

ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки
Кафедра ЕОМ

Розробка і дослідження методу
автоматизованого тестування на проникнення
з використанням Deep Learning

КВАЛІФІКАЦІЙНА РОБОТА
Другий (магістерський)

Автор
Дубовик Т.І.
студ. гр. СПзм 20-1

Керівник
Кучук Г.А.
проф. каф. ЕОМ

Актуальність

2

Використання комп'ютерних систем практично у всіх сферах життєдіяльності суспільства та збільшення кількості інцидентів інформаційної безпеки актуалізувало проблему захисту даних та програмного забезпечення. Одним із шляхів підвищення рівня даного питання є використання методів та засобів тестування на проникнення. Це стосується як сфер реального виробництва та практичних послуг, так і сфери розробки програмного забезпечення.

Метою роботи є – розробка методу автоматизованого тестування на проникнення з використанням технології Deep Learning. 3

Завдання:

- 1) Дослідити можливості системи Shadow у збиранні фактичних даних для проектування дерев атак, а також платформи Mulval для генерації дерев атак.
- 2) Розробити метод формування матриці кібервторжень із використанням інструменту Mulval.
- 3) Удосконалити метод Deep Q – Learning Network для аналізу матриці кібервторжень та знаходження оптимальної траєкторії атаки.
- 4) Провести порівняльне дослідження методу автоматизованого тестування проникнення.

4

Об’єктом дослідження є процес тестування.

Предмет дослідження. Метод автоматичного тестування на проникнення.

Методи дослідження. Застосовано методи порівняння та аналізу, а також інтеграції різного роду систем.

Аналіз сучасного стану вирішення завдань 5 тестування на проникнення



Етапи тестування на проникнення

Розвідка та пошук цілей ;

Пошук вразливостей ;

Отримання доступу;

Розширення привілеїв;

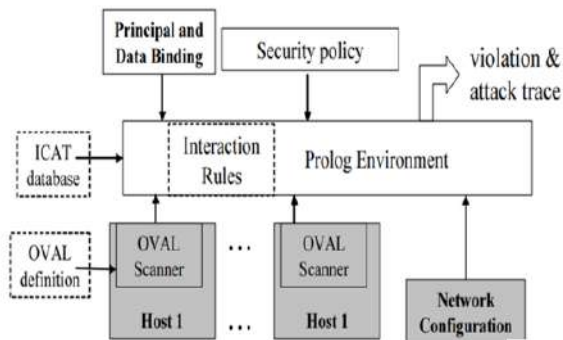
Аналіз конфігурації;

Експлуатація;

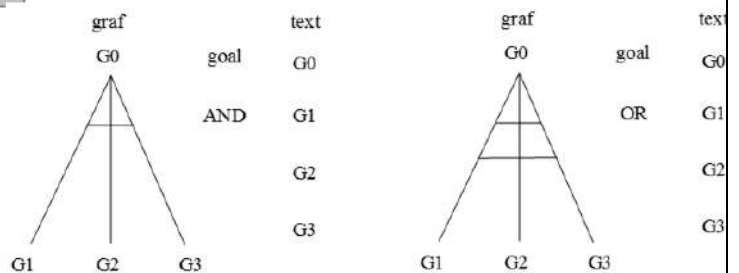
Аналіз результатів та підготовка звіту.

