УДК 004.056, 004.491
Лізунов С.І.[1], Корольков Р.Ю.[2], Алексєєв Д.К.[3]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] канд. техн. наук ,старш. викл. НУ «Запорізька політехніка»
[3] студ. гр. РТ-819 НУ «Запорізька політехніка»

АНАЛІЗ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ СИСТЕМ ЗАСОБАМИ METASPLOIT FRAMEWORK

Останнім часом все більше конфіденційної інформації зберігається в електронному вигляді в комп'ютерних системах, які найчастіше підключені до комп'ютерних мереж. Це ставить нові завдання щодо забезпечення максимальної безпеки таких систем з метою недопущення розкриття конфіденційної інформації. Для визначення рівня безпеки комп'ютерної системи проводять аналіз захищеності. Ефективним способом аналізу є тестування на проникнення (пентест). Тестування на проникнення здатне виявляти загальновідомі проблеми безпеки, які були виявлені та опубліковані раніше [1].

Існує багато методів тестування [2] на проникнення, кожен з яких підходить для різних видів тестів, а також часто підказує як структурувати тест на проникнення. Більш того, вони часто пропонують розділити тест на фази, де вихідні дані кожної фази є вхідними даними для наступної. Наслідком такого підходу є те, що для різних етапів пентесту підходять різні види інструментів.

Першим кроком кожного пентесту є пошук комп'ютерної системи у мережі, цікавої, з погляду тестувальника, на подальших етапах тесту на проникнення. Це можна зробити за допомогою мережного сканера, такого як Nmap. Найбільш цінна інформація, яку надає Nmap тестувальнику – це, як правило, версія та тип операційної системи, стан мережних портів, типи та версії служб, що працюють у конкретній системі. Наступними кроками є пошук і використання вразливостей (або самої операційної системи, або будь-якого встановленого програмного забезпечення). Пошук на наявність вразливостей можна виконати за допомогою таких інструментів як Nessus або OpenVAS, а спробувати використати знайдені вразливості за допомогою експлойту. В результаті успішної експлуатації вразливості тестувальник часто отримує дозвіл на виконання довільних команд цільової системи.

Такі завдання, як експлуатація вразливостей або дослідження цільової системи після експлуатації, можуть бути певною мірою автоматизовані. Для цих цілей доступний інструментарій Metasploit Project [3], а саме Metasploit Framework, який складається з різних компонентів, таких як важливі бібліотеки, модулі, плагіни та інструменти, рис.1.

Перевага використання Metasploit Framework полягає в ефективному керуванні експлойтами (пошук, оновлення, документація) та безлічі корисних навантажень (завдань, які виконуються після успішної експлуатації цільової системи).

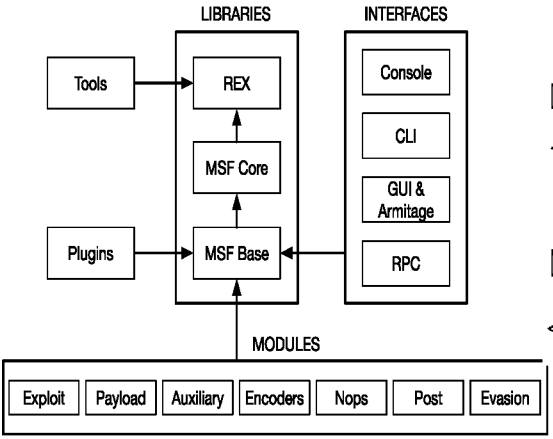

Рисунок 1 – Архітектура Metasploit

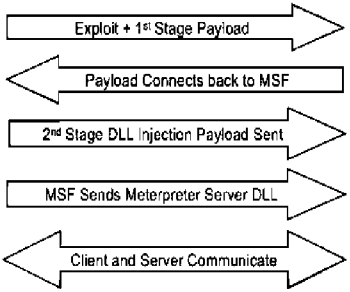

Рисунок 2 – Встановлення з'єднання Metasploit

Корисні навантаження можуть або виконувати одну конкретну задачу (наприклад, створення користувача), або можуть бути складнішими і пропонувати більш просунуту функціональність (наприклад Meterpreter). На рис.2 показано послідовність кроків, необхідних для встановлення двостороннього каналу зв'язку, щоб мати можливість дистанційно керувати цільовою системою. За допомогою Metasploit Framework можна маніпулювати файлами, процесами та службами на цільовій машині; обійти антивірусне програмне забезпечення і встановити бекдор; маніпулювати таблицями маршрутизації хостів (що може призвести до атаки людини посередині); можна видалити журнали подій (що ускладнює діагностику та розслідування порушення безпеки) та багато іншого.

В роботі розглянуто можливості використання Metasploit Framework для аналізу безпеки програмного забезпечення сучасних комп'ютерних систем та відзначається, що серед безлічі наборів інструментів та утиліт для тестування на проникнення, Metasploit Framework пропонує набагато більше можливостей для маніпулювання цільовою системою та автоматизації громіздких завдань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The Mitre Corporation. CVE® Program Mission Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities [online]. Режим доступу:https://www.cve.org [Дата звернення 23 березня 2023].

2. Kalchenko V. Огляд методів проведення тестування на проникнення для оцінки захищеності комп'ютерних систем / V. Kalchenko // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2018. – Т. 4 (50). – С. 109-114. – doi:https://doi.org/10.26906/SUNZ.2018.4.109.

3. Rapid7. Metasploit [online]. Режим доступу:https://www.metasploit.com [Дата звернення 24 березня 2023].