Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Комсомольск-на-Амуре государственный университет»

Факультет компьютерных технологий
Кафедра «Информационная безопасность автоматизированных систем»

ЛАБОРАТОРНАЯ РАБОТА

по дисциплине «Безопасность операционных систем»

Metasploit Framework в kali linux

Студент группы 0ИБ-1 Д.В. Шутрин

Преподаватель И.А. Трещев

2022

Ход работы

MS15-100 – Уязвимость делает возможным удаленное выполнение кода при открытии специально созданного файла связи (.mcl) Media Center, вредоносный код ссылается на Windows Media Center. Злоумышленник, успешно воспользовавшийся данной уязвимостью, может получить те же права, как текущего пользователя. Пользователи, учетные записи которых настроены с меньшими правами, могут подвергаться менее, чем работающие с правами администратора.

Для демонстрации данной уязвимости воспользуемся «Metasploit Framework».

После запуска программы вводим команду «search ms15» и в выпавшем списке ищем уязвимость ms15-100 (рисунок 3).

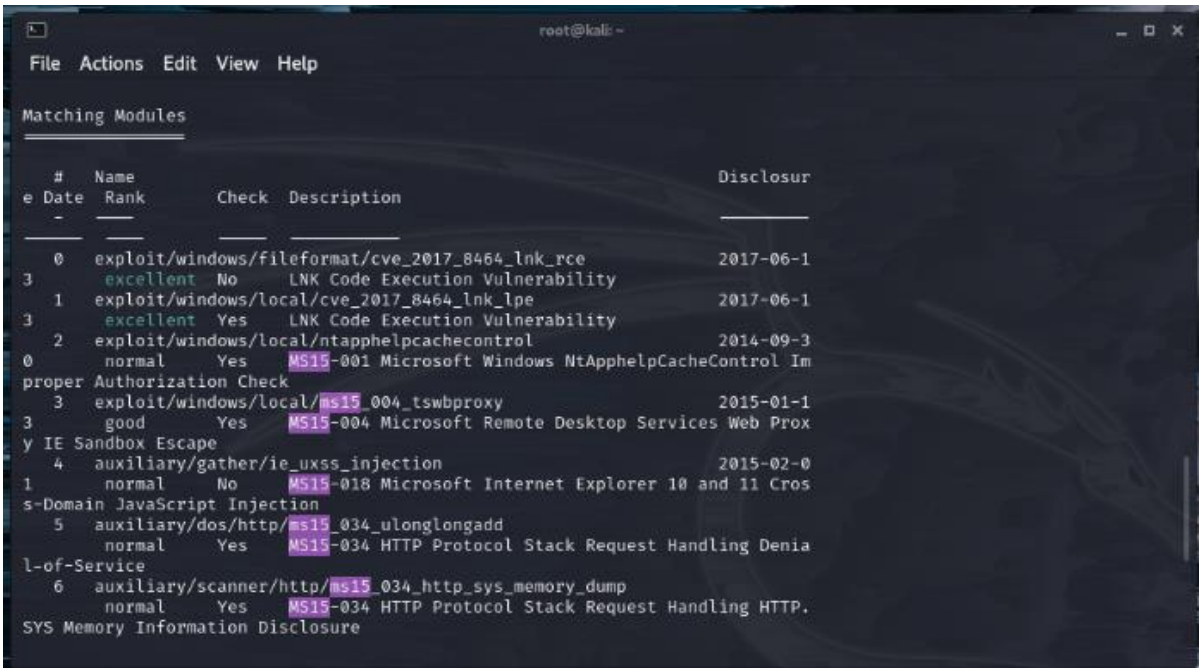

Рисунок 3 – Поиск уязвимости «MS15-100»

Затем командой «use» переходим в настройку эксплоита. Выставляем необходимые опции (рисунок 4).

