УДК 004.056

Д. О. Каракута
О. П. Войтович

ОСОБЛИВОСТІ СКАНЕРІВ ВРАЗЛИВОСТЕЙ

Вінницький національний технічний університет;
Кафедра захисту інформації

Анотація
Досліджено особливості роботи сканерів вразливостей. Наведено основні принципи роботи відомих сканерів, а також з'ясовано їх переваги та недоліки.
Ключові слова: захист, безпека, вразливості, сканування систем.

Abstract
The peculiarities of the operation of vulnerability scanners are studied. The basic principles of operation of well-known scanners are given, as well as their advantages and disadvantages.
Keywords: protection, security, vulnerabilities, scanning systems.

Вступ

У наш час, технології розвиваються особливо швидко. На сьогодні за допомогою комп'ютера можна дуже просто відвідувати різні інформаційні ресурси, передавати інформацію, дивитися фільми і слухати музику. З такими можливостями гостро постало питання про захист інформації, що зберігається на персональних комп'ютерах, вебсайтах, корпоративних мережах.

Метою роботи є дослідження особливостей роботи сканерів вразливостей для аналізу рівня безпеки систем і вебдодатків.

Результати дослідження

Сканер вразливостей – це програмний або апаратний засіб, що служить для сканування інформаційної системи в реальному часі. Він використовується для знаходження в мережі, операційній системі комп'ютера, базах даних та програмах можливих проблем у безпеці. Його головне завдання – оцінити безпеку, виявити вразливості і навести звіт виконаної роботи.

За допомогою сканеру можна знаходити «дірки», якими користуються хакери для отримання несанкціонованого доступу до конфіденційних даних в мережі компанії. Також він може контролювати запущені процеси, служби і сканувати використовувані порти [1].

Сканер вразливостей вебдодатків – займається скануванням на наявність вразливостей і логічних недоліків. Він використовує тести «чорного ящика», так як ці тести не вимагають доступу до вихідного коду, а замість цього запускають зовнішні атаки для перевірки вразливостей безпеки [2]. Ці симульовані атаки можуть виявляти одні з найпопулярніших атак: міжсайтовий скриптинг (XSS) і впровадження команд (SQL injection). Також існують тести «білого ящика», де пентестер (або хакер) має доступ до всіх елементів цільового об'єкта. Якщо це сайт – увесь його вихідний код. Якщо це сервер – доступ до його нутрощів: версії, встановлених програм або до деяких файлів. В цьому випадку можливості значно ширші і збільшується ймовірність знайти проблему, яку здатний експлуатувати тільки досвідчений зловмисник [2].

Сканер вебдодатків відносять до категорії інструментів динамічного тестування безпеки (DAST). Інструменти DAST дають уявлення про те, як ведуть себе вебдодатки під час їх роботи, дозволяючи адміністратору безпеки усунути потенційні вразливості, перш ніж хакер використає їх для проведення атаки. У міру розвитку системи, рішення DAST продовжує сканувати її, щоб компанія могла швидко виявляти й усувати виникаючі проблеми, перш ніж вони переростуть в серйозні ризики [3].

В загальному є два принципи роботи сканерів:

1) зондування. Найефективніший, але повільний метод активного аналізу. Суть його полягає в тому, що сканер сам проводить спроби експлуатації знайдених вразливостей і моніторить мережу, визначаючи, де можуть пройти загрози. У процесі зондування адміністратор може підтвердити свої

здогадки щодо «дірок» і вжити заходів щодо їх закриття [1].

2) сканування. У такому режимі сканер працює максимально швидко, але проводить аналіз лише на поверхневому рівні. Тобто «дивиться» на явні «діри» і аналізує загальну безпеку інфраструктури. Відмінність цього механізму від попереднього в тому, що сканер вразливостей не підтверджує наявність вразливості, а лише попереджає про неї адміністратора [1].

Функціональність сканера вразливостей дає, наприклад, можливість провести інвентаризацію IT-ресурсів і визначити, які програми і якій версії встановлені на робочих станціях і серверах. При цьому сканер покаже, яке ПЗ має вразливості, і запропонує встановити патч, оновити версію або зупинити ті чи інші служби і відключити протоколи, якщо вони являють собою загрозу інформаційній безпеці.

Також можна провести сканування мережі, скласти її карту і визначити, які саме мережеві пристрої в інфраструктурі підприємства використовуються. Будуть також визначені всі піддомени. Відразу ж можна виявити відкриті порти, запущені мережеві сервіси, які становлять загрозу для безпеки.

Крім того, сканер дозволяє перевірити на стійкість використовувані паролі на сервісах з доступною авторизацією, при цьому будуть виявлені паролі, встановлені за замовчуванням. Буде проведений і брутфорс (повний перебір можливих варіантів) з використанням актуальної бази паролів.

За результатами перевірки всі сканери дозволяють сформувати звіти різного формату і призначення, де буде відображена вся картина вразливостей в інфраструктурі, а також надано рекомендації щодо їх усунення. Кожній вразливості буде підтверджено номер з баз CVE (Common Vulnerabilities and Exposures) або NVD (National Vulnerability Database) [4].

На жаль сканери вразливостей не вміють активно протистояти міжмережевим екранам, систем виявлення небажаного ПЗ і систем виявлення і запобігання вторгнень. Для максимальної користі від користування сканера потрібно правильно налаштувати програмне забезпечення.

Висновки

Отже, сканери вразливостей – корисні програми для внутрішньомережевого аналізу рівня безпеки систем і вебдодатків. При роботі з вебдодатком сканер знаходить слабкості, намагається провести атаку, використовуючи відомі йому «діри» і видає детальну інформацію про знайдені вразливості, а також рекомендації щодо посилення захисту своїх даних. Але все ж повне усунення вразивостей не можна довірити одним сканерам, результати їх сканування потрібно правильно зрозуміти і прийняти необхідні заходи щодо захисту інформаційної системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Сканер уязвимостей [Електронний ресурс] : [Веб-сайт]. – Режим доступу: URL : https://itglobal.com/ru-ru/company/glossary/vulnerability-scanner/, вільний – Назва з екрана.

2. Kumar M., Singh S.K., Dwivedi R.K. A comparative study of black box testing and white box testing techniques // International Journal of Advanced Research in Computer Science and Management Studies. 2015. P. 32–44.

3. Сканер уязвимостей web-приложений [Електронний ресурс] : [Веб-сайт]. – Режим доступу: URL : https://roi4cio.com/categories/category/skaner-ujazvimostei-web-prilozhenii/, вільний – Назва з екрана.

4. CVE [Електронний ресурс] : [Веб-сайт]. – Режим доступу: URL : https://cve.mitre.org/, вільний – Назва з екрана.

Каракута Денис Олегович — студент групи 1БС-17б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: denys.kyta@gmail.com

Науковий керівник: ***Войтович Олеся Петрівна*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: voytovych.op@gmail.com

Karakuta Denys Olehovych — student of group 1BS-17b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: denys.kyta@gmail.com

Supervisor: **Voytovych Olesya Petrovna** — Cand. Sc., Associate Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: voytovych.op@gmail.com