ЛАБОРАТОРНА РОБОТА №14
Дослідження ефективних методів захисту від експлойтів.

Мета: визначити ефективні способи захисту програмного середовища від експлойтів.
Обладнання: ноутбуки (або персональні комп'ютери), операційна система Windows (Linux) для цільового комп'ютера, Kali Linux – для атакуючого комп'ютера, пакет MetaSploit з набором експлойтів.

ТЕОРЕТИЧНА ЧАСТИНА

Експлойт - це фрагмент програмного коду або послідовність команд, що використовують вразливості програмного забезпечення та призначені для проведення атаки на обчислювальну систему. Метою атаки може бути як захоплення контролю над системою (підвищення привілеїв), так і порушення її функціонування.

У залежності від методу отримання доступу до уразливого програмного забезпечення, експлойти поділяються на віддалені та локальні.

- *Віддалений експлойт* працює через мережу і використовує уразливість в захисті без будь-якого попереднього доступу до уразливої системи;
- *Локальний експлойт* запускається безпосередньо у вразливій системі, вимагаючи попереднього доступу до неї.

Зазвичай використовується для отримання зломщиком прав суперкористувача.

Атака експлойта може бути націлена на різні компоненти обчислювальної системи — серверні програми, клієнтські програми або модулі операційної системи. Для використання серверної уразливості експлойт достатньо сформувати та надіслати серверу запит, що містить зловмисний код. Використовувати вразливість клієнта трохи складніше — потрібно переконати користувача в необхідності підключення до підробленого сервера (переходу за посиланням у випадку якщо уразливий клієнт – браузер).

Експлойти фактично призначені для виконання сторонніх дій на уразливій системі й можуть бути розділені між собою таким чином:

- для операційних систем;
- для прикладного ПЗ (музичні програвачі, офісні пакети і т. д.);
- для браузерів;
- для інтернет-продуктів;
- для інтернет-сайтів;
- інші.

ПРАКТИЧНА ЧАСТИНА

1. Запустіть пакет Metasploit з Kali Linux та вивчіть його можливості.
2. В залежності від цільової операційної системи та прикладного ПЗ відберіть потрібні для атаки експлойти, протестувавши попередньо її та знайшовши потрібні вразливості.
3. За допомогою обраних експлойтів захопіть керування цільовою системою та виконайте адміністративні дії на ній.
4. Знайдіть та використайте вразливості в операційній системі та браузері (а якщо знайдуться вразливості у прикладному ПЗ – використайте їх також).
5. Закрийте використані вразливості (якщо це можливо, звичайно) на цільовій системі та повторіть атаки.
6. Підготуйте звіт з лабораторної роботи, який має містити:
    a. Аналіз вразливостей атакованої системи;
    b. Обгрунтування вибору тих чи інших вразливостей для атаки;
    c. Протокол Ваших дій;

d. Протокол адміністративних дій на атакованому комп’ютері після отримання доступу;
e. Протокол дій із закриття знайдених вразливостей на цільовому комп’ютері.
f. Протокол повторних атак та причини їх неефективності. Акцент необхідно зробити на ефективних методах захисту проти такого типу атак.

7. Замість звіту можна зняти відеоролик з фіксацією Ваших дій на обох комп’ютерах з супроводжувальним текстом (аудіо-супроводом або «біжучим рядком»), в якому необхідно наголосити на методах захисту від таких атак. Кращі відеоролики будуть розміщені на каналі кафедри на You Tube.

КОНТРОЛЬНІ ПИТАННЯ

1. Що таке експлойт, для чого вони застосовуються?
2. Які існують типи експлойтів, чим вони відрізняються?
3. Які вразливості Ви знайшли у цільовій системі та чим вони викликані?
4. Чому Ви використали саме ці вразливості?
5. Які способи захисту від експлойт-атак Ви використали?
6. Яку небезпеку несуть такі атаки та які методи захисту Ви вважаєте найефективнішими?