DOI: 10.51369/2707-7276-2025-1(38)-8
УДК 004.056 (045)

СИДОРЕНКО Сергій Миколайович
ORCID ID: 0009-0003-1185-1505

СКАНЕРИ ВРАЗЛИВОСТЕЙ ТА ЇХНЯ РОЛЬ У ЗАХОДАХ ІЗ КІБЕРБЕЗПЕКИ

У статті описані й аналізуються функціональні характеристики популярних сканерів уразливостей із метою коректного їх застосування для раннього виявлення загроз і вжиття заходів для усунення вразливостей до того, як вони призведуть до серйозних наслідків. Сканери вразливостей дають змогу виявляти потенційні вразливості в програмному забезпеченні, налаштуваннях серверів, мережах та інших компонентах IT-інфраструктури. Сьогодні існує велика кількість різноманітних сканерів уразливостей, проте використовуються вони для різних цілей. Тому перед застосуванням сканера певного типу необхідно дослідити особливості його роботи, виокремити специфічні області захисту даних, на які спрямовано функціональні особливості роботи сканера, та з'ясувати, чи підходить такий інструмент для поставленого завдання у сфері кібербезпеки.

Саме дослідженню особливостей роботи таких сканерів уразливостей як Nmap, Nessus Professional, Acunetix та Aircrack-ng присвячено матеріали статті, адже сканери вразливостей – це важлива складова стратегії кібербезпеки, яка допомагає зберігати цілісність і безпеку систем.

Ключові слова: *кібербезпека, кіберзагрози, сканери вразливостей, уразливості систем і мереж, усунення вразливостей.*

Постановка проблеми. Сканери вразливостей є критично важливими інструментами для забезпечення безпеки IT-інфраструктури організацій, їхніх інформаційних систем і мереж. Сканери вразливостей дають можливість виявляти потенційні вразливості в програмному забезпеченні, налаштуваннях серверів, мережах та інших компонентах IT-інфраструктури.

Хоча сканери вразливостей є потужним інструментом для виявлення слабких місць у системах і мережах, їхнє використання пов'язане з низкою проблем та обмежень. Наприклад, якщо сканер помилково ідентифікує безпечні компоненти як вразливі, це може призвести до витрат часу на аналіз і виправлення непотрібних проблем. Сканери вразливостей не завжди здатні виявити нові, невідомі вразливості або специфічні для певного середовища проблеми в конфігурації. Тому автоматичні сканери не можуть замінити повноцінний тест. Проведення сканування вразливостей може створити значне навантаження на систему або мережу, особливо, у великих або складних інфраструктурах. Щоби правильно інтерпретувати результати сканування і зрозуміти, які вразливості дійсно є критичними, необхідні висо-

кокваліфіковані спеціалісти з безпеки. Без такої кваліфікації організація може витратити час на менш важливі вразливості або знехтувати серйозними проблемами. Сканери вразливостей зазвичай фокусуються на відомих уразливостях і технічних проблемах, однак вони не можуть повністю замінити інші аспекти безпеки, такі як людський фактор, соціальна інженерія, зовнішні загрози.

Беручи до уваги ці особливості, важливим є ретельне дослідження роботи сканерів уразливості як одного з основних інструментів під час роботи системи захисту інформації з метою виявлення недоліків і доцільності їхнього використання в певній системі. Адже сканери не аналізують логіку процесів і механізмів, а тому можуть давати велику кількість хибних спрацювань, відповідно виправлення вразливостей потребує додаткового аналізу результатів сканування.

Аналіз останніх досліджень і публікацій. Сканери вразливостей використовують для раннього виявлення загроз, тобто ще до того, як їх можуть застосувати зловмисники. Це дає можливість своєчасно вжити заходів для усунення вразливостей до того, як вони призведуть до серйозних наслідків, таких як витоки даних, зараження шкідливим програмним забезпеченням або інші види атак, про що свідчать висновки, викладені у статтях провідних IT-компаній і ресурсів, зокрема «TechExpert IT company» [1], «ITS Red Team», «Get PCI compliance», відомого у сфері пентестингу ресурсу Микити Книша hackyourmom.com [2] та ін.

