DOI: https://doi.org/10.36910/6775-2524-0560-2021-42-31
УДК 004.7:336.71
Шваюк Андрій Віталійович, студент
Бортник Катерина Яківна, к.т.н., доцент
http://orcid.org/0000-0001-5282-099X
Гринюк Сергій Васильович, асистент
https://orcid.org/0000-0002-0080-3167
Луцький національний технічний університет

АНАЛІЗ МЕТОДІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В КОМП'ЮТЕРНІ СИСТЕМИ ДЛЯ ОЦІНКИ ЯКОСТІ ЗАХИСТУ БАНКІВСЬКИХ ДАНИХ КОРИСТУВАЧІВ

Шваюк А.В., Бортник К.Я., Гринюк С.В. Аналіз методів тестування на проникнення в ком'ютерні системи для оцінки якості захисту банківських даних користувачів. Матеріал статті містить огляд основних підходів до тестування на проникнення в комп'ютерні системи, перехоплення даних. В роботі викладено опис та аналіз стандартів тестування безпеки, описано план підготовки для тестування, виконання та підготовку результатів роботи.
Ключові слова: тестування на проникнення , тестування, захист банківськи даних користувачів, проникнення ком'ютерні системи, методи тестування.

Шваюк А.В., Бортник Е.Я., Гринюк С.В. Анализ методов тестирования на проникновение в комъютерних системы для оценки качества защиты банковских данных пользователей. Материал статьи содержит обзор основных подходов к тестированию на проникновение в компьютерные системы, перехват данных. В работе изложено описание и анализ стандартов тестирования безопасности, описаны план подготовки для тестирования, выполнения и подготовку результатов работы.
Ключевые слова: тестирование на проникновение, тестирования, защиты банковских данных пользователей, проникновение в комъютерних системы, методы тестирования**.**

A.V. Shvayuk, Bortnyk K.Ya., Hrinyuk S.V. Analysis of computer system penetration testing methods for assessing the quality of user banking data protection. The article contains a review of the main approaches to computer system penetration testing, data interception. The paper describes and analyzes security testing standards, describes the preparation plan for testing, execution and preparation of the results of the work.
Keywords: penetration testing, testing, protection of bank user data, penetration into computer systems, testing methods.

Постановка проблеми та аналіз досліджень. На сучасних цифрових інформаційних об'єктах зберігання даних сьогодні сконцентрована велика кількість чутливої інформації користувачів. До таких об'єктів можна віднести бази даних банків та IT-проектів, що взаємодіють із такого роду інформацією. Враховуючи можливість отримання віддаленого доступу до цих даних, існує потреба в тестуванні систем на проникнення для мінімізації ризиків витоку інформації та потрапляння її до третіх осіб. Кожного дня зростає кількість сервісів, що надають послуги, доступ до інформаційних ресурсів (та іншого) користувачам, що вимагає здійснення оплати способом надання своїх банківських даних таким сервісам. В подальшому такі дані відправляються на спеціалізовані платіжні гетвеї у спосіб визначений ними. Надалі, якщо сервіс передбачає регулярність платежів або ж з інших причин, коли є необхідність використання таких даних, вони можуть зберігатися на серверах подібного сервісу. Усі ці фактори вказують на ризики витоку даних на кожному із вище описаних етапів взаємодії із сервісом.
Існує перелік основних пунктів, згідно з якими проводиться робота із тестування на проникнення:

- Визначення вимог до тестування. Безпосередньому процесу пошуку вразливостей передує визначення цілей такої роботи із замовником роботи. Цілі виконавця та замовника повинні сходитись для ефективного результату роботи та можливості ефективного подальшого впровадження рішень для виправлення проблем, що були знайдені в процесі тестування.
- Дослідження об'єкту тестування. Вивчення наявної документації проекту, збір інформації, вивчення архітектури, ознайомлення із кодом проекту. Даний етап важливий для попереднього висновку по можливих слабких місцях. У процесі можна отримати відомості щодо кластерерів багів, де найчастіше виникають «дірки».

