https://orcid.org/0000-0002-5080-1856
https://orcid.org/0009-0008-2886-1626

УДК 004.056.5

Ю.М. ЛИСЕЦЬКИЙ[*], О.О. СТАРОВОЙТЕНКО[**]

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ЯК ЗАСІБ ПІДВИЩЕННЯ РІВНЯ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

[*]ДП «ЕС ЕНД ТІ УКРАЇНА», м. Київ, Україна
[**]Інститут соціальної та політичної психології НАПН України, м. Київ, Україна

Анотація. *Тестування на проникнення є одним з основних типів оцінювання рівня кібербезпеки інформаційних систем та зособом його підвищення. Оцінювання захищеності системи чи мережі відбувається шляхом часткового моделювання дій зовнішніх зловмисників із проникнення у неї і внутрішніх зловмисників. Основою цього процесу стає активний аналіз системи з виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативне відставання в процедурних чи технічних контрзаходах. Такий аналіз проводиться з позиції потенційного нападника і має містити активне використання вразливостей системи принаймні у частині тестування, що виконується експертом. Зазвичай у ході тесту на проникнення виявляється певний набір вразливостей у системи, яку було протестовано. Зібрана інформація оформлюється у стандартизований звіт, який представляють власнику системи. Важливою частиною такого звіту є аналіз, який поєднує цю інформацію з детальною оцінкою потенційного впливу на організацію та окреслює межі технічних і процедурних контрзаходів для зменшення ризиків. Головною перевагою тестів на проникнення є рання ідентифікація ризиків: вони допомагають визначити слабкі місця до того, як їх використають зловмисники. Також регулярне тестування дозволяє організаціям покращити свою репутацію, бо у такий спосіб вони демонструють свою відповідальність у питаннях кібербезпеки і кіберзахисту. В цілому тестування на проникнення все більше стають обов'язковими у різних регіонах та галузях економіки, бо, зокрема, допомагають продемонструвати відповідність вимогам таких стандартів, як ISO27001, SOC 2, PCI DSS та інших. Сьогодні розвиток напряму тестування на проникнення поєднує тренди на подальшу автоматизацію, використання хмарних інструментів, штучного інтелекту в аналізі вразливостей, збільшення ролі тестів, що використовують соціальну інженерію. Тестування на проникнення продовжить своє подальше розповсюдження та розвиток методологічної й інструментальної компонент.*

Ключові слова: *кібербезпека, інформаційні системи, тестування на проникнення, типи, різновиди, штучний інтелект.*

Abstract. *Penetration testing is one of the primary methods for assessing the cybersecurity level of information systems and a means of improving it. The security evaluation of a system or network is conducted by partially simulating the actions of external attackers attempting to infiltrate it, as well as internal malicious actors. This process is based on an active analysis of the system to identify any potential vulnerabilities that may arise due to improper system configuration, known and unknown hardware and software defects, or delays in procedural or technical countermeasures. Such analysis is conducted from the perspective of a potential attacker and must include the active exploitation of system vulnerabilities, at least during the portion of testing performed by an expert. Typically, a penetration test reveals a certain set of vulnerabilities within the tested system. The gathered information is compiled into a standardized report presented to the system owner. A crucial part of this report is the analysis, which combines this information with a detailed assessment of the potential impact on the organization and outlines the scope of technical and procedural countermeasures to mitigate risks. The primary advantage of penetration testing is the early identification of risks, since it helps to detect weaknesses before they can be exploited by malicious actors. Additionally, regular testing enables organizations to enhance their reputation by demonstrating responsibility in cybersecurity and cyber defense. Overall, penetration testing is becoming increasingly mandatory across various regions and industries, as it helps organizations comply with stand-*

ards such as ISO 27001, SOC 2, PCI DSS, and others. Today, the development of penetration testing aligns with trends toward further automation, the use of cloud-based tools, artificial intelligence in vulnerability analysis, and the growing role of tests incorporating social engineering techniques. Penetration testing will continue to expand and develop both methodologically and instrumentally.
Keywords: *cybersecurity, information systems, penetration testing, types, variations, artificial intelligence.*

