

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

Burp Suite, атака «Человек посередине»
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.

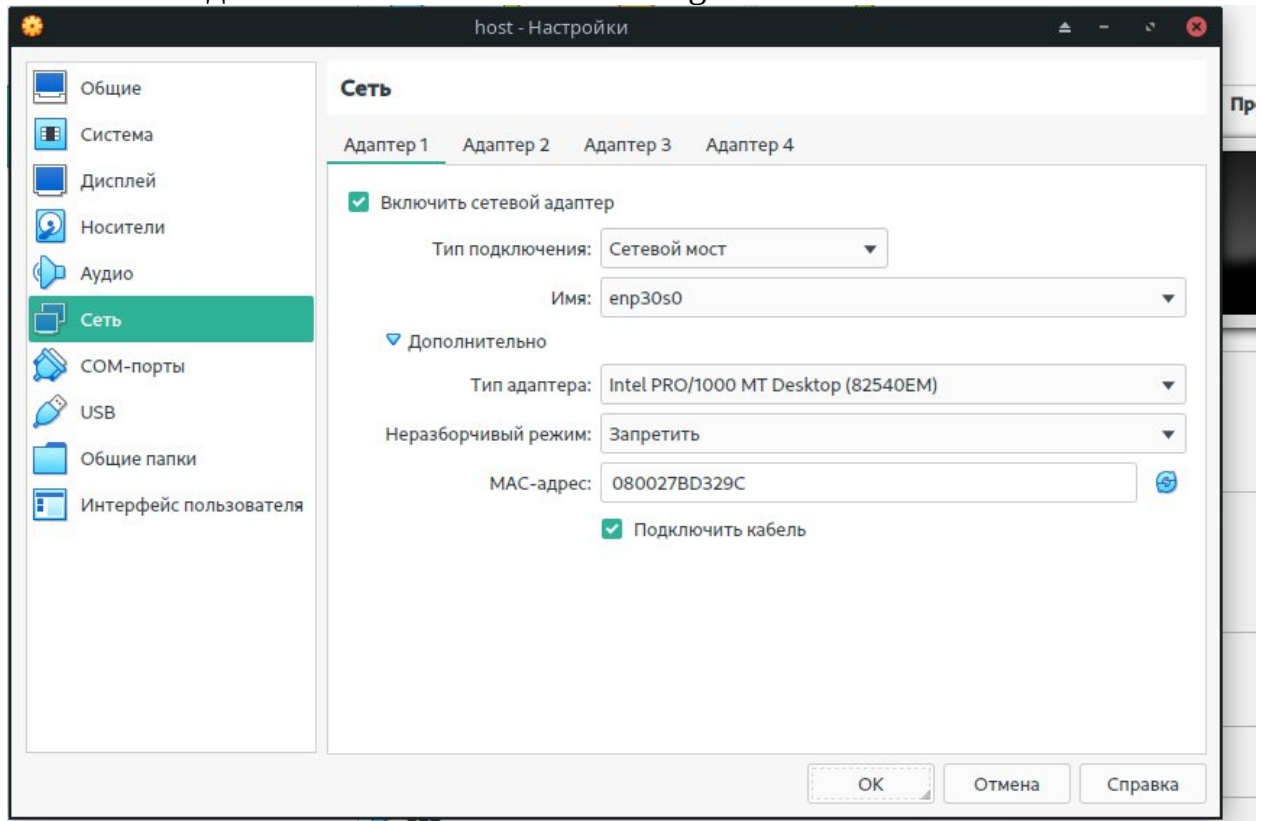
подпись, дата

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

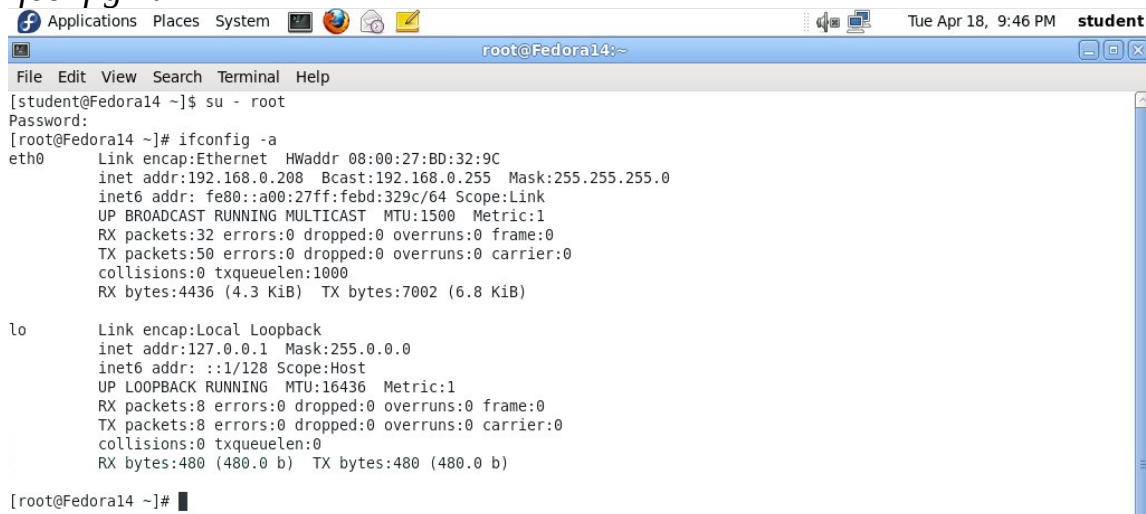
Смените текущего пользователя на root

`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. Исправление прав доступа к папке с загрузками

- Откройте консоль и выполните следующие команды:
 - `chown root:apache /var/www/html/dvwa/hackable/uploads/`
 - `chmod 775 /var/www/html/dvwa/hackable/uploads/`
 - `chmod 775 /var/www/html/dvwa/hackable/uploads/`

