

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ №4**

# **В РАМКАХ ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»**

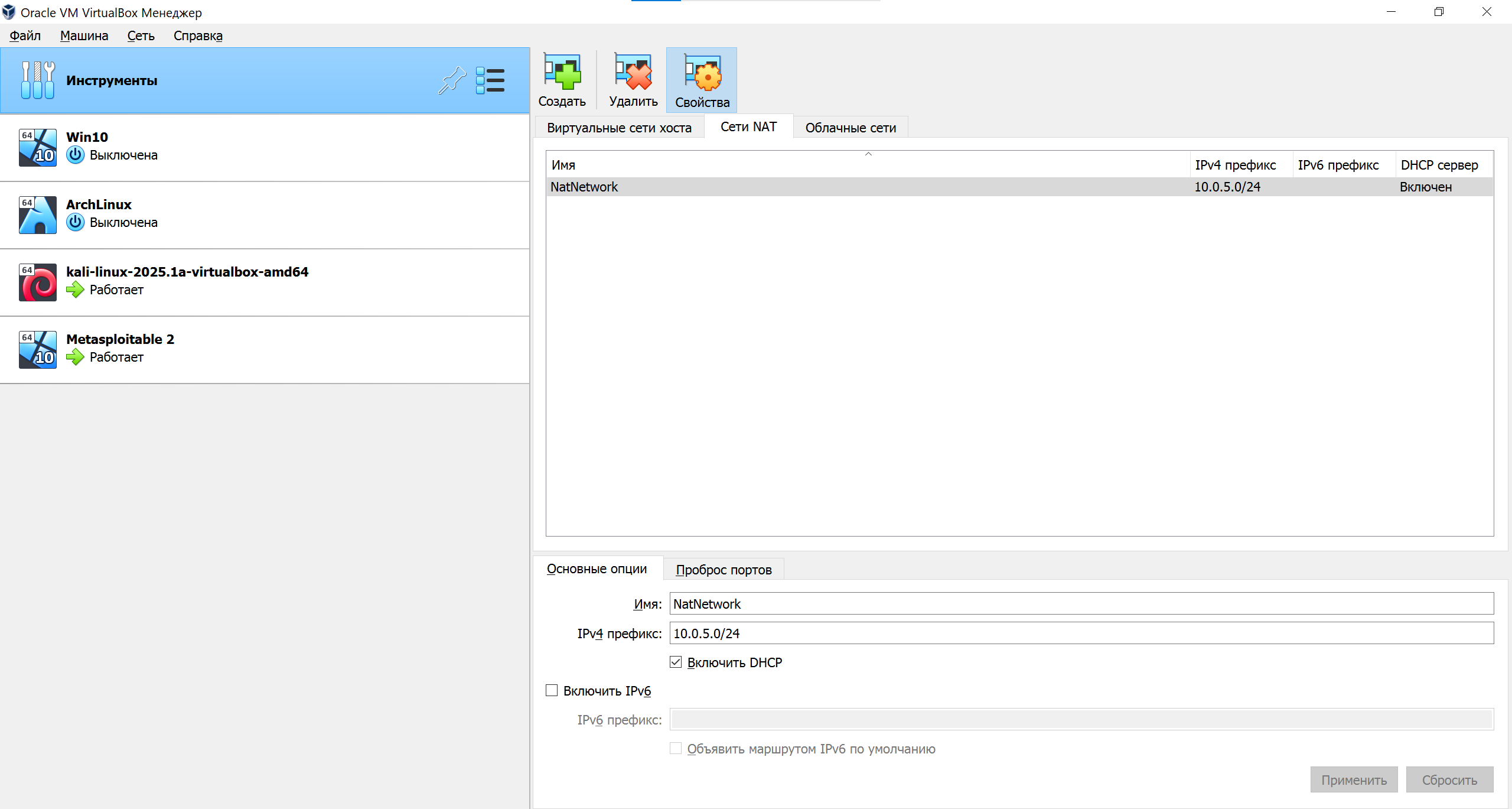
Выполнил:

Студент 3-ого курса

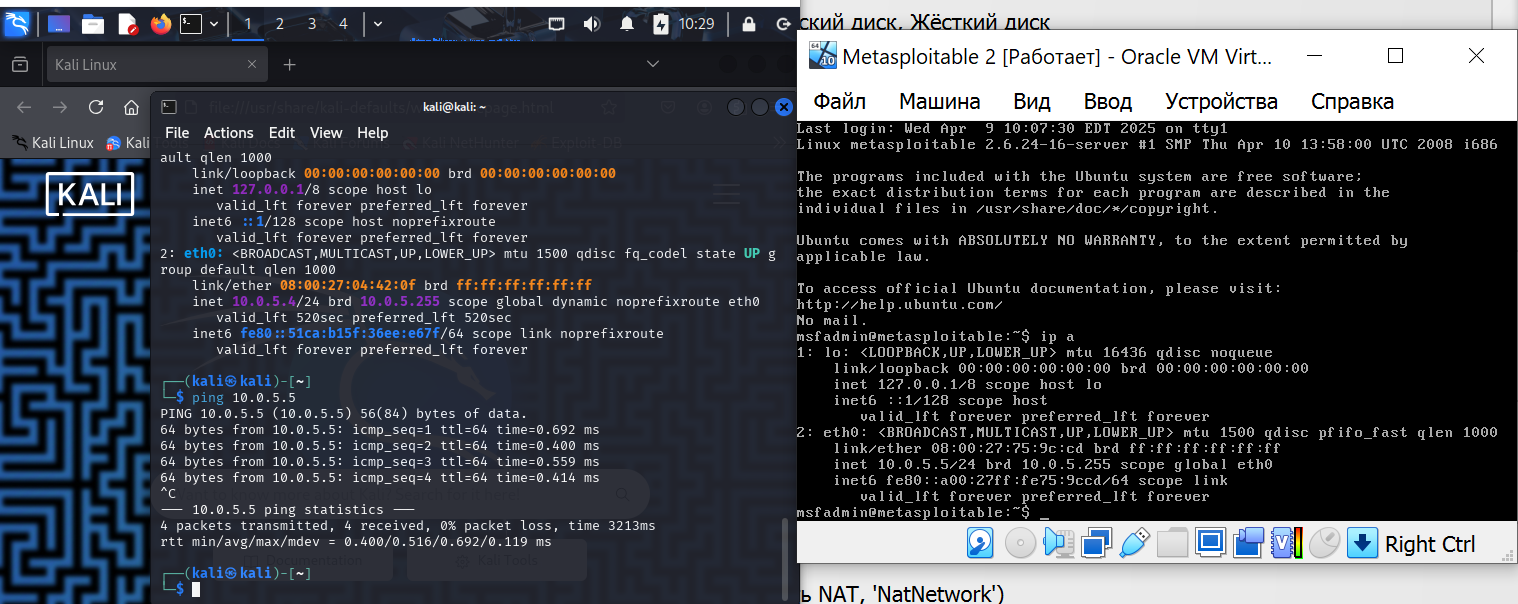
Учебной группы БИСО-02-22

Зубарев В.С.

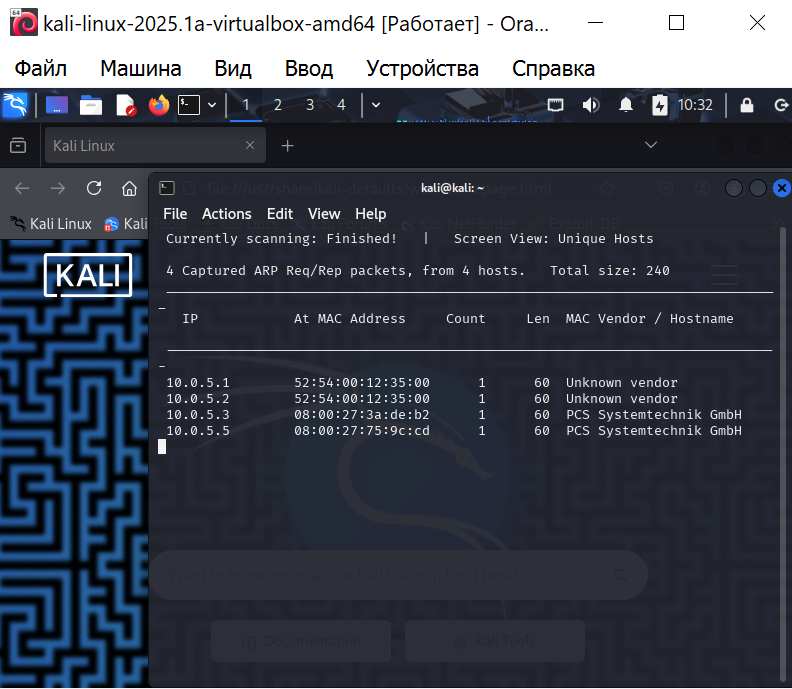
Создание сети NAT



Проверка настроек сети NAT



Поиск цели с помощью инструмента netdiscover



Перечень известных систем виртуализации, их отличительные особенности.  
Oracle VirtualBox, VMWare Workstation  
**VirtualBox** — это бесплатное решение с открытым исходным кодом для виртуализации, которое поддерживает широкий спектр операционных систем, включая Windows, macOS, Linux и Solaris. Подходит для личного использования и тестирования. [1](https://www.securitylab.ru/blog/personal/xiaomite-journal/354260.php)

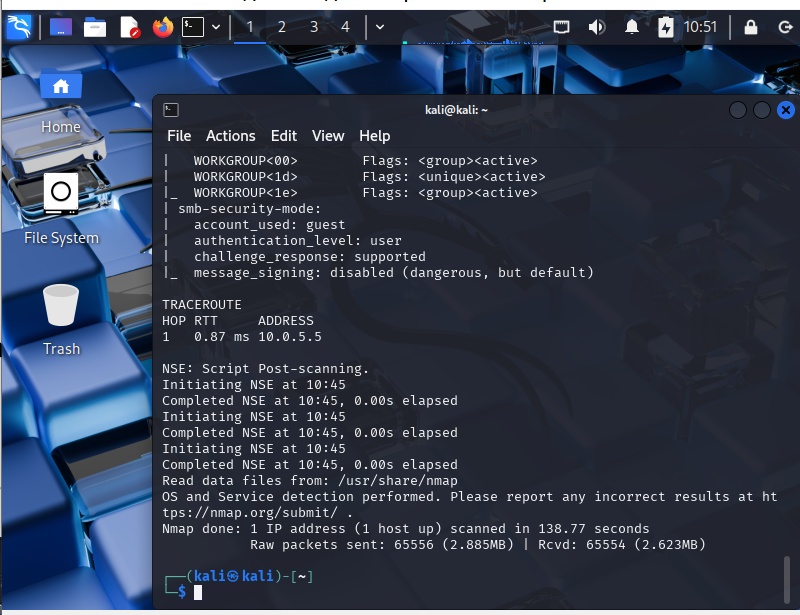
**VMware** — это платное решение для профессиональной виртуализации, которое часто используют в корпоративной среде. Предлагает высокую производительность и поддержку сложных сетевых инфраструктур.

Краткое описание установленных ОС с описанием их назначения.  
Kali Linux – UNIX подобная ОС, нацеленная на тестирование систем на защищенность.

Metasploitable2 -UNIX подобная ОС, которая специально разработана на уязвимых версиях приложений, для практики пентеста.  
Полный перечень использованных команд с кратким описанием их назначения. Основные ключи и их описание.  
Ping – команда для проверки соединения между двумя устройствами

Netdiscover – инструмент для поиска устройств в сети. -r – указание диапазона  
Ifconfig – показывает информацию о сетевых интерфейсах хоста

Примеры выполнения команд, которые были использованы в ходе работы с описанием их результатов

Результаты сканирования портов с помощью nmap  


Объединение данных в папке  


Полный перечень использованных команд с кратким описанием их назначения. Основные ключи и их описание.

Nmap – инструмента для анализа отрытых портов и получения информации о работающих на них сервисах. -v подробный, -p – задет диапазон сканируемых портов, -A отображает версию операционной системы..

Примеры выполнения команд, которые были использованы в ходе работы с описанием их результатов.

Перечень открытых портов, названия и версии сервисов, которые их используют.  
PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

53/tcp open domain ISC BIND 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup:WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login?

514/tcp open tcpwrapped

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open vnc VNC (protocol 3.3)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

6697/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

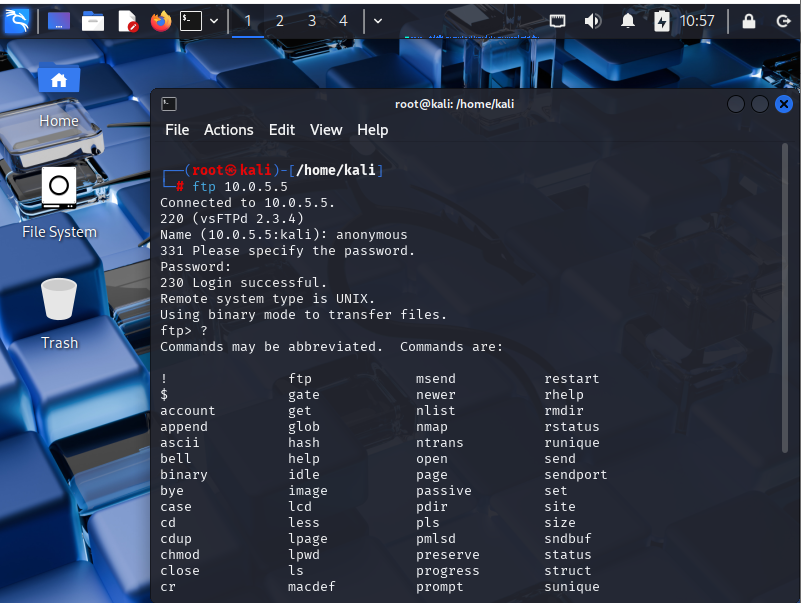
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)

