

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, функция «Паук»

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.

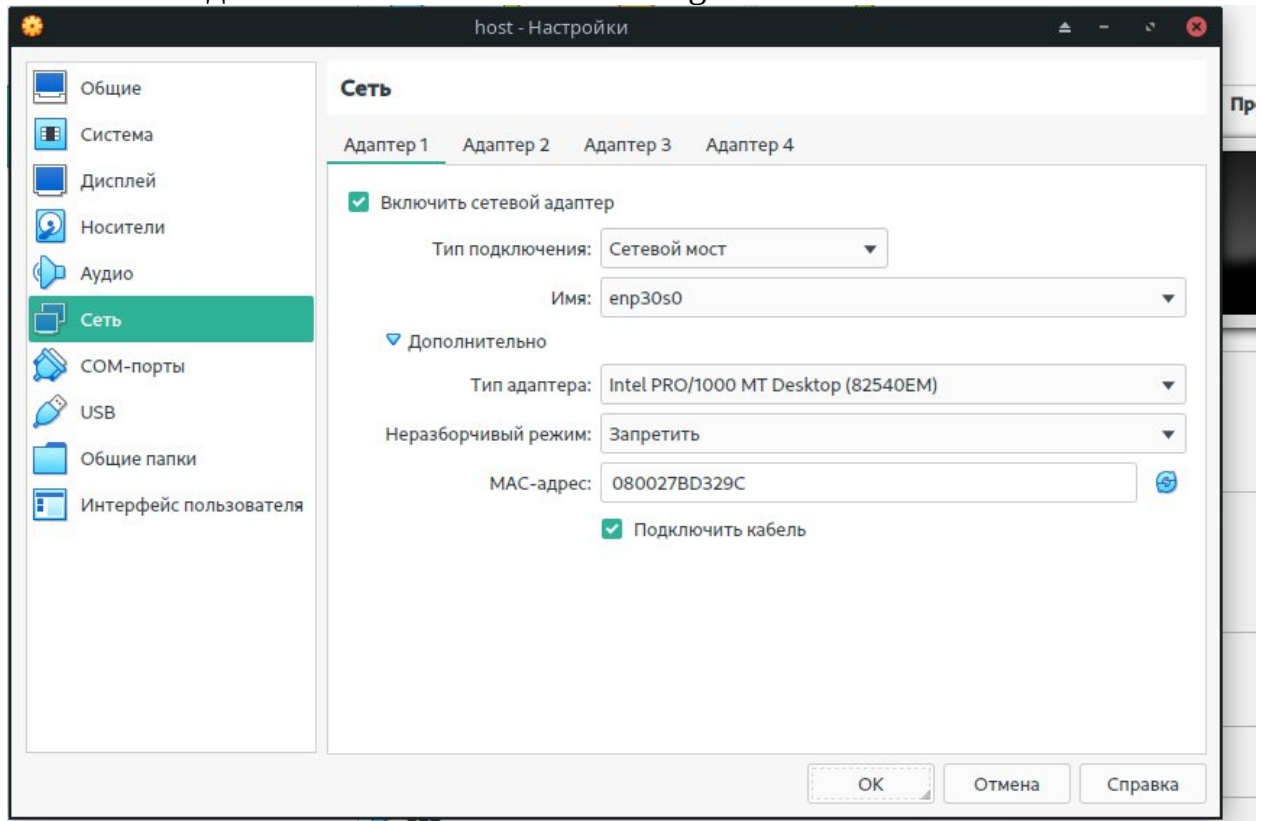
подпись, дата

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>.