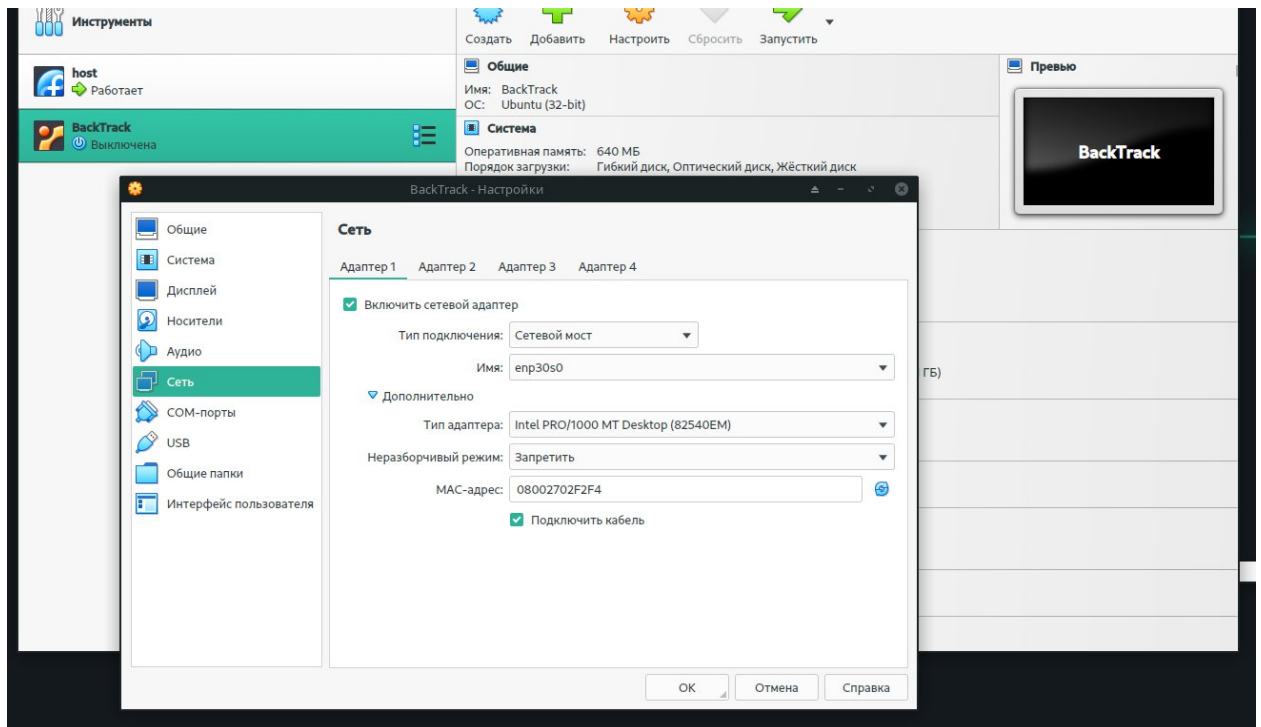
Выполнено!

Замечания:

- По умолчанию, папка `/var/www/html/dvwa/hackable/uploads/` принадлежит пользователю `root` и его группе.
- К тому же, у `apache` нет права записи в папку `hackable/uploads`, что позволило бы пользователю загружать файлы именно туда.

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»



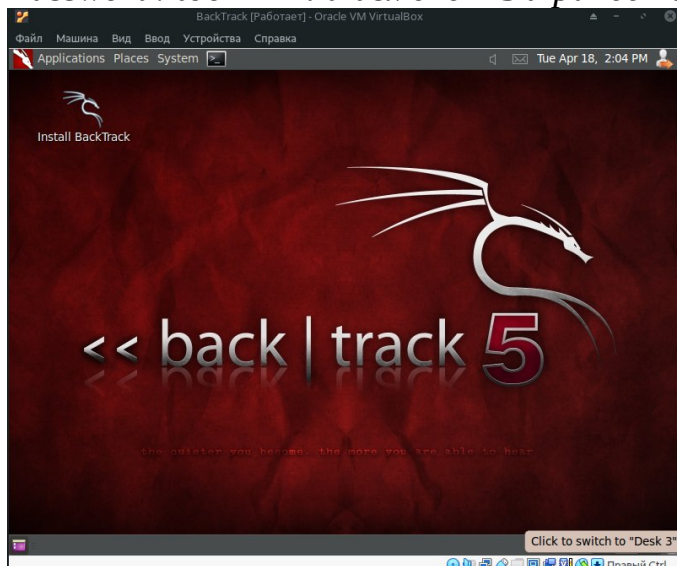
Раздел 6. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

Login: root

Password: toor <Или измененный ранее пароль>.



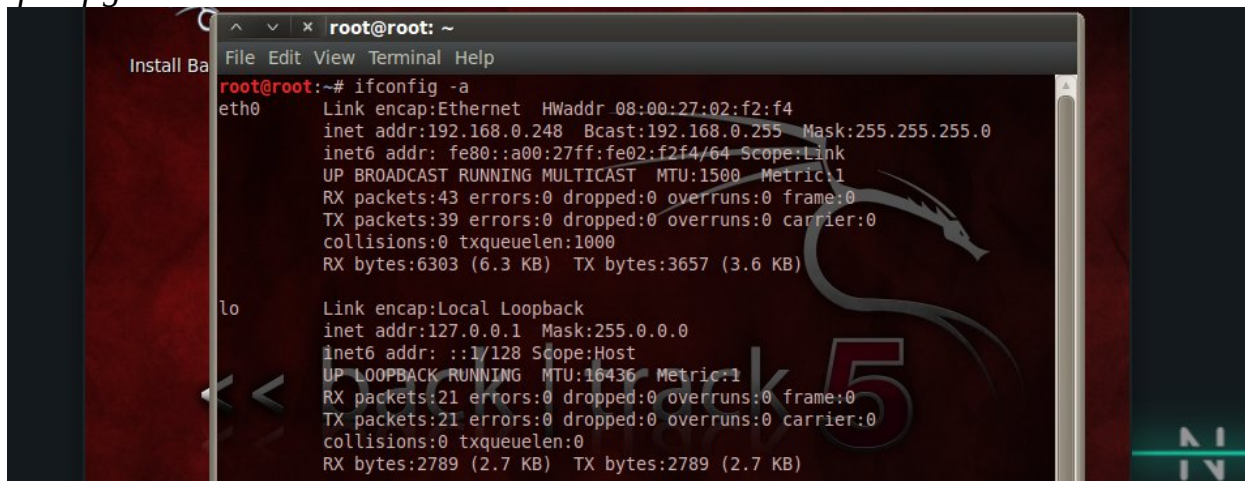
Раздел 7. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