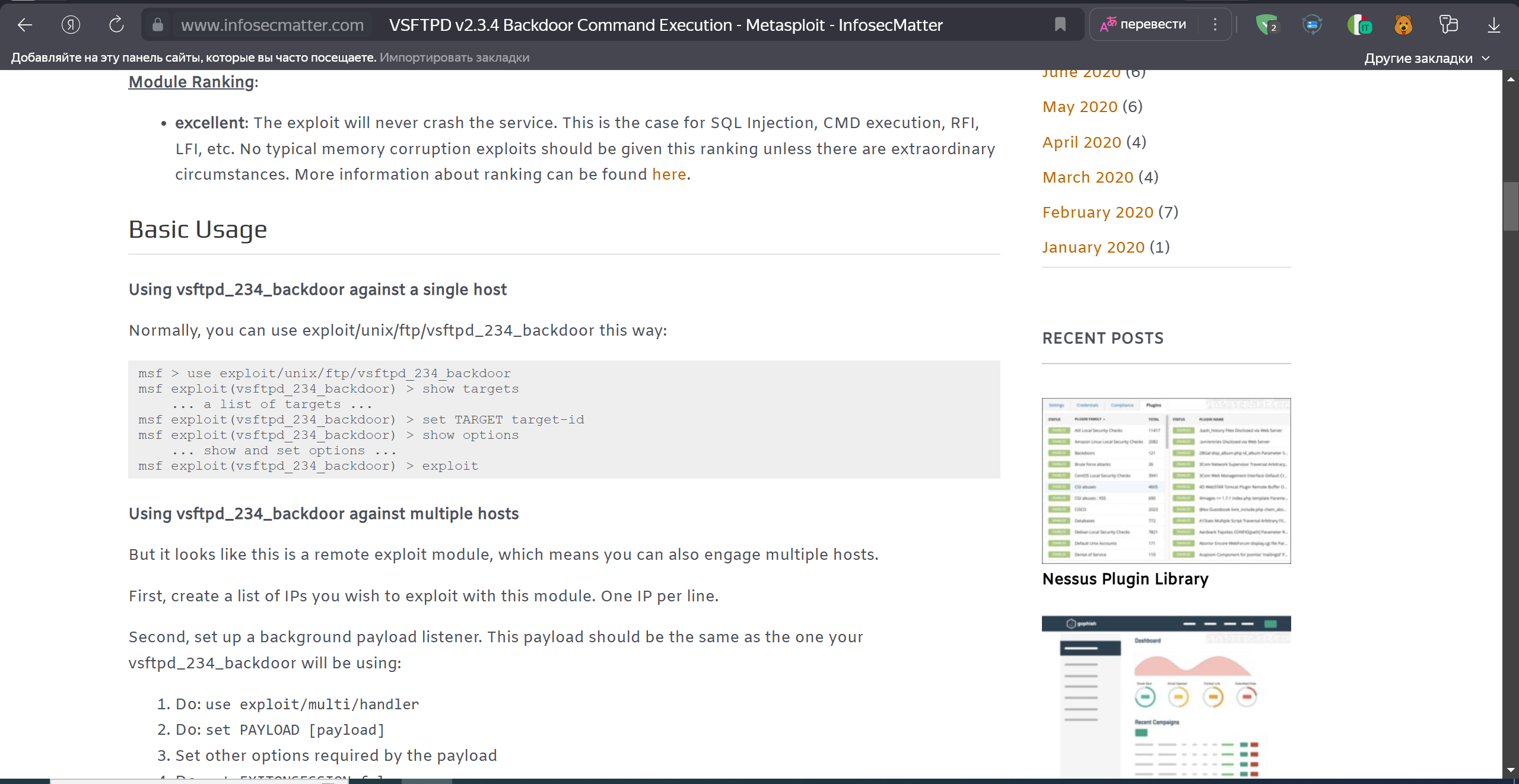
36226/tcp open mountd 1-3 (RPC #100005)