DOI: 10.34121/1028-9763-2025-2-24-29

1. Вступ

Історія тестування на проникнення практично дорівнює історії IT-галузі. Ще у 1960-х рр., з появою перших великих обчислювальних мереж, як-от ARPANET, почали виникати і перші загрози безпеці, та під час роботи урядових організацій США, як-от RAND Corporation, зародилась ідея тестів на проникнення. 1980-ті рр., коли розвиток мережевих технологій призвів до поширення хакерських атак, як контрзахід з'явилася концепція «білих хакерів», які використовували свої навички для підвищення безпеки інформаційних систем (ІС). Це заклало основу для офіційного тестування ІС на проникнення [1]. 2000-ті рр. було ознаменовано формалізацією методологій: появою таких стандартів, як OSSTMM, NIST SP 800-115 та OWASP. Завдяки цьому, тести на проникнення стали більш структурованими, а організації почали проводити їх на регулярній основі для забезпечення безпеки своїх ІС. 2010-ті рр. було ознаменовано появою різноманітних автоматизованих систем для тестування на проникнення, які можна використовувати онлайн, а також подальшим поширенням цієї послуги, оскільки урядові організації по всьому світу почали вимагати проведення регулярних тестів на проникнення для забезпечення кібербезпеки критичної, державної та комерційної інфраструктур [2]. Тому завдання підвищення рівня кіберзахисту ІС із застосуванням тестів на проникнення є дуже актуальним.

Мета статті — дослідити можливості підвищення рівня кіберзахисту ІС за допомогою тестування на проникнення.

2. Основні класифікації тестів на проникнення

Тести на проникнення (англ. penetration tests) — це процеси, спрямовані на виявлення слабких місць в ІС, додатках або мережах шляхом симуляції реальних атак. Оцінювання захищеності комп'ютерної системи чи мережі відбувається шляхом часткового моделювання дій зовнішніх зловмисників із проникнення у неї (які не мають авторизованих засобів доступу до ІС) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу). Основою цього процесу стає активний аналіз ІС із виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативне відставання в процедурних чи технічних контрзаходах [3]. Відзначимо, що такий аналіз проводиться з позиції потенційного нападника і має містити активне використання вразливостей ІС принаймні у частині тестування, що виконується експертом.

Зазвичай у ході тесту на проникнення виявляється певний набір вразливостей у ІС, яку було протестовано. Зібрана інформація оформлюється у стандартизований звіт, який представляють власнику системи. Важливою частиною такого звіту є аналіз, який поєднує цю інформацію з детальною оцінкою потенційного впливу на організацію та окреслює межі технічних і процедурних контрзаходів для зменшення ризиків.

Головною перевагою тестів на проникнення є рання ідентифікація ризиків: вони допомагають визначити слабкі місця до того, як їх використають зловмисники. Також регулярне тестування дозволяє організаціям покращити свою репутацію, бо у такий спосіб вони демонструють свою відповідальність у питаннях кібербезпеки і кіберзахисту. В цілому тестування на проникнення все більше стають обов'язковими у різних регіонах та галузях

економіки завдяки тому, що допомагають продемонструвати відповідність вимогам таких стандартів, як ISO27001, SOC 2, PCI DSS та інших.

2.1. За типом доступу до інформації

Існує багато різновидів тестів на проникнення. Найбільш поширені ті, що класифікуються за типом доступу до інформації, що надається тестерам, та за основним об'єктом тестування.

