НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

76-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

ТОМ 1

14 травня – 23 травня 2024 р.

УДК 004.05

Живило Є.О., к.держ.упр., доцент
Сімонькін А.А., бакалавр з комп'ютерної інженерії
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ПЕНТЕСТІНГ - ІНСТРУМЕНТ АУДИТУ ЦИФРОВИХ КОМУНІКАТИВНИХ СЕРЕДОВИЩ

Тестування на проникнення – це метод оцінки захищеності комп'ютерних систем і мереж, який частково імітує діяльність зовнішніх зловмисників (які не мають доступу до системи) або внутрішніх зловмисників (які мають певний рівень прав доступу). Процес передбачає проактивний аналіз системи з метою виявлення потенційних вразливостей, що виникають через неправильну конфігурацію системи, відомі та невідомі недоліки апаратного та програмного забезпечення, операційні затримки в процедурах та технічних заходах тощо. Цей аналіз проводиться з точки зору потенційного зловмисника і може включати активну експлуатацію вразливостей.

Сьогодні провідною платформою для тестування на проникнення є Kali Linux (Рисунок 1). Kali Linux – це дистрибутив Linux із відкритим вихідним кодом на основі Debian, призначений для виконання різноманітних завдань інформаційної безпеки (далі – ІБ), таких як тестування на проникнення, дослідження безпеки, комп'ютерна експертиза та зворотнє проектування.

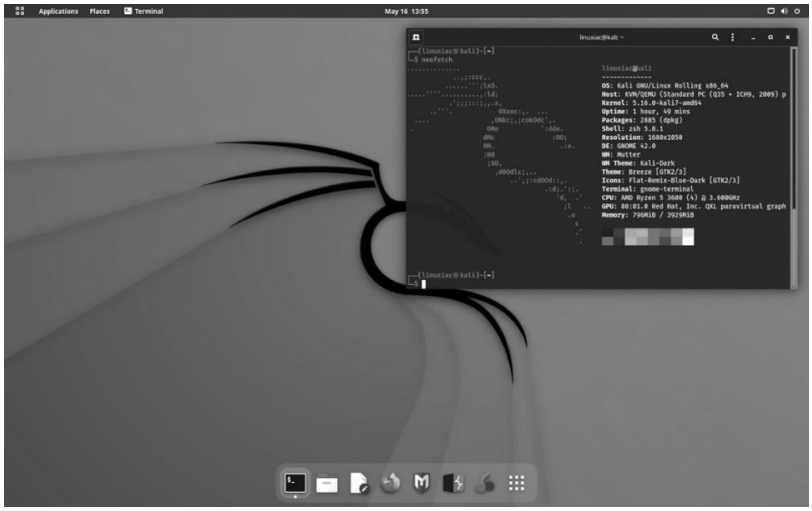

Рисунок 1. Дистрибутив Kali Linux з графічною оболонкою Gnome shell.

Так платформа тестування на проникнення Kali Linux включає широкий спектр інструментів та утиліт, від збору і аналізу інформації до кінцевого звіту, що дозволяє фахівцям з безпеки та ІТ-спеціалістам оцінити безпеку власних систем/архітектури.

Отже суть цього дослідження полягає в розкритті послідовності та етапів реалізації заходів, що складаються з санкціонованих спроб обходу існуючого набору засобів захисту досліджуваної інформаційної системи.

З огляду на зазначене, нижче наведено основні етапи тесту на проникнення, а саме:

- аналіз загальнодоступної інформації про компанію та її інформаційне середовище;
- проведення досліджень пов'язаних із соціальною інженерією;
- аналіз вразливостей внутрішніх і зовнішніх ресурсів;
- здійснення проникнення;
- створення звітної документації.

По завершенню всіх етапів тестінгу, формується звіт, в якому зазначається наступна інформація:

- детальне відображення виявлених вразливостей і недоліків, що становлять загрозу для бізнес-процесів компанії, рівень їхніх ризиків, оцінка можливостей зловмисника ними скористатися;
- опис сценаріїв, за допомогою яких проводилося проникнення;
- детальний опис структури об'єктів тестування;
- методи і засоби, використані під час проведення тесту на проникнення;
- рекомендації щодо усунення виявлених вразливостей і недоліків.

Слід зазначити, що основними об'єктами аудиту є зовнішні веб-ресурси та локальна мережа замовника.

З огляду на те, що аудитори проводять тестування систем за повним циклом, вкрай важливо розуміти використання ними методів соціальної інженерії, на додаток до технічних з метою оцінки рівня підготовки співробітників з ІБ.

При цьому всі умови, методи та етапність, а також дії аудиторів заздалегідь обговорюються та узгоджуються з замовником.

Як результат, підсумкові рекомендації, що надаються аудитором комунікаційного середовища, включають визначення застосованого підходу, характер та специфікацію системи, що перевіряється, а також стан ІБ відповідно до рівня деталізації, що використовується в аудиті. У будь-якому випадку, рекомендації аудитора повинні бути застосовні до конкретної та відповідної телекомунікаційної системи, економічно обґрунтовані, аргументовані (підкріплені результатами аналізу) та класифіковані відповідно до рівня їх важливості.

При цьому заходи щодо забезпечення захисту на організаційному рівні майже завжди мають пріоритет над конкретними програмними та апаратними методами захисту. Водночас, наївно очікувати, що за результатами аудиту зазначені "уповноважені суб'єкти" нададуть детальні рекомендації щодо технічного проектування підсистем ІБ або впровадження конкретних програмно-апаратних засобів захисту інформації. З цією метою внутрішні аудитори могли б брати активну участь у цій роботі, але вони

повинні були б проводити більш глибокі дослідження конкретних питань, пов'язаних з організаційним захистом.

Аудиторський звіт є основним результатом роботи аудиту. Його якість характеризує кваліфікаційний рівень аудитора. Аудиторський звіт повинен містити, як мінімум, опис цілей аудиту, опис досліджуваної комунікативної системи, вказівку на обсяг аудиту і використані методи, результати аналізу даних аудиту, висновок, що узагальнює ці результати, оцінку рівня захищеності автоматизованої системи або її відповідності вимогам стандартів, і, звичайно, рекомендації аудитора щодо усунення наявних недоліків і підвищення рівня захищеності. Обов'язково повинні бути включені рекомендації аудитора щодо вдосконалення системи.

Таким чином, можна зробити висновок, що пентестування відіграє важливу роль у сфері ІБ та кібербезпеки. Це пов'язано з тим, що, знаючи всі загрози та вразливості системи, можна побудувати комплексну систему захисту інформації, мереж тощо.

Література

1. Zhyvylo Y. O., Zhyvylo I. O. Joint training of the cyber security defense forces personnel in the conditions of total state defense. Theory and Practice of Public Administration. 2021. No 2 (73). C. 144–153. DOI: https://doi.org/10.34213/tp.21.02.16.

2. Onyshchenko S., Zhyvylo Y., Cherviak A., Bilko S. Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. Eastern-European Journal of Enterprise Technologies. 2023. Vol. 5 (13 (125). P. 65–76. URL: https://journals.uran.ua/eejet/article/view/288175/283817 DOI: https://doi.org/10.15587/1729-4061.2023.288175.

3. Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS). URL: https://csrc.nist.gov/pubs/sp/800/94/final.

4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" : Указ Президента України No 96/2016р. (у ред. від 28 серпня 2021 року). URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html.

5. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо за-хисту якої встановлена законом : Постанова Кабінету міністрів України від 11 листопада 2020 р. No 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text.