- Планування процесу тестування. Тестувальник здійснює опис процесу, що буде виконуватись. Викладається попереднє бачення можливих вразливих місць системи, описується процес із зазначенням етапів і послідовності перевірки тестових випадків.
- Виконання роботи із пошуку вразливостей. Проводиться реалізація перевірок згідно тестплану та, використовуючі інші методики, зокрема ед-хок тестування, перевірка, що опирається на досвід виконавця.
- Оцінка безпеки системи, підготовка звіту за результатом роботи. Готується виклад знайдених прогалин у системі, детально описуються шляхи відтворення проблем та можуть надаватись рекомендації із покращень. Звіт включає в себе визначення ризиків із використання в подальшому наявних рішень та оцінку критичності проблем за відповідною градацію від критичних до мінорних.

Метою статті проаналізувати методи тестування на проникнення в комп'ютерні системи для оцінки якості захисту даних банківських даних користувачів та оцінити ефективність таких методів.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження.

Тестування на проникнення повинно ставити своєю метою перевірку надійності захисту банківських даних користувачів у системах обробки, зберігання, використання інформації, яка є конфіденційною. Процес тестування має бути спланований, базуючись на перевірці усіх можливих користувацьких випадків, що можуть призвести до потрапляння їх банківських даних третім особам або ж способів заволодіння такими, за допомогою методологій проникнення в інформаційні системи.

Варто розглядати проблематику комплексно, враховуючи, що перевірку потрібно здійснювати на усіх вузлах, де є введення, вивід, обробка та зберігання даних. Змістивши фокус лише на вузли, де дані зберігаються чи обробляються, можна не запобігти витоку, наприклад, на фронтальній стороні користувача. Потрібно визначити основні джерела витоку інформації для коректного планування роботи із тестування. До таких джерел можна віднести погано організовану архітектуру баз даних, відсутність програмних алгоритмів захисту, середовище розгортання системи.

Розглянемо ряд основних можливих способів проникнення в систему або ж заволодіння чутливою інформацією.

1. Різноманітні ін'єкції. Також даний метод може називатись «впровадженням коду». Він передбачає поміщення своїх програмних блоків або ж скриптів у систему, яка піддається атаці. Код може бути поміщений завдяки прогалинам у валідації даних, які передаються в систему різними джерелами. Далі, якщо вдалось обійти алгоритм валідації, чужорідний код потрапляє інтерпритатору, який його виконує. В залежності в типу коду, може здійснюватись пошук чутливих даних у базі даних з подальшою їх відправкою на вузли атакуючого, зміна даних, підміна кінцевих точок запису даних (перехоплення).
2. Використання вразливостей аутентифікації. Банківські системи або сервіси можуть бути піддані спробі перехоплення та подальшого використання авторизаційних даних через неправильно спроектовану роботу із веб-сесіями. Даний спосіб може комплексно використовуватись із незахищеними точками інтернет-доступу, маршрутизаторами. Знаходячись в одній мережі із жертвою, використовуючи відкриту мережу, проблеми із захистом сесій, можна перехопити аутентифікайні дані та в подальшому їх використати для авторизації в інтернет-банкінгу або внутрішній системі банку.
3. Вразливості API та некоректне зберігання чутливих даних. Після оцінки якості архітектури проекту, тестувальник може спробувати отримати доступ до даних через відсутність шифрування при передачі даних на API та подальшого зв'язку із сховищем.
4. Використання проблем із порушенням роботи прав доступу різнорівневих користувачів. Банківська система обов'язково включає різні права доступу для внутрішніх користувачів системи. У процесі тестування можуть виконуватись спроби використання посилань, доступних лише вищому в ієрархіє користувачеві на низькорівневих ролях для перевірки закритості даних та відхиленню системою таких спроб. Також може виконуватись спроба ручної підміни ролі у запитах до системи для обходу аутентифікації користувача

5. Оцінка конфігурації безпеки системи. Етап включає перевірку конфігурації налаштувань системи, версій програмного забезпечення, що використовується на серверній стороні. Проводиться оцінка актуальності задля мінімізації можливого використання відомих експлоїтів для проникнення в систему. Несвоєчасні оновлення залишають можливість обходу через HTTP запити та інше.
6. Тестування на використання відомих програмних компонентів із відомими вразливостями. Дослідження використовуваних бібліотек, фрейморків та сторонніх програмних рішень дозволяє протестувати систему через відкриті вразливості у цих частинах. Може ефективно використовуватись при відсутності додаткових самописних захистів.

