仮想マシンを用いた自動攻撃・評価機能を有する ネットワークセキュリティ演習システムの開発

A Network Security Exercise System with Functions for Attacking Networks and Checking Answers Automatically Using Virtual Machines

鈴木　翔太[*1]，　立岩　佑一郎[*2]，　山本　大介[*3]，　高橋　直久[*4]，
Shota SUZUKI[*1]，Yuichiro TATEIWA[*2]，　Daisuke YAMAMOTO[*3]，　Naohisa TAKAHASHI[*4]
*1 名古屋工業大学工学部情報工学科
*1 Nagoya Institute of Technology, Computer Science and Engineering
Email: shota@moss.elcom.nitech.ac.jp

あらまし： 受講者がネットワークに対する攻撃の痕跡を分析し，結果を答案として提出するネットワークセキュリティ演習を対象とする，以下の特徴をもつ演習システムを提案し，その実現法について述べる．（1）仮想マシンを用いたネットワーク構築機能により，少ない機材で同時に複数の受講者が演習できるようにする．（2）指導者の設定に従って攻撃する機能，及び，答案を正誤判定する機能を実現して，指導者の負荷を減じるとともに，受講者の利便性を向上させる．
キーワード：ネットワークセキュリティ，e-learning，仮想マシン

1.　はじめに

仮想マシンとは，計算機上で擬似的に稼働する計算機である．LiNeS は，仮想マシン User-mode Linux（以下，UML）によるネットワーク（以下，VMN）を提供する．

LiNeS を用いて，攻撃の特定方法の学習とサーバ管理の学習を目的とする演習を行う．受講者には VMN が与えられ，その中で受講者は攻撃を発生させる．攻撃を調査し，その証拠となる部分を見つけ，それを答案として指導者に提出する．指導者は答案を評価し，評価結果に応じて答案の再提出や，次の演習の指示を受講者に行う．

しかし，この演習では以下の問題が発生する．

問題 1：受講者の行動でネットワークの状況が変化し，想定していた答案と異なる可能性がある．

問題 2：攻撃の特定方法をより深く学ぶために，受講者に攻撃の種類を通知することなく発生させる必要がある．

問題 3：指導者の評価結果を待つ間，学習者に待機時間が発生してしまう．

これらの問題を解決するために，演習開始時に VMN を構築し，攻撃と評価を自動化した演習システムを提案する．

2.　提案システム

各攻撃に対する攻撃の種類，実行マシン，発生（終了）タイミング（演習開始からの経過時間（秒）），対象マシンからなる設定を攻撃設定，攻撃の種類，対象マシン，攻撃証拠の所在場所（ファイルパス）と内容（文字列）からなる４つ組（攻撃様式と呼ぶ）に対する正解の基準を正解基準と定義する．

提案システムは以下の特徴を持つ．

特徴 1：指導者により，VMN の構成，攻撃設定と正解基準のリストを演習シナリオとして設定する機能を実現する．また，演習開始時に，毎回，演習シナリオに従い，VMN を新たに構築する．これにより，受講者は同じ状況下で演習に取り組むことができる．

特徴 2： 演習シナリオに従い，攻撃を自動的に発生させ，終了後に受講者に答案開始を通知する機能を実現する．これにより，受講者に攻撃の種類を通知することなく，演習を実施できる．

特徴 3：受講者が，VMN 内のログなどを調べて，攻撃様式を作成し答案として送る機能を実現する．また，答案と，演習の正解基準とを照合し，答案の正誤を判定する機能を実現する．これにより，指導者の負担を軽減するとともに，受講者が直ちに答案の正誤を確認して次の演習に進めるようにする．

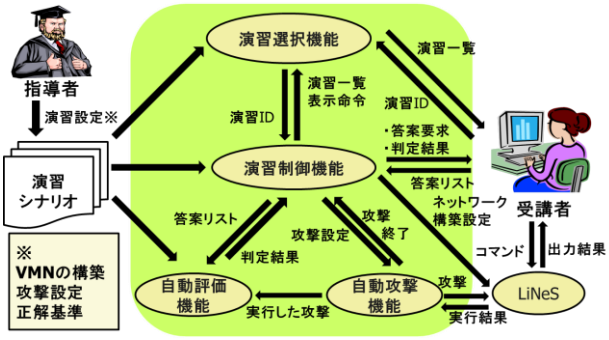

図 1：提案システムの構成図

次に，各機能の実現法を示す．

機能 1：自動攻撃機能

演習シナリオの攻撃設定のリスト（以下攻撃リスト）を入力として用いる．演習時刻が読み込んだリスト内の発生（終了）タイミングと一致した攻撃をすべて発生（終了）させる．すべての攻撃が終了したら，そのことを演習制御機能に通知する．攻撃設定で用いるタグ，属性の一覧を表 1 で示す．