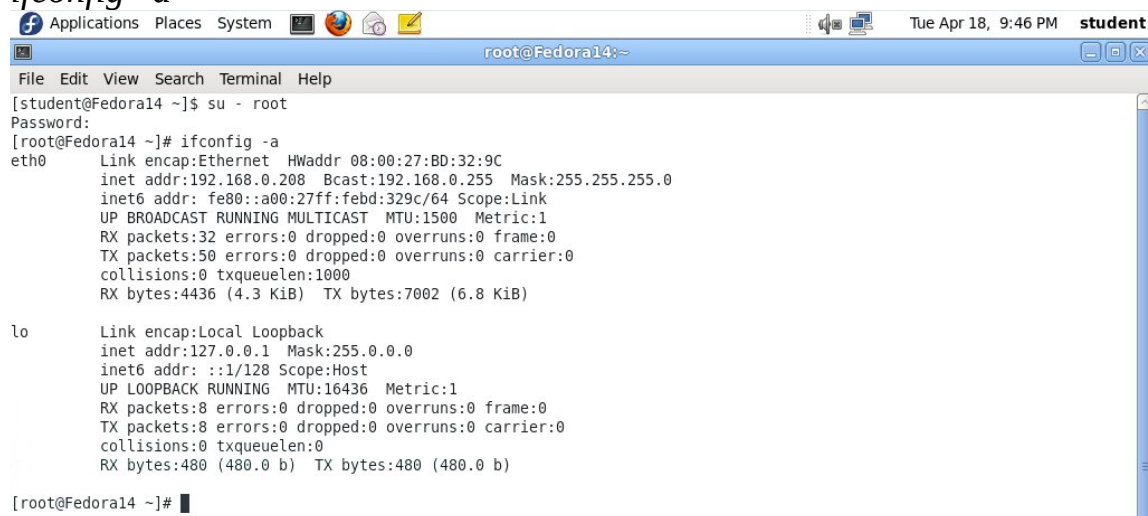


Раздел 3. Запуск консоли и определение IP адреса

Откройте терминал
Applications --> System Tools--> Terminal

Смените текущего пользователя на root
`su - root`
<Ранее созданный пароль root>

Определите IP адрес
`ifconfig -a`



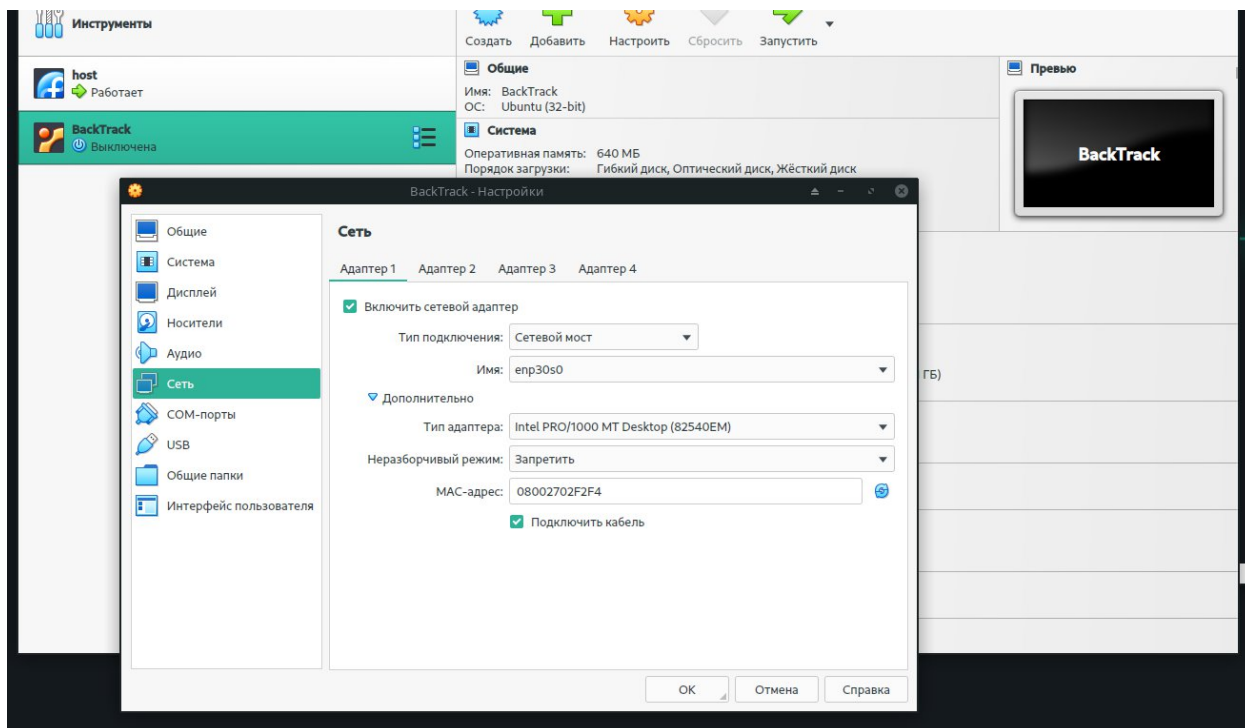
```
[student@Fedora14 ~]$ su - root
Password:
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:BD:32:9C
          inet addr:192.168.0.208  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febd:329c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  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. 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»

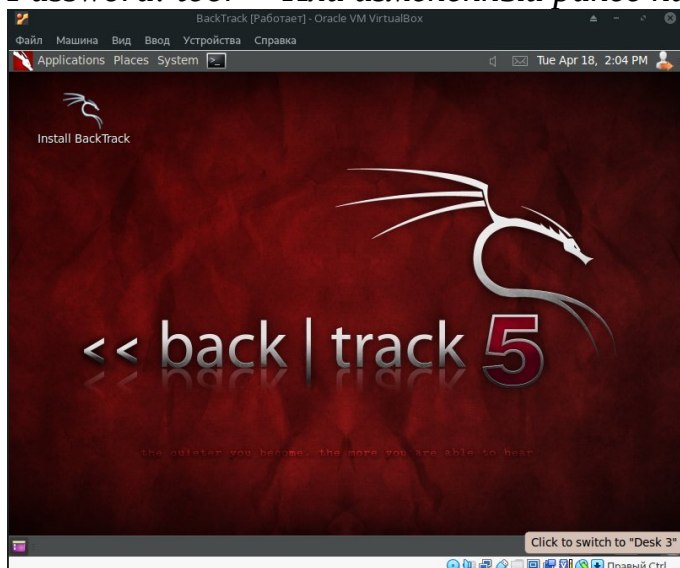


Раздел 5. Вход в BackTrack