Системи, що зберігають або обробляють конфіденційну інформацію, є основною ціллю для хакерів. Використання сканерів допомагає знаходити недоліки у захисті даних, такі як неправильні налаштування доступу, відсутність шифрування або вразливості у вебдодатках, що можуть стати причиною витоку конфіденційної інформації. Своєчасне усунення таких уразливостей мінімізує ризик витоків персональних даних, фінансової чи іншої важливої інформації. Ці проблеми висвітлені в інформаційно-аналітичному дайджесті «Кібербезпека в інформаційному суспільстві» [3], роботах іноземних і вітчизняних дослідників: Дж. Еріксона [4], П. Енгебредсона [5], А. Аносова, В. Бурячка [6], М. Шелеста, В. Хорошка [7] та ін.

Ще одним основним аспектом роботи сканера вразливостей є перевірка застарілих версій програмного забезпечення. Вразливості в програмному забезпеченні часто виникають через те, що розробники припиняють випускати оновлення або патчі для старих версій. Сканери автоматично виявляють такі ситуації та повідомляють про необхідність оновлення. Таким чином зменшується кількість уразливих систем, які можуть бути атаковані.

Сканери вразливостей також автоматизують процес перевірки всіх компонентів складних IT-систем та інфраструктур, що дає можливість ефективно виконувати регулярні аудити безпеки й забезпечити цілісність інформаційної системи. Багато організацій повинно відповідати вимогам стандартів безпеки, наприклад, для платіжних систем, для охорони здоров'я

або для захисту персональних даних. Сканери вразливостей допомагають не лише виявляти загрози, але й оцінювати відповідність цих систем установленим вимогам. Зокрема в стандартах НАТО STANAG 4774 ADATP – 4774 йдеться про аспекти управління інформацією, необхідні для забезпечення безпеки обміну інформацією [8].

Безпека даних і надійність ІТ-систем мають великий вплив на репутацію компанії. Будь-який інцидент безпеки, який призводить до втрати даних клієнтів або інфраструктурних збоїв, може серйозно підірвати довіру до організації. Сканери вразливостей допомагають знизити ймовірність таких інцидентів [9], підтримуючи високий рівень захисту даних і систем.

Мета – дослідити особливості роботи найпопулярніших сканерів уразливостей, визначити їхні переваги та недоліки для використання в заходах з організації у сфері кібербезпеки, що також дасть можливість виокремити специфічні області захисту даних, для тестування вразливості яких потрібно застосовувати певні види сканерів уразливостей.

Виклад основного матеріалу. Використання сканерів уразливостей дає змогу знизити ймовірність успішної атаки на систему, що в результаті економить значні кошти, необхідні для виправлення наслідків інциденту. Атаки, що призводять до втрати даних або зупинки бізнес-процесів, можуть коштувати організації набагато більше, ніж просте усунення вразливостей ще до початку атаки.

ІТ-системи постійно змінюються, так само як і методи атак. Сканери вразливостей зазвичай регулярно оновлюються, щоб ураховувати нові загрози, експлойти та вразливості, що з'являються на ринку. Це дає можливість організаціям адаптуватися до нових типів атак і зберігати високий рівень безпеки своїх систем.

Для аналізу особливостей сканерів уразливостей та їхнього специфічного функціонального призначення розглянемо приклади роботи сервісів, що найчастіше застосовуються.

Nmap – це утиліта Kali Linux із відкритим вихідним кодом для дослідження мережі та перевірки безпеки, розроблена для швидкого сканування великих мереж, визначає доступні хости в мережі та їхні характеристики. Для роботи з Nmap потрібні права суперкористувача (root), тому перед здійсненням команд для сканування потрібно перейти в режим суперкористувача, ввівши в командний рядок sudo su та підтвердивши пароль.

