

Automated penetration testing using reinforcement learning

Raju Molla

2421791

Research Context / Background

- Cyber-attacks are increasing in frequency and complexity, requiring continuous security assessment
- Traditional penetration testing is manual, time-consuming, and relies heavily on expert skills.
- Reinforcement Learning (RL) can automate penetration testing, enabling adaptive, multi-step vulnerability discovery.

Research Context / Background

- Cyberattacks are happening more often and getting smarter, so security checks need to be done all the time [1].
- Penetration testing finds weaknesses [2] so that people can't use them. Penetration testing the old-fashioned way is done by hand, takes a long time, and costs a lot of money [3].
- Manual methods depend a lot on what people know and can't be used on a large scale [3].
- Most automated technologies that are already available rely on rules or signatures and can't be changed [4].
- Reinforcement Learning (RL) lets agents figure out what to do by working together [5].
- RL is useful for jobs that need to be done in order, like cyberattacks that happen in steps [6].
- DeepExploit and other early RL-based pentesting tools show promise, but they don't work well when you need to use them on a large scale or repeat them [3].

Research Problem (Based on Literature Gap)

- Automated tools work based on rules [3], [4], but traditional pentesting relies on what people know.
- Automated tools today can't quickly adapt to new weaknesses [4].
- RL-based frameworks show promise, but only a few can be used in many situations or on a large scale [3], [6].

Research Gap: Lack of a flexible, reproducible, and adaptable RL-based penetration testing framework for academic and commercial purposes.

Research Aim and Objectives

Aim:

- Develop an adaptive RL-based automated penetration testing system.

Objectives:

- Design a virtual test environment with vulnerable machines.
- Implement an RL agent capable of scanning, enumeration, and exploitation.
- Evaluate RL agent performance against traditional pentesting tools.
- Analyse efficiency, accuracy, and adaptability of RL-driven testing.

Brief Literature Review / Gap

- RL has been successfully applied to sequential decision-making and autonomous systems [5], [6].
- DeepExploit demonstrates automated exploitation with RL but lacks modularity and scalability [3].
- Existing RL pentesting research focuses on limited tasks and controlled environments [3], [6].
- **Gap:** No comprehensive RL-based framework exists for adaptive, multi-step vulnerability discovery applicable in research and teaching.

Research Methodology

- Build virtual environment: Kali Linux, Metasploitable2/3, DVWA.
- Define action set: scanning, enumeration, exploitation.
- Implement RL agent using DQN or PPO via Stable Baselines3.
- Train agent through iterative interactions and reward-based learning.
- Evaluate agent performance compared to manual and automated tools.
- Document results, analyse metrics, and assess ethical considerations.

Project Planning and Resources

Resources:

- VirtualBox / VMware, Kali Linux, Metasploitable2/3, DVWA
- Python, Gym, Stable Baselines3, PyTorch/TensorFlow
- Metasploit Framework, Nmap, Nikto

Timeline:

- Week 1: Literature Review
- Week 2-3: Environment Setup & RL Design
- Week 4-6: RL Implementation & Training
- Week 7: Evaluation and Analysis
- Week 8: Thesis Writing

Project Impact and Limitations

Impact:

- Adaptive automated pentesting reduces human dependency.
- Enables repeatable and consistent security evaluation.
- Advances AI-driven cybersecurity research.

Limitations:

- RL requires significant computational resources.
- Ethical constraints prevent testing on live production systems.
- Performance may vary with different network configurations.

References

- [1] ENISA, “ENISA Threat Landscape Report,” 2023.
- [2] K. Scarfone, P. Mell, and M. Souppaya, *Guide to Penetration Testing and Vulnerability Assessment*, NIST, 2008.
- [3] Y. Shin et al., “DeepExploit: Fully Automatic Penetration Test Framework,” *BlackHat Asia*, 2019.
- [4] H. M. Almohri, D. Yao, and S. Pan, “Automated security assessment: Challenges and opportunities,” 2020.
- [5] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*, 2nd ed., MIT Press, 2018.
- [6] M. C. Ghanem and T. M. Chen, “Reinforcement learning for autonomous cyber operations,” 2020.

Thank You