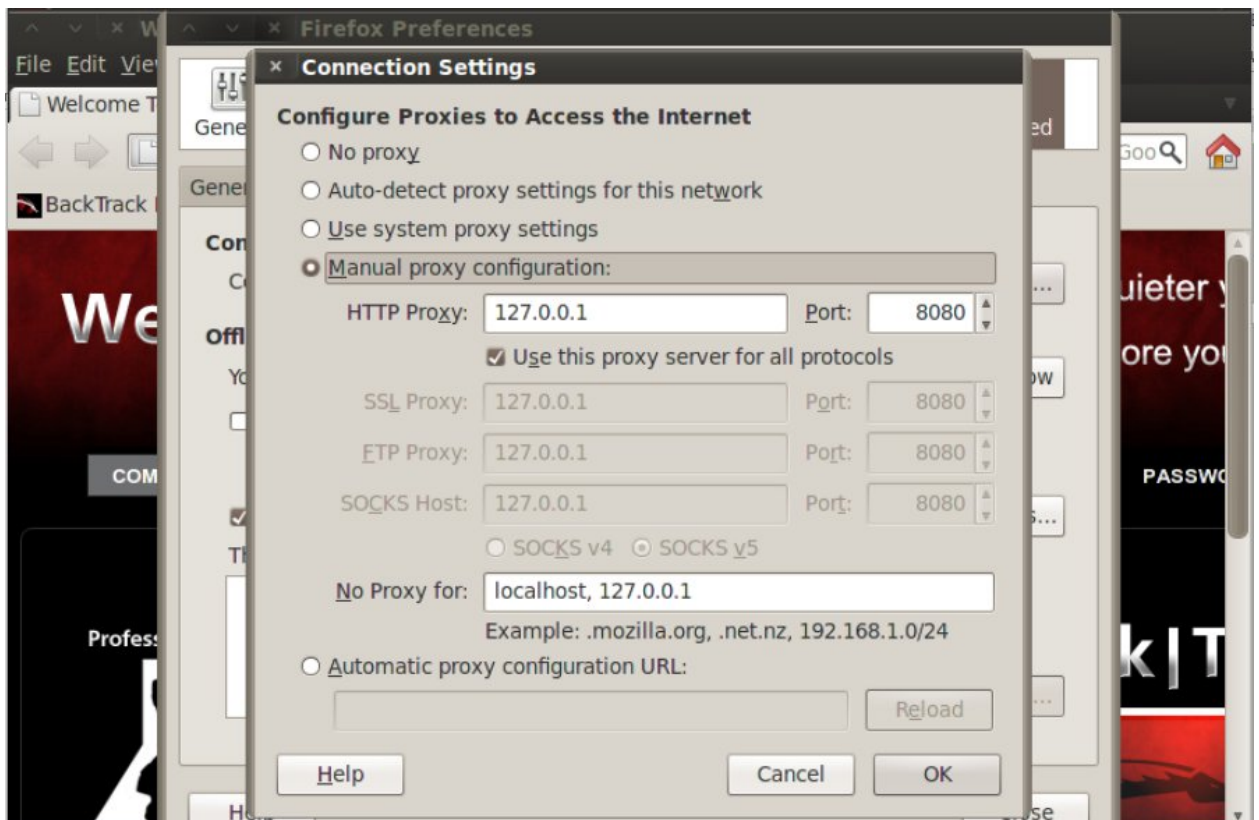
`ifconfig -a`



```
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)
```

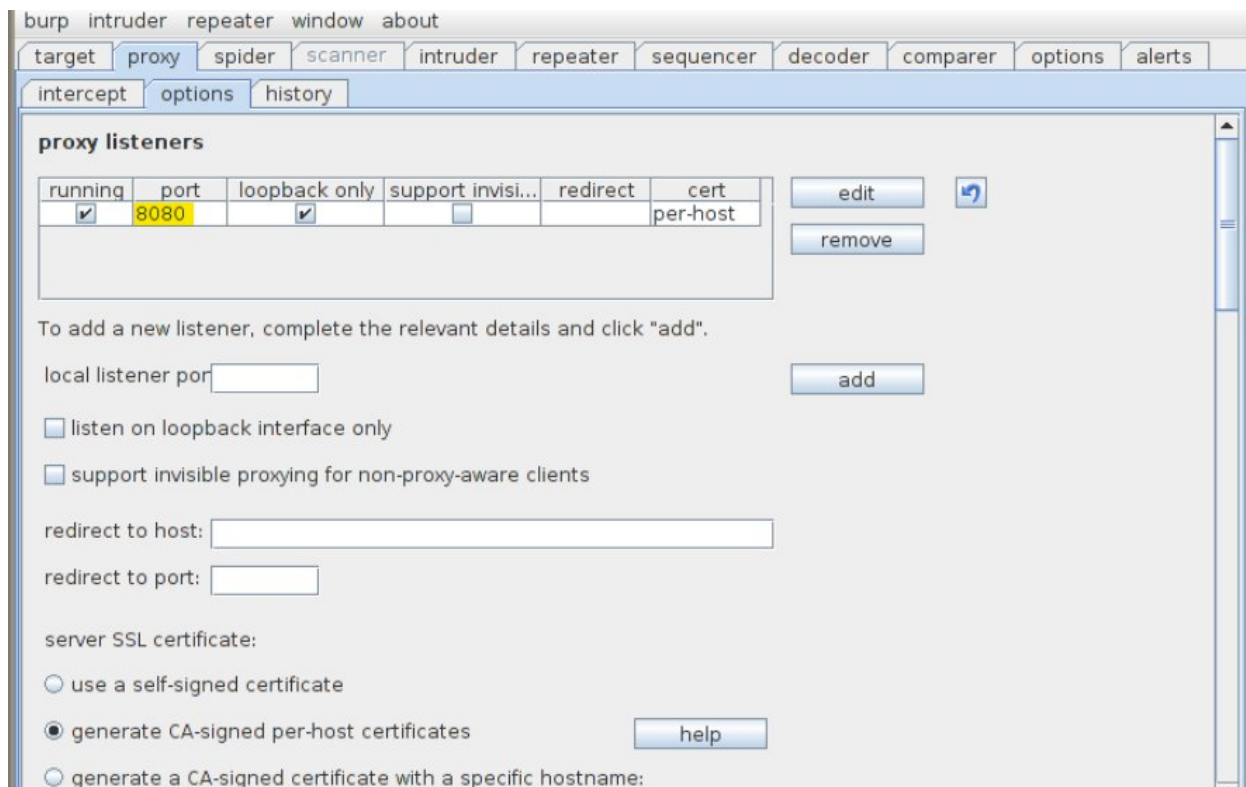
Раздел 8. Конфигурация настроек Firefox Proxy