Усі викладені методи можуть застосовувати в комплексі і мають на меті знайти найвразливіші місця в системі. Не менш важливим є перевірка інтерфейсу користувача системи, де відбувається введення чутливої інформації. Існують правила захисту, зокрема, полів введення інформації, коли після набору символів, текст приховується спеціальними графічними елементами. Якщо ж дані стандарти ігноруються, це може створити ризик перехоплення даних, якщо пристрій заражений вірусним програмним забезпеченням.

Це ж стосується виведення чутливої інформації у розділах управління, наприклад, банківськими картками. Кожне поле має бути захищене від перехоплення. Ціллю тестування є перевірка усіх можливих варіантів, коли дані можна викрити, використовуючи програмне забезпечення.

Розглянемо основні відомі методології тестування на проникнення. Стандартизація процесів значно спрощує роботу із планування. За основу можна обрати необхідний алгоритм дій із пентестування, викладений в документаціях, описаних нижче.

1. Методологія OSSTMM - The Open Source Security Testing Methodology Manual. Є досить формалізованим і добре структурованим документом для тестування мереж. Документ має так звану «Карту безпеки» - візуальний показник безпеки. На карті вказуються основні галузі безпеки, які включають в себе набори елементів, які повинні бути протестовані на відповідність методиці. У документі присутній підпункт «Методологія» / «Тестування технології інтернет-безпеки» / «Огляд мережі» / «Тестування брандмауера», де перерахована очікувана інформація, яку може отримати пентестувальник в результаті вдалої атаки або відсутності потрібної функції у засоби захисту. Також описуються конкретні коректні реакції мережі на атаки і їх наявність, наприклад, вимір часу відгуку на пакет або перевірка наявності втрат пакетів на маршруті до мети. Мінусами методики вважається формализованность і відсутність додаткового опису до вимог.

2. Методологія NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment. Створена і підтримується підрозділом NIST - CSRC, центром з комп'ютерної безпеки, який об'єднує фахівців федеральних служб, університетів, найбільших IT-компаній США. У розділі «Техніки оцінки вразливостей мети», як одна з технік описуються Тести на проникнення, а саме Фази і Логістика тестів. За даним документом тести на проникнення, в доповнення до стандартних їх можливостям, можна застосовувати для визначення:

- наскільки добре система переносить реально існуючі моделі атак;
- зразкового рівня складності, який необхідно подолати атакуючому;
- додаткових заходів протидії, які могли б послабити загрози на адресу системи;
- здатності захищати систему на виявлення атак і забезпечення відповідної реакції на них.

3. Методологія BSI - Study A Penetration Testing Model. Розроблено німецьким підрозділом «Federal Office for Information Security ». У документі описується проведення коректних випробувань системи на міцність. Детально описуються тільки сама методологія тестів, але і необхідні вимоги, правові аспекти застосування методології та процедури, які необхідно виконати для успішного проведення тестів. Наводиться класифікація тестів на міцність і визначені її критерії. У додатках містяться опис ПО, яке можна використовувати для тестування об'єктів, описаних в методиці. Методика є досить докладної і намагається передбачити всі аспекти тестів на міцність, як технічні, організаційні, так і правові.

4. Методологія ISSAF - Information System Security Assessment Framework. Розроблено OISSG (Open Information Systems Security Group) для внутрішніх контрольних перевірок. Документ охоплює величезну кількість питань, пов'язаних з інформаційною безпекою. Присутні глави, що описують оцінку безпеки міжмережевих екранів, маршрутизаторів, антивірусних систем і багато іншого.

5. Методологія OWASP (Open Web Application Security Project) Testing Guide. OWASP (Open Web Application Security Project) - міжнародне відкрите співтовариство, яке орієнтоване на поліпшення безпеки програмного забезпечення. Кожен має право брати участь в OWASP, і всі їхні матеріали вільно розповсюджувані. OWASP Testing Guide має більш широку методологію в порівнянні з іншими, тому що дає вказівки не тільки по тестах на проникнення, але із аналізу веб-додатків в цілому (наприклад - вихідний код), оскільки ця методика фокусує свою увагу саме на виявленнях вразливостей веб-додатків.

