УДК 004.056.57 + 004.492

Є.А. Олійник

ТЕСТУВАННЯ ЗАХИЩЕНОСТІ IP-КАМЕР ПІДКЛЮЧЕНИХ ДО МЕРЕЖІ ІНТЕРНЕТ У ВІННИЦЬКІЙ ОБЛАСТІ

Вінницький національний технічний університет

Анотація

В даній роботі описуються найпоширеніші вразливості IP-камер, проведено їх аналіз. Відповідно до проведеного аналізу проведено тестування на проникнення підключених до глобальної мережі IP-камер у Вінницькій області.

Ключові слова: Кібербезпека, *IP-камера, вразливість , тестування на проникнення,атака*.

Abstract

In the present research work the most common vulnerabilities of IP cameras are described, their analysis is carried out. According to the analysis, tests were conducted to penetrate the IP-cameras connected to the global network in the Vinnytsia region.

Keywords: *Cybersecurity, IP Camera, Vulnerability, Penetration Testing, Attack.*

Вступ

Міцність ланцюга визначається його найслабшою ланкою. Це відноситься і до цифрового захисту. Зв'язок через Інтернет реалізовується набагато простіше ніж протягування кілометрів кабелів. Саме тому все частіше передача в локальних і глобальних мережах здійснюється через мережу Інтернет. Однак отримавши доступ до принтера, камери, роутера, сервера і навіть кавоварки зловмисник зможе отримати доступ до всієї системи [5]. Це означає, що отримати доступ до систем може не лише власник, але й зловмисник. Неправильне налаштування, стандартні паролі та відриті порти стандартна проблема у для сучасних інформаційно-телекомунікаційних мереж.

Об'єктом дослідження є вразливості IP-камер з відкритими портами та вільним доступом через мережу Інтернет.

Метою наукової роботи є пошук вразливих IP-камер та тестування на проникнення для формування рекомендацій з покращення кібербезпеки [1].

Для досягнення мети необхідно розв'язати такі задачі:

- проаналізувати відомі вразливості;
- здійснити пошук камер у яких можна реалізувати вразливості;
- надати рекомендації для покращення кібербезпеки.

Результати аналізу відомих вразливостей

Проаналізувавши вразливості IP-камер стає зрозуміло, що реалізувати захист на 100% неможливо оскільки усі існуючі системи спостереження є не досконалими і в кожній наявні дірки в системі. До кожної вразливості додається також фактор помилки людей, які є не достатньо технічно освічені для налаштування таких систем [3].

Найбільш поширеними вразливостями виявлено такі.

- Некомпетентність фахівців, які займалися установкою і налаштуванням відеокамер.
- Використання стандартних або слабких (менш ніж 8 символів паролів). Для злому як правило використовуються брутфорс атаки по словнику (метод перебору), який містить всі стандартні паролі: admin, 888888, 123456, 12345 і.т.д.
- Відкриті порти використовуються для встановлення з'єднання між пристроями у системі, однак часто вони можуть стати вразливим місцем для проведення атак.

– Проблема зі сторони виробника. Часто виробники в результаті бажання зменшити вартість виготовлення камери, економлять на складових, втому числі на тих, що призначені для забезпечення безпеки [2].

Результати пошуку камер у яких можна реалізувати вразливості

Для пошуку вразливих камер можна скористатись різноманітними сканерами портів або спеціалізованими сервісами. Один із таких сервісів є Censys.io. Даний сервіс дозволяє здійснювати запити за різними критеріями такими як заголовки, місце розташування, відкриті порти, заголовки і т.д.

Пошук вразливостей здійснювався для камер у Вінницькій області з відкритим 80 портом. Даний порт використовується для підключення камери до мережі Інтернет та для здійснення http-автентифікації.

Для того щоб знайти потенційно вразливі об’єкти необхідно скласти пошуковий запит пошуку по місцевості та відкритому порту. Приклад викладки з результатами пошуку показані на рис. 1.

