

– Виявлення певних подій, яку відбулися у різних місцях у різний проміжок часу але є пов'язані між собою спільним павутинням злочинної діяльності, для подальшого спостереження та аналізу таких подій.

В Україні є досвід запровадження такої системи, а саме у місті Маріуполі, вона вже показала себе з найкращого боку та залишила за собою статус кращої системи відеоспостереження в очах українців та й усього світу. Запроваджена система у Маріуполі дає змогу стверджувати, що відбулося зниження рівня злочинності, підвищення виявлення та документування кількості правопорушників, здійснення розшуку викрадених транспортних засобів та багато інших позитивних моментів. Нажаль, запровадження інтелектуальної системи відеоспостереження на території України є досить проблематичним питанням, пов'язаним першим чином з нехваткою коштів у Міністерства внутрішніх справ для закупівлі належного обладнання та облаштування ним країни. Тож потрібно зробити висновки, що цілком виправданим та, можливо, навіть необхідним є будь-який вид фінансової підтримки з боку місцевих державних адміністрацій, спонсорів та навіть приватного сектору.

УДК 004.9 +343.1

ВІТАЛІЙ ВІКТОРОВИЧ НОСОВ

кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ДЕЯКІ АСПЕКТИ АВТОМАТИЗАЦІЇ РОЗГОРТАННЯ І УПРАВЛІННЯ ТЕСТОВОГО СЕРЕДОВИЩА НАВЧАННЯ КІБЕРБЕЗПЕКИ

Навчання спеціалістів для підрозділів Департаменту кіберполіції Національної поліції України потребує створення, оновлення і підтримки в актуальному стані тестового середовища навчання кібербезпеки і цифрових криміналістичних досліджень.

Суттєва специфіка навчання за цим напрямом полягає у постійній необхідності швидкої зміни налаштувань і оновленні тестового середовища навчання разом із швидким розвитком та виявленням нових вразливостей інформаційних технологій, що у свою чергу потребує великих витрат часу і зусиль при завжди обмежених ресурсах.

Автоматизувати розгортання і управління тестовим середовищем можна шляхом застосування технологій:

- ізольованих віртуальних контейнерів Docker - для розгортання вразливих застосувань;
- приватної обчислювальної хмари (Private Cloud Computing) - для створення хмарного сховища тестового середовища.

Технологія Docker дозволяє швидко розгорнути у вигляді контейнерів вразливі застосування у тестовому середовищі із значно меншим

навантаженням на хостову операційну систему ніж віртуальні машини. Деякі, вже налаштовані, контейнери можна знайти на [hub.docker.com](https://hub.docker.com/u/vulnerables). Наприклад, у профілі "vulnerables" (hub.docker.com/u/vulnerables) доступно 18 контейнерів вразливих застосувань. В [1] наведений приклад встановлення і налаштування:

- Damn Vulnerable Web Application (DVWA);
- OWASP Mutillidae;
- OWASP WebGoat;
- bWAPP;
- OWASP Juice Shop;
- WPScan Vulnerable WordPress;
- OpenDNS Security Ninjas;
- Altoro Mutual.

Технологія Private Cloud Computing дозволяє створити хмарне сховище для користувачів тестового середовища. В [2] зазначені три способи розгортання Private Cloud Computing на базі рішення ownCloud (owncloud.com):

- у хостовій ОС Ubuntu 18.04 LTS;
- в Docker контейнері;
- в віртуальній машині Bitnami Owncloud Stack Virtual Machines.

З огляду на зручність і швидкість доцільно використовувати розгортання ownCloud в Docker контейнері.

Окрім ownCloud існують альтернативні рішення Private Cloud Computing з відкритим кодом (Open Source) [3]:

- Nextcloud (github.com/nextcloud);
- Syncthing (github.com/syncthing/syncthing);
- Seafile (github.com/haiwen/seafile);
- IPFS (ipfs.io);
- Cozy (github.com/cozy/cozy-stack);
- та інші.

Розгортання Docker контейнерів вразливих застосувань і приватного хмарного сховища в тестовому середовищі дозволить суттєво підвищити ефективність навчання спеціалістів для підрозділів Департаменту кіберполіції Національної поліції України.

Список використаних джерел:

1. Raj Chandel. Web Application Pentest Lab setup Using Docker. URL: <https://www.hackingarticles.in/web-application-pentest-lab-setup-using-docker/>.
2. Raj Chandel. Multiple Ways to Setup Cloud Pentest Lab using OwnCloud. URL: <https://www.hackingarticles.in/multi-ways-to-setup-cloud-pentest-lab-using-owncloud/>.
3. Alternatives to ownCloud for all platforms with Open Source License. URL: <https://alternativeto.net/software/owncloud/?license=opensource>.