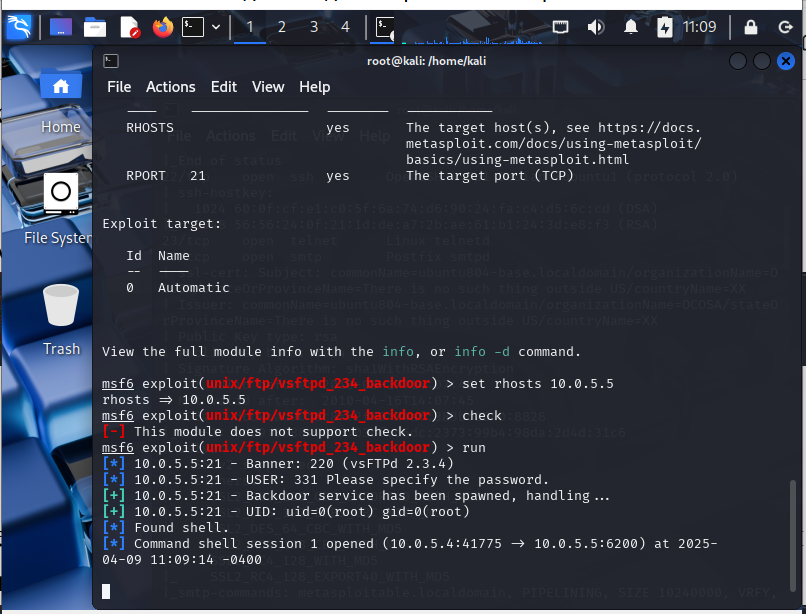
38847/tcp open status 1 (RPC #100024)

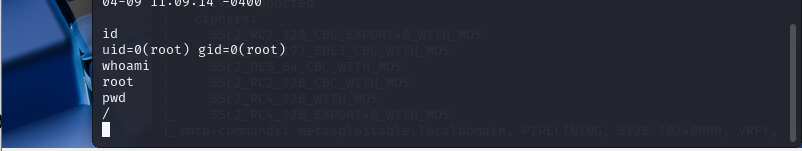
48338/tcp open java-rmi GNU Classpath grmiregistry

51043/tcp open nlockmgr 1-4 (RPC #100021)

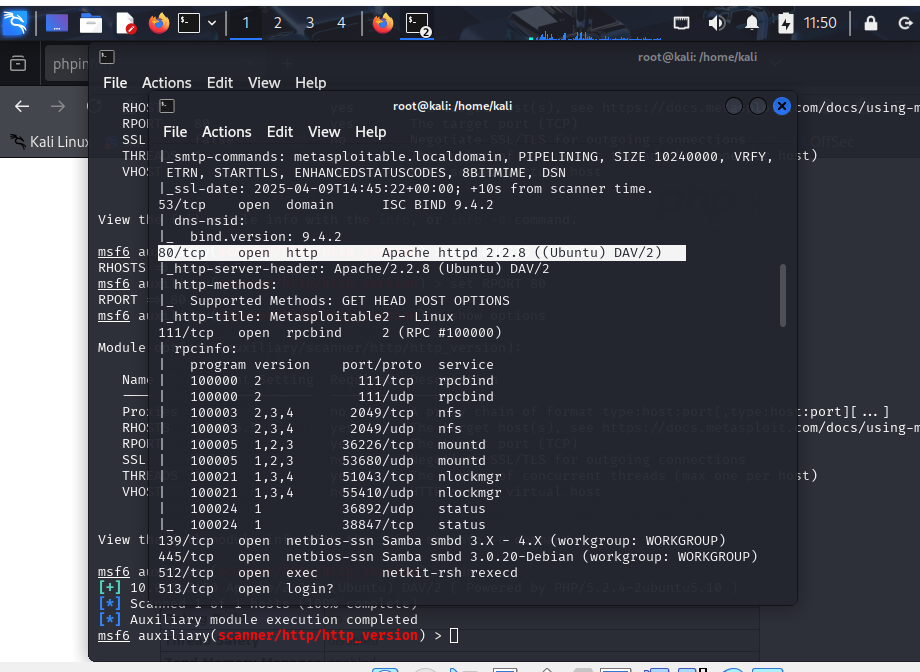
Авторизация на FTP сервере, просмотр доступных команд  


