ІНСТРУМЕНТ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ НА БАЗІ ОДНОПЛАНИХ КОМП'ЮТЕРІВ PIRat

Автори: Грушка М.О., Скарга-Бандурова І.С.

Основні характеристики, суть розробки

Інструмент тестування на проникнення PIRat являє собою програмно-апаратний засіб, що реалізує методи моделювання дій зовнішніх зловмисників, зокрема дозволяє здійснювати комбіновані атаки та відображати поточний стан виконання атак. Керування процесом тестування здійснюється з наявних мобільних пристроїв з використанням одноплатних комп'ютерів.

Патенто-конкурентоспроможні результати

Розроблене програмне забезпечення системи PIRat дозволяє використовувати одноплатні комп'ютери для здійснення тестування на проникнення в умовах, що максимально наближені до реальних.
Основною перевагою такої реалізації є те, що вона не потребує ніякої додаткової установки або системи розгортання для проведення тестів, як наприклад, в Cyber Ranges.
Для початку тестування достатньо лише підключити атакуючий одноплатний комп'ютер, керований через мобільний пристрій з попередньо підготовленим Linux дистрибутивом.

Порівняння із світовими аналогами

Для виконання тестування на проникнення найбільш популярними є спеціальні оптимізовані Linux дистрибутиви (Kali Linux, BlackArch Linux), що в своєму складі містять безліч окремих програмних пентест інструментів.
Розроблене програмне забезпечення являє собою графічне середовище Linux. Це дозволяє встановити його на пентест дистрибутив і окрім власних технік виявлення та використання вразливостей використовувати інструменти, що містить дистрибутив. Одна із ключових переваг – єдиний інтерфейс для різних програмних пентест інструментів.

Економічна привабливість розробки для просування на ринок, впровадження та реалізації, показники, вартість

PIRat є ефективним автоматизованим інструментом для тестування безпеки, що імітує реальні атаки і техніки злому і дозволяє виконувати всебічний аналіз локальних мереж.
Використання PIRat дозволяє перевірити надійність кожного елементу мережі всередині організації та якісно оцінити політику безпеки без додаткових інвестицій в програмне забезпечення і персонал.
Інструмент оснащено спеціально розробленою графічною оболонкою, яка забезпечує зручне управління програмами тестування.
Хоча розробка в основному орієнтована на одноплатні комп'ютери, використані кросплатформені засоби дозволяють використовувати розроблене програмне забезпечення не тільки з одноплатними комп'ютерами, а і з будь-якими пристроями під управлінням Linux: настільними комп'ютерами, ноутбуками, робочими станціями, серверами.

Галузі, міністерства, відомства, підприємства, організації, де планується реалізувати результати розробки

Продукт призначений для організацій та спеціалістів, що займаються проведенням аудиту захищеності комп'ютерних систем та мереж.

Стан готовності розробки - (100%)
Система знаходиться на стадії бета-тестування

Результати впровадження

Спрощена структурна схема програмного забезпечення для керування процесом тестування захищеності комп'ютерних систем та мереж на одноплатних комп'ютерах з використанням наявних мобільних пристроїв представлена на рис. 1.

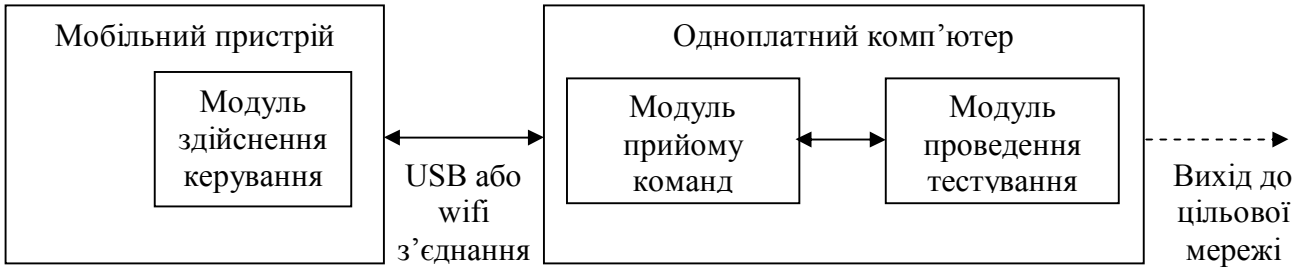

Рисунок 1 – Структурна схема інструменту PIRat

Графічна оболонка розроблена з використанням фреймворку Qt. Для імплементації технік тестування на проникнення використані мови програмування: C, C++, Python 3, Bash script.

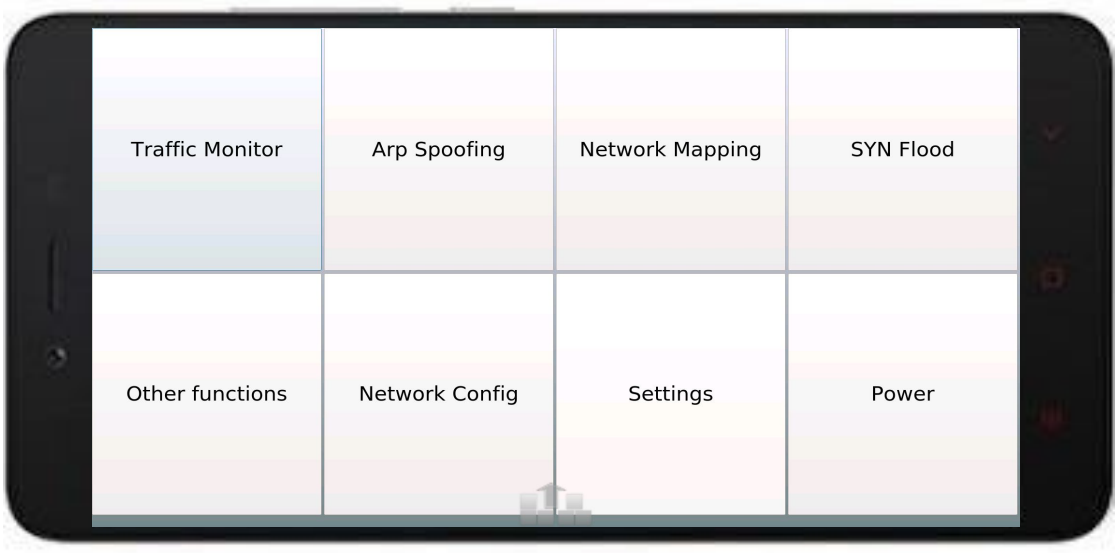

Рисунок 2 – Основне вікно програми керування процесом тестування на проникнення з мобільного пристрою