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

# 深層強化学習による Web アプリケーションのペネトレーションテストの自動化に向けて

# Towards Automation of Penetration Testing for Web Applications by Deep Reinforcement Learning

久野　朔 *　　松浦　幹太 *
Hajime Kuno　　Kanta Matsuura

**キーワード** ペネトレーションテスト、深層強化学習、PPO、metasploit,exploit

## あらまし

近年、サイバー攻撃による情報の流出やシステムの改竄などの危険性が問題視されている。これに対抗する方策の一つとして、実際に対象環境に対して疑似的な攻撃を行い、侵入につながりうる脆弱性を発見するペネトレーションテストは非常に有効であるとされる。しかし、これには十分に訓練された人員が必要であり、大きなコストが要求される。

この問題を解消するために強化学習・深層学習・深層強化学習などを用いてペネトレーションテストを自動化・効率化する研究が存在している。[1-4]。しかし、実際のペネトレーションテストにおいて利用される脆弱性および複数のツールの情報を直接利用し、なおかつ強化学習・深層強化学習の本領ともいえる状態の遷移をペネトレーションテストに根差した形で取り入れた研究は確認した限りでは存在していない。

本稿では、多様な攻撃手法と対象の種類が存在しており、非常に使用頻度の高い web アプリケーションというカテゴリを対象としたペネトレーションテストの効率化のために深層強化学習を用いて、既存のツールおよび exploit を統合することを目標とする。最初に、単純なペネトレーションテスト環境の再現として、著名な web アプリケーション 15 種類の現存しているバージョンと公開されている exploit を元に模擬環境を作成し、それぞれのアプリケーションに対し、バージョンに適応する exploit を見つけ出すタスクを設定する。その後、このタスクに PPO アルゴリズムを用いた深層強化学習を適用し、学習を行ったエージェントが正しい exploit を見つけ出せることを示す。

次いで、exploit だけではない多数のツールの効力と、状態遷移の概念を導入した模擬環境を作成し、これに対し同様に PPO 深層強化学習を行い、より複雑なペネトレーションテスト分野における深層強化学習の有効性について検討する。

## 参考文献

[1] https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit, accessed on October 25, 2021.

[2] https://github.com/rapid7/metasploit-framework/wiki, accessed on October 31, 2021.

[3] Mohamed C. Ghanem and Thomas M. Chen, “Reinforcement Learning for Intelligent Penetration Testing”, 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2018.

[4] Ovidiu Valea and Ciprian Opris, “Towards Pentesting Automation Using the Metasploit Framework”, 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP), 2020.

* 生産技術研究所, 〒 153-8505 東京都目黒区駒場 4-6-1 Institute of Industrial Science, the University of Tokyo, Komaba, Meguro Ku, Tokyo To, 153-8505