6. Огляд методології PTES - Penetration Testing Execution Standard - Technical Guidelines. Стандарт, розроблений для об'єднання як бізнес вимог, так і можливостей служб безпеки, і масштабування тестів на проникнення. На першому підготовчому етапі детально розглядаються встановлюються канали комунікацій, правила взаємодії і контролю конкретні способи реагування і моніторингу інцидентів. Далі виділені наступні етапи:

- збір інформації;
- моделювання загроз;
- методи аналізу вразливостей;
- експлоїтація - забезпечення обходу контрзаходів і виявлення найкращого шляху атаки;
- пост-експлоїтація - аналіз інфраструктури, подальше проникнення в інфраструктуру, зачистка і живучість. Визначено структуру звітів, що складаються

Висновки. Усі наведені методології та сукупність стандартів перевірки на проникнення широко використовуються у сфері пентестування. Варто комплексно підходити до планування та детально вивчати кожен проект та систему в особливостях, притаманних їм. Захист фронтальної частини проекту напряму залежить від використання рекомендацій побудови інтерфейсу стандартами безпеки для забезпечення конфіденційності даних та унеможливлення перехоплення їх засобами запису екрану чи іншим програмним забезпеченням. Розробка захисних механізмів, прокладок в API, використання свіжого конфігурування системи, коректна валідація даних дозволяє зберегти рівень безпеки системи на високому рівні.

Список бібліографічного опису

1. Бортник К.Я., Делявський М.В., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л. Основні загрози безпеці інформаційних систем. // Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво» – Луцьк: Видавництво ЛНТУ. – Вип. 41. – 2020. – С. 136-141.
2. Бортник К.Я., Ломінська Г.Ю. Технології аналізу наслідків кібератак // Науковий журнал "Комп'ютерно-інтегровані технології: освіта, наука, виробництво" – Луцьк: Видавництво ЛНТУ. – Вип. 30-31. – 2018. – С. 10-13.
3. What You Need to Know About OSSTMM [Електронний ресурс] – Режим доступу до ресурсу: https://kirkpatrickprice.com/blog/what-you-need-to-know-about-osstmm/.
4. COMPUTER SECURITY RESOURCE CENTER [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/publications/.
5. Penetration Testing Methodologies [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-project-web-security-testing-guide/v41/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies.
6. OWASP Web Security Testing Guide [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-project-web-security-testing-guide/.
7. PTES Technical Guidelines [Електронний ресурс] – Режим доступу до ресурсу: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines.

References

1. Bortnik K.Y., Delyavskiy M.V., Kuzmich O.I., Bagnyuk N.V., Chernyashchuk N.L. (2020) Basic threats to security of information systems. // Scientific journal "Computer-Interactive Technologies: Education, Science, and Production" (pp. 136-141). (Vol. 41) Lutsk: LSTU Publishing House [in Ukrainian].
2. Bortnik K.Y., Lominska G.Y. (2018) Technologii analizu analizu naslidkiv kiberatakov // Scientific journal "Computer-integrated technologies: education, science, production" (pp.10-13). (Vols. 30-31). Lutsk: Publishing house LNTU [in Ukrainian].
3. What You Need to Know About OSSTMM [Electronic resource] - Mode of access to the resource: https://kirkpatrickprice.com/blog/what-you-need-to-know-about-osstmm/.

4. COMPUTER SECURITY RESOURCE CENTER [Electronic resource] - Access mode to the resource: https://csrc.nist.gov/publications/.
5. Penetration Testing Methodologies [Electronic resource] - Accessible from: https://owasp.org/www-project-web-security-testing-guide/v41/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies.
6. OWASP Web Security Testing Guide [Electronic resource] - Access mode to the resource: https://owasp.org/www-project-web-security-testing-guide/.
7. PTES Technical Guidelines [Electronic resource] - Accessible from http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines.