МЕТОДИ ТЕСТУВАННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Стрілець А.М. Чернікова В.Г Скирда С.О.
Науковий керівник – док.т.н. Шостко І.С.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-55-92)

This work is devoted to actual of choosing a method of testing information security tools. Because, at any stage in the life cycle of an automated system, be it design, configuration or operation, the administrator must know whether the system actually meets the required security level. The paper describes two methods of testing information security tools. And also we are talking about automated means of exploitation and their algorithm of work. The main tools of automatic information audit were also considered.

Останнім часом зростає значимість інформаційної безпеки, так як з'являється безліч незаконних способів отримання доступу до інформації. Тому, на будь-якому етапі життєвого циклу автоматизованої системи, будь то проектування, конфігурація або експлуатація, адміністратор повинен знати, чи дійсно система задовольняє необхідному рівню захищеності.

Існує кілька підходів до тестування безпеки системи. По-перше, можна провести ряд тестів на проникнення (пентестов), тобто, використовуючи всілякі утиліти, бази даних вразливостей і експлойтів спробувати отримати доступ до цільової системі, серверу, комп'ютера, обійти тестуючу програму. Перевага пентестов в тому, що їх проводять люди, відповідно, вони можуть в реальному часі приймати ті чи інші рішення, змінювати стратегії, засоби атак та інше. Однак, в цьому ж і недолік даного підходу - все залежить від компетентності тих, хто ці пентести проводить. Не можна після проведення ряду атак стверджувати, що система володіє потрібним рівнем захисту. Адже можливо, що просто були вибрані не ті засоби або використовувалися застарілі вразливості.

Другий метод полягає у відтворенні попередньо записаного трафіку комп'ютерних атак. Налаштовується спеціальний стенд, до якого підключається тестуюча система. Перевагою цього підходу є можливість забезпечення багаторазової повторюваності умов експерименту за умови, що трафік комп'ютерних атак кожен раз буде відтворюватися ідентичним чином. Відсутність у складі стенду реальних атакованих систем усуває проблему відновлення стану окремих його елементів після проведення атак. Але розглянутий спосіб тестування не дозволяє варіювати параметри атак (наприклад, кодування HTTP-запитів і використовуваний експлойтом shell-код) в процесі тестування, оскільки це вимагає серйозної модифікації вже сформованих пакетів мережевого трафіку.

Оскільки проводити тестування цільової системи вручну дуже складно, останнім часом стали з'являтися автоматизовані засоби експлойтинга. Такі програми дозволяють в автоматичному режимі виявити уразливості цільового хоста, а потім провести ряд атак для експлуатації цих вразливостей. Загальний алгоритм роботи таких засобів складається з наступних кроків:

1. Сканування портів і ідентифікація сервісів на досліджуваних об'єктах.

2. На основі бази знань висувається припущення про наявність вразливостей в виявлених сервісах.

3. Перевірка можливості експлуатації передбачуваних вразливостей.

Розглянемо найпопулярніші засоби автоматичного аудиту безпеки:

• Core Impact - це програмний продукт для проведення тестування несанкціонованих проникнень в систему. Перевіряє досліджувані системи на наявність вразливостей. За допомогою нього можна протестувати безпеку веб-додатків, мережевих систем, кінцевих пристроїв, мобільних пристроїв, бездротових мереж і т.д. Дозволяє моделювати багатоступінчасті атаки і взаємодіяти з успішно атакованою системою. Має свою БД експлойтів, яка щомісяця поповнюється власною командою розробників. З недоліків можна відзначити досить високу ціну;

• CANVAS / D2 / Nessus Bundle. Збірка CANVAS з D2 Exploit Pack інтегровані сканером виявлення вразливостей Nessus дозволяють досягти аналогічного підходу, закладеного в продукті CORE IMPACT. На відміну від свого конкурента, під платформу CANVAS, крім власних експлойтів, можливий імпорт сторонніх експлойтів. Це дозволяє CANVAS-у охопити набагато більше вразливостей для проведення атак в порівнянні з іншими рішеннями даного сегмента;

• SAINT Vulnerability Scanner && SAINTexploit. Аналог інтегрованого CANVAS і Nessus з тією лише відмінністю, що у SAINT Vulnerability Scanner і SAINTexploit один виробник. Функціональність же практично повністю ідентична.

За результатом аналізу можна констатувати, що на даний момент не існує комплексної методології проведення тестування на проникнення. Кожен з розглянутих методів фокусується на певних питаннях, і як наслідок, при проведення комплексного тестування на проникнення неможливо повністю опиратись лише на одну методологію. Також є очевидно, що використання автоматизованих засобів тестування значно збільшує ймовірність успішного виконання тесту на проникнення.

Перелік посилань:

1. Автоматизований експлойтінг [Електронний ресурс].– Режим доступу до ресурсу: https://www.securitylab.ru/blog/personal/evteev/13705.php. (дата звернення:10.02.2020).