Скалецький В.А., магістрант
Єфіменко А.А., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ НАВЧАННЯ З ПІДКРІПЛЕННЯМ У ТЕСТУВАННІ НА ПРОНИКНЕННЯ

Тестування на проникнення (або пентест) – це проактивний підхід до кібербезпеки, який імітує кібератаки, використовуючи спільні методи зі зловмисниками, що допомагає виявити вразливості до того, як вони будуть використані в реальних інцидентах. Інтеграція методів машинного навчання (ML) дозволяє автоматизувати рутинні процеси, покращує точність аналізу великих обсягів даних і швидкість реагування на нові загрози, в порівнянні з традиційними методами пентесту.

Відповідно до технік навчання, алгоритми ML розділять на кероване (supervised), некероване (unsupervised) і навчання з підкріпленням (reinforcement learning, RL). В контексті кібербезпеки, методи керованого і некерованого навчання частіше використовують для виявлення кіберінцидентів. Тоді як для тестування на проникнення обирають навчання з підкріпленням.

В RL пентестинг розглядається як задача послідовного прийняття рішень, середовище і завдання зазвичай моделюються як марковський процес вирішування (МПВ) або частково спостережуваний МПВ. В більш ранніх дослідженнях середовище моделювалося за допомогою графів атак або дерев рішень. А агент, взаємодіючи із середовищем, обирає дії для максимізації накопиченої винагороди.

Однією з ключових переваг навчання з підкріпленням є його здатність до самонавчання. Починаючи з мінімальних знань, агент вдосконалює свою стратегію протягом численних ітерацій, з часом набуваючи навичок і запам'ятовуючи найефективніші тактики. Такий підхід дозволяє динамічно адаптувати свою поведінку.

Агенти RL спроможні виявляти багатоетапні шляхи атаки, які можуть бути неочевидними при статичному аналізі. Такі інструменти, як DeepExploit, використовуючи глибоке навчання з підкріпленням, не лише виявляють вразливості, а й визначають найефективнішу послідовність атаки.

Основні переваги від інтеграції навчання з підкріпленням в процес пентесту:

- Адаптивність. Агенти RL здатні пристосовуватись до мінливого середовища, шляхом взаємодії з ціллю та оновленням своєї стратегії на основі зворотного зв'язку (успіх або невдача атаки). Така гнучкість дозволяє конструювати вектори атак у більш реалістичний спосіб.
- Ефективність. Навчаючись на досвіді, агенти RL розробляють ефективні стратегії, які знаходять слабкі місця швидше ніж методи перебору. Такий підхід веде до більш дієвого виявлення вразливостей у великих, складних мережах.
- Економічна вигода. Автоматизація пентесту за допомогою RL може зменшити вартість і час операцій. На відміну від традиційних інструментів автоматизації, які часто тестують кожне корисне навантаження, агент глибокого навчання з підкріпленням здатен розумно визначати пріоритети ймовірних експлойтів.

Хоча тестування на проникнення на основі RL пропонує вагомі переваги, воно також має недоліки і обмеження:

- Високі обчислювальні вимоги. Агенту RL зазвичай потрібна велика кількість ітерацій проб і помилок, щоб вивчити ефективну стратегію, особливо в складних середовищах. У мережах з великою кількістю хостів, служб і можливих експлойтів, комбінація станів і дій зростає експоненційно, що значно збільшує час навчання. Таке навчання вимагає значних обчислювальних потужностей і часу.
- Етична та юридична невизначеність. Інструмент пентесту на основі RL в руках зловмисників може стати грізною зброєю. Тому розробка таких інструментів піднімає етичні питання. Також існує питання відповідальності. Автономна система тестування може не розпізнати ситуацію, коли потрібно зупинити атаку, яка може вивести з ладу цільову систему, тоді як людина експерт могла б проявити обережність.

Таким чином, впровадження методів навчання з підкріпленням у тестуванні на проникнення є цікавим та перспективним напрямком для досліджень. Вибір конкретного методу залежить від конкретної задачі, наявних даних та очікуваних результатів. Однак, для реалізації повного потенціалу потрібно вирішити відомі виклики та обмеження.

Список використаних джерел:

1. Ghanem M. C., Chen T. M. Reinforcement Learning for Efficient Network Penetration Testing. *Information*. 2020. Vol. 11, no. 1. P. 6. URL: https://doi.org/10.3390/info11010006.

2. Automated Vulnerability Exploitation Using Deep Reinforcement Learning / A. AlMajali et al. *Applied Sciences*. 2024. Vol. 14, no. 20. P. 9331. URL: https://doi.org/10.3390/app14209331.