УДК 681.322.067

Головецька О. - ст. гр. СІсзп-52
Тернопільський національний технічний університет імені Івана Пулюя

АУДИТ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ СИСТЕМ ЗАСОБАМИ METASPLOIT FRAMEWORK

Науковий керівник: к.т.н., доцент, Луцків А.М.

Аудит безпеки передбачає контроль безпеки системи, під яким розуміють збір, накопичення інформації про події, що відбуваються в інформаційній системі та аналіз записів журналів безпеки з метою перевірки ефективності управління системою, забезпечення гарантій відповідності функціонування системи політиці безпеки та вироблення рекомендацій про необхідні зміни в управлінні, політиці та процесах безпеки. Особливістю аудиту є його сильна залежність від інших послуг та механізмів безпеки. Особливої актуальності набувають системи аналізу захищеності комп'ютерних систем, які призначені для виявлення вразливостей в програмно-апаратному забезпеченні. Прикладами таких вразливостей можуть бути неправильна конфігурація мережевих служб, наявність програмного забезпечення без встановлених модулів оновлення (service packs, patches, hotfixes), наявність “таємних дверей” тощо.

Metasploit Framework[1] — засіб для проведення аудиту інформаційної безпеки, який створено для надання інформації про вразливість та дає змогу створювати сигнатури для IDS та прогнозувати діяльність зловмисників, зокрема шляхом використання експлойтів.

Експлойт — це комп'ютерна програма, фрагмент програмного коду або послідовність команд , що використовують вразливості в програмному забезпеченні та призначені для проведення атаки на обчислювальну систему. На сьогодні наявні експлойти, які ставлять під загрозу необізнаних і непідготовлених адміністраторів та професіоналів безпеки. Для адміністратора безпеки типової ІТ-компанії експлойти суттєво ускладнюють процедуру захисту системи.

Автором доповіді здійснюється дослідження можливості використання Metasploit Framework для аудиту безпеки програмного забезпечення сучасних комп'ютерних систем. Проводився аналіз уразливостей операційних систем Microsoft Windows 2003/XP та Ubuntu Linux 10 LTS. Дане програмне забезпечення використовується в ТОВ “Бучач-Агроавто”. На основі дослідження сформульовано рекомендації по підвищенню захищеності мережевого програмного забезпечення, та здійснено відповідні зміни в інформаційній інфраструктурі організації з метою усунення виявлених недоліків.

Література:

- Metasploit penetration testing software [Електронний ресурс]. - Режим доступу: URL: http://www.metasploit.com/