Запустите виртуальную машину BackTrack
Войдите в систему

Login: root

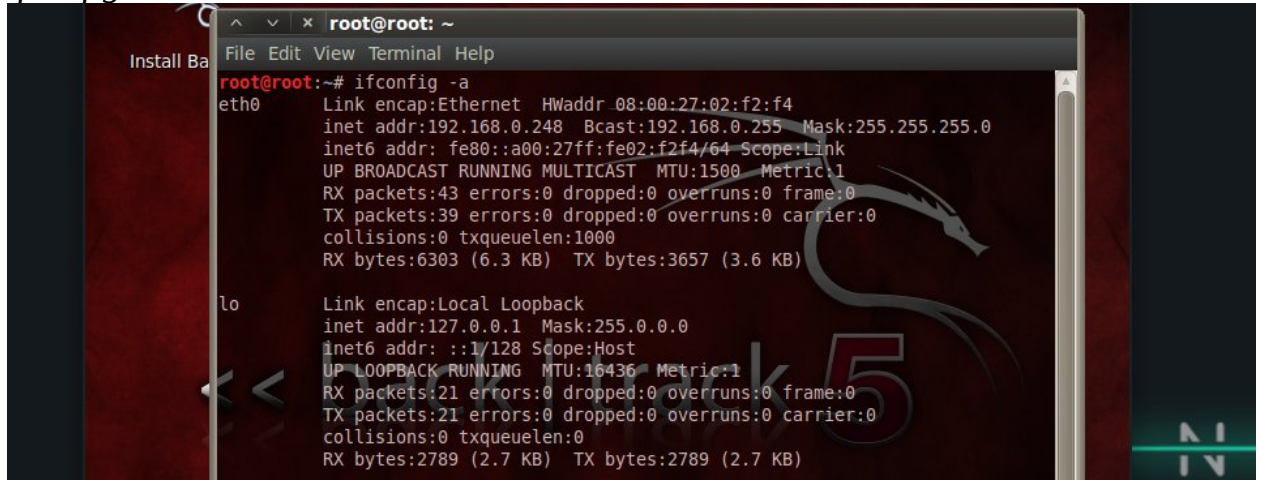
Password: toor <Или измененный ранее пароль>.



Раздел 6. Запуск консоли и определение IP адреса

Откройте терминал

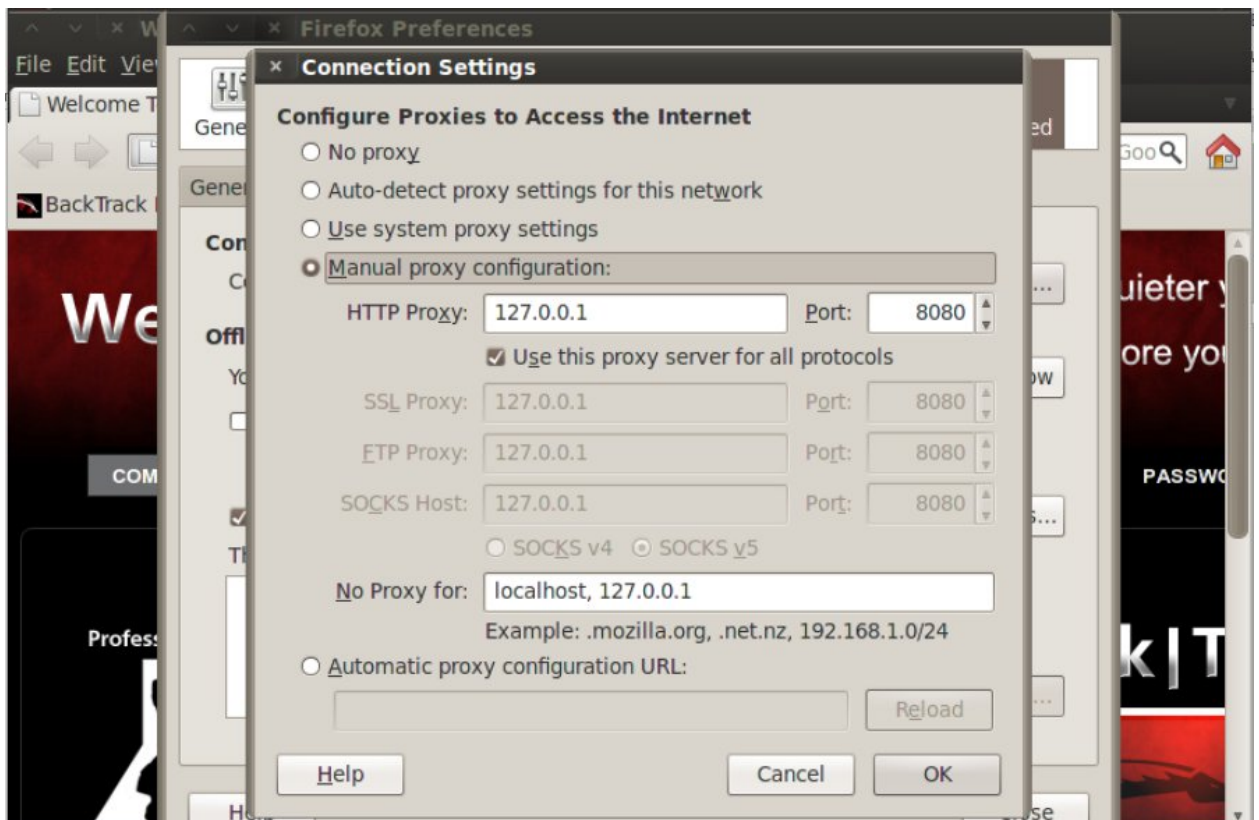
Щелкните на значок консоли в строке быстрого запуска
Определите IP адрес
ifconfig -a



