Лабораторная работа №4

ДОПОЛНИТЕЛЬНЫЕ МЕТОДЫ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ НА ОБЪЕКТЕ ЗАЩИТЫ ИНФОРМАЦИИ

1. Цель и задачи работы

Ознакомится с дополнительными средствами эксплуатации уязвимостей, используемых для упрощения автоматизации контроля степени защищённости объекта защиты информации.

2. Теоретические положения

Использование методов активного сбора информации являются одним из основных этапов проведения аудита и проверки уровня защищённости автоматизированных систем. Однако использование средств, рассмотренных в лабораторных работах, выполняемых ранее, может потребовать значительное количество ресурсов, особенно в случае, если требуется проводить анализ защищённости большого числа объектов.

Для упрощения работы с ПО Metasploit Framework, или просто Metasploit, были созданы различные графические интерфейсы, позволяющие упростить доступ к его различным возможностям.

В качестве графического интерфейса Metasploit, рассмотрим ПО Armitage, входящий в базовых дистрибутив ОС Kali Linux.

Для нормальной работы Armitage, необходимо использование базы данных Postgre SQL, причём крайне желательно, чтобы версия Armitage соответствовала версии Metasploit. В противном случае для использования ПО Armitage необходимо будет задать путь к БД, при помощи команды db connect, который в свою очередь может быть получен с помощью команды db locate.

Так как ПО Armitage вызывает команды Metasploit, то для его нормальной работы, необходимо запустить данное ПО с правами администратора.

ПО Armitage обладает следующими возможностями.

1. Представление всех модулей Metasploit, сгруппированных по категориями в виде графического интерфейса.
2. Предоставление списка всех целей, ранее сканированных при помощи ПО Metasploit, работающем в режиме записи операций в БД.
3. Возможность одновременного запуска сразу нескольких команд Metasploit в различных окнах консолях.
4. Возможность задания различных портов полезных нагрузок.
5. Возможность сканирования и анализа защищённости сразу нескольких систем.
6. Возможность использования модулей автоматического поднятия привилегий.
7. Возможность настройки эксплойтов Metasploit при помощи графического интерфейса.

8. Возможность автоматической отправки полученных хешей паролей в программу JhonTheRipper и автоматическая запись полученных результатов в БД.
9. Запись всех действий в БД с возможностью их последующего повторения и автоматизации выполнения действий.

1.

3. Оборудование

Персональный компьютер с количеством процессорных ядер не менее 2, работающих на частоте не менее 2 GHz, работающий под управлением операционной системы Kali Linux, Ubuntu Linux с пакетом дополнений Forensic Tools и NMap, Windows 7, или более новая, а так же наличие возможности одновременного развёртывания не менее 2 виртуальных машин формате Virtual BOX, содержащих ОС Kali Linux и ОС Windows 7, 8, или 10. Видеокарта с поддержкой технологий CUDA или Open CL. Не менее 6GB оперативной памяти. Не менее 40GB свободного места на HDD.

4. Задание на работу

4.1 Скачайте виртуальную машину Linux и операционную систему Windows
Kali Linux
Windows 8.1
Windows 7

4.2 Настройте сеть и запустите обе ОС.

4.3 В системе Windows отключите защитника и фаервол, а также включите сетевое обнаружение.

4.4 В системе Linux запустить сервер базы данных командой `sudo service postgresql start`.

4.5 В системе Linux запустить Armitage командой `sudo Armitage`.

4.6 В системе Linux подключите базу данных Metasploit. Если она была использована в предыдущей работе, то БД инициализируется автоматически, если нет, но настройте подключение к ней и повторите процедуру.

4.7 Используя msfvenom скомпилируйте файл с полезной нагрузкой meterpreter с расширением .exe , указав lhost (IP адрес машины Linux). Рекомендуется использовать модуль Metasploit под названием reverce tcp, запущенных при помощи Armitage.

4.8 С помощью python3 -m http.server разместите вредоносный файл на web-интерфейсе Kali Linux (запускается из каталога с файлом).

4.9 Скачайте файл и запустите его с правами администратора на Windows.

4.10 Скопируйте хеши паролей пользователей ОС Windows.

4.11 Отправить полученных хеши паролей на расшифровку в ПО JhonTheRipper и получить пароль администратора.

4.12 Получите скриншот подтверждения расшифровки пароля администратора и скриншот логов.
4.13 Удалить логи из журнала событий Windows, Windows Event Log и показать это на советующем скриншоте.
4.14 Предоставить скриншот каждого этапа выполнения задания.
4.15 Сделать выводы о проделанной работе.

6. Оформление отчета

Отчет оформляется в тетради или листах формата А4 и должен содержать:
- название курса, название и номер лабораторной работы;
- цель работы и задание на исследование;
- скриншоты окон приложения командной строки, содержащие скриншоты окон выполнения команд Metasploit (msfconsole), полученных из ПО Armitage;
- скриншот окна окна получения файла на атакуемой системе;
- скриншот окна успешного получения хешей паролей пользователя на атакуемой системе;
- скриншот успешной расшифровки пароля администратора, полученный в результате использования ПО Armitage.
- скриншот наличия логов на атакуемой системе;
- скриншот подтверждающий очистку логов на атакуемой системе.
- Скриншот окна ПО Armitage, полученный в момент подключения атакуемой системы к компьютеру, на котором установлено ПО Armitage.

7. Контрольные вопросы

7.1 Каково назначение приложения средства эксплуатации уязвимостей Armitage?
7.2 Под управлением каких операционных систем может работать ПО Armitage. Какие ограничения в работе данного средства, присутсвуют на ОС Windows?
7.3Какие основные проблемы возникают при взаимодействии ПО Armitage и ПО Metasploit и типовые способы их решения.
7.4Ким образом возможно производить настройку БД для работы с Armitage и каким образом можно контролировать наличие соединения с БД в процессе работы с приложением?
7.5Какие модули Metasploit, необходимые для выполнения лабораторной работы, наиболее часто используются в ПО Armitage?
7.6Почему в качестве цели был собран тестовый стенд, а не использовались атаки на публично размещённые машины?
7.7Какая юридическая ответственность наступит, или может наступить в случае использования средства эксплуатации уязвимостей Armitage , для тестирования уровня защищённости локальной сети ТулГУ? !!!Внимание!!! Использовать Armitage вне собранного в рамках выполнения работы тестового стенда, категорически запрещается!