Існує багато ключів для здійснення сканування портів [10], наприклад, основні з них [11]:

– сканування за однією IP-адресою: **nmap 192.168.1.1** (див. рис. 1);

– визначення топпортів: **nmap -top-ports 25 192.168.1.17**;

– сканування всіх IP-адрес із підмережі: **nmap 192.168.1.x**;

– сканування цілей, список яких знаходиться у файлі *.txt: **nmap -iL targets.txt**;

– сканування TCP-портів, і якщо порт відкритий і прослуховується, то результат виконання успішний, тобто

з'єднання буде встановлене, у протилежному випадку вказаний порт є закритим або доступ до нього заблоковано засобами захисту: **nmap -sT 192.168.1.17** (див. рис. 2);

– ping-сканування для отримання інформації про активні хости в сканованій мережі: **nmap -sn 192.168.1.17**;

– визначення операційної системи віддаленого хосту: **nmap -O 192.168.1.17**;

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 16:04 EST
Nmap scan report for 192.168.1.1
Host is up (0.00070s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
2000/tcp open  cisco-sccp
8291/tcp open  unknown
MAC Address: 64:D1:54:5E:66:D6 (Routerboard.com)

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
```

Рисунок 1 – Приклад сканування за однією IP-адресою

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.17
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 17:19 EST
Nmap scan report for 192.168.1.17
Host is up (0.0083s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
8080/tcp open  http-proxy
MAC Address: F4:39:09:2C:99:46 (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds
```

Рисунок 2 – Приклад сканування TCP-портів

– сканування хоста, захищеного брандмауером, за його IP-адресою: **nmap -PN 192.168.1.1**;

– сканування за заданими портами: **nmap -p 21,53,80 192.168.1.17**.

Отже, використання сканера Nmap дає можливість дізнатися інформацію про відкриті порти, їхні характеристики і в результаті завчасно закрити небажані входи в мережу.

Nessus Professional – це сканер, призначений для виявлення вразливостей у мережах, системах і додатках, зокрема вразливостей в операційних системах, мережевих пристроях та сервісах [12]. Він використовується для оцінювання конфігурацій, правильності налаштування систем і мереж, виявляючи потенційно небезпечні служби, а також для створення власних політик безпеки щодо проведення спеціалізованих перевірок і генерації детальних звітів із рекомендаціями (див. рис. 3).

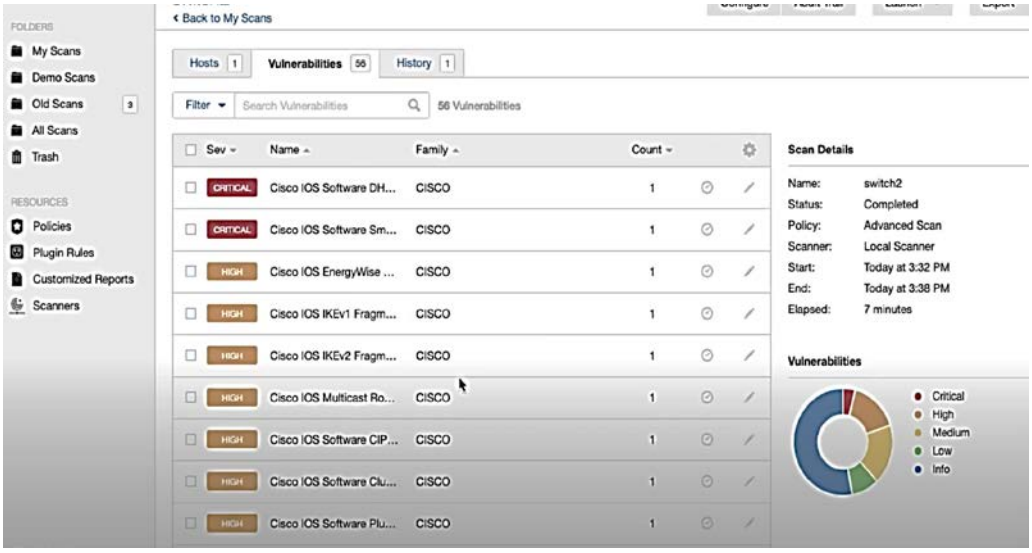

Рисунок 3 – Приклад роботи Nessus Professional

Nessus підтримує роботу з різними операційними системами, зокрема Windows, Linux, macOS, із мережевими пристроями та віртуальними середовищами. Перевагами Nessus є регулярні оновлення бази вразливостей, інтеграція з іншими продуктами Tenable та масштабованість, що дає змогу використовувати його як у малих компаніях, так і на великих підприємствах.