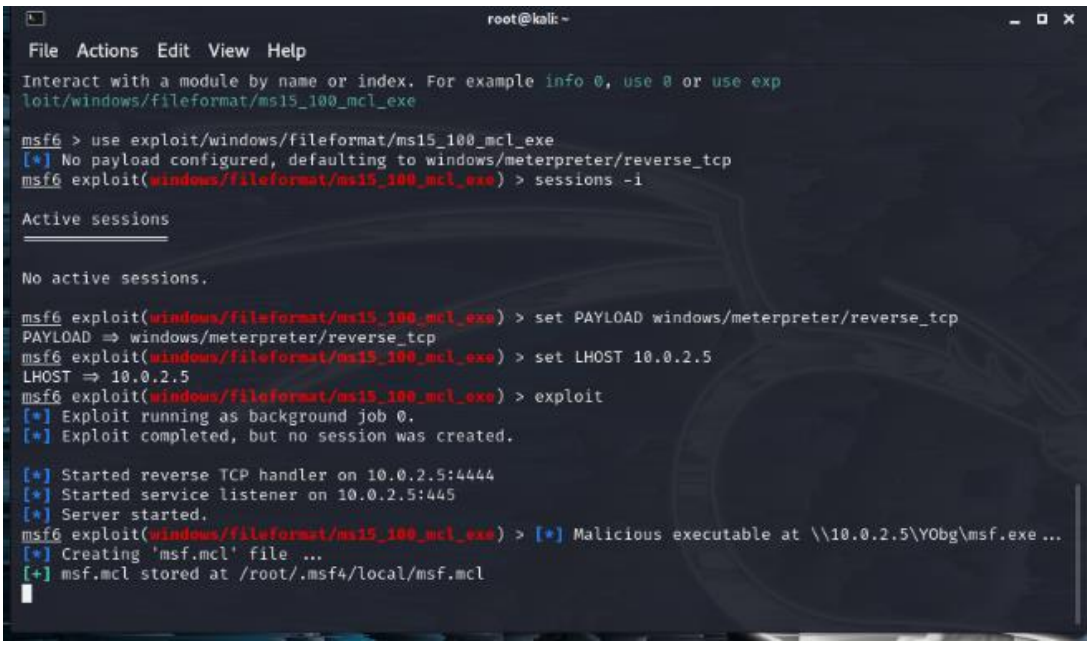

Рисунок 4 – Настройка эксплоита

После этого создастся файл. После этого закидываем полученный файл в Windows 7 (рисунок 5).

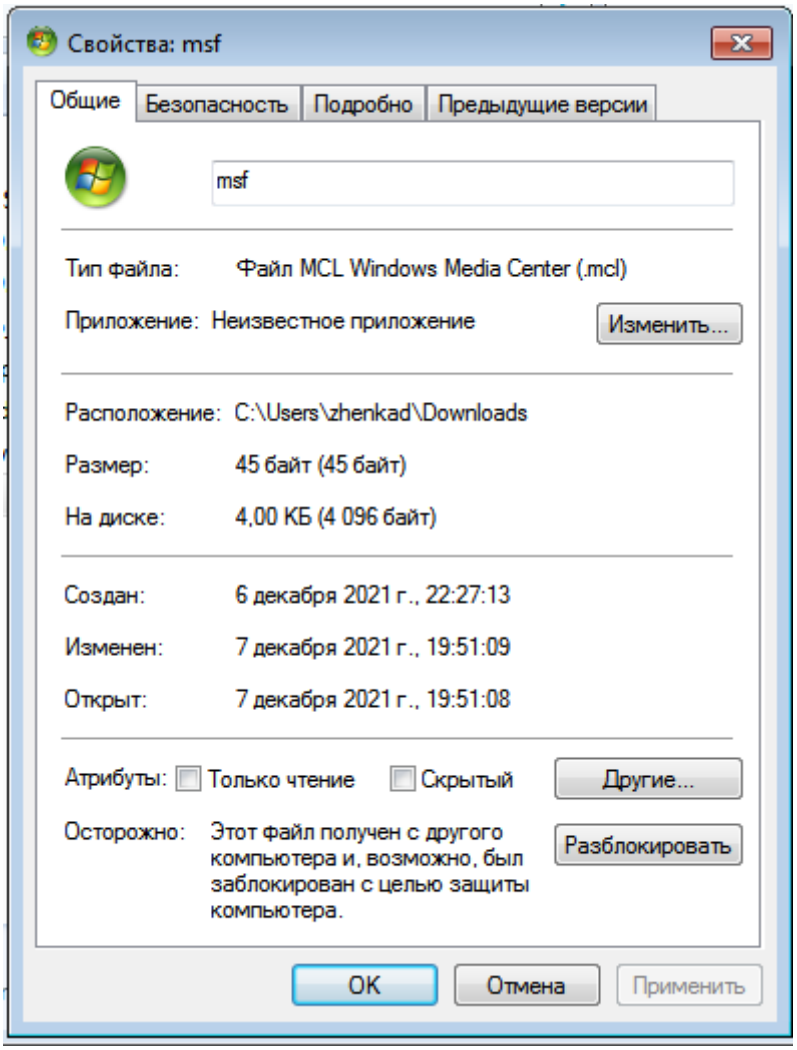

Рисунок 5 – Файл на Windows 7

Откроем его, после этого начнется сессия (рисунок 6).

