Жакун Г.А., *студент 6 курсу, факультет інформаційних технологій та комп'ютерної інженерії, кафедра захисту інформації, Вінницький національний технічний університет, м. Вінниця;*
Лукічов В.В., *к.т.н., старший викладач, факультет інформаційних технологій та комп'ютерної інженерії, кафедра захисту інформації, Вінницький національний технічний університет, м. Вінниця*

СИСТЕМА ВИЯВЛЕННЯ АТАК З ВИКОРИСТАННЯМ HONEYPOT

В сучасному світі доволі часто проводять Bruteforce атаки і взлам пароля з допомогою соціальної інженерії. Незважаючи на десятиліття досліджень і досвіду, досі все ще не вдається створити безпечні комп'ютерні системи або навіть виміряти безпеку системи.

В результаті використання нововиявлених вразливостей часто проводять атаки нульового дня. Завдяки автоматизації експлуатації та масштабному глобальному пошуку вразливостей, супротивники часто можуть піти на компроміс невдовзі після того, як вразливості стали відомі [1].

Одним із способів завчасного попередження про нові вразливості є встановлення комп'ютерних систем у мережі з очікуванням, що буде проводитися проникнення. Ці системи не мають інших законних функцій, і кожна спроба підключитися до них є підозрілою. Дану систему називають Honeypot. Honeypot може працювати з будь-якою операційною системою та будь з якою кількістю послуг.

Налаштовані служби визначають місця, де противник може вибрати скомпрометувати систему. Honeypot з високою взаємодією імітує всі аспекти операційної системи, тоді як honeypot з низькою взаємодією імітують лише деякі частини, наприклад мережевий стек [2]. Також розрізняється фізичні і віртуальні honeypot. Фізичний honeypot існує як машина з відповідною IP-адресою в мережі, тоді як віртуальний honeypot розміщений на іншій машина, яка реагує на мережевий трафік, спрямований на віртуальний Honeypot. Віртуальні Honeypot приваблюють тим, що вони це роблять не потребує додаткових комп'ютерних систем. Використовуючи віртуальні honeypot, можна заповнити мережу з хостами, що працюють над різними операційними системами. Однак, щоб переконати супротивників у тому, що віртуальний honeypot працює під певною операційною системою, необхідно ретельно моделювати стек TCP/IP цільової операційної системи. По іншому є необхідність вміти підмінювати інструменти відбитків пальців стека TCP/IP, наприклад Xprobe [1] або Nmap [3].

Доволі часто Honeypot дає змогу тільки направити зловмисника в заздалегідь заготовлене середовище та дослідити його атаку. Також це дає змогу зрозуміти які способи та методи атаки були використані. Тільки дана методика не дає можливості виявити зловмисника а в окремих випадках Honeypot вдається розкрити. Тому було запропоновано об'єднати системи моніторингу для виявлення атак та Honeypot.