1. Запустите Firefox
2. Перейдите к настройкам proxy
 - a. Edit -> Preferences
 - b. Щелкните на Advanced
 - c. Щелкните на Network Tab (вкладку сеть)
 - d. Щелкните на кнопку настроек
3. Настройте proxy
 - a. Щелкните на Manual proxy configurations (ручная конфигурация прокси)
 - b. Наберите "127.0.0.1" в графе "HTTP Proxy".
 - c. Наберите "8080" в графе "Port".
 - d. Отметьте галочкой "Use the proxy server for all protocols" (использовать прокси сервер для всех протоколов)
 - e. Щелкните OK
 - f. Щелкните Close

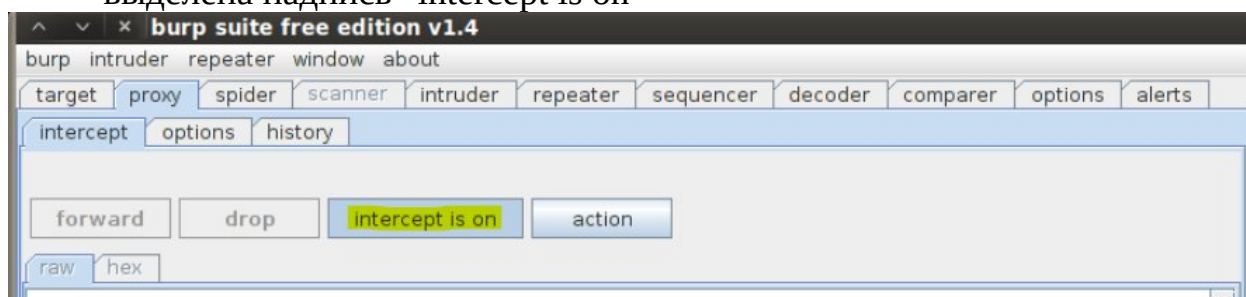


Раздел 9. Конфигурация Burp Suite

1. Запустите Burp Suite
 - a. Applications--> BackTrack --> Vulnerability Assessment --> Web Application Assessment ---> Web Vulnerability Scanner--> burpsuite
 - b. Нажмите ОК в появившемся окне
2. Настройте Proxy в Burp Suite
 - a. Щелкните на вкладку проху
 - b. Щелкните на вкладку «options»(настройки)
 - c. Проверьте, что прописан порт 8080



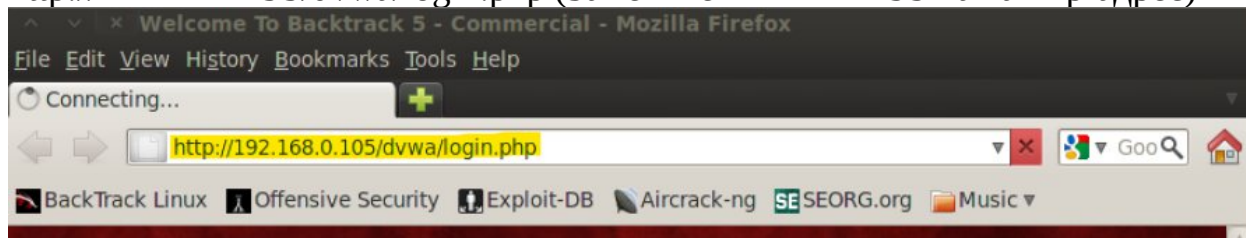
3. Активируйте перехват
 - а. Во вкладке proxy -> intercept убедитесь, что перехват установлен, выделена надпись "intercept is on"



Раздел 10. Перехват с Burp Suite

Войдите в DVWA через Firefox

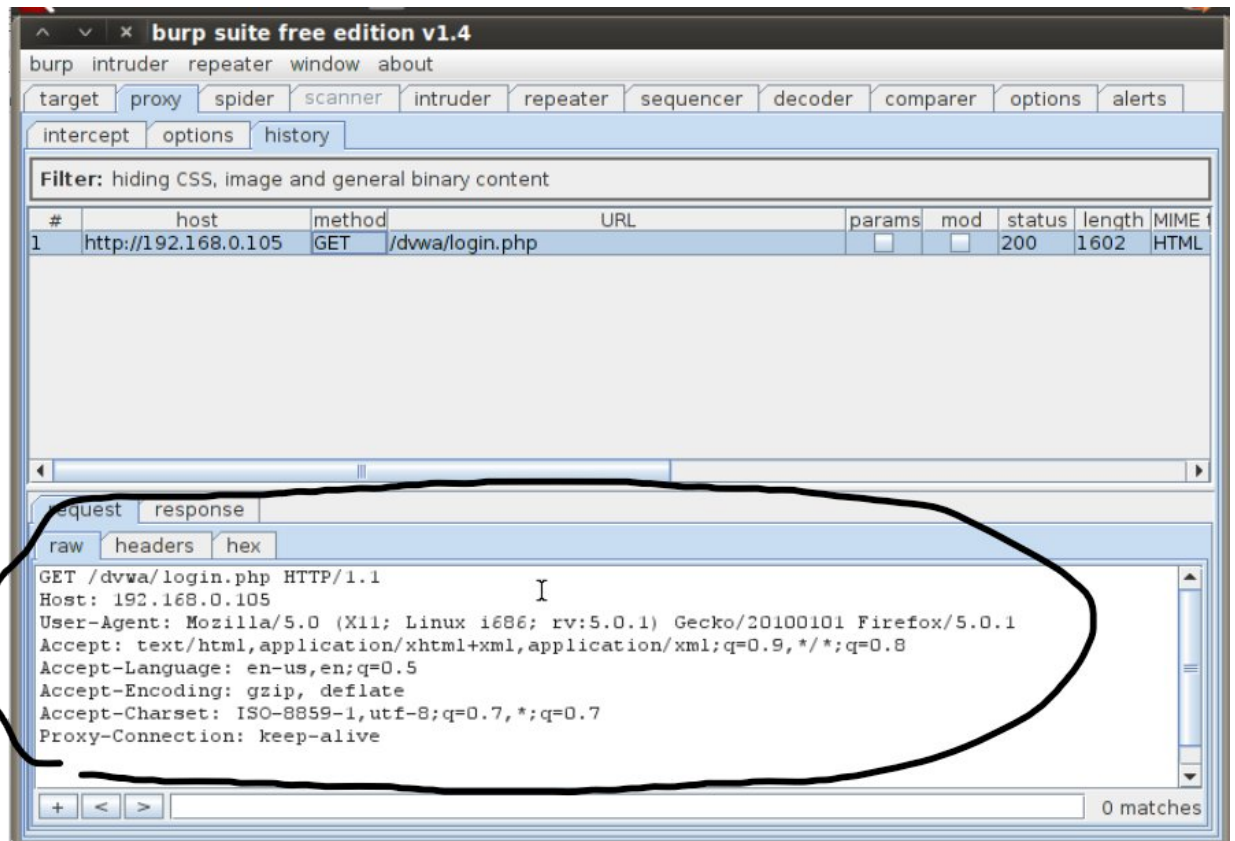
<http://IPADDRESS/dvwa/login.php> (Замените IPADDRESS на ваш ip-адрес)



