[ポスター発表] 研究報告

仮想マシンを活用し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性能評価実験の検討

湯川 誠人[1]　井口 信和[2,a)]

Examination of Performance Evaluation Experiment of a System for Supporting Learning of Network Security Enabling Offensive and Defensive Battle Exercise Using Virtual Machines

1. はじめに

警察庁が企業や教育機関など，692 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 62%と，半数を上回っていた [1]．その原因として，予算やセキュリティ技術者の不足などが挙げられている．この現状の改善には，不正アクセス対策など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．

さらに総務省の報告によると，1 年間で観測されたサイバー攻撃回数が 3 年で約 10 倍に増えている [2]．このように，サイバー攻撃の増加やその複雑さ [2] から，対策難易度が向上している．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，そこから実際の対策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，攻防戦型の演習が存在する Capture The Flag がある．しかし，このような攻防戦型の演習を，運用しているネットワーク上で実施する場合，ネットワークに障害が発生し，利用者に影響を与える可能性がある．さらに，実機を新たに用意して演習を実施する場合，実機の OS 等の動作に支障をきたすおそれがある．

これまでに，我々は攻撃視点を取り入れたネットワークセキュリティの演習が安全・手軽に実施できる環境の提供を目的に，仮想マシンを活用し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（以下，本システム）を開発してきた [4]．本システムは，2 人の学習者が攻撃側と防御側に分かれてネットワークセキュリティの演習を実施することを可能とする．本システムにより，学習者は実環境・実機に影響を与えることなく，安全に攻防戦型の演習を実施できる．また，システムの利用の手軽さから，学習者が繰り返し演習できる．前回の報告で，本システムにおける各仮想機器 1 台の起動に要するメモリ使用量と時間を確認する実験を述べた．本稿では，起動している仮想機器の種類やその台数によって新たに追加する仮想機器の起動に影響があるかを検証する実験と本システムを円滑に利用できるかを確認するための実験を検討する．

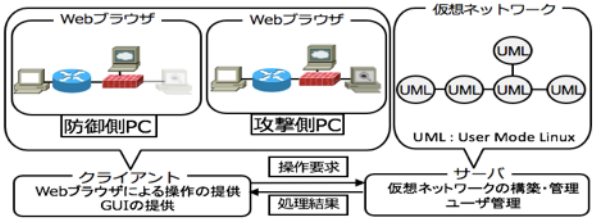

図 1　システムの構成

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を構築・管理するための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 端末上の Web ブラウザで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へ送信する．サーバは，受信した操作要求の処理を行い，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．

続いて，攻防戦型演習の流れについて述べる．始めに，防御側が Host，Router，Hub，Web Server，Firewall，NIDS を用いて仮想ネットワークの構築を実施する．構築を終

1　近畿大学大学院　総合理工学研究科
Graduate School of Science and Engineering Research, Kindai University
2　近畿大学 理工学部　情報学科
Department of Informatic, Faculty of Science and Engineering, Kindai University
a)　iguchi@info.kindai.ac.jp

えると，攻撃側に構築完了の旨を伝える．それを受け取った攻撃側は，防御側が構築した仮想ネットワークに攻撃用 Host を配置する．配置が終わると，攻撃側は防御側が構築した仮想ネットワークに対して攻撃を実施し，防御側に攻撃開始の旨を伝える．それを受け取った防御側は，攻撃箇所や攻撃の種類を特定し，その対応を実施する．攻撃側は自身が実施した攻撃が失敗したことに気づくと，次の攻撃を実施する．以上のように，攻撃と防御を交互に繰り返す．なお，本システムで実施可能な攻撃は，DoS 攻撃，ARP Spoofing 攻撃，不正侵入攻撃，SQL インジェクション攻撃の 4 つである．

DoS 攻撃を実施する場合，攻撃側は，攻撃用ホストを用いて攻撃対象の仮想機器に SYN Flood 攻撃を実施してもらう．防御側は，ネットワーク監視ツールなどを用いて SYN Flood 攻撃が実施されていることに気づいてもらう．その後，防御側はアクセスリストや iptables の設定などを施し，DoS 攻撃に対応してもらう．

ARP Spoofing 攻撃を実施する場合，攻撃側は，攻撃用ホストを用いて攻撃対象の仮想機器に ARP Spoofing 攻撃を実施してもらう．防御側は，仮想ネットワーク内にあるいずれかの仮想機器に対して ARP テーブルの確認を実施してもらい，IP アドレスと MAC アドレスの対応付けが正しくないものを見つけてもらう．その後，対応付けが正しくない仮想機器の ARP キャッシュに対して静的エントリを登録し，ARP Spoofing 攻撃に対応してもらう．

不正侵入攻撃を実施する場合，攻撃側は，攻撃対象の仮想機器に対してポートスキャンを実行し，23 番ポートが開いている場合，Telnet 接続をしてもらう．なお，接続時に聞かれるユーザ名・パスワードは脆弱なものを設定している．防御側は，仮想機器のログを確認し，不正な侵入がされていることを確認すると，ポートフィルタリングの設定などを実施して不正侵入攻撃に対応してもらう．

SQL インジェクション攻撃を実施する場合，攻撃側は，Web Server が提供している Web ページに対して SQL インジェクション攻撃を実施し，データベースを不正に参照，破壊，改竄してもらう．防御側には，Web Server が提供している Web ページを利用してログや登録ユーザ情報を確認し，SQL インジェクション攻撃に気づいてもらう．その後は Web Application Firewall の設定をしてもらい，SQL インジェクション攻撃に対応してもらう．

3. 性能評価実験

性能評価実験において，サーバとして使用する PC のスペックは，CPU: Core i7 @3.4GHz，Mem: 16GB，OS: Ubuntu 14.04 LTS である．

一つ目の実験として，仮想ネットワークの各規模において，各仮想機器の起動に要する時間（以下，起動時間）を計測する予定である．これにより，仮想ネットワークの規模が仮想機器の起動に影響があるかを検証する．想定する演習のネットワークの規模は，Web Server と攻撃用ホスト，NIDS がそれぞれ 1 台，その他の仮想機器はそれぞれ 1 台以上 10 台以下としている．システムの仕様上 1 台と想定する仮想機器は実際の演習でも 2 台以上使用することを禁じている．本実験では，Hub，Host，Router，Firewall，Web Server，NIDS，攻撃用ホストをそれぞれ複数台起動した仮想ネットワークを 10 パターン用意し，各仮想ネットワークにおいて新たに仮想機器 1 台を起動した場合のその起動時間を計測する．なお，Hub はコンソール部を使用しないため起動時間を計測しない．計測回数はそれぞれ 20 回とし，その結果から平均起動時間，標準偏差，最長起動時間，最短起動時間を算出する．

二つ目の実験として，攻撃を実施している仮想マシン及び攻撃が実施されている仮想マシンの応答時間・CPU 使用率・メモリ使用量をそれぞれ 20 回計測する予定である．これにより，本システムを円滑に利用できるかを確認する．応答時間は，コンソールに対して入力を施してからその結果が出力されるまでの時間としている．CPU 使用率は，攻撃中の最大 CPU 使用率としている．メモリ使用量は，攻撃後と攻撃前のメモリ使用量の差分としている．本実験は，1 台の Hub，2 台の Router，4 台の Host で構成される仮想ネットワークにおいて実験を実施する．実験対象となる攻撃は，一定時間攻撃が自動的に実行される DoS 攻撃と ARP Spoofing 攻撃とする．攻撃時間は 1 分間とする．

4. おわりに

本稿では，仮想ネットワークの規模が仮想機器の起動に影響があるかを検証する実験と本システムを円滑に利用できるかを確認するための実験を検討した．今後の予定として，有用性を確認するため，利用評価実験を実施する予定である．

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 30 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/h30/h30countermeasures.pdf >（参照 2019-10-15）．
[2] 経済産業省：IT 人材の最新動向と将来推計に関する調査結果，入手先 <http://www.meti.go.jp/press/2016/06/20160610002/20160610002.pdf >（参照 2019-10-15）．
[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）．