Основні різновиди тестів на проникнення за типом доступу — це «чорна скринька» (англ. black box), «сіра скринька» (англ. gray box) та «біла скринька» (англ. white box). Тестування на проникнення типу black box відбувається тоді, коли тестери не мають жодної інформації про систему або мережу, яку вони тестують. Їх завдання — симулювати атаку з точки зору зовнішнього зловмисника, щоб виявити слабкості, доступні без внутрішньої інформації. Перевагами такого підходу є реалістичність та симуляція реальних зовнішніх атак. З іншого боку, потенційно це може призвести до пропущення вразливостей, які можуть бути виявлені при більш глибокому аналізі, оскільки тестери не завжди можуть ідентифікувати всі вразливості з таким підходом. У цьому варіанті тестування на проникнення багато залежить від знань тестера [4].

Тестування на проникнення типу grey box відбувається тоді, коли тестерам надають частковий доступ до внутрішньої інформації (документація, обмежені дані про архітектуру), що дозволяє ефективніше оцінити вразливості. Це імітує сценарій симуляції атаки інсайдера з обмеженим доступом; також добре підходить для тестування окремих компонентів системи. Такий підхід є певним компромісом між реалістичністю та глибиною аналізу, він вимагає більше часу, ніж black box, але менше — у порівнянні з white box підходом. Як і у випадку з black box, такий підхід потенційно може призвести до пропуску вразливостей через обмежений доступ, що може бути викликано складнощами у визначенні обсягу інформації, яка надається тестерам [5].

У випадку з white box підходом тестери мають повний доступ до інформації про систему, включаючи архітектуру, код, мережеві топології та ін. Цей підхід використовують із метою здійснити найглибший аналіз безпеки, наприклад, при аналізі коду додатків або перевірці комплексної архітектури системи. Незважаючи на безумовні переваги такого підходу, він не завжди здатний врахувати реалістичні варіанти атаки зовнішнього зловмисника та вимагає значних витрат часу і ресурсів [6].

Кожен із вищеназваних підходів до тестування має свої переваги та недоліки. Вибір підходу залежить від цілей тестування: якщо для перевірки зовнішньої безпеки доцільно використовувати black box, то для аналізу внутрішніх компонентів чи специфічних вразливостей підійде grey box. Для детального аудиту безпеки системи краще підходить white box підхід.

2.2. За типом об'єкта доступу

Основні різновиди тестів на проникнення за об'єктом доступу:

- тестування вебзастосунків (Web Application Pentesting);
- тестування мобільних застосунків (Mobile Application Pentesting);
- тестування мереж (Network Pentesting);
- тестування бездротових мереж (Wireless Network Pentesting);
- тестування соціальної інженерії (Social Engineering Pentesting);
- фізичне тестування на проникнення (Physical Pentesting).

Варто зазначити, що всі вищезгадані типи тестування на проникнення потребують спеціальних знань та навичок. Розглянемо ці типи детальніше.

Тестування вебдодатків (Web Application Pentesting). Цей тип тестування на проникнення спрямований на виявлення вразливостей у вебдодатках. Це досить складний процес, оскільки він охоплює фронтенд, базу даних, бекенд та інші складові вебдодатка, щоб ідентифікувати вразливості в коді, конфігурації або архітектурі вебдодатків. У межах тестування перевіряються всі кінцеві точки взаємодії застосунку з користувачем. Деякі перевірки, які можуть бути частиною такого оцінювання безпеки, містять використання відкритих джерел (OSINT), визначення серверів, IP-адрес, субдоменів, аналіз HTTP-запитів та заголовків, атаки типу Cross-Site Scripting, клікджекінг, викрадення форм, HTML-ін'єкції, відкриті перенаправлення та багато інших [7].

Тестування мобільних додатків (Mobile Application Pentesting). Цей тип тестування на проникнення стає надзвичайно популярним, оскільки все більше бізнесів та державних сервісів використовують мобільні додатки. Тестування мобільних додатків містить такі перевірки, як отримання інформації про додаток, сервери та API; аналіз архітектури додатка (мобільна частина, бекенд, API); збір даних про залежності та бібліотеки; перевірка поведінки додатка під час виконання; моніторинг трафіку між клієнтом та сервером; аналіз уразливостей API; перевірка механізмів аутентифікації та авторизації та інші. Симуляція атак для підтвердження знайдених вразливостей у мобільному додатку може підтвердити такі вразливості, як небезпечне зберігання даних, недостатнє шифрування чи механізми автентифікації даних, помилки валідації вводу, відкриті API тощо [8].

