**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

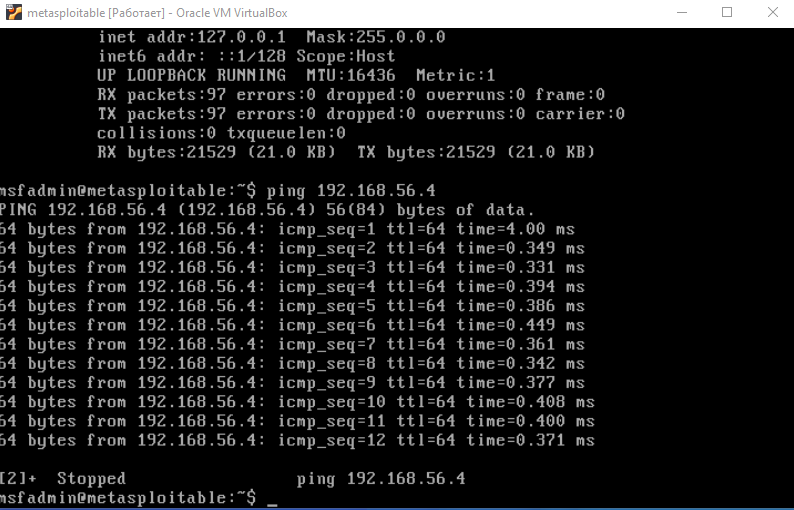
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент | | |  | | | курса | | | |
| очно-заочной формы обучения | | | | | | | |
| Группа №: | ИЭ-41-20 | | | | | | | |
| ФИО: | Ахтямов В.И. | | | | | | | |
| Проверил |  | | | | | | | |
| ФИО: | Дратвяк А.В. | | | | | | | |
| дата проверки: | « |  | | » |  | | 2023г. | |
| Оценка: |  | | | | | | | |

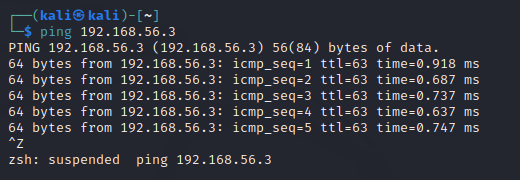
Москва, 2023г.

