УДК 343.1+004

Владислав Васильович ЛЕЙКО,
студент факультету № 6
Харківського національного університету внутрішніх справ;
Віталій Вікторович НОСОВ,
кандидат технічних наук, доцент,
професор кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-7848-6448

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СЕРВІСІВ SHODAN І CENSYS ДЛЯ ПОШУКУ ВРАЗЛИВИХ ПРИСТРОЇВ З МЕРЕЖНИМ ІНТЕРФЕЙСОМ

З активним розвитком інформаційних технологій росте й потреба у пристроях, що підключені до мережі Інтернет і мають функцію віддаленого доступу. До таких пристроїв відносяться: сервери; камери відеоспостереження; принтери, роутери; холодильники; різноманітні системи управління (енергогенеруючими станціями, медичними комплексами, міським транспортом, розумним домом та інше) і керуванням доступом до об'єктів. Ці пристрої і системи часто мають вразливості, які сприяють несанкціонованому доступу до інтерфейсів їх управління.

Пошукові сервіси Shodan (https://www.shodan.io) і Censys (https://censys.io) здійснюють безперервну індексацію доступних в Інтернеті пристроїв з мережним інтерфейсом та формують відповідні бази даних. При порівняльному аналізі цих сервісів можна зазначити наступне.

Сервіс Shodan для повноцінного користування потребує реєстрацію користувача, за замовчуванням враховує точний запит. Основний пошук виконується шляхом зіставленням запиту з банером вузла (інформація, яку надає про себе сам вузол). Відповідь на запит може містити дані про призначення вузла, відкриті порти, версію програмного забезпечення та інше. Для звуження області пошуку у сервісі передбачені фільтри, які дозволяють здійснювати пошук по:

– країні «country:» в форматі UA, UK, US, наприклад: default password country:UA;
– місту «city:», наприклад: nginx city:«Kyiv» country:UA;
– операційній системі «os», наприклад: os:"windows xp";
– хосту «hostname», наприклад: nginx hostname: .com;
– координатам «geo», наприклад: apache geo: 24.7396,-45.1312;
– IP «net», наприклад: net: "192.168.64.25";
– порту «port», наприклад: http port:443.

Фільтр для пошуку пристроїв з паролями за замовчуванням у місті Київ з Web-автентифікацією буде виглядати так: "default password city: Kyiv port:80". Як правило, логін та пароль за замовчуванням доступний

на сайті виробника конкретного пристрою. Більш складний фільтр для пошуку у визначеній локації маршрутизаторів Cisco з web-інтерфейсом, конфігурації яких були змінені в певний період та доступ до яких не потребує автентифікації виглядає так: «HTTP/1.0 200 OK cisco geo:49.933375,36.273704 after: 11/08/2009 before: 12/12/20110».

Особливий інтерес становлять web-камери, які мають пусті або встановленні за умовчанням паролі. Як наслідок, відео потік з таких пристроїв доступний кожному, хто до них підключиться. На даний момент кількість незахищених web-камер рахується мільйонами [1], місця розташування яких також можна встановити через Shodan.

Потужність сервісу Shodan було перевірено Деном Тентлером [2], який заявив що за допомогою пошукової системи було виявлено незахищені командно-контрольні системи ядерних електростанцій і прискорювача атомних частин.

Пошуковий сервіс Censys підтримує повнотекстовий пошук, логічні оператори пошуку, умовні знаки та фільтри. Параметри фільтрів пошуку майже такі самі, як і в Shodan. Censys може шукати мережний пристрій за виробником, для якого вже відомі вразливості. За допомогою пошукового запиту «certificate has expired» можна дізнатися список вузлів з простроченими SSL сертифікатами.

Практичне використання зазначених сервісів дозволяє стверджувати, що Censys на відміну від Shodan видає більш актуальну інформацію про стан пристрою, але Shodan додатково сканує вузли мережі Інтернет (по всіх портах и протоколах із дотриманням безпечних тайм-аутів), а не тільки збирає банери, через що може видавати дещо застарілу за часом інформацію. Тому за актуальною інформацією слід звертатися до Censys, а за більшим об'ємом інформації - до Shodan. Наприклад, при пошуку мережних web-камер (в Censys фільтр: «80:http netcam», в Shodan «80:http netcam») Censys видав 3457 вузлів, а Shodan – 1885, але кількість інформації про вузол в Shodan в рази більше ніж в Censys.

Складність несанкціонованого проникнення до пристроїв та систем з мережевим доступом можна представити як на рис. 1.

