УДК 004.056.5:005.334

Кравчук В.С., аспірант
Дорогий Я.Ю., д.т.н., професор
Донецький національний технічний університет

МЕТРИКИ ЕФЕКТИВНОСТІ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ

Анотація. У цих тезах розглядається еволюція підходів до оцінки ефективності тестування на проникнення (пентесту). Акцентується увага на переході від періодичних перевірок, зумовлених нормативними вимогами, до моделі безперервної валідації, орієнтованої на продуктивність та бізнес-результати. Визначаються ключові метрики та показники ефективності (KPI), які перетворюють пентест із центру витрат на стратегічний інструмент управління ризиками.

Вступ. Сучасний ландшафт кібербезпеки зазнав фундаментальних змін: від періодичних оцінок безпеки до моделі безперервної перевірки. Оскільки організації інтегрують складні вебзастосунки в кожен аспект своєї архітектури, традиційний "точковий" пентест стає недостатнім показником реального стану безпеки. Формалізація поняття ефективності тестування на проникнення є критично важливою вимогою сучасних циклів розробки програмного забезпечення, таких як CI/CD та DevSecOps. Ефективність більше не вимірюється лише кількістю знайдених вразливостей; на перший план виходять такі показники, як швидкість, точність та відтворюваність результатів.

Аналіз літературних джерел. Фундаментом для побудови ефективного процесу пентесту є стандартизовані методології, які гарантують послідовність та професіоналізм. Такі фреймворки, як OWASP, PTES (Penetration Testing Execution Standard) та OSSTMM, забезпечують необхідні структурні рекомендації для переходу від несистематичного тестування до наукового підходу, заснованого на даних. Наприклад, PTES формалізує процес у п'ять основних етапів: розвідка, сканування, оцінка вразливостей, експлуатація та звітування [1].

Крім того, для якісної оцінки ризиків та пріоритезації результатів у літературі часто застосовується модель DREAD, яка оцінює п'ять параметрів: потенційну шкоду (Damage), відтворюваність (Reproducibility), експлуатованість (Exploitability), кількість уражених користувачів (Affected users) та виявлюваність (Discoverability) [2].

Основна частина. Ефективність тестування на проникнення формалізується через розкладання процесу на окремі вимірювані етапи, кожен з яких регулюється набором строгих метрик:

1. Метрики операційного охоплення та частоти (Operational Scope & Activity Velocity). Важливими показниками є охоплення портфеля (Portfolio Coverage) — відсоток відомих активів, кінцевих точок та API, що підлягають тестуванню. Не менш важливою є частота тестування (Test Cadence) по відношенню до циклів випуску програмного забезпечення [3].

2. Технічна ефективність (Technical Efficacy). Ключовим показником на етапі виявлення є рівень виявлення вразливостей (Vulnerability Discovery Rate - VDR), який вимірює кількість унікальних вразливостей, знайдених за одиницю часу або за одне залучення. Високий VDR повинен супроводжуватися низьким рівнем хибних спрацьовувань (False Positive Rate), щоб запобігти "виснаженню від сповіщень" (alert fatigue) серед персоналу та не витрачати ресурси на марне сортування [4,5].

3. Метрики швидкості реагування (Speed Metrics). Серед ключових часових метрик виділяють: середній час до виявлення (Mean Time to Detect - MTTD): час від початку аномальної події до її ідентифікації [1] та середній час на усунення (Mean Time to Remediate - MTTR): середній час, необхідний для вирішення проблеми безпеки після її виявлення [4, 5]. Зниження MTTR є прямим свідченням того, що команди безпеки та розробки ефективно співпрацюють [6, 7].

4. Економічна ефективність та ROI (Return on Investment). Вартість професійного пентесту може варіюватися від $5,000 до понад $150,000 [8]. Однак ефективність цих витрат оцінюється через моделювання рентабельності інвестицій. ROI розраховується шляхом порівняння вартості залучення пентестерів зі зниженням очікуваних збитків. Оскільки середня вартість витоку даних перевищує $10 мільйонів, навіть дорогий пентест, який запобігає одному інциденту, може забезпечити окупність у співвідношенні 340:1 [8]. Відстеження тенденцій щільності вразливостей (Vulnerability density trends) з часом також допомагає довести керівництву (наприклад, CFO), що інвестиції у безпеку приносять реальну користь та зменшують кількість вразливостей на одиницю коду [8].

5. Відтворюваність та якість звітування. Ефективний звіт про пентест має бути дієвим. Це досягається через відтворюваність (Reproducibility) доказів концепції (Proof-of-Concept). Відтворюваний PoC є необхідним для того, щоб захисники могли перевірити вразливість, провести аналіз першопричин та підтримати регресійне тестування. Звіт повинен перекладати технічні знахідки на мову бізнес-ризиків та надавати чіткі кроки для їх усунення [9].

Висновки. Поняття ефективності пентесту вийшло далеко за межі складання простого переліку знайдених технічних помилок. Формалізація ефективності вимагає переходу до багатовимірної системи кількісних індикаторів, кожен етап якої (аналіз, виявлення, оцінка впливу, звітування) оптимізується за критеріями швидкості, точності та відтворюваності. Систематичне відстеження таких метрик, як VDR, MTTR, рівень хибних спрацьовувань та ROI, а також застосування перевірених методологій (PTES, OSSTMM, DREAD), дозволяє організаціям перетворити тестування на проникнення зі звичайної вимоги для комплаєнсу на суворий, вимірюваний та високоефективний процес, що активно посилює цифровий захист компанії.

Список використаних джерел

1. Learn About The Five Penetration Testing Phases | Pentesting. EC-Council. 2022. URL: https://lnk.ua/bskZscvm8
2. Nilsson T., Andersson L. External Threat Assessment and Internal Network Security Evaluation: A Penetration Test and Vulnerability Analysis of IVA's Internal Infrastructure Against External Threats. KTH Royal Institute of Technology. 2025. URL: https://lnk.ua/afryw7pfg
3. Wong C. Pen Test Metrics 101: Detailed Definitions. Cobalt. 2017. URL: https://lnk.ua/mNpkyN3lD
4. Hinojosa G. Less Findings in your Pentest? Measuring the Effectiveness of a Penetration Test. Cobalt. 2025. URL: https://lnk.ua/caxTjTO3R
5. Mukherjee A. Measuring the Impact of Penetration Testing with Metrics. Threat Intelligence. 2023. URL: https://lnk.ua/bhGCG53BE
6. Application Security Metrics and KPIs for Security Posture. Legit Security. URL: https://lnk.ua/1tLnfjthv
7. Callegari C. Penetration Testing ROI: 5 Metrics to Communicate Real Value. Software Secured. URL: https://lnk.ua/Zrd5iuqQu
8. Penetration Testing Pricing 2026: Enterprise Cost Guide. DeepStrike. URL: https://lnk.ua/43EQpKgcN
9. Odom C. Essential Elements of a Penetration Testing Report. Emagined Security. 2024. URL: https://lnk.ua/D8YvsUl66