УДК 004.7

Приходько Д.С., здобувач
Дячук О. Ю., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ IT-ІНФРАСТРУКТУРИ НА ОСНОВІ OPENVAS

У сучасних умовах розвитку інформаційних технологій забезпечення кібербезпеки є одним із ключових завдань функціонування IT-інфраструктури. Вразливість визначається як недолік або слабкість активу, що може бути використана загрозою для порушення конфіденційності, цілісності або доступності інформації. Еволюція підходів до класифікації вразливостей пройшла шлях від базових таксономій до сучасних стандартів, зокрема Common Weakness Enumeration (CWE), який пропонує ієрархічну структуру типових помилок [2]. Значну роль у формуванні сучасного розуміння загроз відіграє OWASP Top 10, що акцентує увагу на першопричинах вразливостей та помилках у конфігурації систем [1].

Актуальність дослідження зумовлена зростанням кількості кіберзагроз, ускладненням IT-інфраструктур та необхідністю впровадження ефективних засобів виявлення вразливостей, особливо в умовах використання гібридних і розподілених середовищ.

Метою дослідження є аналіз сучасних методів виявлення вразливостей IT-інфраструктури та оцінка можливостей платформи OpenVAS у порівнянні з комерційними рішеннями.

Для забезпечення контролю стану безпеки активів застосовуються різні підходи до сканування [5]:

1. **Активне сканування**, що передбачає ініціювання взаємодії з цільовими системами з метою отримання детальної інформації про їхній стан. Такий підхід забезпечує високу точність виявлення, однак може створювати додаткове навантаження на мережеву інфраструктуру. Для поглибленого аналізу також застосовується агентний підхід.
2. **Пасивний аудит**, який базується на аналізі копій мережевого трафіку без безпосереднього втручання в роботу систем. Його перевагою є непомітність, проте можливості обмежуються лише виявленням вразливостей, що проявляються в мережевій активності.
3. **Тестування на проникнення (penetration testing)**, яке використовується для перевірки реальної експлуатованості виявлених вразливостей та зменшення кількості хибнопозитивних результатів.

Аналіз сучасного ринку засобів виявлення вразливостей показує, що він представлений як комерційними, так і відкритими рішеннями. Серед комерційних продуктів варто виділити Nessus, який

характеризується широкою базою перевірок та високою точністю результатів, а також Qualys VMDR, що реалізує хмарний підхід до управління вразливостями [3]. Водночас такі рішення можуть мати обмеження, пов'язані з вартістю використання та залежністю від інфраструктури постачальника.

Платформа OpenVAS є відкритим рішенням для сканування вразливостей, яке забезпечує достатній рівень виявлення для більшості типових IT-середовищ. За даними порівняльних досліджень, рівень виявлення окремих віддалених вразливостей для OpenVAS може становити близько **43%**, тоді як у комерційних рішень цей показник досягає **67–71%** [4]. Водночас для типових корпоративних середовищ ефективність виявлення може досягати **85–90%**, що підтверджує можливість практичного використання системи [4].

Незважаючи на зазначені відмінності, OpenVAS дозволяє ефективно здійснювати базовий аудит безпеки та адаптувати механізми перевірки за рахунок використання відкритого коду.

Важливою перевагою OpenVAS є можливість розгортання в ізольованих середовищах, що забезпечує контроль над даними та відповідає вимогам інформаційного суверенітету. Крім того, відсутність ліцензійних витрат знижує загальну вартість володіння системою.

У результаті проведеного аналізу встановлено, що сучасні підходи до забезпечення кібербезпеки потребують переходу від периметрального захисту до безперервного моніторингу стану активів. Комерційні рішення забезпечують високий рівень автоматизації та точності, однак можуть бути обмежені економічними та організаційними чинниками. Водночас OpenVAS може розглядатися як ефективний інструмент для виявлення вразливостей, який забезпечує баланс між функціональністю, економічною доцільністю та контролем над даними.

Список використаних джерел

1. OWASP Foundation. OWASP Top Ten Web Application Security Risks. URL: https://owasp.org/www-project-top-ten/

2. MITRE. **Common Weakness Enumeration (CWE).** URL: https://cwe.mitre.org

3. SenseLearner. Best Vulnerability Scanners: OpenVAS, Nessus & Qualys. URL: https://senselearner.com/best-vulnerability-scanners-openvas-nessus-qualys/

4. Pentest-Tools. A comprehensive benchmark of network vulnerability scanners 2024. URL: https://pentest-tools.com/benchmarks/network-vulnerability-scanners-benchmark-2024.pdf

5. Scarfone K., Souppaya M., Cody A., Orebaugh A. Technical Guide to Information Security Testing and Assessment. – NIST SP 800-115. https://csrc.nist.gov/pubs/sp/800/115/final