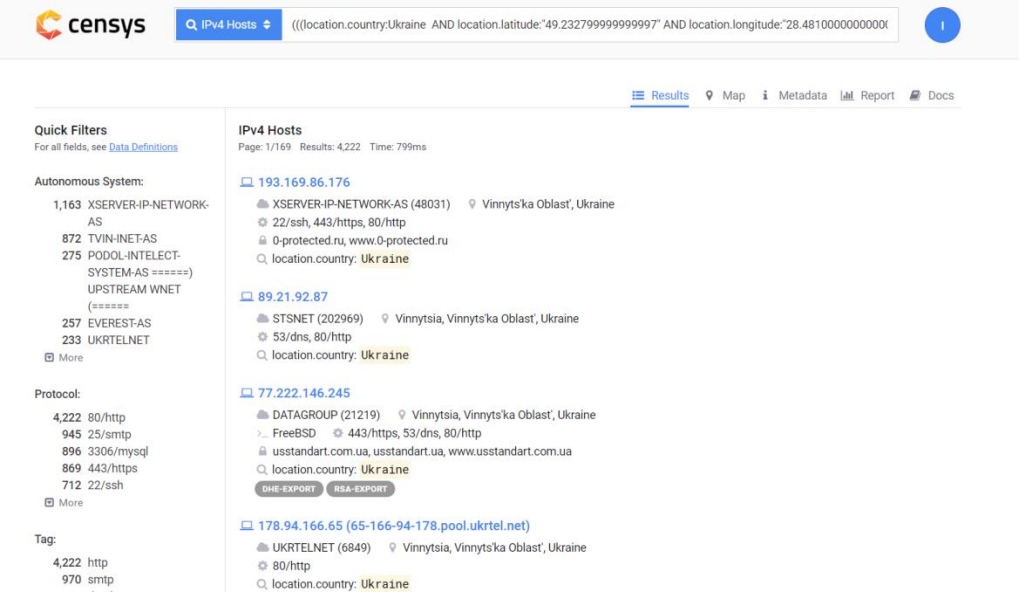

Рисунок 1 – Вікно з результатами пошуку

В результаті запиту у Вінницькій області було виявлено 4,222 потенційно вразливих об’єкти.

Рекомендації для покращення кібербезпеки

Відповідно до найбільш відомих вразливостей було запропоновано рекомендації для покращення кібербезпеки [4]:

– Зміна стандартних паролів. Багато користувачі не змінюють стандартні паролі, що надає можливість зловмиснику проникнути в систему. Зміна пароля на більш складний сильно зменьший імовірність проникнення.

– Перевірені виробники. Купувати IP-камери необхідно лише у перевірених виробників та які пройшли сертифікацію.

– Перевірка портів. Після встановлення необхідно здійснити перевірку портів та доступу до камери. Усі порти, що не будуть використовуватись необхідно закрити.

– Встановлення Firewall. Встановивши firewall можна розмежувати доступ та вказати адреси пристроїв які можуть доступ отримувати.

– Безпечне зберігання ключів автентифікації. Ключі для автентифікації мають зберігатись в фізично безпечному місці та бути у зашифрованому вигляді для випадку, якщо автентифікаційні дані будуть скомпрометовані їх потрібно буде ще розшифрувати.

– Оновлення системи. Необхідно постійно відстежувати наявність оновлень програмної частини камер відео спостереження і своєчасно здійснювати оновлення.

– Здійснення аудиту системи. Частий аудит дозволяє виявити інциденти безпеки та ліквідувати прогалини у безпеці.

Висновок

Внаслідок аналізу вразливостей було здійснено пошук IP-камер у яких дані вразливості задіяти, отримано кількість камер які можуть бути атаковані, та визначено рекомендації щоб покращити рівень безпеки.

Перелік використаних джерел

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи/ Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
2. Прогноз на 2019 год: интернет (уязвимых) вещей [Електронний ресурс]. – Режим доступу: URL: https://blog.avast.com/ru/prognoz-na-2019-god-internet-uyazvimyh-veschej– Назва з екрану.
3. Дудатьев А. В., Баришев Ю. В., Войтович О. П. Метод оцінювання безпеки інформаційних ресурсів підприємства на основі аналізу вразливостей // Вісник Хмельницького національного університету, - № 4, - 2008. - С.78-83
4. Рекомендації по забезпеченню безпеки «інтернету речей» [Електронний ресурс]. –Режим доступу: URL: https://docs.microsoft.com/ru-ru/azure/iot-fundamentals/iot-security-best-practices– Назва з екрану.
5. Войтович О.П. Дослідженння безпеки системи розумного будинку / Войтович О.П., Вишньовський В.В., Савченко К.В //Тези доповідей Шостої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації» м. Вінниця, 24-25 жовтня 2017 року. – Вінниця: ВНТУ, 2017. – С. 67-70.

Олійник Євген Анатолійович **–** студент факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет.

Науковий керівник: ***Дудатьєв Андрій Веніамінович***– канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет.

Oliynyk Yevgeny Anatolyevich- student of the Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University.

Supervisor: ***Dudatev Andriy Veniaminovich***– Cand. Sc. (Eng), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine.