УДК 004.056

МЕТОДИ ТЕСТУВАННЯ СИСТЕМИ НА ПРОНИКНЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Микита Купріков, Валентина Ящук
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто можливість проникнення до інформаційно-комунікаційної мережі підприємства, проаналізовано дії реального порушника контурів захисту інформації, наведено загальний порядок оцінювання та забезпечення вдосконалення систем захисту інформації шляхом проведення тестування на проникнення. Запропоновані методи проведення тестування на проникнення можуть використовуватись при розробці та тестуванні нових систем захисту інформації, а також оцінюванні ефективності та вдосконаленні вже існуючих систем.

Ключові слова: захист інформації, несанкціонований доступ, тестування на проникнення, соціальна інженерія.

The possibility of penetration into the information and communication network of the enterprise is considered, the actions of the real violator of information protection circuits are analyzed, the general order of evaluation and improvement of information protection systems by penetration testing is given. The proposed methods of penetration testing can be used in the development and testing of new information security systems, as well as evaluating the effectiveness and improvement of existing systems.

Key words: information protection, unauthorized access, penetration testing, social engineering.

Питання захисту інформації займає провідне місце в процесі проектування, створення та використання сучасних інформаційних систем. Одним із методів перевірки захищеності інформації є тестування на проникнення. Тест на проникнення (пентест) це симуляція атаки на систему, з метою виявлення вразливостей при реальному нападі. Під час тестування визначається, як система відреагує в разі атаки і яку інформацію можна отримати в системі.

Тестування на проникнення дозволяє виявляти недоліки у сфері інформаційної безпеки (ІБ) із погляду стороннього спостерігача, не враховані при розробці політики безпеки; розкривати внутрішні і зовнішні спроби проникнення в інформаційну систему (ІС) й запобігати їм. Тестування на проникнення може виявити, наскільки безпеці ІТ-систем загрожує атака з боку хакерів, зловмисників, тощо, а також чи здатні заходи безпеки в даний час забезпечити ІТ безпеку. Воно проводиться з метою виявлення ризику безпеки, який може бути присутнім у системі. Тестування на проникнення зазвичай оцінює здатність системи захищати свої мережі, програми, кінцеві точки та користувачів від зовнішніх або внутрішніх загроз. Воно також намагається захистити засоби контролю безпеки і забезпечує лише авторизований доступ.

Тестування на проникнення є важливою функцією, яку необхідно регулярно виконувати для забезпечення функціонування системи. Тестування доцільно виконувати коли система безпеки виявляє нові загрози з боку нападників; додається нова мережева інфраструктура; проводиться оновлення системи або встановлюється нове програмне забезпечення;змінюється локація офісу; впроваджується нова програму/політика кінцевого користувача.

Тестування на проникнення зводиться до реалізації санкціонованої спроби обійти наявний комплекс засобів захисту ІС. У процесі його проведення аудитор відіграє роль зловмисника, мотивованого на порушення ІБ мережі замовника. Як правило, інтенсивній перевірці підлягають технічні засоби захисту корпоративної мережі. Проте залежно від поставлених умов об'єктом оцінювання можуть бути й інші, наприклад, соціотехнічні аспекти безпеки (рівень поінформованості користувачів тощо).

Тестування на проникнення надає можливість з'ясувати по-перше, чи всі положення політики безпеки досягають своїх цілей і використовуються згідно з попереднім задумом, а по-друге, чи існують прогалини в політиці безпеки, якими може скористатись зловмисник для досягнення своїх цілей. Таке тестування може проводитись як у складі аудиту на відповідність стандартам, так і у вигляді самостійної роботи.

Залежно від вибору мережі, з якої здійснюється проникнення в систему, тести поділяють

на дві групи: зовнішні — моделюються дії зловмисника, що здійснює проникнення в інформаційну систему клієнта з мережі Інтернет; внутрішні — моделюється поводження інсайдера (зловмисника, що якимось чином отримав доступ до внутрішньої мережі компанії й намагається через неї проникнути в інформаційну систему).

У стандарті ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки (як національний стандарт, гармонізований з європейськими та міжнародними стандартами, методом підтвердження з наданням чинності з 01 листопада 2019 року розглядається 6 методів тестування інформаційної безпеки [2]:

1. Сліпий метод (етичний хакінг, white hat). Перевіряючий досліджує об'єкт без будь яких попередніх знань про його характеристики, крім загальнодоступної інформації. Об'єкт підготовлений до дослідження при заздалегідь відомих деталях цього дослідження.

2. Подвійний сліпий метод. Перевіряючий досліджує об'єкт без будь–яких попередніх знань про його характеристики, крім загальнодоступної інформації. Об'єкт не сповіщений заздалегідь про область або напрямок дослідження. Метод тестує готовність об'єкта до невідомих видів впливу.

3. Метод сірого ящику. Тестеру надаються всі повноваження крім безпосереднього доступу до сервера. Перевірки відбуваються на предмет підвищення повноважень, виявлення помилок обробки даних, реакції на некоректні дані. Даний спосіб дозволяє оцінити коректність роботи ресурсу при введенні різних вихідних даних, але не дозволяє інсценувати атаку на ресурс.

4. Метод подвійного сірого ящику. Перевіряючий досліджує об'єкт з обмеженими знаннями про його активи і захист і повним знанням направленого допустимого дослідження. Об'єкт повідомлений заздалегідь про область і час але не про напрямок дослідження.

5. Тандемний метод. Перевіряючий і об'єкт готові до дослідження, заздалегідь знаючи всі деталі дослідження. Цей метод тестує захист і засоби управління об'єкта. Широта і глибина залежить від якості інформації, що надається перевіряючому перед тестом, а також від його знань.

6. Інверсійний метод (red team). Перевіряючий досліджує об'єкт, знаючи всі його процеси та захист, але сам об'єкт не знає нічого про те, що, як і коли перевіряючий буде тестувати. Найбільш близький до реальних дій зловмисників так званий комплексний тест на проникнення. Використовуючи різні технічні й соціоінженерні прийоми, аудитори в ході його проведення намагатимуться обійти наявні захисні механізми для виконання поставлених завдань (підвищення привілеїв, отримання доступу до конфіденційної інформації, модифікація даних із СУБД тощо).

Отже, необхідність дотримання нормативних чинників – стандартів, законів, інфраструктурних рішень, бібліотеки кращих практик ITIL (IT Infrastructure Library) дозволить підвищити рівень захищеності комп'ютерних мереж та систем. Доцільним є використання проактивного захисту, одним з методів якого є тестування на проникнення. Такий підхід є єдиним способом отримати реальну картину стану захищеності системи, і, отже, отримати контроль над мінливим IT-середовищем. Нами проаналізовано найрозповсюдженіші міжнародні методології проведення тестування на проникнення. Визначення правильної стратегії оцінювння залежить від технічних деталей, наданих про систему, наявних ресурсів, знань пентестера, бізнес-цілей організації і нормативних питань. Такий підхід є єдиним способом отримати реальну картину стану захищеності системи.

Література

1. Ric Messier. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems / Apress, 2016. – 115 p.
2. ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Інформаційні технології. Методи захисту.
3. Суліма О.А. Методи організації захисту доступу до інформаційних систем на основі використання багаторівневих моделей: автореф. дис. … канд. техн. наук: 05.13.21 [Електронний ресурс] / Суліма Олександр Андрійович. – К., 2017. – 23 с. – Режим доступу: http://er.nau.edu.ua/handle/NAU/30881.
4. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах № 26 від 2005 р." [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2594-15.