機能 2：自動評価機能

攻撃リスト A，複数の答案まとめた答案リスト B，正解基準を入力とする．各答案の評価結果を格納するリストを C としたとき，以下の手順で動作する．

STEP1：総合評価を格納する変数 judge = true とする．

STEP2：リスト B が空の時，STEP6 へ．そうでなければ先頭から要素を 1 つ取出し b とする．
STEP3：b に空白行が一つでもあれば judge = false，リスト C の末尾に false を追加し STEP2 へ．
STEP4：b の攻撃証拠の所在場所がコマンドであれば b の対象マシンで実行結果を，ファイルパスであれば b の対象マシンからそのファイルの中身を変数 r へ格納する．A の内容（文字列）が r に含まれていなければ judge = false，リスト C の末尾に false を追加し STEP2 へ．
STEP5：b の攻撃の種類がリスト A に存在していればその要素を取出し，正解基準を用いて正誤判定を行う．正解ならリスト C の末尾に true を追加し，存在していない，または不正解なら judge = false，リスト C の末尾に false を追加する．その後 STEP2 へ．
STEP6：リスト A が空でなければ judge = false．
STEP7：演習制御機能にリスト C 及び judge を渡す．

表 1：攻撃設定のタグ・属性一覧

攻撃タグ	
passwordcrack	パスワードクラックを行う（略称 p）
synflood	DoS 攻撃を行う（s）
backdoor	バックドアの設置を行う（b）
サービス利用タグ	
remote	Ssh によるリモートログインを行う（r）
ftp_get	ftp を使用しファイルを受信する（fg）
ftp_send	ftp を使用しファイルを送信する（fs）
タグで使用する属性一覧 （特に記載がなければすべてのタグで使用する）	
start_time	発生タイミング
end_time	終了タイミング
a_id	実行するマシンの ID
t_id	対象となるマシンの IP アドレス
t_user	対象となるユーザ名（s 以外）
t_srvice	対象となるサービス（p）
t_port	対象となるポート番号（s）
t_pass	使用するパスワード（b，r，fg，fs）
t_file	送信（受信）するファイル名（fg，fs）

3. プロトタイプシステム

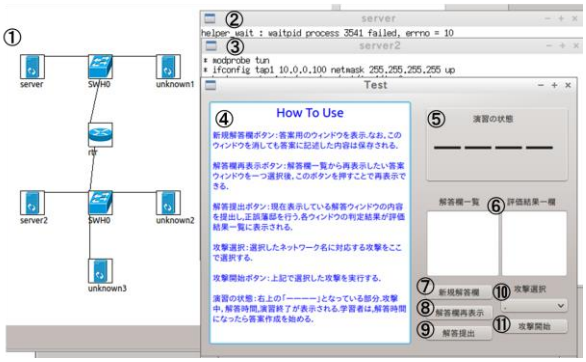

図 2：受講者画面

図 2 で，評価実験中の受講者の演習画面を示す．(1)は演習するネットワークのトポロジーである．ネットワークで発生させる攻撃設定を(10)で選択し，選択した攻撃を(11)を押すことで開始する．開始すると(5)が「攻撃中」に，攻撃が終了すると「解答時間」に切り替わる．「解答時間」になったら学習者はコンソール(2)(3)を調査し，発生した攻撃を特定する．特定した攻撃分(7)のボタンを押し解答欄を表示し，答案を記述する．記述後(9)のボタンを押すことで表示している解答欄すべての評価を行い，各評価結果が(6)に表示される．発生したすべての攻撃を特定できたら，演習の状態が「演習終了」に切り替わる．

4. 評価実験

プロトタイプを用いて，9 名の被験者が演習に取組んだ．これにより得られた総計 54 答案からランダムに選んだ 10 答案に対し，提案システムと指導者による正誤判定を比較評価した．この実験で，提案システムが評価結果を表示するまでにかかった時間は約 0.24 秒，指導者が評価結果を出すまでの平均時間は約 32 秒で，提案システムによる正誤判定は指導者より約 130 倍程度高速であり，答案に混入した空白行のあった答案を除く総ての答案で指導者と同じ判定結果であったため，有効性が高いことが分かった．

5. 関連研究

文献(1)では，仮想マシンによる仮想的なネットワークを用いて，遠隔演習環境の実現と攻撃を自動的に行う仮想クラッカーとサービスを自動的に利用する仮想ユーザの開発を行うことで，防衛方法のみを効率的に学べる演習環境の実現方法と評価実験を述べている．本稿では，指導者による攻撃の設定を文献(1)より簡略化し，受講者の答案を評価する機能を実装することで指導者の負担と受講者の待機時間の軽減を目指した．

文献(2)では，学習者のための仮想マシンネットワークの実現のための演習コースである．学習者は浸り一組となり，相手の管理するネットワークを攻撃したり，自身の管理するネットワークを相手の攻撃から防衛したりする．しかしながらこの手法は問題 1 を解決するものではない．

6. おわりに

本稿では，攻撃と評価を自動化した演習システムを提案した．今後の課題としては，特定した攻撃に対する防衛の設定を受講者が行い，それを評価する機能の開発などが挙げられる．

参考文献

(1) 立岩佑一郎，岩崎智弘，安田孝美：仮想マシンネットワークによる継続的なクラッキング防衛演習システム，電子情報通信学会論文誌 Vol.J96-D No.7 pp.1585-1594(2013)
(2) W. Du and R. Wang，”SEED: A suite of instructional laboratories for computer security education，” Journal on Educational Resources in Computing (JERIC)，vol.8，no.1，Article no.3，(2008)