УДК 004.05+519.83

Ігнатова К.Є., студентка гр. 125м-20-2
Мєшков В.І., старший викладач
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

МЕТОДИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ СИСТЕМИ. ТЕСТ НА ПРОНИКНЕННЯ.

В даний час жодна компанія не може обійтися без використання інформаційних технологій. Для захисту даних, в яких зберігаються персональна і конфіденційна інформація, розробляються способи захисту інформації від витоків. Одним із таких методів захисту є аудит інформаційної безпеки.

Аудит інформаційної безпеки (тест на проникнення) дозволяє Компанії отримати оцінку реального рівня захищеності інформаційних активів в умовах сучасного стану методів отримання несанкціонованого доступу до інформаційних активів, оброблюваних в автоматизованих інформаційних системах організацій. Отримання такої оцінки забезпечується шляхом моделювання атак потенційних зловмисників на вибрані інформаційні активи Компанії.

Тест на проникнення дозволяє:

- виявити найбільш вразливі місця в системі інформаційної безпеки;
- зрозуміти яким способом, і через які уразливості зловмисник може проникнути в інформаційне середовище організації;
- отримати об'єктивну оцінку загального рівня безпеки інформаційного середовища організації;
- оцінити можливі наслідки від таких дій.

Основні причини, через які компанії замислюються про проведення даного виду аудиту наступні:

- оцінка існуючої системи управління інформаційної безпеки;
- оцінка захищеності окремих ресурсів або засобів захисту організації;
- аналіз можливих збитків від дій зловмисників;
- оцінка дій персоналу організації;
- об'єкти тесту на проникнення.

Основними об'єктами аудиту є зовнішні web-ресурси і локальна мережа Замовника.

При проведенні тесту крім технічних методик також використовуються методи соціальної інженерії, що дозволяють оцінити рівень підготовки співробітників в питаннях інформаційної безпеки. Може бути зроблена розсилка електронних листів, які змушують користувачів виконати певні дії, або спроба дізнатися потрібну інформацію від співробітників організації за допомогою телефонного дзвінка в IT-службу. Всі умови і дії заздалегідь обговорюються і затверджуються з Замовником.

Кожен новий інцидент в сфері інформаційної безпеки – це привід провести позачерговий тест на проникнення, однак приймати таке рішення краще після ретельного аналізу ситуації.

Мінімальний термін тесту на проникнення займає від 2-х тижнів. На першому етапі аудиту використовуються автоматизовані засоби, що дозволяють визначити відомі і існуючі уразливості, якщо такі не перебувають, то фахівці розробляють спеціалізовані рішення для тесту на проникнення, при цьому враховується специфіка атакується об'єкта і людський фактор.

Основні етапи тесту на проникнення:

- аналіз загальнодоступної інформації про компанію, і її інформаційному середовищі;
- проведення досліджень пов'язаних з соціальною інженерією;

– аналіз вразливостей внутрішніх і зовнішніх ресурсів;
– здійснення проникнення;
– створення звітної документації.

Зазвичай тестування на наявність вразливостей починається із зовнішньої мережі, а потім тестуються внутрішні послуги.

З одного боку, тести на проникнення містять багато типових процедур, які можна автоматизувати для прискорення. З іншого боку – будь-який замовник має свої особливості, які доводиться враховувати, проводячи ряд перевірок вручну.

Після проведення комплексу тестів складається докладний звіт із рекомендаціями щодо усунення проломів у безпеці. За домовленістю перевіряється відповідність різним стандартам та надається клас захищеності.

У тестах на проникнення використовуються певні програми для роботи з уразливими систем, наприклад:

– Metasploit – програма для надання інформації про уразливість, допомоги в створенні характерних ознак вірусних програм для систем виявлення вторгнень (наприклад, антивірусів), створення і тестування атак на обчислювальні системи
– Nmap – утиліта, призначена для налаштування сканування IP-мереж з будь-якою кількістю об'єктів, визначення стану об'єктів скануємої мережі (портів і відповідних їм служб). Програма доступна в різних версіях для безлічі операційних систем Пентест: програма zenmap Пентест: програма Nmap
– Nessus – інструмент для автоматизації перевірки і виявлення вразливостей і проломів в захисті інформаційних систем. Програма поширюється по General Public License, тобто, програма має відкритий вихідний код.аналіз уразливості (pentest) тестування на проникнення за допомогою Nessus
– Kali Linux - дистрибутив з певними настройками, програмами та інструментами, призначений для етичного хакинга і тестування на проникнення.

В останні роки тести на проникнення стали частиною стандартної процедури перевірки рівня інформаційної безпеки організацій. Вони повинні виконуватися в різному обсязі і мати свою специфіку.

Періодичність їх проведення і різні особливості регламентують галузеві стандарти, проте крім них є ряд ситуацій, коли доцільно виконувати позапланову перевірку. Зовнішній тест на проникнення дозволяє заощадити за рахунок оптимізації витрат на ІБ. Він виявляє реальні проблеми і допомагає побудувати ефективну стратегію щодо їх усунення.

Перелік посилань

1 Чуб В.С. «Аудит безопасности информационной системы с использованием тестов на проникновение» Молодой исследователь Дона – [Електронний ресурс] – 2018 – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/audit-bezopasnosti-informatsionnoy-sistemy-s-ispolzovaniem-testov-na-proniknovenie/viewer

2 Пентест (pentest) – внешний аудит безопасности – [Електронний ресурс] – 18.07.2019 – Режим доступу до ресурса: https://itglobal.com/ru-ru/company/blog/penetration-testing/

3 Pentest. «Тестирование на проникновение» – [Електронний ресурс] – 29.09.2019 – Режим доступу до ресурса: https://cybershield.su/2019/09/29/pentest/

4 Тестирование на проникновение (аудит информационной безопасности) – [Електронний ресурс] – Режим доступу до ресурса: https://www.dialognauka.ru/services/penetration_testing/

5 Что такое пентест (pentest)? – [Електронний ресурс] – Режим доступу до ресурса: https://rtmtech.ru/articles/chto-takoe-pentest/