Структурна схема фреймворку Mulval

6

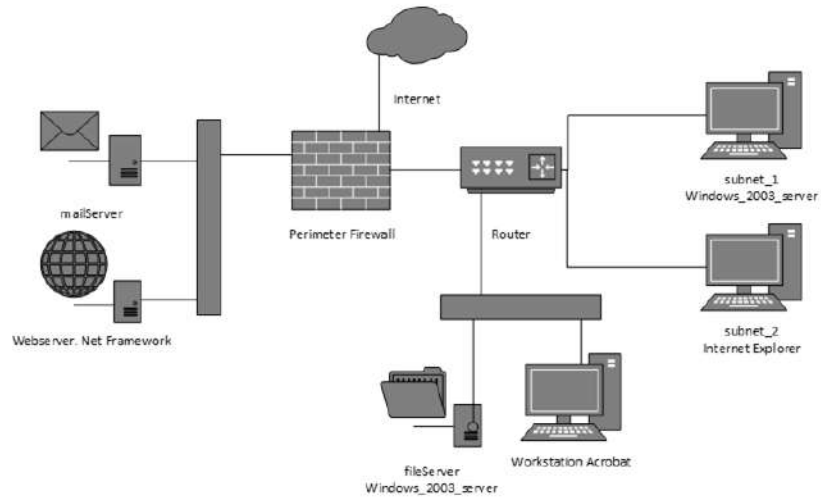


Граф та текстового представлення кожного з можливих типів вузлів



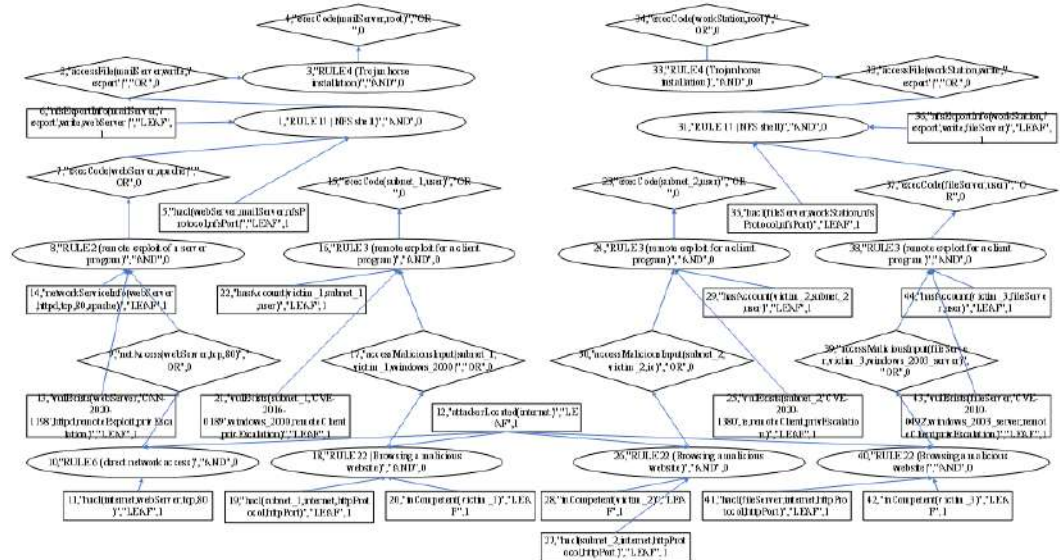
Топологічна структура досліджуваної комп'ютерної мережі

7



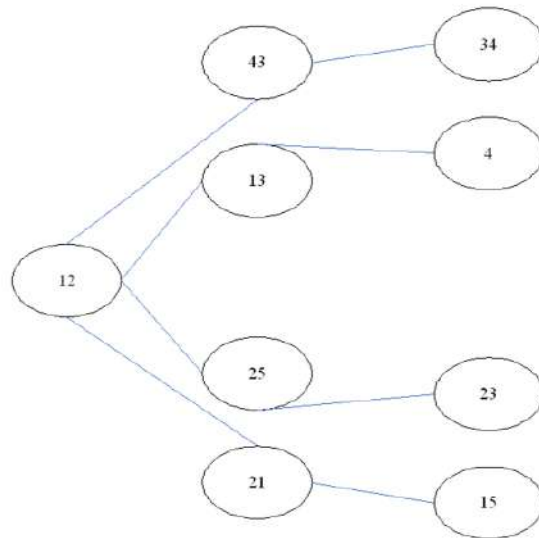
Граф атак на досліджувану комп'ютерну систему

8



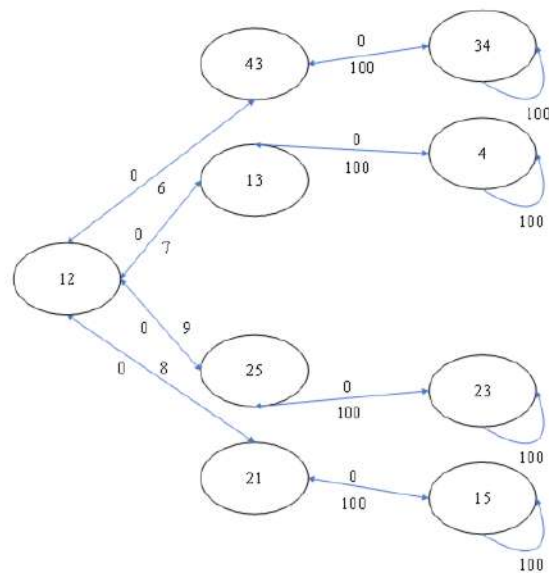
Уточнений граф атак

9



Модель графа з винагородою

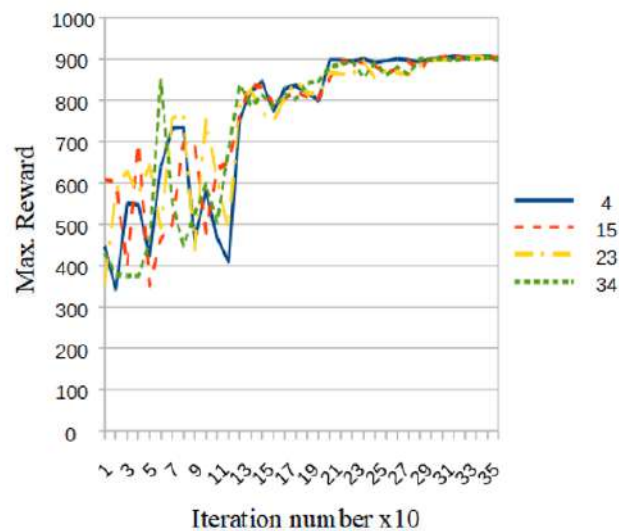
10



Практичні приклади результатів використання ¹¹ методу автоматизованого тестування на проникнення

Імітатор вузла зломисника	Ціль	Максимальна винагорода
12	4	908
12	15	907
12	23	906
12	34	906

Графік залежності винагороди за кожну ітерацію виконаного тесту кількості ітерацій ¹²



Висновки

13

Розроблено метод автоматичного тестування на проникнення. Відмінною особливістю методу є комплексне використання пошукової системи Shodan, платформи аналізу мережевої безпеки MulVal, а також даних про вразливість програмного забезпечення – CVE для отримання вхідних даних та побудови реалістичних сценаріїв атак та перевірки у рамках технології глибокого навчання із підкріпленням. Це дозволило згенерувати дерево атак для різних процедур навчання та провести оптимізацію відповідних сценаріїв автоматичного тестування безпеки програмного забезпечення.