Сканер Acunetix дає можливість виявити більше семи тисяч уразливостей, серед яких SQL-ін'єкції, неправильні конфігурації, XSS-ін'єкції, слабкі паролі, відкриті бази даних і зовнішні вразливості, сканувати всі сторінки та вебпрограми [13], складні багаторівневі форми та навіть захищені паролем області сайту (див. рис. 4).

Acunetix аналізує та створює структуру сайту, обробляючи всі знайдені посилання і збираючи інформацію про всі виявлені файли, далі тестує всі вебсторінки з елементами для введення даних із використанням усіх можливих комбінацій і досліджує отримані результати. Коли вразли-

вість виявлена, Acunetix видає попередження, яке містить опис уразливостей і рекомендації для їх усунення.

Сканер Aircrack-ng являє собою набір інструментів для аудиту безпеки бездротових мереж, а його основна мета – тестування безпеки мереж для виявлення можливих уразливостей та зламу ключів шифрування Wi-Fi [14]. Також сканер використовується для перевірки надійності паролів і захисту бездротових мереж від несанкціонованого доступу, може захоплювати пакети даних у реальному часі, використовує зібрані пакети для спроби зламу ключів WEP, WPA, або WPA2 за допомогою статистичного аналізу, атак за словником або brute-force, а також надає можливість перехоплювати й аналізувати мережеві пакети (див. рис. 5).

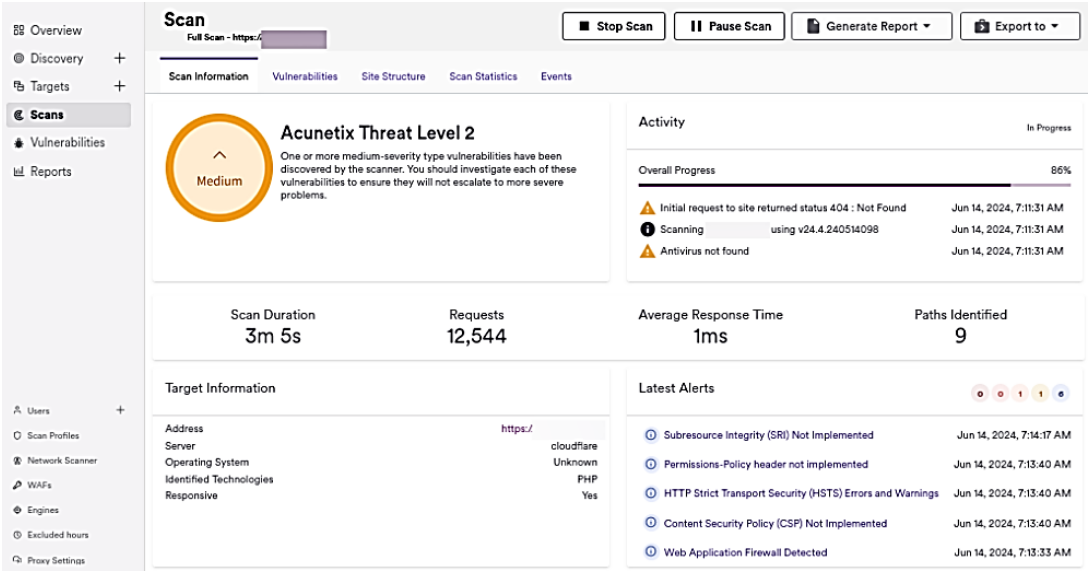

Рисунок 4 – Інтерфейс роботи сканера вразливостей Acunetix

Інструмент Aircrack-ng став популярним через доступність, відкриті ліцензії, його також часто використовують як освітній інструмент для навчання етичних хакерів і тестувальників безпеки.

Отже, проаналізувавши описані вище сканери вразливостей, можна зробити висновок, що кожен із них має певні функціональні особливості, залежно від яких їх можна використовувати для конкретних поставлених задач. Так, Nmap сканує доступні хости з метою визначення їхніх характеристик; сканер Nessus Professional працює з регулярно оновленою базою вразливостей та оцінює конфігурації систем і мереж; сканер Acunetix аналізує вразливості вебдодатків, а Aircrack-ng здійснює тестування на надійність паролів. Навіть аналіз особливостей роботи невеликої кількості популярних сканерів уразливостей показує, наскільки важливо знати, для яких потреб слід використовувати певний інструмент сканування.