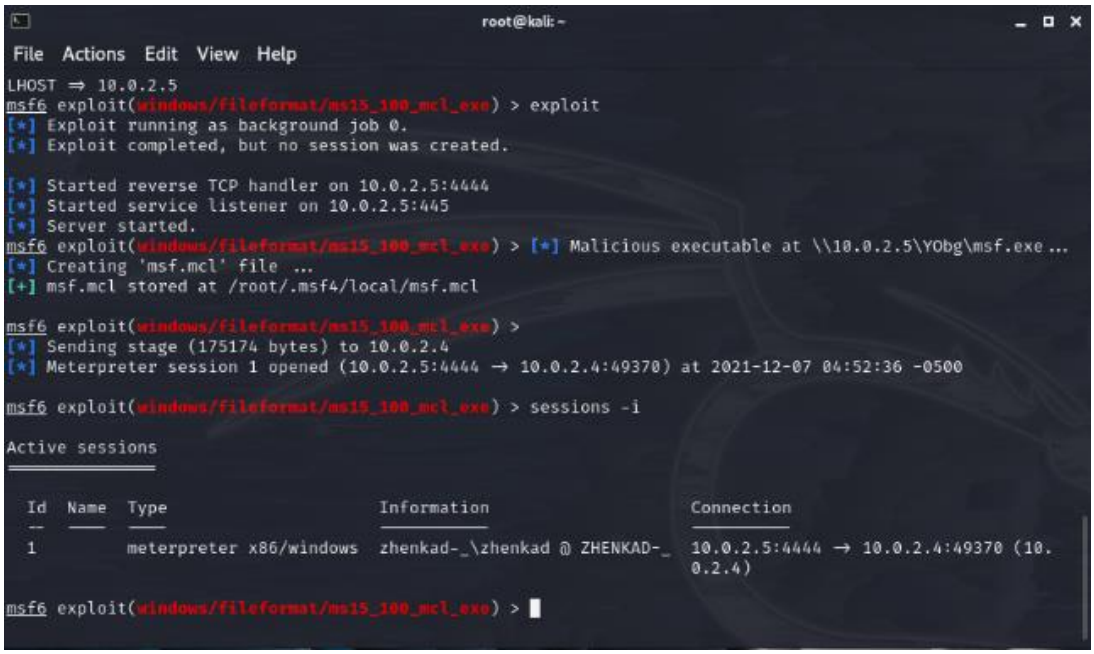

Рисунок 6 – Создание сессии

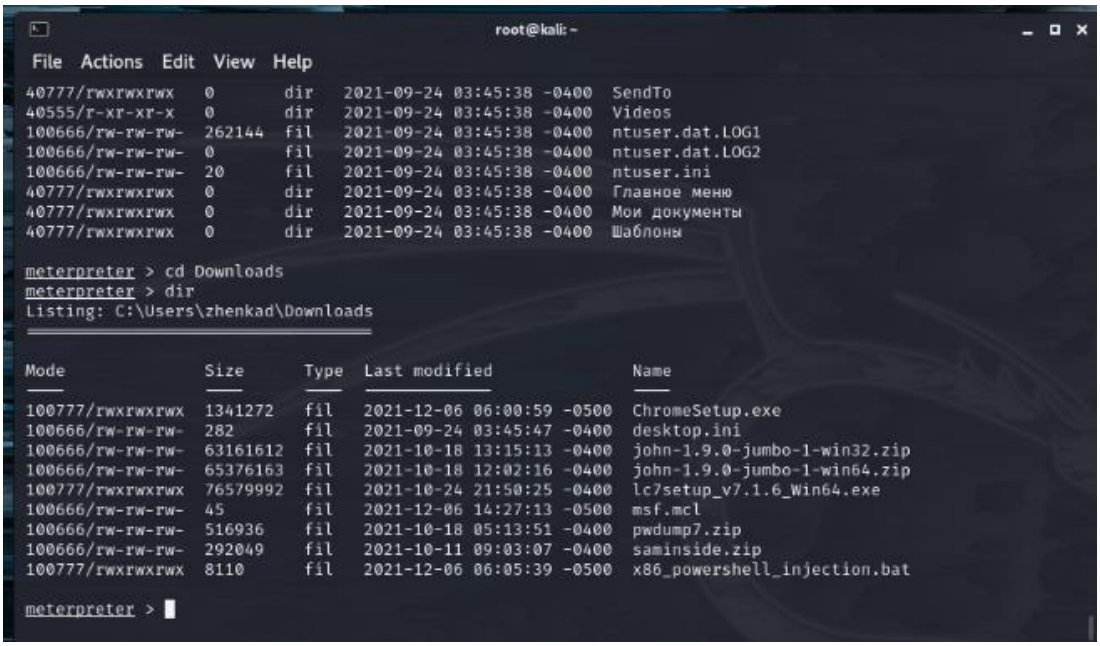

Рисунок 7 – Файл в папке с загрузками

Для того, чтобы убедится, что эксплоит сработал перейдем в папку с загрузками, в которой находится в наш файл (рисунок 7).

Список использованных источников

1 РД ФГБОУ ВО «КнАГУ» 013-2016. Текстовые студенческие работы. Правила оформления. – Введ. 2016-03-10. – Комсомольск-на-Амуре : ФГБОУ ВО «КнАГУ», 2016. – 55 с.

2 MasterHost [Электронный ресурс] // masterhost.ru: информационная интернет-статья. 2005. URL: https://masterhost.ru/support/mail/hosting/#program_settings (дата обращения: 10.12.2022).

3 Ship [Электронный ресурс] // snipp.ru: информационная интернет-статья. 2012. 11 мая. URL: https://snipp.ru/handbk/hosting-mail-servers#link-masterhost (дата обращения: 10.12.2022).