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

部分観測マルコフ決定過程に基づいたニューラルエージェントを使用したペネトレーションテスト手法の提案

Proposal of a penetration testing method using neural agents based on partially observable markov decision process

米田　智紀 *　　大塚　玲 *
Tomonori Yoneda　　Akira Otsuka

キーワード　深層強化学習，ペネトレーションテスト，部分観測マルコフ決定過程

あらまし

ペネトレーションテストは機器やシステムに対して様々な技術を駆使して侵入を試みることで, 対象のセキュリティ上の脆弱性を検査する手法であり, 特に機械学習ベースの自律的ペネトレーションテスト技術は,offensive security を実現する重要な手法として, ますます増加, 巧妙化するサイバー攻撃への対応策になると目されている. 既に Deepexploit や Gyoison 等, 様々な機械学習ベースの自律的ペネトレーションテストツールが生み出されている. 中でも, 訓練データを予め準備しなくても自律的に攻撃手法を獲得できる強化学習によるペネトレーションテスタが注目を集めている.

本研究では, 従来から多くの提案があるマルコフ決定過程 (MDP) に基づく強化学習モデル [2] ではなく, ペネトレーションテストの過程で得られるシステムレスポンスをニューラル自然言語処理技術により解釈して状態を推定しながら次の最適攻撃行動を推定する部分観測マルコフ決定過程に基づく強化学習モデルに注目している.2020 年に発表された LeDeepChef[1] は, テキストベースのダンジョンゲームである Textworld を部分観測マルコフ決定過程 (POMDP) に基づく強化学習で効率的にゴールを見いだすニューラルエージェントを提案している. 本論文では, このニューラルエージェントを Windows/Linux 等の OS 環境に作用させ, エクスプロイトコマンドを行動集合に持たせることで, 実システムのペネトレーションテストへの適用可能性を評価した.

* 情報セキュリティ大学院大学, 神奈川県横浜市神奈川区鶴屋町 2-14-1 Institute of Information Security, 2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama, Kanagawa, Japan.

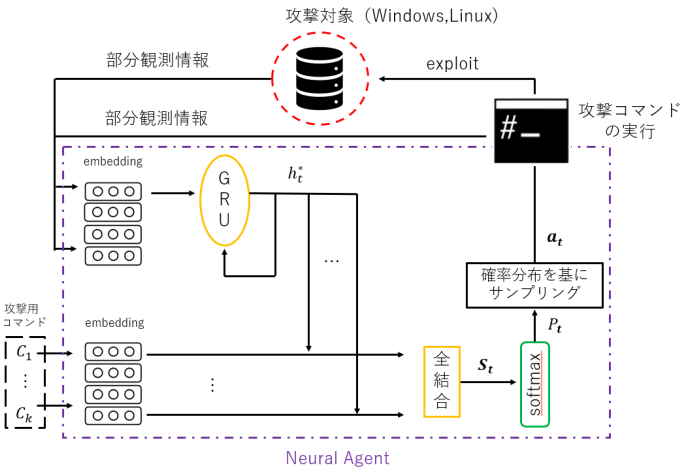

図 1: 部分観測マルコフ決定過程 (POMDP) モデルに基づくペネトレーションテスタの構成図 (提案手法)

参考文献

[1] Adolphs, Leonard, and Thomas Hofmann. “ LeDeepChef: Deep Reinforcement Learning Agent for Families of Text-Based Games.” In 34th Association for the Advancement of Artificial Intelligence Conference on Artificial Intelligence (AAAI 2020), 5180, 2020.

[2] Zennaro, Fabio Massimo, and Laszlo Erdodi. ”Modeling Penetration Testing with Reinforcement Learning Using Capture-the-Flag Challenges and Tabular Q-Learning.” arXiv preprint arXiv: 2005.12632 (2020).