Тестування мереж (Network Pentesting). Це один із найпоширеніших типів тестування на проникнення, який спрямований на виявлення вразливостей та слабких місць у мережевій IT-інфраструктурі. Сюди входять не лише міжмережеві екрани (firewalls), комутатори та маршрутизатори, але й сервери, сховища даних, робочі станції, принтери тощо. Цей тип тестування допомагає оцінити рівень готовності до атак, як-от обхід міжмережевого екрану, атаки на маршрутизатори, проксі-сервери, бази даних тощо. Такі тестування передбачають ідентифікацію мережевих сегментів (LAN, WAN, VPN); визначення обладнання; встановлення рівня тестування: зовнішній (External) або внутрішній (Internal); аналіз відкритих портів і служб; визначення потенційних вразливостей; аналіз неправильно налаштованих мережевих служб; ідентифікацію застарілих протоколів (наприклад, SMBv1, FTP); атаки на слабкі паролі; експлуатацію вразливих служб (наприклад, RDP, SSH); оцінку глибини компрометації та пошук шляхів для горизонтального або вертикального переміщення в мережі [9].

Тестування бездротових мереж (Wireless Network Pentesting). Це специфічний тип тестування мереж, який зосереджується на з'єднаннях між бездротовими пристроями та домашніми чи офісними Wi-Fi мережами. Особливість бездротового пентесту полягає в тому, що він виконується на місці, оскільки потрібно знаходитися в зоні дії сигналу. Проте певні пристрої можуть підключатися до бездротової мережі, що дозволяє віддаленому тестувальнику проводити перевірки. Бездротові мережі необхідно тестувати, оскільки вони є одним із найпоширеніших джерел витоку даних через їх відносно менш контрольований характер використання.

Тестування соціальної інженерії (Social Engineering Pentesting). Цей тип тестування відрізняється від інших, оскільки більше покладається на соціальні, комунікаційні та дизайнерські навички, а не суто технічні. Під час соціальної інженерії зловмисник намагається змусити жертву розкрити таку інформацію, як, наприклад, облікові дані. Існує широкий спектр технік соціальної інженерії, як-от фішинг, вішинг, смішинг, атаки видавання і багато інших.

Незважаючи на здавалося б менш агресивний характер соціальної інженерії, це небезпечна ілюзія. Вражаючі 98 % усіх кібератак зараз використовують елементи соціальної інженерії [10]. Такі атаки занадто часто виявляються успішними, оскільки людський фактор залишається найслабшою ланкою у складній системі кібербезпеки. Тестування

соціальної інженерії, поєднане з навчанням підвищення обізнаності про кібербезпеку, стало основою сучасної кібербезпеки будь-якої організації.

Фізичне тестування на проникнення (Physical Penetesting). Цей тип тестування на проникнення теж є специфічним та стоїть трохи осторонь інших типів, оскільки обов'язково передбачає спроби обійти фізичні бар'єри, як-от замки, камери, паркани, різні датчики тощо, що захищають певну інфраструктуру чи системи. Це — моделювання дій потенційного зловмисника, який намагається отримати доступ до об'єктів, приміщень або критичних фізичних ресурсів. Цей тип тестування дозволяє виявити слабкі місця в фізичній безпеці, як-от системи контролю доступу, відеоспостереження або поведінкові аспекти співробітників (11). У типовому фізичному тестуванні на проникнення відбувається визначення ключових об'єктів, як-от серверні кімнати, склади, офіси тощо; проходить оцінювання систем захисту: сигналізації, охорони, замків, камер; узгоджуються дозволені та заборонені методи тестування. Після цього починається сам процес, що передбачає спостереження, аналіз та спроби фізичного проникнення на об'єкт.