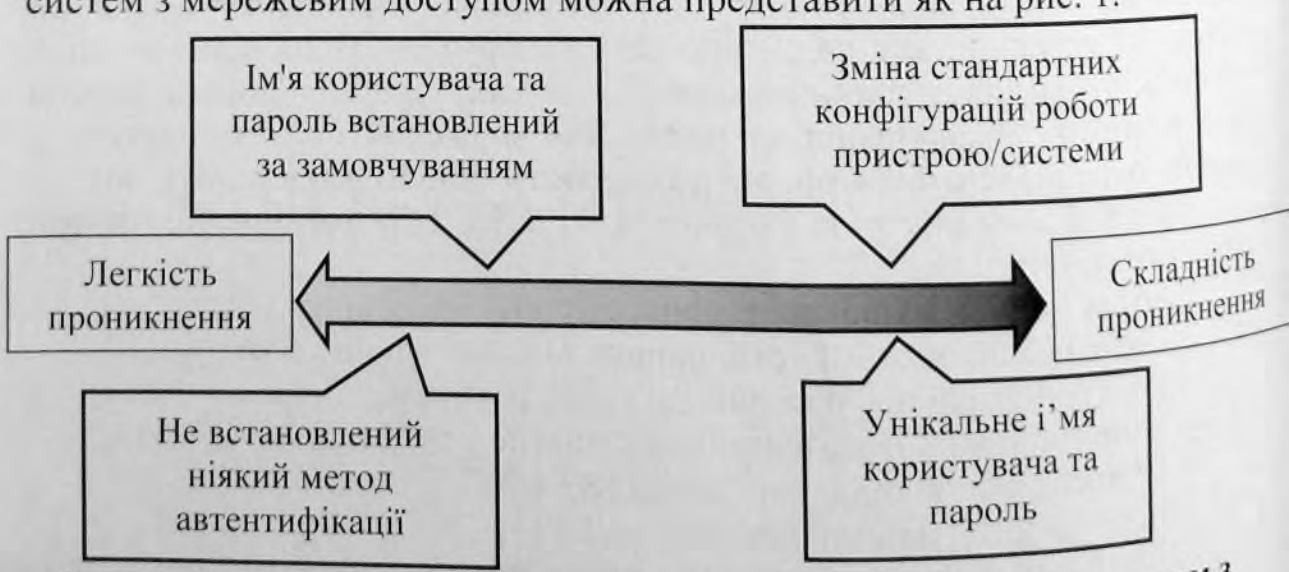

Рис. 1. Шкала складності проникнення до пристроїв та систем з мережевим доступом.

Основні рекомендації з безпечного підключення пристроїв/систем (мереж) до мережі Інтернет звучать так:

1. Не підключати пристрої/системи (мережі), які не мають власних засобів захисту від проникнення до мережі Інтернет, та які для цього не призначені.
2. При підключенні пристрою/системи (мережі) до мережі Інтернет обов'язково змінювати стандартну конфігурацію роботи цих пристроїв/систем (мереж) та налаштовувати методи доступу користувачів із дотриманням політики конфіденційності.
3. Використовувати міжмережний екран рівня «застосування» (web application firewall).
4. Використовувати при можливості шифрування даних.
5. Використовувати складні паролі.
6. Своєчасне оновлювати програмне забезпечення.
7. Використовувати ліцензійне програмне забезпечення.
8. Обмежити список IP-адрес, з яких дозволено підключення до пристрою/системи (мережі).
9. Змінити стандартну відповідь (банер) на HTTP запит, в якій за замовчування відображається версія web-серверу.
10. Проводити навчання користувачів пристроїв/систем (мереж) щодо дотримання правил користування та недопущення розголошення даних.

На даний момент користувачі не усвідомлюють важливість захисту мережних пристроїв і, відповідно, не готові за це додатково витрачатися. В свою чергу виробники не зацікавлені в підвищенні обізнаності користувачів про можливі наслідки такого підходу, оскільки це збільшує їх витрати.

Таким чином, використання пошукових сервісів Shodan і Censys для оцінки вразливостей пристроїв з мережним інтерфейсом (Internet of things[8]) показує основну їх проблему – стандартні паролі і неоновлені версії програмного забезпечення, що ставить під загрозу вже всі вузли локальної мережі.

Список бібліографічних посилань

1. Что не так с безопасностью в Интернете Вещей: Как Shodan стал «поисковиком спящих детей» // «Хабр» – крупнейший в Европе ресурс для IT-специалистов. Дата оновлення: 25.01.2016. URL: https://habr.com/company/pt/blog/275853/ (дата звернення: 10.10.2018).
2. Shodan – самый страшный поисковик Интернета // «Хабр» – крупнейший в Европе ресурс для IT-специалистов. Дата оновлення: 02.05.2013. URL: https://habr.com/post/178501/ (дата звернення: 11.10.2018).
3. Internet-of-things // Cambridge Dictionary URL: https://dictionary.cambridge.org/dictionary/english/internet-of-things (дата звернення: 10.10.2018).

Одержано 31.10.2018.

[8] Internet of things – концепція мережі з пристроями в ній, які можуть підключатися одне до одного і обмінюватися даними з використанням мережі Інтернет [3]