

ДОСЛІДЖЕННЯ ЗАСОБІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ IP- КАМЕР

Вінницький національний технічний університет

Анотація

Вразливості IP-камер є серйозною загрозою для безпеки користувачів. У роботі розглянуто утиліти для тестування на проникнення IP-камер, які включають атаки грубої сили, використання вразливостей прошивки, використання відкритих портів та знаходження шляху до потокового відео. Зроблено висновки і порівняння роботи інструментів для тестування на проникнення відеокamer.

Ключові слова: IP-камери, тестування на проникнення, кібербезпека, атаки грубої сили, вразливості прошивки.

Abstract

Vulnerabilities of IP cameras pose a serious security threat to users. This paper considers utilities for IP cameras penetration testing, including brute-force attacks, exploitation of firmware vulnerabilities, exploitation of open ports, and path enumeration to access streaming video. Conclusions and comparisons of the performance of penetration testing tools for video cameras are provided.

Keywords: IP cameras, penetration testing, cybersecurity, brute-force attacks, firmware exploits.

Вступ

Безпека камер відеоспостереження грає важливу роль в захисті будь-якого підприємства. Існує різноманіття IP-камер, які використовуються в воєнних та комерційних підприємствах, медичних і освітніх закладах та у домашньому використанні. Захист IP-камер в цих галузях використання є критично важливим, скомпрометовані камери можуть бути використані для промислового шпигунства, викрадення особистих даних, несанкціонованого моніторингу персоналу або житлових приміщень. У Російсько-українській війні скомпрометовані камери відеоспостереження використовуються у проведенні та плануванні різноманітних стратегічних операцій, наведення ракет та БПЛА їх коригування, для уточнення місцезнаходження ППО, критично важливих об'єктів, переміщення військової техніки [1, 2]. Скомпрометовані камери відеоспостереження можуть мати серйозні та потенційно катастрофічні наслідки.

Організації, які використовують такі камери, важливо вживати заходів для зменшення цих ризиків. Зміна стандартних паролів після налаштування пристрою, регулярне оновлення прошивки, автоматизація оновлень, впровадження механізму управління доступом на основі ролей, уникати прямого підключення IP-камер до інтернету. Ці рекомендації дозволять зменшити ризик того що пристрій буде скомпрометовано, однак для визначення ефективності цих заходів необхідно застосовувати засоби тестування на проникнення.

Метою цього дослідження є покращення захисту конфіденційності шляхом зменшення ризиків витоку інформації через IP-камери. Оскільки IP-камери часто стають об'єктами кібератак, розуміння ефективності різних методів та інструментів тестування дозволяє виявляти вразливості та запобігати ним.

Результати дослідження

Існує низка інструментів для тестування на проникнення камер відеоспостереження. У таблиці 1 наведено порівняльний аналіз найпопулярніших утиліт, які використовуються для оцінки безпеки IP-камер.

Таблиця 1. Порівняння інструментів тестування безпеки камер.

Засіб	Cameradar[3]	Routersploit[4]	Hikka[5]	CheckVideo IP Camera Tool[6]
Функція сканування портів	Присутня функція вказувати порти для сканування, стандартні значення 554, 5554, 8554	Можливе сканування деяких стандартних портів. Вже буде залежати від вибраного модуля.	—	Програма виявляє IP-адреси пристроїв але не демонструє доступні відкриті порти
Функція розпізнавання моделі камери	Програма здатна розпізнати у більшості випадків модель камери при скануванні	—	—	Розпізнає модель камери в локальній мережі
Функція підбору паролів	Користувач вказує місце з словником для перебору логінів і паролів для RTSP потоку. Після цього відбувається атака.	Присутній модуль для виконання атаки грубої сили проти служби автентифікації HTTP Basic/Digest. Присутня перевірка на стандартні логіни і паролі від виробника.	Наявна можливість для використання словникових атак	Програма використовує вбудований список паролів і логінів який не можна змінити

При аналізі даних інструментів можна виділити наявність деяких особливих функцій порівняно з іншими проаналізованими програмами. Унікальною особливістю програми Cameradar є наявність функції перебору посилань відеопотоку камери. При застосуванні можливий варіант використання користувачького або вбудованого в програму словника. Однією з найголовніших проблем у підтримці безпеки IP-камер є потреба у регулярному оновленні прошивки. Багато IP-камер працюють із застарілою прошивкою, що робить їх незахищеними від типових вразливостей безпеки. Перевагою Routersploit є функція тестування на вже відомі вразливості прошивки відеокамери. На відміну від інших засобів, ця програма має власну базу відомих вразливостей та може автоматично перевіряти камери на них. У Hikka особливістю є функція здійснення скріншоту зі скомпрометованої камери. Після завершення атаки, при вдалих спробах перебору буде збережено скріншоти з камери. Для виконання комплексного дослідження вдалим є поєднання таких інструментів як Routersploit і Cameradar. Перший інструмент рекомендується використовувати для знаходження вже відомих вразливостей, після цього є доцільним проводити атаки грубої сили та знаходження посилання відеопотоку. Є можливість використати замість Cameradar інструмент Hikka якщо завданням є лише знаходження паролю шляхом атаки грубої сили, при цьому порти і посилання відеопотоку вже відомі.

Висновки

У результаті для вдалого тестування на проникнення IP-камер доцільним є використання комплексного підходу до тестування. Використання декількох утиліт збільшить шанс на знаходження вразливостей у IP-камерах. Надано рекомендації для мінімізації того щоб пристрій не був скомпрометований. Використання утиліт з тестування на проникнення дозволяє виявляти вразливості та запобігати їхньому використанню зловмисниками у майбутньому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Росіяни приховано слідували за Києвом: СБУ заблокувала камери, які "засвітили" роботу ППО. URL: https://24tv.ua/rosiyani-prihovano-slidkuvali-za-kiyevom-sbu-zablokuvala-kameri_n2464485 (дата звернення: 15.03.2025)
2. Is Hacking IP Cameras Just for Voyeurs or Does it Have Strategic and National Security Implications? URL: <https://hackers-arise.net/2025/01/16/is-hacking-ip-cameras-just-for-voyeurs-or-does-it-have-strategic-and-national-security-implications/> (accessed: 19.03.2025)

3. Документація до утиліти cameradar URL: <https://github.com/Ullaakut/cameradar/blob/master/README.md> (дата звернення: 19.03.2025)
4. 9 Ways To Hack CCTV Cameras and How to Prevent URL: <https://hackeracademy.org/10-ways-to-hack-cctv-cameras-and-how-to-prevent-it/> (accessed: 19.03.2025)
5. Sofa cyber eye diamond (Cyber eye open) URL: <https://hackyourmom.com/kibervijna/dyvannyj-kiber-glaz-almaz-cyber-eye-open/> (accessed: 15.03.2025)
6. IP Camera Scan Tool URL: <https://www.checkvideo.com/knowledge-center/tools/> (accessed: 15.03.2025)

Гаврилюк Максим Юрійович — студент групи ІБС-216, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: signedint737@gmail.com

Науковий керівник: Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: yuriy.baryshev@vntu.edu.ua

Maksym Havryliuk – student 1BS-21b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: signedint737@gmail.com

Supervisor: Yurii Baryshev — Ph.D., Associate Professor of the Information Protection Department, Vinnytsia National Technical University, e-mail: yuriy.baryshev@vntu.edu.ua