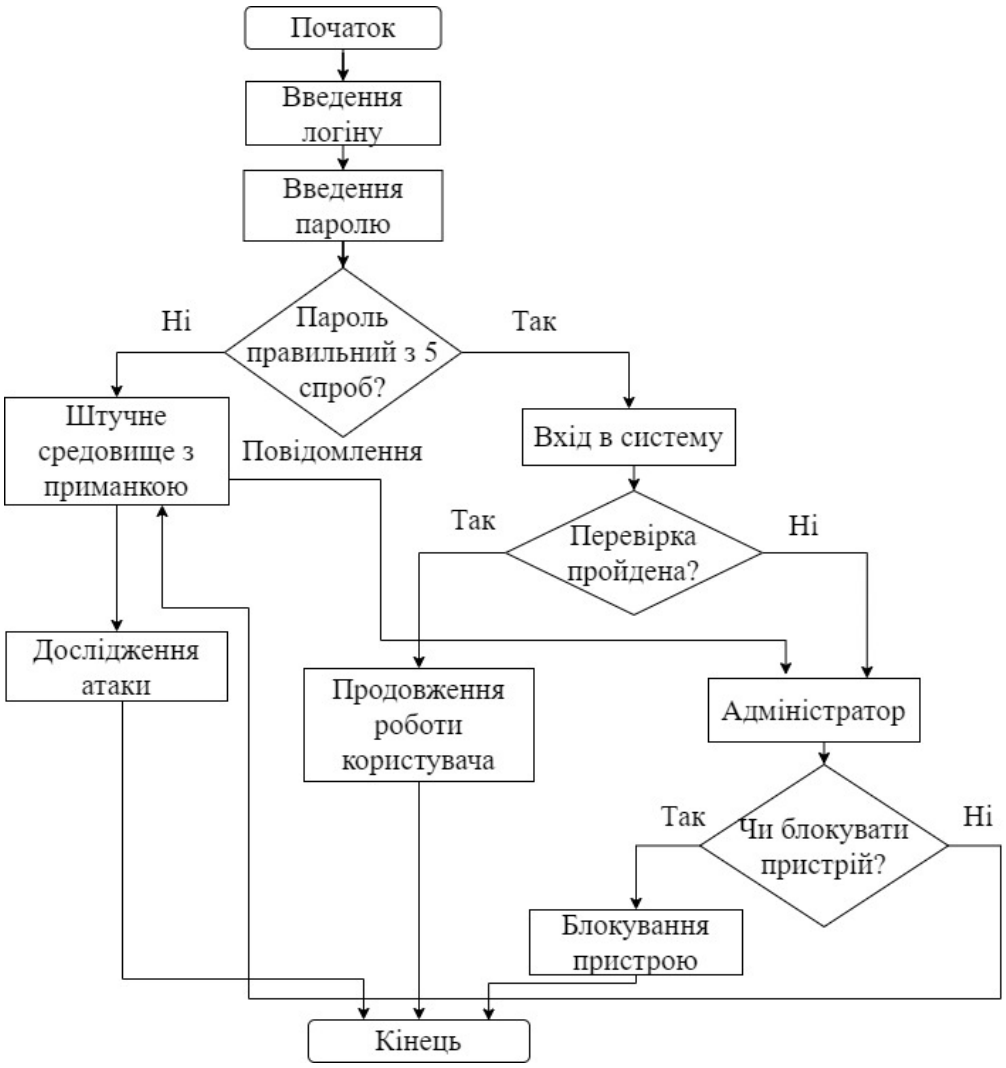

Рисунок 1 – Блок-схема виявлення атака з використанням Honeypot.

На рисунку 1 продемонстровано програмний модуль, який об’єднує Honeypot та систему виявлення атак. Перевіркою буде дії користувача, а також спеціальні файли, які не повинні бути відкриті або змінені Honeypot, додатково будуть використовуватися дані про особливості користувача. Функція блокування буде запускатися в тому випадку, коли Адміністратор не прийме рішення за певний період часу. В такому випадку навіть якщо зловмисник проникне в систему, буде можливість його виявити та прийняти дії, Honeypot буде надавати можливість дослідити атаки. Також зловмисник який виявить honeypot не буде очікувати підміни файлів в системі.

Висновком даного рішення є можливість виявити зловмисника в системі. Також ця система має викликати у зловмисника сумніви в тому чи інформація, яка буде скопійована або розкрита чи є інформація достовірна, і чи зловмисника не було розкрито. Дана система вирішує проблему Honeypot, коли виявляється підміна середовища або можливість відкривання користувачем.

Література:
1. Lance Spitzner. Honeypots: Tracking Hackers. Addison Wesley Professional, September 2002.
2. Stuart Staniford, Vern Paxson, and Nicholas Weaver. How to Own the Internet in your Spare Time. In Proceedings of the 11th USENIX Security Symposium, August 2002.
3. Fyodor. Remote OS Detection via TCP/IP Stack Fingerprinting. http://www.nmap.org/nmap/ nmap-fingerprinting-article.html, October 1998. 1, 6

Кметь О.І., магістр, кафедра електронних обчислювальних машин,
Харківський національний університет радіоелектроніки, м. Харків

МУРАШИНИЙ АЛГОРИТМ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧ МАРШРУТИЗАЦІЇ ТРАНСПОРТУ

В даний час йде стрімка зміна інфокомунікаційних технологій (ІКТ). Зміни, що виникають, зачіпають мережеві технології, власне – обчислювальні і комунікаційні пристрої, а також обробку даних. В результаті, інформаційні технології застосовуються у всебільшій кількості сфер життя і господарського життя людини. Однією з актуальних областей наукових досліджень є сфера життєвого оточення, яка з області Smart House розвивається в даний час в область Smart city, Smart transport system и т.п. Таким чином, у органів міського управління виникають нові завдання, які повинні не тільки вирішити цілий комплекс проблем, що виникають, а й провести кардинальну трансформацію міст. Комплекс проблем у всіх міст наступний:

- транспортні проблеми;
- екологічні проблеми;
- соціальні проблеми, пов'язані з ростом злочинності і соціальної напруженості;
- обмеження природних ресурсів;
- зникнення культурної та історичної спадщини.

Важливим моментом є детальний аналіз, розуміння даних проблем, а також можливість розгляду різних варіантів рішення. Всі перераховані проблеми, як результат активної урбанізації, є основними тригерами і вимушеними процесами розвитку міст і їх трансформації в Smart city. Рішенням цих проблем може бути застосування нової моделі розвитку міст – реалізація концепції Smart city, яка в своїй основі застосовує інфокомунікаційні технології для вирішення всіх сфер життєдіяльності населення. Було виявлено, що на поточному етапі не існує універсальної моделі Smart city і точного її визначення. Модель є сучасною стратегією об'єднання різноманітних факторів міського розвитку, спрямована на модернізацію інфраструктури з принципово новими можливостями централізованого управління, новим рівнем послуг і безпеки.

Однією з основних проблем в контексті всього міста, було виявлено цілий