Замечания:

- Заметьте, что домашняя страница DVWA не отобразится, но вы увидите сообщение о соединении.

2. В Burp Suite нажмите “Forward” 2 раза
3. Изучите данные запросов
 - a. Выберите “proxy -> history”
 - b. Выберите “/dvwa/login.php”
 - c. Выберите “request -> raw”



Замечания:

- Обратите внимание, получены PHP cookie, даже без входа в систему
4. Войдите в DVWA
 - a. Логин: admin
 - b. Пароль: password

Username

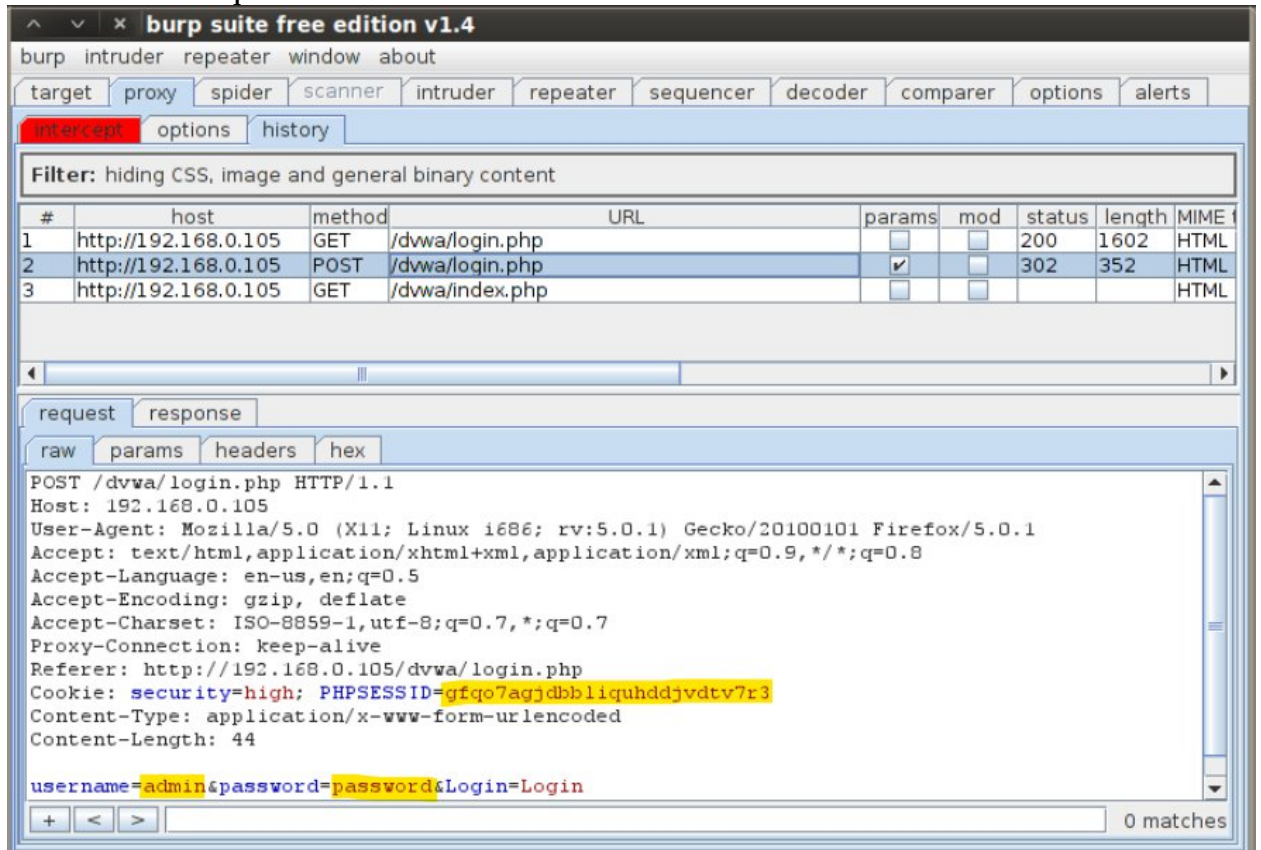
Password

Login

Замечания:

- Заметьте, что страница DVWA не отобразится, но вы увидите сообщение о соединении.
5. В Burp Suite нажмите “Forward” 2 раза

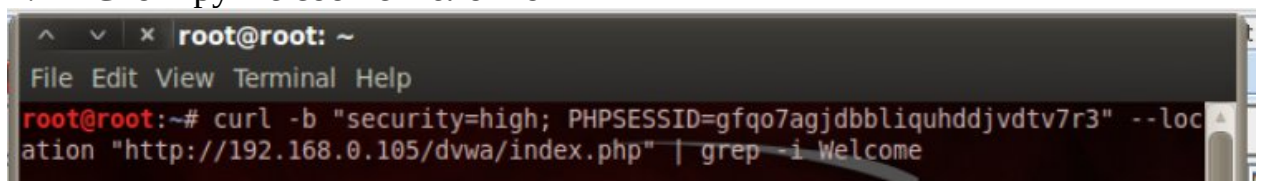
6. Изучите детали запроса
 - a. proxy->history
 - b. Выберите POST запрос на /dvwa/login.php
 - c. request -> raw