Отже, відзначимо, що обидві вищезгадані класифікації — за типом доступу до інформації та за об'єктом тестування — можна та треба використовувати у комбінації, бо за деякими виключеннями кожен із тестів на проникнення буде відповідати одному з типів з обох класифікацій.

3. Висновки

Так, тестування на проникнення є одним з основних типів оцінювання рівня кібербезпеки ІС та засобом його підвищення. Оцінювання захищеності системи чи мережі відбувається шляхом моделювання дій зовнішніх зловмисників із проникнення у неї і внутрішніх зловмисників. Основою цього процесу є активний аналіз системи з виявлення будь-якої потенційної вразливості, що може виникати внаслідок її неправильної конфігурації, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, оперативного відставання в процедурних чи технічних контрзаходах. Зазвичай у ході тесту на проникнення виявляється певний набір вразливостей у системи, яку було протестовано. Зібрана інформація оформлюється у стандартизований звіт, важливою частиною якого є аналіз, що поєднує цю інформацію з детальною оцінкою потенційного впливу виявлених вразливостей ІС на організацію та окреслює межі технічних і процедурних контрзаходів для зменшення ризиків. Головною перевагою тестів на проникнення є рання ідентифікація ризиків, що допомагає визначити слабкі місця до того, як їх використають зловмисники.

Отже, сьогодні розвиток напряму тестування на проникнення поєднує тренди на подальшу автоматизацію, використання хмарних інструментів, штучного інтелекту в аналізі вразливостей, збільшення ролі тестів, що використовують соціальну інженерію. Тестування на проникнення продовжать своє подальше розповсюдження й розвиток методологічної та інструментальної компонент.

СПИСОК ДЖЕРЕЛ

1. Penetration Testing History. Retrieved. URL: https://christianespinosa.com/blog/penetration-testing-history/ (дата звернення: 12.12.2024).
2. Bacudio A., Yuan X., Chu B., Jones M. An Overview of Penetration Testing. *International Journal of Network Security & Its Applications*. 2011. Vol. 3. P. 19–38. DOI: https://doi.org/10.5121/ijnsa.2011.3602 (дата звернення: 16.12.2024).
3. Тести на проникнення. Retrieved on 12.12.2024. URL: https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F (дата звернення: 12.12.2024).

4. Alhamed M., Rahman M. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences*. 2022. Vol. 13 (12). P. 6986. URL: https://doi.org/10.3390/app13126986 (дата звернення: 22.12.2024).
5. Ferdous R., Suchi U. Evaluating Penetration Testing and Methodologies. 2024. URL: https://www.researchgate.net/publication/382617676_Evaluating_Penetration_Testing_and_Methodologis (дата звернення: 22.12.2024).
6. Software Testing — White Box Penetration Testing. 2024. URL: https://www.geeksforgeeks.org/software-testing-white-box-penetration-testing/ (дата звернення: 02.01.2025).
7. Altulaihan E., Alismail A., Frikha M. A Survey on Web Application Penetration Testing. *Electronics*. 2023. Vol. 12 (5). P. 1229. URL: https://doi.org/10.3390/electronics12051229 (дата звернення: 02.01.2025).
8. Makadia H., Kotadia J. Mobile Security and Penetration Testing. *International Journal of Advanced Research in Science, Communication and Technology*. 2021. Vol. 12, Issue 1. P. 455–460. DOI: https://doi.org/10.48175/IJARSCT-2215.
9. Network Penetration Testing. 2024. URL: https://www.blackduck.com/glossary/what-is-network-penetration-testing.html (дата звернення: 04.01.2025).
10. Соціальна інженерія: що це та як уберегтися від шахрайства. 2024. URL: https://www.zen.com/uk/blog/personal-finance-uk/social-engineering-how-to-protect-yourself-from-fraud/ (дата звернення: 02.01.2025).
11. Physical pen testing methods and tools. 2023. URL: https://www.techtarget.com/searchsecurity/tip/Physical-pen-testing-methods-and-tools (дата звернення: 08.01.2025).

Стаття надійшла до редакції 18.12.2024