FULLY AUTOMATED PENETRATION TESTING TOOL USING DEEP REINFORCE LEARNING

Lê Thành Đạt

Trường ĐH Công Nghệ Thông Tin. ĐHQG TP.HCM.

What ?

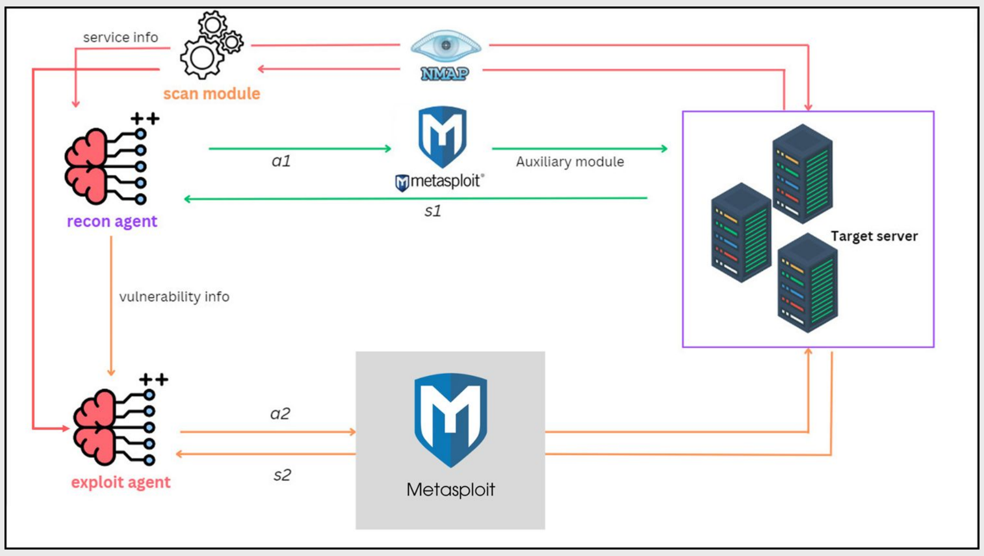
We introduce a framework to perform penetration testing automatically, in which we have:

- Integrate a Deep Reinforcement Learning Agent to assist with automation.
- Extend the ability to exploit complex vulnerabilities
- Evaluated several Policy Optimization methods for Deep Reinforcement Learning.

Why ?

- Penetration testing is one of the most effective methods for securing private assets and preparing organizations against potential cyberattacks.
- Traditional pentesting is often **time-consuming** and susceptible to **human error.**
- There is a global **shortage of qualified cybersecurity professionals**.

Overview



Description

1. Penetration Testing

- Penetration Testing is performed using open-source tool like **Metasploit** and **Nmap**.

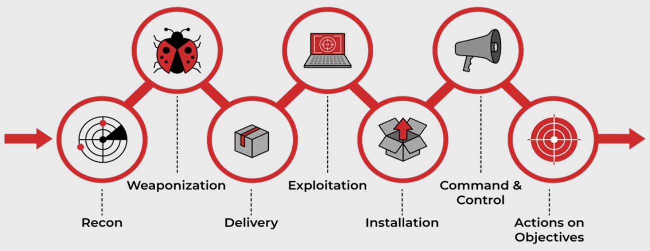


Figure 1. Process-flow of Penetration Testing.

- Metasploit provides tools for discovering, exploiting, and validating vulnerabilities in systems and networks.
- Nmap maps network topologies, identify vulnerabilities, and assess the security posture of systems efficiently.

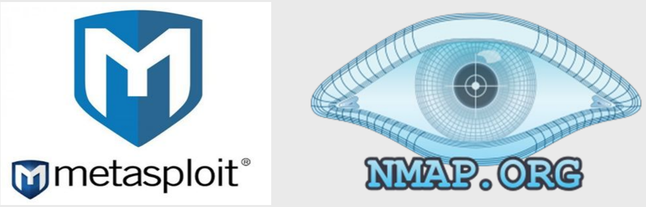


Figure 2. Logo of Metasploit and Nmap

2. Deep Reinforcement Learning Agent

- Agent automatically choose suitable modules for recon and exploitation
- Record choices that lead to successful exploit attempts (Acumulate Experience)

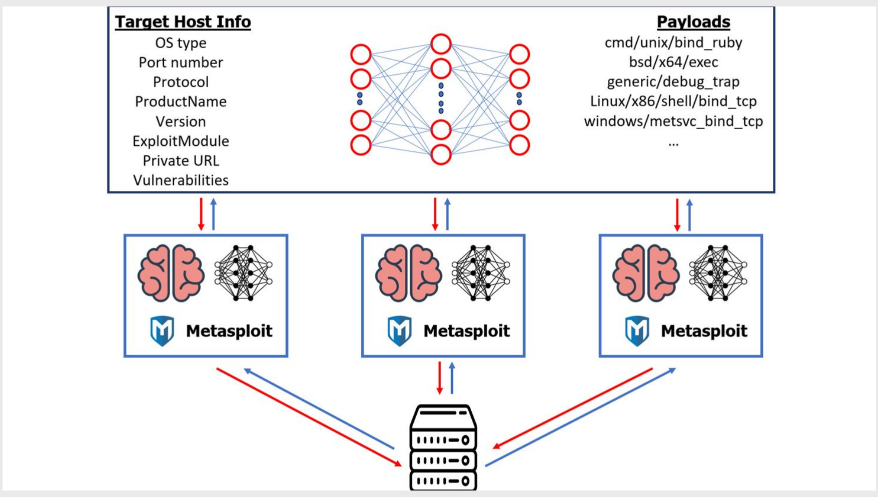


Figure 3. Detailed Working Flow in automated mode

3. Asynchronous Advantage Actor-Critic (A3C)

- Core of the framework
- Most optimized algorithms for Deep Reinforcement Learning problem when applied to Automated Pentesting

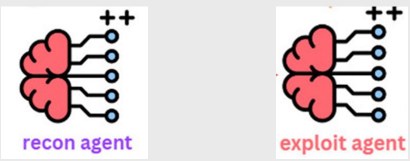


Figure 4. Agents learn to solve problems with A3C

NII

Lê Thành Đạt – Trường Đại học Công nghệ Thông tin. ĐHQG TP.HCM
TEL : 0765427461 Email : datlt.19@grad.uit.edu.vn