Замечания:

- Заметьте, здесь отображается PHP Session Id, логин и пароль

7. Скопируйте cookie в блокнот

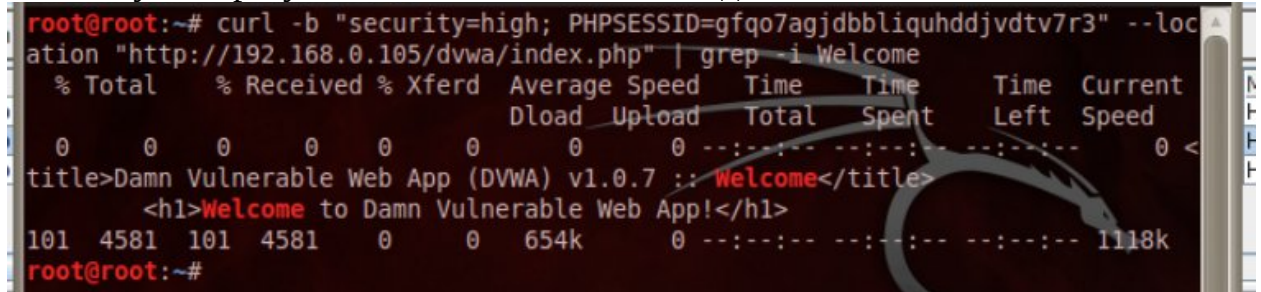


8. Соберите корректную curl-команду, вставив свои cookie и ip-адрес в следующую строку:

- a. `curl -b "security=high; PHPSESSID=reoctn5dfb89qlcggl2sm5jfe4" -location "http://IPADDRESS/dvwa/index.php" | grep -i Welcome`

Раздел 11. Атака «Человек посередине» через curl

1. Скопируйте созданную ранее команду в консоль и запустите ее
2. Изучите результаты выполнения команды



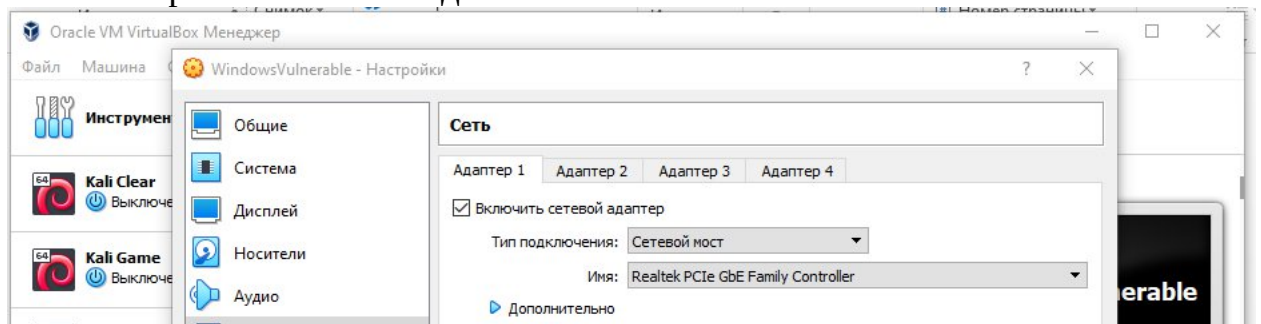
```
root@root:~# curl -b "security=high; PHPSESSID=gfqo7agjdbbliquhddjvdtv7r3" --location "http://192.168.0.105/dvwa/index.php" | grep -i Welcome
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left     Speed
  0     0    0     0     0     0      0     0  --:--:-- --:--:-- --:--:--    0
title>Damn Vulnerable Web App (DVWA) v1.0.7 :: Welcome</title>
      <h1>Welcome to Damn Vulnerable Web App!</h1>
101 4581 101 4581    0     0  654k    0  --:--:-- --:--:-- --:--:-- 1118k
root@root:~#
```

Замечания:

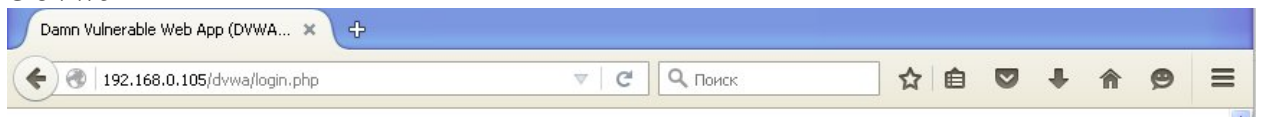
- Заметьте, что вы видите экран входа в DVWA, хотя не вводили имя пользователя или пароль.

Раздел 12. Атака «Человек посередине» через Firefox

1. Создайте в VirtualBox виртуальную машину “WindowsVulnerable”, используя полученный у преподавателя файл виртуального диска “winvulnerable.vmdk” (хватит 256 Мб оперативной памяти)
2. Настройте сетевые подключения типа «сетевой мост»