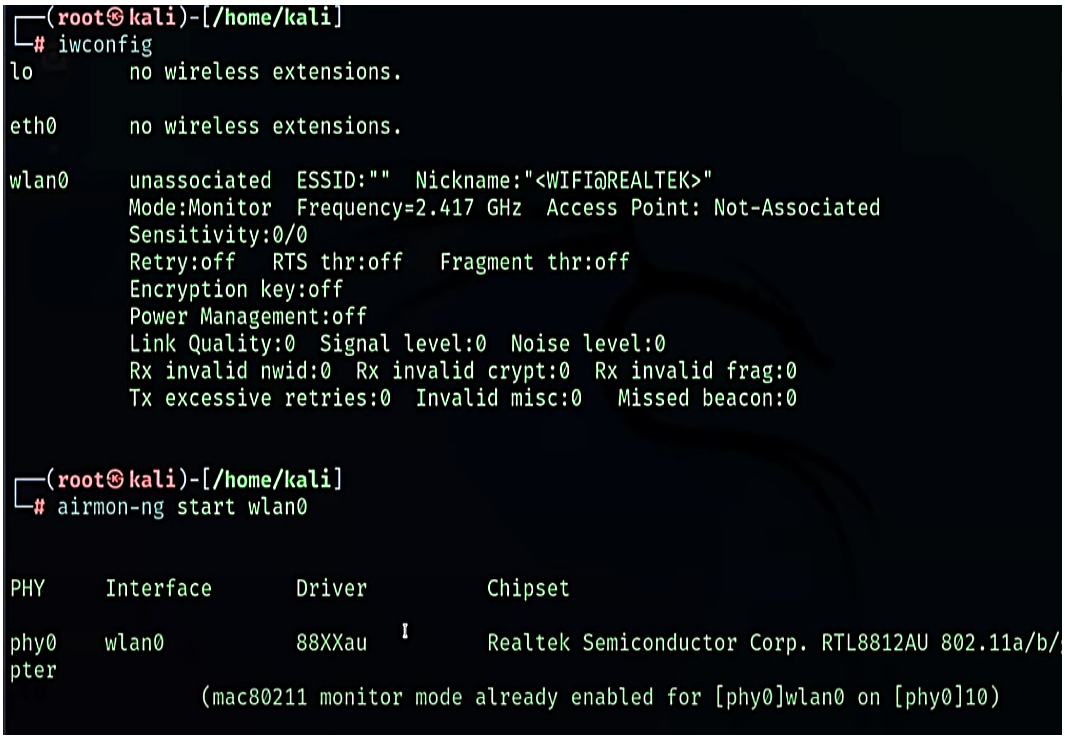

Рисунок 5 – Приклад роботи сканера вразливостей Aircrack-ng

Висновки. У процесі дослідження визначено особливості роботи найпопулярніших сканерів уразливостей Nmap, Nessus Professional, Acunetix і Aircrack-ng та їхні функціональні особливості для використання у заходах з організації кібербезпеки. Зокрема перевагами використання сканерів уразливостей є можливість ідентифікації та усунення вразливості на ранньому етапі, забезпечення належної безпеки даних і уникнення витоків, підвищення ефективності управління безпекою через автоматизацію процесів сканування та звітності, підтримання відповідності стандартам безпеки й зниження ризиків збоїв у роботі систем. Сканери вразливостей – це важлива складова стратегії кібербезпеки, яка допомагає зберігати цілісність і безпеку систем, знижуючи ризики, пов’язані з кіберзагрозами.