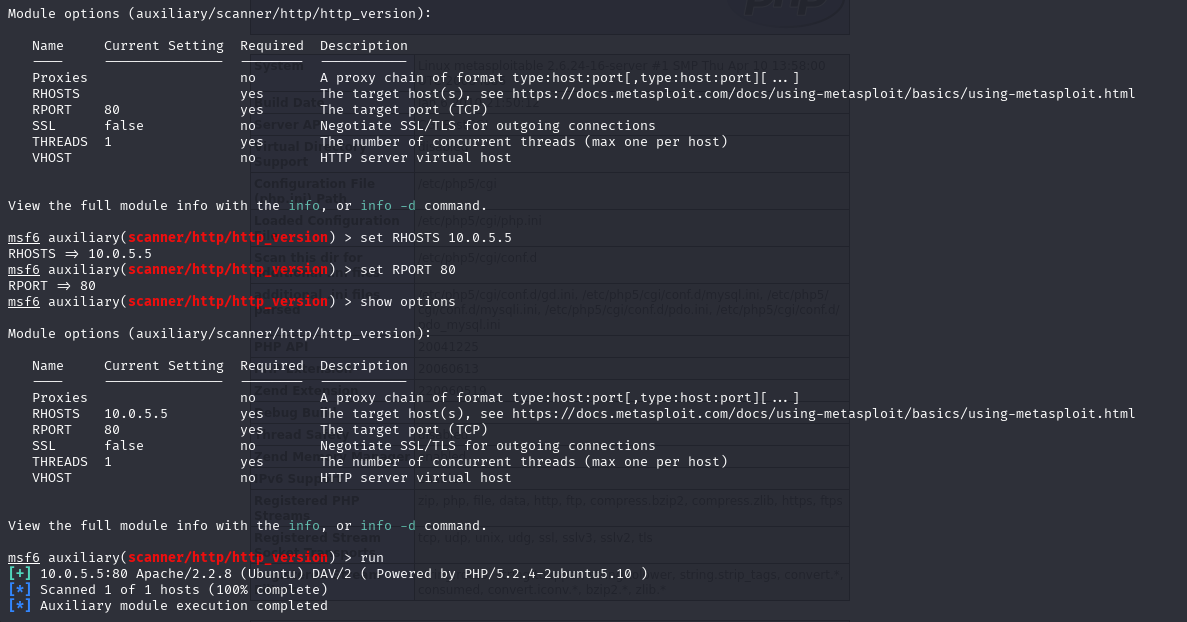
Обнаружение эксплойта  


Изменение входных данных для работы скрипта и его запуск  


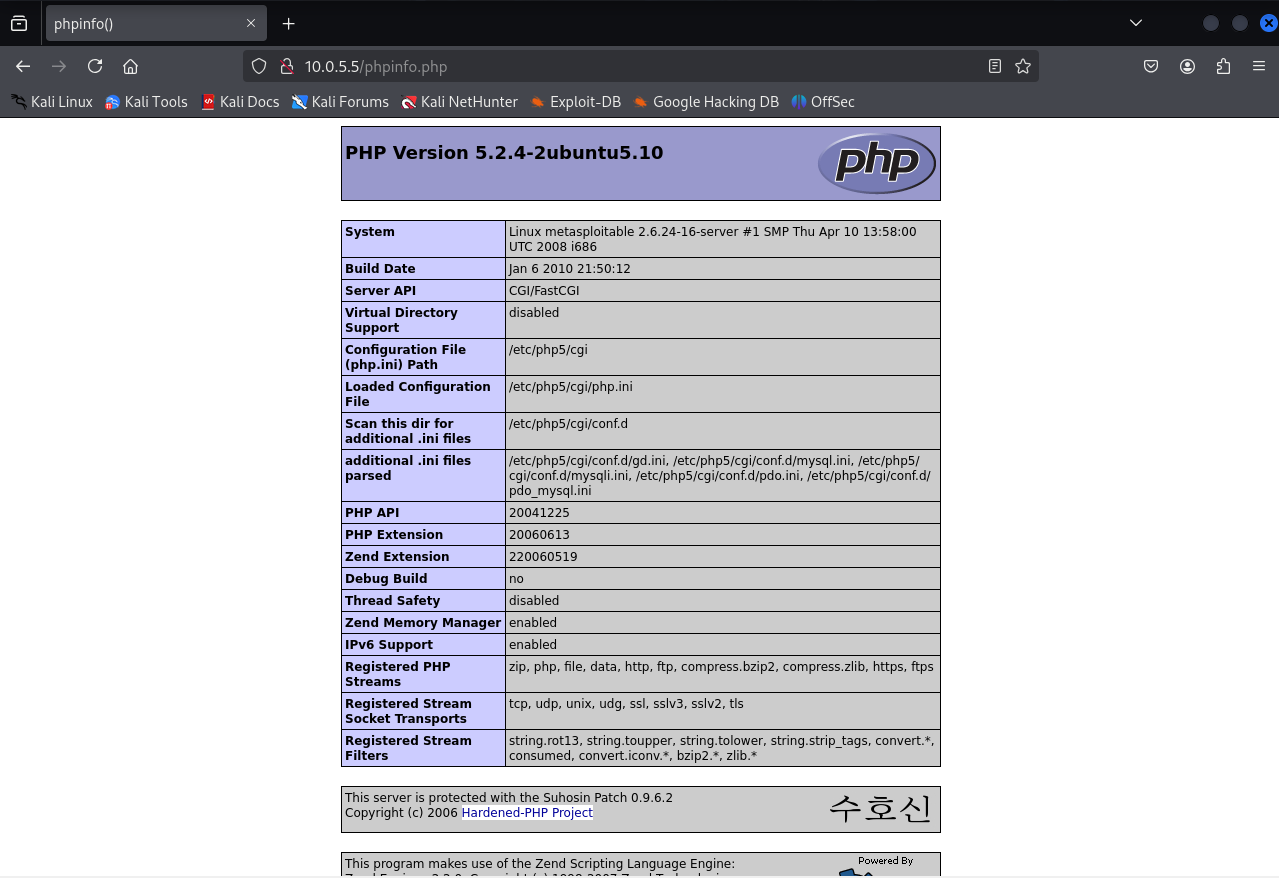
Проверка полученных привилегий  


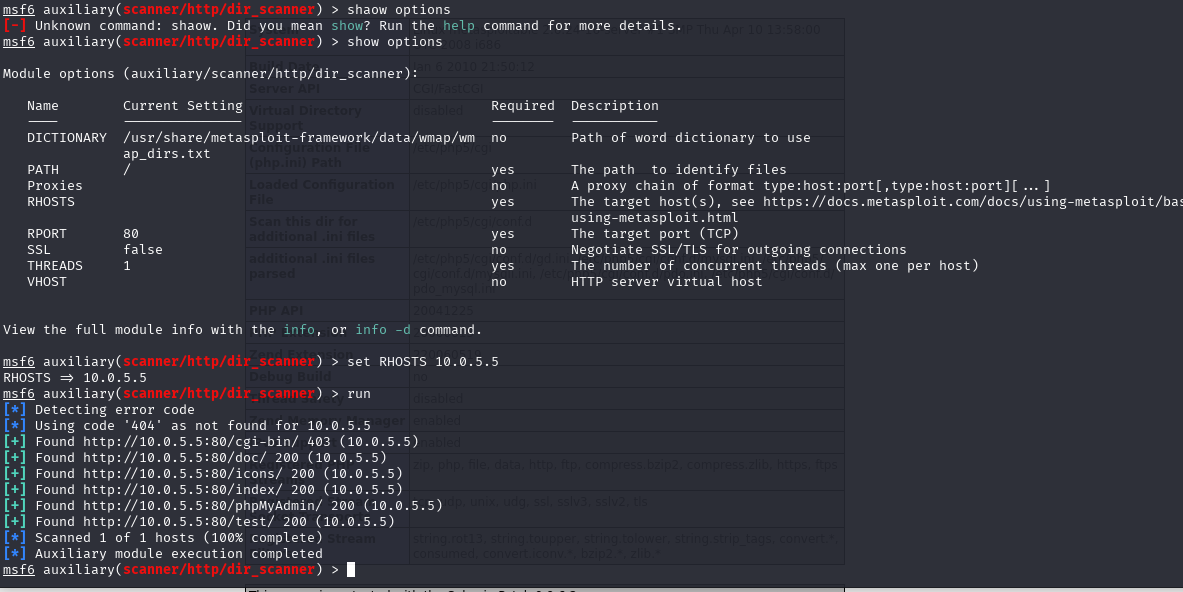
Атака на сервер Apahe

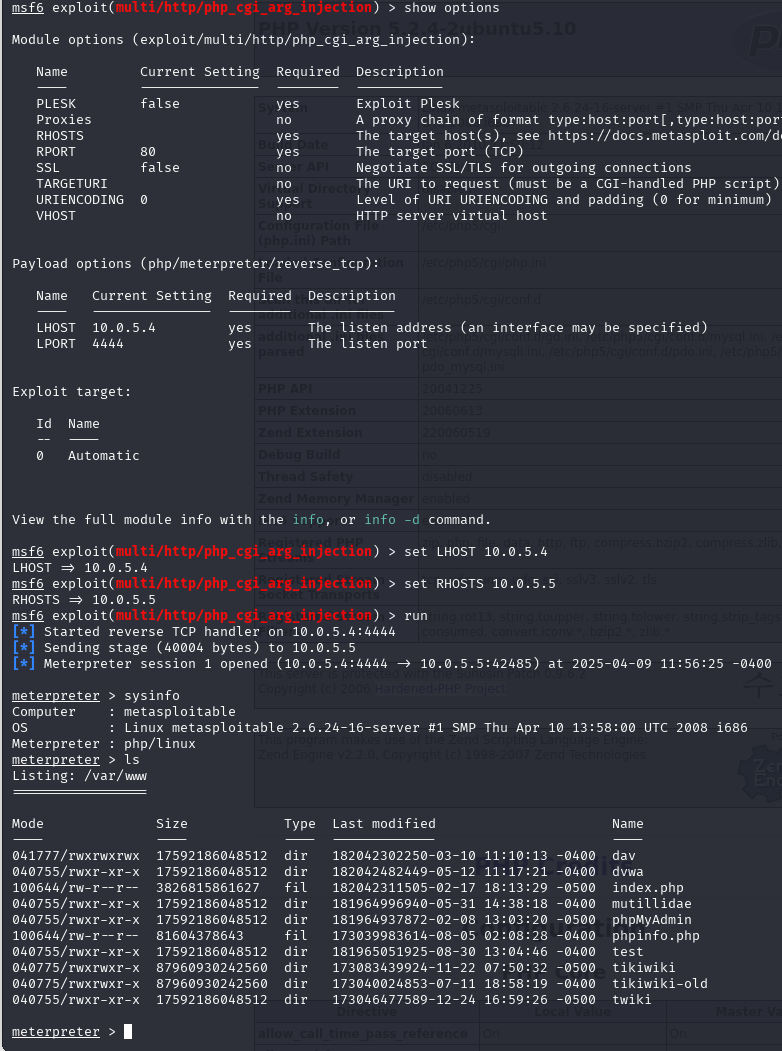
Эксплуатирование найденной уязвимости



Переход на страницу конфигурации php\_модуля



Поиск целевых папок на сервере  


Получение доступа к серверу через сессию meterpretter  


Полный перечень использованных команд с кратким описанием их назначения. Основные ключи и их описание.

FTP – сервис для подключения к удаленному ftp сервису  
mscfconcole – команда для запуска модуля Metasploite  