```
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)
```

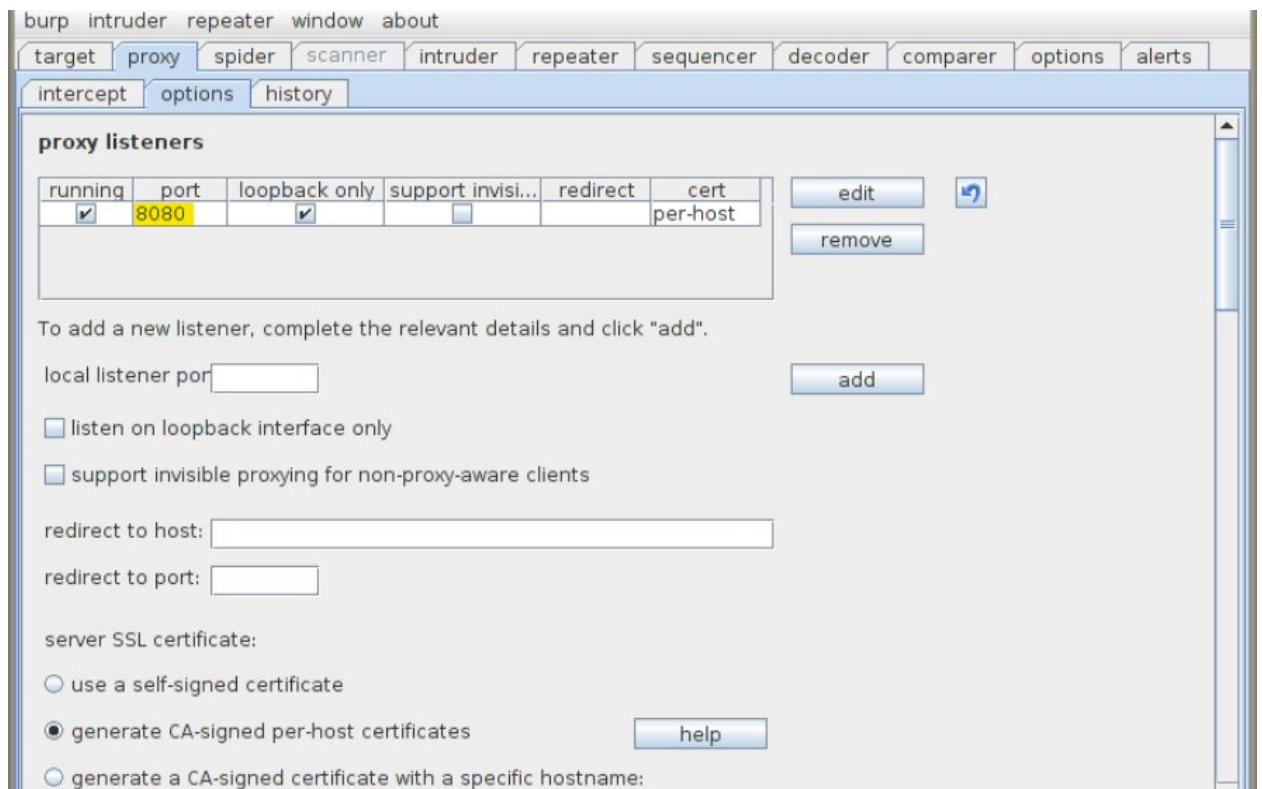
Раздел 7. Конфигурация настроек Firefox Proxy

1. Запустите Firefox
2. Перейдите к настройкам проху
 - a. Edit -> Preferences
 - b. Щелкните на Advanced
 - c. Щелкните на Network Tab (вкладку сеть)
 - d. Щелкните на кнопку настроек
3. Настройте проху
 - 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

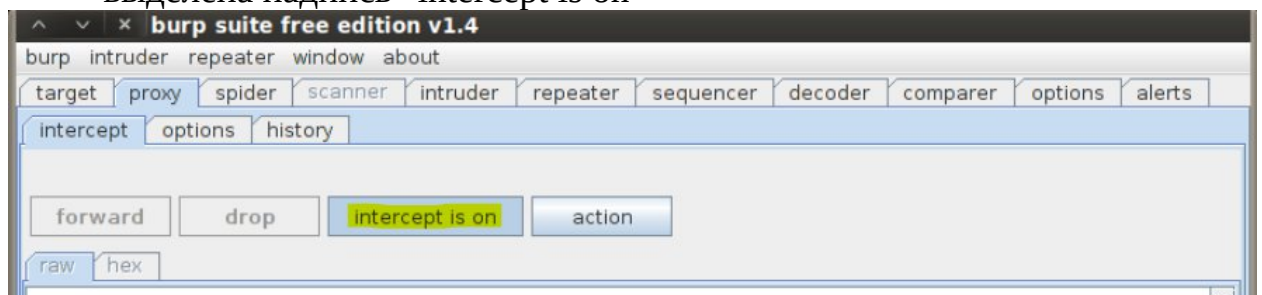


