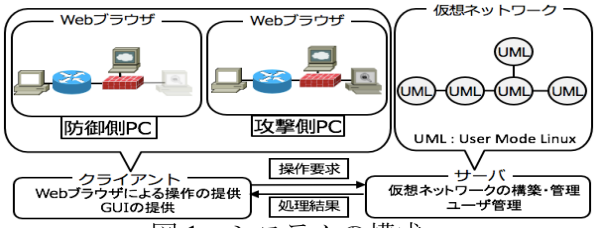

図 1：システムの構成

2. 研究内容

本システムの構成を図 1 に示す．本システムは，仮想的なネットワークの構築・管理などを実施するサーバとユーザインタフェースを提供するクライアントから構成される．サーバは，User Mode Linux と呼ばれる仮想化技術を用いて複数の仮想マシンを作成する．作成した仮想マシンは，Host またはネットワーク機器（以下，総称して仮想機器）として動作させる．

学習者は，PC 端末上にある Web ブラウザを用いてクライアントを操作する．クライアントは，学習者が操作した内容を操作要求としてサーバに送信する．サーバは，受信した操作要求を処理し，その結果をクライアントに送信する．クライアントは，受信した処理結果を Web ブラウザに表示する．

Implementation of a SQL Injection Attack Exercise on Virtual Machine-based Network Security Learning System Enabling Offensive and Defensive Battle Exercise

†Makoto YUKAWA, Graduate School of Science and Engineering Research, Kindai University

‡ Nobukazu IGUCHI, Department of Informatics, Faculty of Science and Engineering, Kindai University

2.1 学習者の役割と演習の終了条件

本システムを使用するにあたって，学習者には役割を与えている．攻撃側には，攻撃者の役割を与えており，継続的な攻撃を実施してもらう．防御側には，ネットワーク管理者の役割を与えており，ネットワークの監視や攻撃の対応などを実施してもらう．

演習は，攻撃側が実施した攻撃に防御側が気づいて，それに対応し，その攻撃が失敗したことを攻撃側が確認すると次の攻撃を実施するという流れを繰り返す．この演習の終了タイミングは，次の２つである．1 つ目は，制限時間が経過した時である．2 つ目は，本システムのクライアントが提供している画面に降参ボタンがあり，両側の学習者の内どちらかがそのボタンを押下した時である．

2.2 SQL インジェクション攻撃に関する演習

Web サーバが提供している Web ページには，攻撃側と防御側がアクセス可能なページと防御側のみアクセス可能なページが存在する．攻撃側と防御側がアクセス可能なページからは，ユーザの新規登録ページとログインページ，パスワード変更ページにアクセスできる．新規登録には，ID・名前・メールアドレス・パスワードを使用する．攻撃側は，ログインページとパスワード変更ページに対して SQL インジェクション攻撃を実施できる．

また，防御側のみアクセス可能なページからは Web サーバのログの確認が可能なページと登録ユーザの確認が可能なページ，ログインとパスワード変更が可能なページに関する各ソースの修正が可能なページ（以下，修正ページ）にアクセスできる．防御側は，修正ページを用いて SQL インジェクション攻撃に対応する．

防御側は，Web サーバを含む仮想ネットワークを構築する．そして，Web サーバのログと登録ユーザを確認する．構築を終えたことを確認した攻撃側は，ログインページないしパスワード変更ページにアクセスして，SQL インジェクション攻撃を実施する．Web サーバのログと登録ユーザから，SQL インジェクション攻撃が実施されたことを知った防御側は，修正ページにアクセスしてログインページとパスワード変更ページの各ソースに対して入力データのエスケープ処理を実施する．エスケープ処理が完了すると，そのページにある完了ボタンを押下する．押下すると，そのソース内容が実際のログインページとパスワード変更ページに反映される．

3. 実験・考察

動作検証として，実装した SQL インジェクション攻撃に関する演習が正しく動作するかを確認した．実験の手順は次の通りである．最初に，防御側が Web サーバを含む仮想ネットワークを構築する．構築を終えると，ユーザの新規登録ページにアクセスしてユーザを新規に登録する．正常に登録されたかは，ログインの実施と登録ユーザから確認する．次に，攻撃側がログインページへアクセスし，ID 欄は空欄，パスワード欄には「’ OR ‘A’=’A」を入力してログインする．その結果，個人情報の取得ができたかを確認する．次に，防御側が Web サーバのログと登録ユーザを用いて SQL インジェクション攻撃が実施されたことを確認する．確認すると，修正ページへアクセスして，その攻撃に対応する．最後に，攻撃側が最初と同じ行為を実施した結果，個人情報の取得ができなくなっていることを確認する．実験の結果，目的通り正しく動作していることを確認した．

4. 結論

本稿では，SQL インジェクション攻撃に関する演習を実施できるようにした．これにより，攻撃側は SQL インジェクション攻撃の攻撃方法を学習でき，それを防御に活かすことができる．防御側は，その対応方法を学習できる．今後の予定として，DNS サーバを用いた新たな演習の実装を検討している．

謝辞

本研究は JSPS 科研費 18K11592 の助成を受けたものです．

参考文献

1) 警察庁サイバー犯罪対策：平成 29 年度不正アクセス行為対策等の実態調査，入手先<https://www.npa.go.jp/cyber/research/h29/h29countermeasures.pdf>（参照 2018-12-21）．
2) 総務省事務局：サイバーセキュリティの現状と総務省の対応について，入手先<http://www.soumu.go.jp/main_content/000467154.pdf>（参照 2018-12-21）．
3) Uma, M. and Padmavathi, G.: A Survey on Various Cyber Attacks and Their Classification, *IJNS*, Vol.15, No.5, pp.390-396(2013).
4) 湯川誠人，井口信和：仮想マシンを用いた攻防戦型ネットワークセキュリティ学習支援システムにおけるネットワーク型 IDS を用いた不正侵入シナリオの実装，インターネットと運用技術シンポジウム論文集，Vol.2018，pp.92-99（2018）．
5) IBM Security Services : 2017 年下半期 Tokyo SOC 情報分析レポート，入手先<https://www.ibm.com/blogs/tokyo-soc/wp-content/uploads/2018/06/tokyo_soc_report2017_h2.pdf>（参照 2018-12-21）．