Недоліками роботи сканерів уразливостей є те, що для їхньої ефективної роботи повинні регулярно оновлюватися бази даних уразливостей, оскільки в разі відсутності актуальних оновлень сканер може пропустити нові загрози. Якщо конфігурація мережі або програмного забезпечення змінилася після сканування, це може призвести до нових уразливостей, які сканер не виявить, оскільки він працюватиме за застарілими налаштуваннями. Сканування вразливостей може бути використане не тільки для підвищення безпеки, але й зловмисниками для пошуку вразливостей. Якщо сканер має вразливості або недостатньо захищений доступ до сис-

теми, це можливий несанкціонований доступ або атака. Також багато сучасних сканерів уразливостей можуть бути дорогими у придбанні та обслуговуванні, а їхнє ефективне використання потребує спеціалізованих знань і навичок.

Список використаних джерел

1. TechExpert IT company. WithSecure Elements Endpoint Detection and Response. URL: https://techexpert.ua/it-products/withsecure/ (дата звернення: 10.10.2024).

2. Сканування спеціальних компонентів або категорій вразливостей. Сканери пошуку вразливостей. URL: https://hackyourmom.com/servisy/revers-inzhyniryng-ta-skrypty/skanuvannya-speczialnyh-komponentiv-abo-kategorij-vrazlyvostej/ (дата звернення: 10.10.2024).

3. Кібербезпека в інформаційному суспільстві : інформаційно-аналітичний дайджест / відп. ред. О. Довгань ; упоряд. О. Довгань, Л. Литвинова, С. Дорогих ; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України» ; Національна бібліотека України ім. В. І. Вернадського. Київ, 2023. № 9 (вересень). 351 с.

4. Jon Erickson. Hacking: The Art of Exploitation. 2nd Edition. No Starch Press, 2008. 488 p.

5. Patrick Engebretson. The Basics of Hacking and Penetration Testing. 1st Edition Syngress. 2011. 204 p.

6. Бурячок В. Л., Аносов А. О., Семко В. В. та ін. Технології забезпечення безпеки мережевої інфраструктури : підручник. Київ : КУБГ, 2019. 218 с.

7. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О. О. Захист інформації в комп'ютерних системах : підручник. Ніжин: ФОП Лук'яненко В. В., ТПК «Орхідея», 2020. 236 с.

8. Інформаційні матеріали щодо стандартів НАТО STANAG 4774 ADATP – 4774 (зв'язок, захист інформації).

9. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки : підручник. Київ : НА СБ України, 2020. 256 с.

10. Nmap Cheat Sheet 2024: All the Commands & Flags. 2024. URL: https://www.stationx.net/nmap-cheat-sheet/ (дата звернення: 10.10.2024).

11. Вавіленкова А. І. Методи і моделі протидії кібератакам: навчальний посібник. Київ : НА СБУ, 2023. 136 с.

12. Tenable Nessus. The first tool in your cybersecurity toolbox. URL: https://www.tenable.com/products/nessus (дата звернення: 10.10.2024).

13. Acunetix. Less time on web application and API security, more time on innovation. URL: https://www.acunetix.com/ (дата звернення: 12.10.2024).

14. Aircrack-ng. URL: https://www.aircrack-ng.org/ (дата звернення: 12.10.2024).

Стаття надійшла до редакції 25.11.2024

UDC 004.056(045)

Sydorenko S. M.

VULNERABILITY SCANNERS AND THEIR ROLE IN CYBERSECURITY MEASURES

The article provides a description and analysis of the functional characteristics of popular vulnerability scanners to ensure their correct application for the early detection of threats and the implementation of measures to eliminate vulnerabilities before they lead to serious consequences. Vulnerability scanners allow for identifying potential weaknesses in software, server configurations, networks, and other components of IT infrastructure. Today, there is a wide variety of vulnerability scanners, but not all of them are used for the same purposes. Therefore, before applying a scanner of a certain type, it is necessary to study the specifics of its operation, identify the specific data protection areas targeted by the scanner's functional features, and determine whether this tool is suitable for the assigned task in the field of cybersecurity.

This article focuses on the study of the operational features of vulnerability scanners such as Nmap, Nessus Professional, Acunetix, and Aircrack-ng, as vulnerability scanners are an important component of a cybersecurity strategy that helps maintain the integrity and security of systems.

Key words: *cybersecurity, cyber threats, vulnerability scanners, system and network vulnerabilities, vulnerability remediation.*