3. Запустите ВМ и Firefox в ней. Проверьте доступ в интернет и к серверу с dvwa

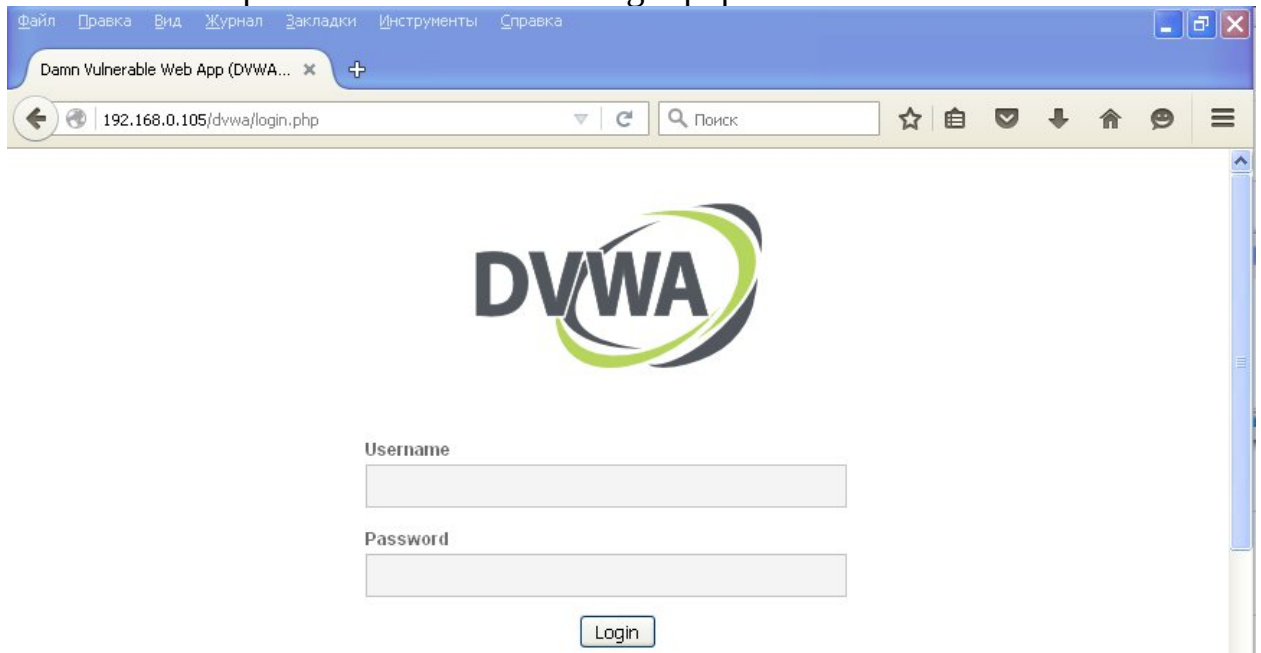


4. Если доступа нет – проверьте настройки сети и при необходимости пропишите вручную данные
 - a. Пуск -> Сетевое окружение
 - b. Отобразить сетевые подключения
 - c. Нажмите правой клавишей на «Подключение по локальной сети 2», выберите «Свойства»
 - d. Выберите “Протокол Интернета (TCP/IP)», нажмите «свойства»

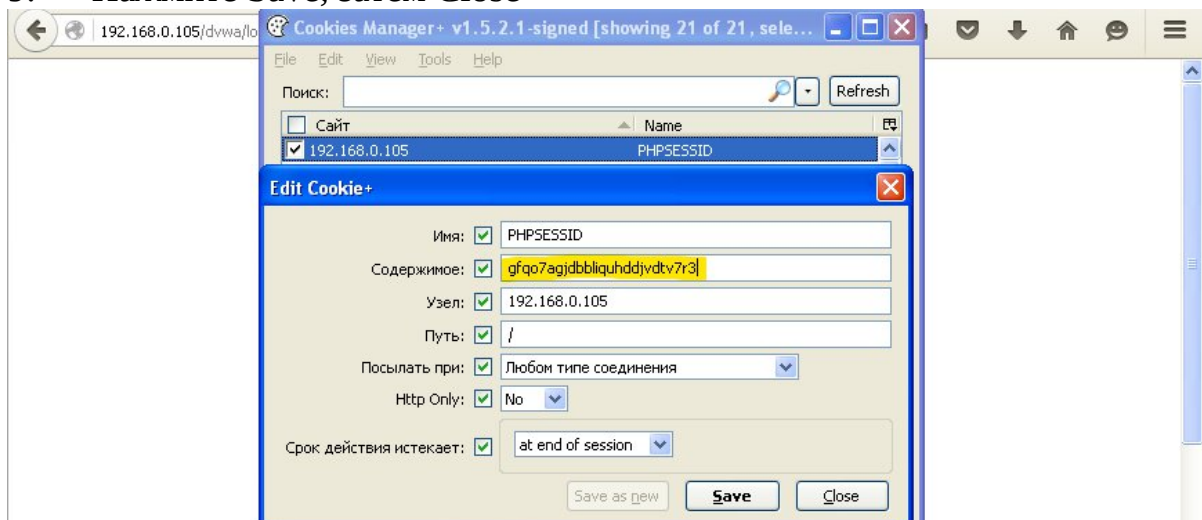
- е. Выберите везде «использовать следующий...»
- ф. Пропишите вручную IP-адреса и DNS-сервера. Узнать их можно либо у преподавателя, либо переписать у хоста (основная ОС, из-под которой запущен Virtual Box) (узнать – командой ipconfig в командной строке)

