

研究タイトル：サイバーセキュリティ技術者育成のための演習環境開発



氏名：	嶋田 / 泰幸	E-mail：	shimada@kumamoto-nct.ac.jp
職名：	制御情報システム工学科 教授	学位：	博士(工学)
所属学会・協会：	電子情報通信学会, 電気学会, 日本情報教育学会		
キーワード：	サイバーセキュリティ, 学習環境プラットフォーム		
技術相談 提供可能技術：	・サイバーセキュリティ学習環境の構築		

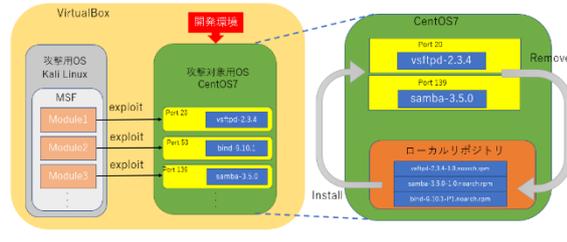
研究内容：

研究目的

多様な攻撃・防御演習が可能である演習環境(被攻撃環境)を開発し、サイバーセキュリティを学ぶ場で使用していただくことを目的とする

- ・多彩な攻撃・防御演習の実装
 - 学習効率の向上
- ・ローカルリポジトリを用いたサービスのパッケージ管理の実装
 - 新規脆弱性の追加、アプリケーション追加・管理の簡易化
- ・学生と講師にとって有用なツールの実装
 - 教育機関での使用に最適化

提案手法：演習環境



学生向け演習支援ツール



講師向け演習支援ツール



実装：攻撃・防御演習

実装した攻撃方法：8種類
実装した攻撃対象のサービス：9種類
実装した攻撃演習：10種類
実装した防御演習：8種類

サービス名	サービスの種類	攻撃方法	防御演習実装の有無(防御方法)
vsftpd-2.3.4	FTP	バックドア	○ (update to 2.3.5)
samba-3.5.0	ファイル	内部権限昇格	○ (patch file)
bind-9.10.1	DNS	DoS	○ (update to 9.10.4)
OpenSSH-7.4	SSH	脆弱性漁(列挙)	×
WordPress-4.7.1	Webアプリケーション	コンテンツインジェクション, XSS	○ (update to 4.7.2)
RHEL dhclient	DHCP	内部権限昇格	○ (patch file)
PostgreSQL-9.6.20	データベース	OSコマンドインジェクション	○ (update to 9.6.21)
Apache-2.4.6	Web	内部権限昇格	○ (change options)
MariaDB	データベース	ブルートフォースアタック	○ (change password)

Metvenomを用いたマルウェア演習

評価実験

- <「講師」目線からの実験>
- ・アプリケーション管理の容易さの検証
 - Metasploit2と本環境でvsFTPdのバージョン変更にかかる手順を比較
 - ・講師向けツールの有効性の検証
 - 講師向けツールを実際に教育機関でサイバーセキュリティの講義を行っている教授に使用してもらい、コメントを頂く
- <「学生」目線からの実験>
- ・初学者への対応と学習効率の検証
 - 学生にMetasploit2と本環境で、同じ時間で同程度の課題に挑戦してもらい、終了後にアンケートに回答してもらう(時間内に課題が終了した場合は、追加課題をする)
 - 対象学生：演習をある程度学習している学生4人、演習は初学者の学生6人
 - 実施時間：再環境ともに30分、課題数：再環境ともに2つ
 - アンケート内容：課題終了にかかった時間、追加課題の進捗、環境の学習効率や使いやすさに関する質問(演習をスムーズに進めることができましたか、などを1-5で回答)

実験結果

<「講師」目線からの実験>

- ・アプリケーション入れ替え手順数
 - 既存環境：6(操作はGUIのみ)、本環境：4(操作はGUIで完結)
- ・教授から、講師向けツールは必要なものであり、実用に適しているが、各種ツールの見た目や少し整えてほしいとコメント頂いた

<「学生」目線からの実験>

質問①：サイバーセキュリティ演習に必要な基礎的な知識を身に付けることができましたか
質問②：演習をスムーズに進めることができましたか、質問③：被攻撃環境の操作はしやすかったですか

学生	長崎県立大学	本校
使用環境	既存環境	本環境
課題1にかかった時間(分)	8.25	9.75
課題2にかかった時間(分)	24.25	18.25
終了後に行った他の演習数	0	1.25
質問①	3.5	3.75
質問②	4.25	4.75
質問③	3.75	4.0

質問②：本校の学生 本環境

現時点での成果と今後の計画

- <現時点での成果>
- ・10種類の攻撃演習と8種類の防御演習、演習に用いるアプリケーションのローカルリポジトリによる管理を実現
 - ・学生向けツールと講師向けツールの実装によって教育機関での学習用途での使用に最適化
 - ・評価実験より、ある程度演習を学んでいる学生から初学者まで広く学習効率を向上させることができることがわかった
- <今後の計画>
- ・攻撃演習の追加
 - ・CSSを用いた各種ツールの見た目の改善
 - ・講師が学生の演習の進捗を把握できるシステムの実装
 - ・講義形式での教育機関での試用実験