SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

ペネトレーションテスト自動化に向けたサイバー攻撃手段の定量的評価法の提案
A Proporsal of Cyber Attack Technique Scoring Method Toward Automatic Penetration Test

木藤 圭亮 * 加藤 駿 * 河内 清人 * 木下 洋輔 * 酒井 康行 *
Keisuke Kito Shun Kato Kiyoto Kawauchi Yosuke Kinoshita Yasuyuki Sakai

吉村 礼子 *
Ayako Yoshimura

キーワード サイバー攻撃手段, 定量的評価, スコアリング, ペネトレーションテスト, 自動化

あらまし

サイバー攻撃は日々増加を続け，国内組織を狙ったサイバー攻撃が横行している．JPCERT/CC に 2021 年 7 月〜9 月の 3 か月間に寄せられたインシデント件数は 8,786 件と前年同期比から約 2,000 件の増加となっている．[1]

サイバー攻撃を未然に防ぐためには，運用システムの脆弱性を積極的に発見し修正することが重要である．脆弱性を発見する一手法として，既知の脆弱性や攻撃手法を用いて疑似的にサイバー攻撃を試みることで脆弱性を発見するペネトレーションテスト (以下，ペンテスト) がある．NIST SP800-115[2] では,「アプリケーション，システム，ネットワークのセキュリティ機能を回避する方法を特定するために評価者が実際の攻撃を模擬して行うセキュリティテスト」をペンテストと定義している．

一般にペンテストは攻撃の起点と目的を設定し，起点から目的に近づくために，テスト対象に適切な攻撃手段の選択と実行を目的達成まで繰り返す．ここでの「適切な攻撃手段」とは，テスト対象に対して高い攻撃効果が得られることや，攻撃が発覚しにくいなどを意味する．そのため適切な攻撃手段の選択には，ペンテスターと呼ばれる高度な知識や経験を有する専門家が必要である．

テスト対象に模擬的に攻撃を行い脆弱性を検出する先行研究に，A2P2V[3] がある．A2P2V はテスト対象のシステム構成情報と攻撃目的を入力することで，目的達成のために必要な攻撃手段をアタックツリー分析する．アタックツリーから攻撃シナリオを生成し，攻撃シナリオに対応する攻撃ツールを実行してペンテストを行う．

先行研究は，テスト対象の構成情報をあらかじめすべて入力することが前提となっているが，実際には完全な構成情報を得ることは難しく，不十分な構成情報ではアタックツリー分析が行えない場合がある．また攻撃手段の検知されやすさなど「適切な攻撃手段」を選択することができず，先行研究で実行可能なペンテストは，ペンテスターが行うものと異なる場合がある．

本研究ではペンテスターが「適切な攻撃手段」を選択するときに，攻撃手段が対象システムに成立するか，攻撃手段を実行することによって攻撃が発覚するか，さらに攻撃手段実行の結果得られる効果の大きさ，の 3 点をもとに判断していると仮定し，攻撃手段を eVc(Evaluation Value of Capture:攻略評価値)，eVd(Evaluation Value of Detectability:発覚評価値)，eVe(Evaluation Value of Effectiveness:効果評価値) としてスコア化する手法を提案する．提案するスコア値を活用することで,「適切な攻撃手段」の選択が自動化可能となり，結果としてペンテスターが行うようなペンテストの自動化が可能になる．

参考文献

[1] JPCERT/CC, インシデント報告対応レポート［2021 年 7 月 1 日〜2021 年 9 月 30 日］,2021-10-24

[2] NIST, SP800-115 Technical Guide to Information Security Testing and Assessment, Sep 2008

[3] Nakanishi et al., Automated Attack Path Planning and Validation (A2P2V), Black Hat USA 2021 Arsenal

* 三菱電機株式会社, Mitsubishi Electric Corporation