5. Перейдите на страницу входа в DVWA, заменив IPADDRESS на IP-адрес Fedora

- а. <http://IPADDRESS/dvwa/login.php>

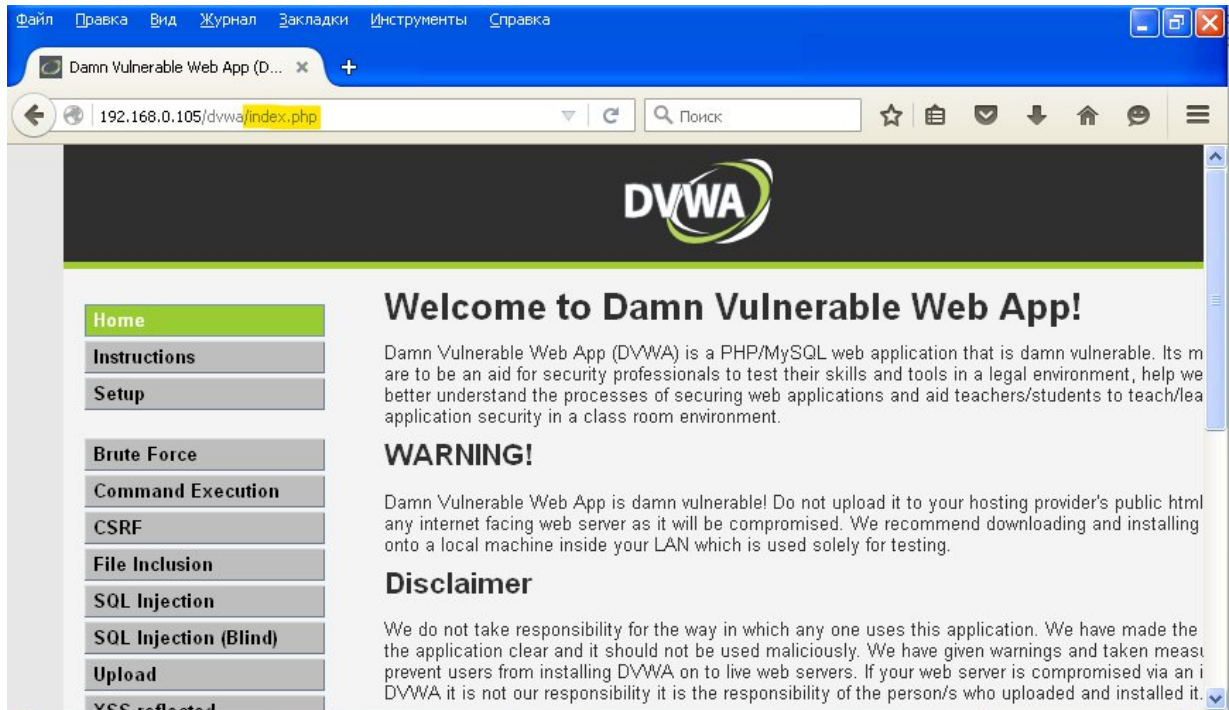


- 6. В Firefox запустите “Cookies Manager +”
 - а. Инструменты -> Cookies Manager +
- 7. Выберите строку с IP-адресом Fedora и нажмите Edit
- 8. Замените содержимое поля “content” PHPSESSID, полученными в разделе 9 на шаге 7
- 9. Нажмите Save, затем Close



10. Иницилируйте атаку

- a. В адресной строке замените login.php на index.php.
Ваш URL будет выглядеть примерно так:
`http://IPADDRESS/dvwa/index.php`
- b. Нажмите Enter

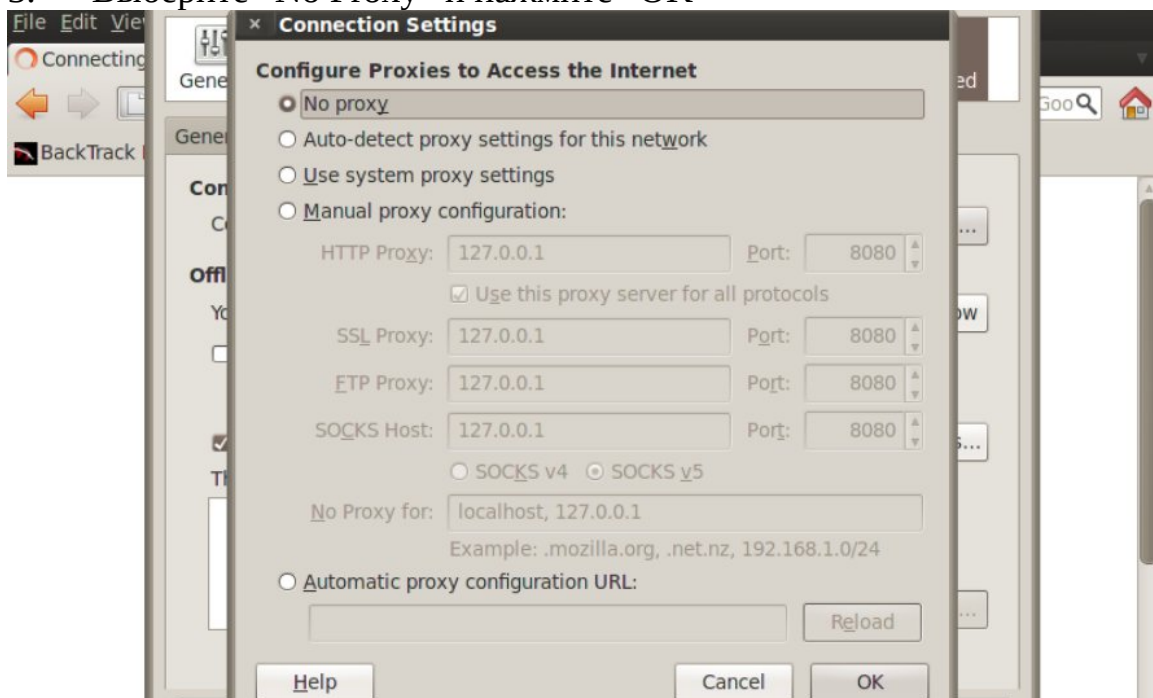


Замечания:

- Заметьте, что вы только что обошли экран входа и успешно завершили атаку "человек посередине".

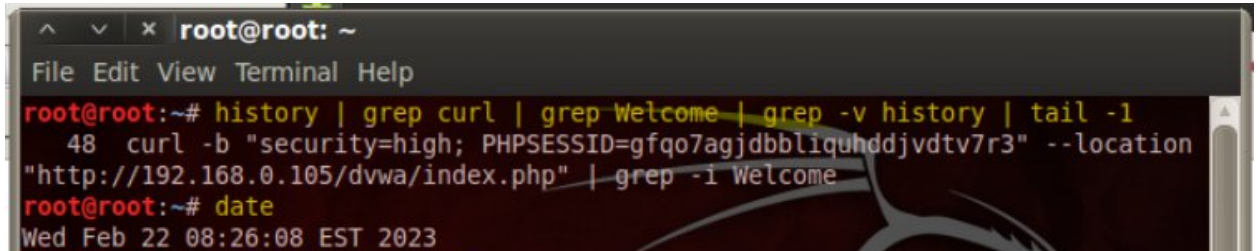
Раздел 13. Удаление Proxy в BackTrack

1. Перейдите в Firefox на BackTrack
2. Снова зайдите в настройки сети
3. Выберите "No Proxy" и нажмите "OK"



Раздел 14. Отчет о работе

1. В Backtrack откройте консоль и выполните:
 - a. `history | grep curl | grep Welcome | grep -v history | tail -1`
 - b. `date`



```
root@root: ~  
File Edit View Terminal Help  
root@root:~# history | grep curl | grep Welcome | grep -v history | tail -1  
48 curl -b "security=high; PHPSESSID=gfqo7agjdbbliqubddjvdtv7r3" --location  
"http://192.168.0.105/dvwa/index.php" | grep -i Welcome  
root@root:~# date  
Wed Feb 22 08:26:08 EST 2023
```