МЕТОД ВИКОРИСТАННЯ КІБЕРПАСТОК В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

Сєвєрінов О.В., Ярова О.С.
Харківський національний університет радіоелектроніки, Харків, Україна

На даний час для забезпечення захисту інформації в ІКС організації все частіше використовуються кіберпастки (honeypot). Honeypot унікальні, вони працюють нестандартно, але дуже ефективно, що дає змогу швидко розвиватися сфері захисту інформації.

Метою доповіді є опис роботи і оцінка важливості кіберпасток в кіберпросторі для підвищення захисту інформації в ІКС. В доповіді наводиться імітаційна кібератака на кіберпастку і реакція на цю атаку KfSensor. Наведений приклад роботи кіберпастки показує принцип роботи KfSensor і принципи захисту інформації використання кіберпасток.

На прикладі роботи VMware Pro 17 з ОС Windows 10, KfSensor, та Kali Linux описаний процес роботи кіберприманки і атаки на неї. KFSensor діє як приманка, призначена для залучення та виявлення хакерів і хробаків шляхом імітації вразливих системних служб і троянів. KFSensor попередньо налаштований для моніторингу всіх портів TCP і UDP разом із ICMP.

Навмисно «зручна» комп'ютерна система дозволяє хакерам використовувати вразливості і наносити по ним «удари» по пустим системам або напівпустим (деяка інформація, яка не має цінності – фальшивки), щоб можна було вивчати як відбулася атака. Застосування пастки можливе до будь-якого обчислювального ресурсу від програмного забезпечення до файлових серверів і маршрутизаторів, які будуть аналізувати стан кожного з цих ресурсів і надавати дані про атаки, збої тощо, і одночасно з цим, намагатимуться заважати робити чорним капелюхам свою справу, при цьому аналізуючи все, що відбувається в Honeypot. Конкретна робота кіберпастки залежить від її алгоритмів і маштабування.

Наразі з розвитком інформаційної безпеки T-Pot – це все в одному, опціонально розповсюджена багатоархівна (amd64, arm64) платформа honeypot, яка підтримує понад 20 honeypots і незліченну кількість опцій візуалізації за допомогою Elastic Stack, анімованих карт атак у реальному часі та багатьох інструментів безпеки для подальшого покращення досвіду обману. Апгрейд H-Pot безперервний.

Список літератури

1. Honeypot і Honeynet. URL: https://www.security-insider.de/was-ist-ein-honeypot-a-703883/.

2. Виявлення загроз для iot-пристроїв засобами Honeypots. URL: http://elartu.tntu.edu.ua/bitstream/lib/30383/2/IMST_2019_Belma_A-Detection_of_threats_to_iot_devices_23.pdf.

3. Онлайн-платформа для спільної розробки програмного забезпечення і його використання GitHub. URL: https://github.com/paralax/awesome-honeypots.