**Результаты выполнения лабораторной работы**

1. Результаты настройки сети для виртуальных машин

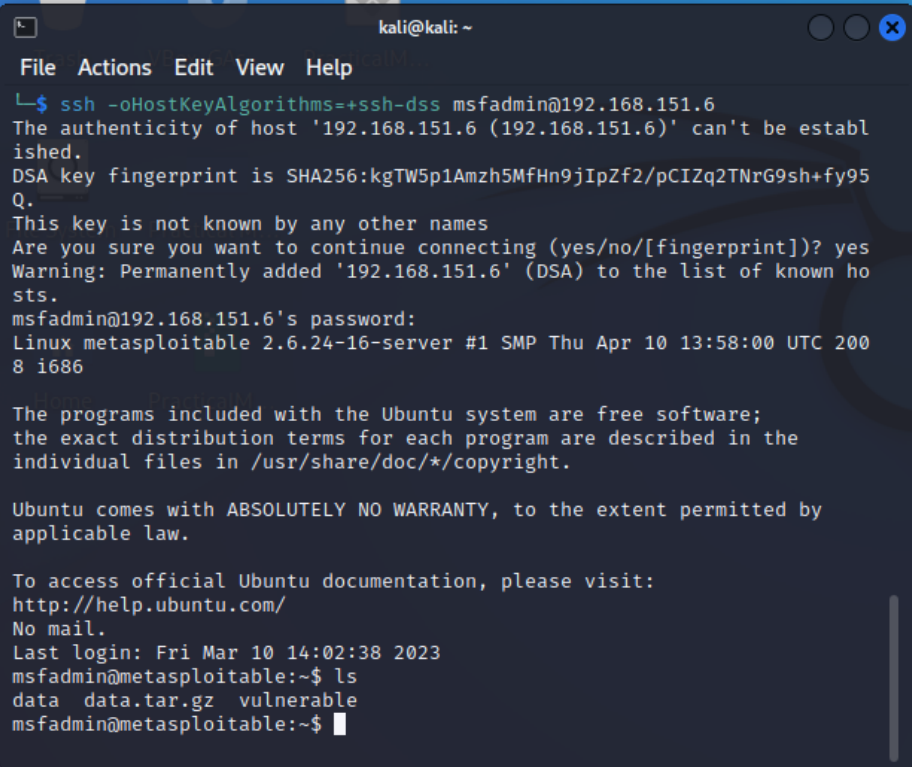
|  |
| --- |
| Скриншот № 1 |





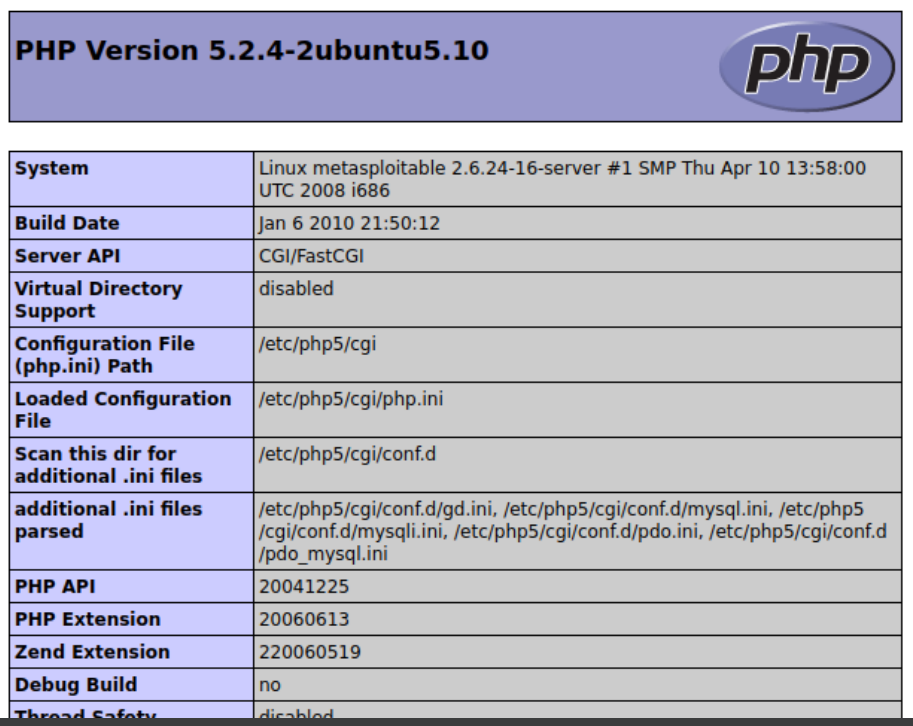
2. Результаты удалённого подключения к виртуальной машине

|  |
| --- |
| Скриншот № 2 |



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

4. Данные, полученные из phpinfo Metasploitable

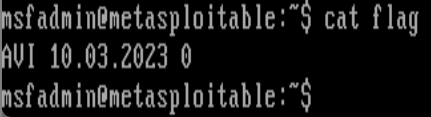


Похоже на конфигурационный файл php сервера

Много настроек сервера – максимальное время выполнения, установлены ли защитные моды, то что он поддерживает

5. Результаты создания flag

|  |
| --- |
| Скриншот № 3 |



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

Устанавливается служба удаленного выполнения команд, distcc предназначен для выполнения компиляции программ по сети, но без нужной защиты позволяет выполнять произвольные команды на удаленной машине

7. Дайте определение «демону» в ОС Linux

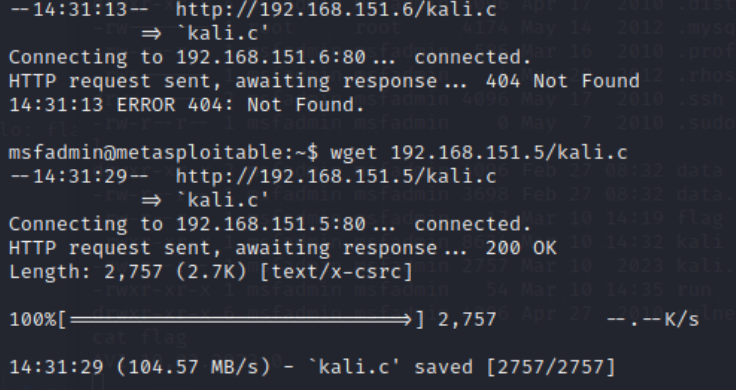
Демон в ОС линукс – это что-то наподобие службы или команда которая запускается самой системой и работает в фоновом режиме.

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

|  |  |
| --- | --- |
| *cat /etc/shells* | Узнаем какие оболочки используются на машине, чтобы в дальнейшем знать какие команды можем на них выполнять |
| *which gcc*  ls -l /usr/bin/ | grep -E -i -w 'gcc|clang' | Смотрим версии компиляторов |
| *which wget* | Команда wget будет использоваться для скачивания эксплойта на машину |

9. Загрузка эксплойта на уязвимую машину

|  |
| --- |
| Скриншот № 4 |

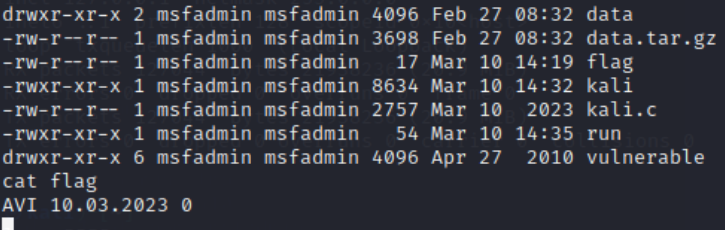


10. Поясните цель использования reverse shell в пункте 37 Л/р

Чтобы получить доступ к командной оболочке уязвимой машины, выполнение команд на ней.

11. Результаты получения секрета из флага

|  |
| --- |
| Скриншот № 5 |



12. Индивидуальные выводы по лабораторной работе.

Вывод

Цель – используя известную нам уязвимость в udev, загрузить эксплойт, полученный с помощью Metasploit, на уязвимую машину, а затем установить reverse shell соединение между машинами, чтобы иметь возможность выполнения команд на уязвимой системе

Результат – было достигнуто выполнение удаленных команд с повышенными привилегиями

Знания – поподробнее разобрался в понятии reverse shell

Умения – использование metasploit

Практические навыки использования уязвимости и установления reverse shell, для доступа к машине