Intelligent Penetration Testing using Deep Reinforcement Learning

Authors: Connor Blanchfield-Tomaszewski, Andrew Mahr, Jordan Zimmitti, Samuel Zurowski
Advisors: Dr. Vahid Behzadan, Dr. Mehdi Mekni, Dr. Adwoa Donyina

Overview

Penetration Testing (PT) is a form of ethical hacking where an attack is performed against a computer network to find vulnerabilities. Many organizations hire penetration testers to evaluate the strengths and weaknesses of a network. PT is both time consuming, expensive, and requires highly trained professionals [1].

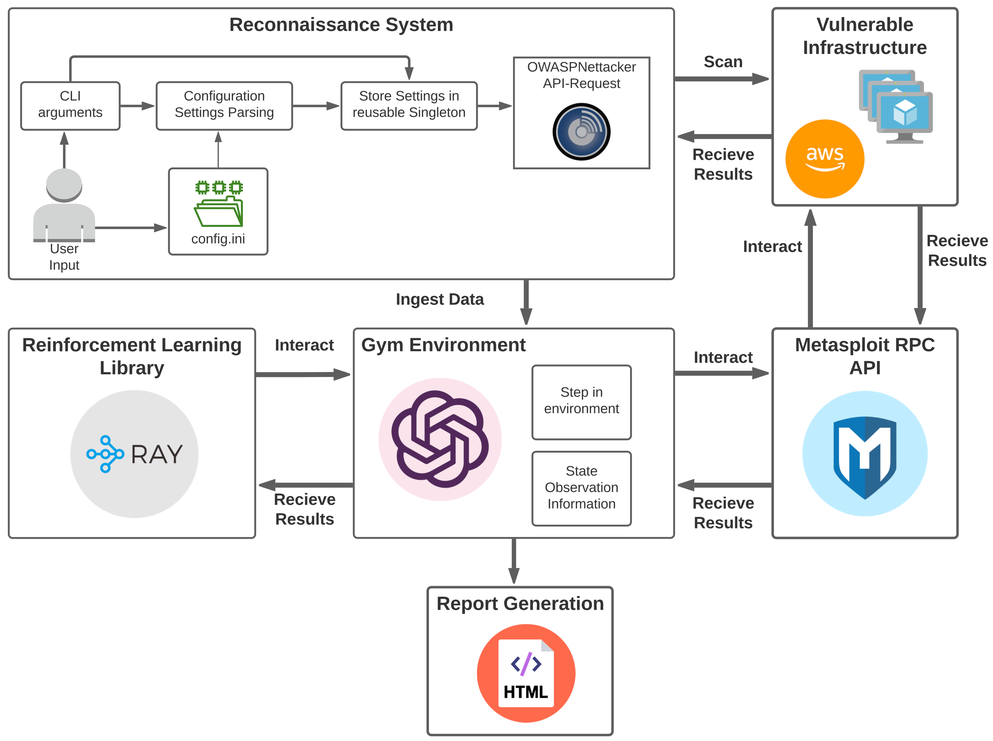
Introduction

Phorcys' use of deep Reinforcement Learning (RL) provides companies with a straightforward and cost effective approach to conduct high-quality and frequent penetration tests. At a high-level, Phorcys will start with a user who tells the agent the scope of the attack. It will then perform reconnaissance that will be ingested into the deep RL model for the given targets. The model will decide on what exploits to leverage in the process, and executes those exploits to compromise the target. After successfully conducting the assessment, Phorcys concludes by automatically generating a report of the penetration test.

Objectives

- Develop a reconnaissance system to discover ports and services running on a host.
- Create an interface with the Metasploit RPC API exploitation system
- Develop and train an agent to intelligently use the Metasploit interface to find vulnerabilities
- Using these systems together generate a report detailing the finding(s).

Software Architecture & Design



Results

Port 22:

Access Level: User level access was obtained

Vulnerability: exploit/unix/ftp/proftpd_133c_backdoor
Vulnerability Description:
sample output 1

Vulnerability: auxiliary/scanner/ssh/ssh_version
Vulnerability Description:
sample output 2

Vulnerability: exploit/windows/smb/psexec
Vulnerability Description:
sample output 3

Figure 1: Shows partial output of the report from the penetration test.

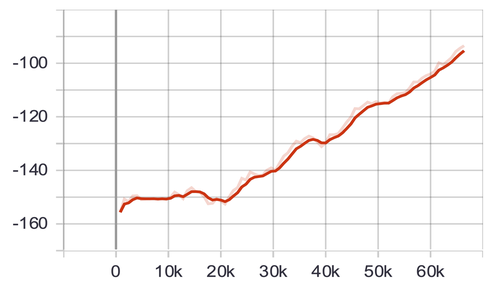


Figure 2: Training PT RL Agent. Shows agent successfully learning how to conduct penetration tests.

Benefits

- Both training and penetration testing are fully autonomous.
- Cost effective solution for affordable penetration tests.
- Companies are able to conduct frequent penetration tests augmenting responsibilities of a penetration test.
- Generation of a comprehensive report to determine weaknesses within a network.

Future Work

- Option to use a user interface alongside the command line interface
- Dynamically create all actions in the action space.
- Implementation of post-exploitation for lateral movement.
- Exploration of different algorithms used for training and how they compare to the current one used.
- Implement Tactics, Techniques, and Procedures (TTPs) for realistic adversary emulation.

Acknowledgments

We would like to thank the SAIL research lab for funding our AWS infrastructure for the project.

References

[1] Sullivan, Chris. "Cybersecurity Skills Shortage: Where Are All the Penetration Testers?" Infosecurity Magazine, 14 May 2018, www.infosecurity-magazine.com/next-gen-infosec/skills-shortage-where-penetration/.