Описание модулей metasploit.

Использованный модуль use exploit/unix/ftp/vsftpd\_234\_backdoor – использует бэкдор для получения root привилегий на сервере ftp в обход авторизации  
Перечень и описание основных команд FTP сервиса

Некоторые основные команды FTP-сервиса и их описание:

* **USER** — команда для авторизации, передаёт имя пользователя серверу. [1](https://oparinseo.ru/article/enciklopedia-ftp-polnyj-putevoditel-po-protokolu-peredaci-fajlov)
* **PASS** — используется для ввода пароля после команды USER.
* **PWD** — показывает текущий рабочий каталог на FTP-сервере.
* **CWD** — изменяет текущий рабочий каталог на сервере.
* **MKD** — создаёт новый каталог на сервере.
* **RMD** — удаляет существующий каталог.
* **RNFR и RNTO** — переименовывает файл или каталог.
* **DELE** — удаляет файл с сервера.
* **LIST** — выводит список файлов и каталогов в текущей директории.
* **NLST** — показывает только имена файлов и каталогов, без дополнительной информации.
* **RETR** — получает копию файла с сервера (скачивает файл). [1](https://oparinseo.ru/article/enciklopedia-ftp-polnyj-putevoditel-po-protokolu-peredaci-fajlov)
* **STOR** — отправляет копию файла на сервер (загружает файл). [1](https://oparinseo.ru/article/enciklopedia-ftp-polnyj-putevoditel-po-protokolu-peredaci-fajlov)
* **QUIT** — завершает FTP-сессию и разрывает соединение. [1](https://oparinseo.ru/article/enciklopedia-ftp-polnyj-putevoditel-po-protokolu-peredaci-fajlov)