

АНАЛІЗ ІНСТРУМЕНТІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Блюма К.А., Балагура Д.С.

Харківський національний університет радіоелектроніки, Харків, Україна

Тестування на проникнення є важливою складовою забезпечення інформаційної безпеки комп'ютерних систем та мереж [1]. Воно дозволяє виявити вразливості до того, як ними скористаються зловмисники, а також оцінити рівень захищеності системи в реальних умовах. Проведення такого тестування імітує дії потенційного атакуючого, що дає змогу виявити не лише технічні недоліки, але й організаційні проблеми безпеки, такі як неправильні налаштування доступу, відсутність політик безпеки або недостатній рівень підготовки персоналу. Таким чином, тестування на проникнення виконує як діагностичну, так і превентивну функцію в системі кіберзахисту.

У сучасній практиці кібербезпеки використовується значна кількість інструментів [2]. **Метою доповіді** є проведення базового аналізу найбільш відомих інструментів.

Одним із найпоширеніших інструментів тестування на проникнення є Nmap, який застосовується для сканування мереж та виявлення активних вузлів і відкритих портів. Даний інструмент є ефективним на етапі попередніх етапах тестування, оскільки дозволяє отримати базову інформацію про цільову систему, включаючи тип операційної системи та запущені служби та їх версії [3]. Додатковою перевагою Nmap є підтримка сценаріїв (NSE – Nmap Scripting Engine), які дозволяють автоматизувати виявлення типових вразливостей та здійснювати більш глибокий аналіз мережевих сервісів.

Metasploit Framework є потужною платформою для експлуатації вразливостей [3]. Він містить велику кількість готових експлоїтів, допоміжних модулів та корисних навантажень (payloads), а також дозволяє автоматизувати процес тестування. Крім того, цей інструмент активно використовується для навчання та відпрацювання практичних навичок у сфері кібербезпеки. Важливою перевагою є також інтеграція з іншими інструментами та можливість розширення функціональності шляхом створення власних модулів.

Burp Suite широко використовується для аналізу безпеки веб-додатків. Його основною перевагою є можливість перехоплення та модифікації HTTP-запитів [3], що дозволяє досліджувати поведінку веб-додатків, знаходити вразливості типу SQL-ін'єкцій, XSS та інші. Додаткові модулі Burp Suite значно розширюють функціональність інструменту.

Wireshark застосовується для аналізу мережевого трафіку та дозволяє детально досліджувати пакети даних у режимі реального часу [1]. Це дає змогу виявляти підозрілу активність, аналізувати протоколи та знаходити потенційні точки витoku інформації. Інструмент є особливо корисним для виявлення атак типу «людина посередині» (Man-in-the-Middle), а також для аналізу некоректної роботи мережевих сервісів та протоколів.

Nessus є автоматизованим сканером вразливостей, який дозволяє швидко отримати звіт про стан безпеки системи. Він підтримує регулярні оновлення бази вразливостей, що робить його ефективним інструментом для постійного моніторингу та аудиту безпеки [1]. Крім того, Nessus дозволяє класифікувати знайдені вразливості за рівнем критичності та надає рекомендації щодо їх усунення, що значно спрощує процес прийняття рішень у сфері управління ризиками.

Кожен із розглянутих інструментів має свої особливості та сферу застосування. Виходячи з аналізу, найбільш ефективним є Metasploit Framework, оскільки він поєднує гнучкість, потужність та можливість практичної експлуатації вразливостей. Водночас найкращі результати досягаються при комплексному використанні декількох інструментів, що дозволяє отримати більш повну та об'єктивну оцінку рівня безпеки системи.

Також варто зазначити, що ефективне тестування на проникнення передбачає дотримання певної методології, яка включає етапи розвідки, сканування, експлуатації та формування звіту [4]. Якісно складений звіт є не менш важливим, ніж сам процес тестування, оскільки саме він містить рекомендації щодо усунення виявлених вразливостей. Вибір інструментів і методів тестування має здійснюватися з урахуванням специфіки досліджуваної інформаційної системи, її архітектури, критичності ресурсів та актуальних загроз [5]. Важливим аспектом є також регулярність проведення тестувань, що дозволяє своєчасно виявляти нові вразливості та підтримувати належний рівень захищеності.

Таким чином, комплексний підхід до тестування на проникнення, що включає використання різних інструментів, дотримання методології та залучення кваліфікованих фахівців, є запорукою ефективного забезпечення інформаційної безпеки сучасних систем.

Список літератури

1. Scarfone K., Souppaya M. Guide to Penetration Testing. NIST Special Publication 800-115. 2018. С. 1–25. DOI: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf>.
2. Дорофеева, К., Северінов, О., Сидоренко, З., & Сухотеплий, В. (2025). Застосування інструмента аналізу безпеки для виявлення критичних вразливостей у веб-додатках. *Вісник Херсонського національного технічного університету*, 3(4 (95)), 62-68.
3. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press. 2014. С. 25–180. <https://repo.zenk-security.com/>
4. Дорофеева, К. І., Северінов, О. В., & Сидоренко, З. М. (2025). Методологія проведення тестування на проникнення веб-додатків // Проблеми інформатизації: тринадцята міжнародна науково-технічна конференція.
5. Д'якова, Н. Є., & Северінов, О. В. (2022). Тестування вразливостей сучасних веб-ресурсів // Проблеми інформатизації : десята міжнародна науково-технічна конференція.