Раздел 8. Конфигурация Burp Suite

1. Запустите Burp Suite
 - a. Applications--> BackTrack --> Vulnerability Assessment --> Web Application Assessment ---> Web Vulnerability Scanner--> burpsuite
 - b. Нажмите ОК в появившемся окне
2. Настройте Проxy в Burp Suite
 - a. Щелкните на вкладку проxy
 - 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"

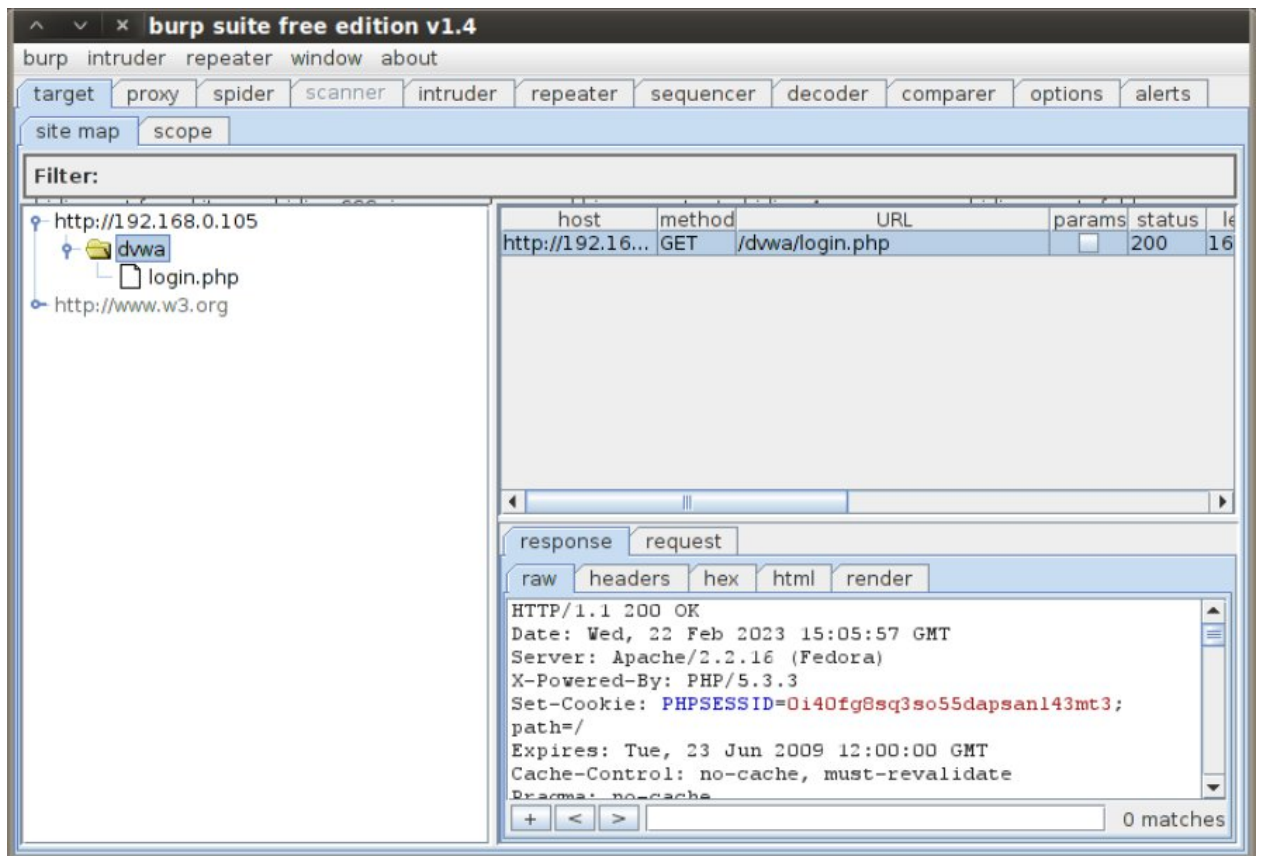


Раздел 9. Разведка с Burp Suite

Войдите в DVWA через Firefox

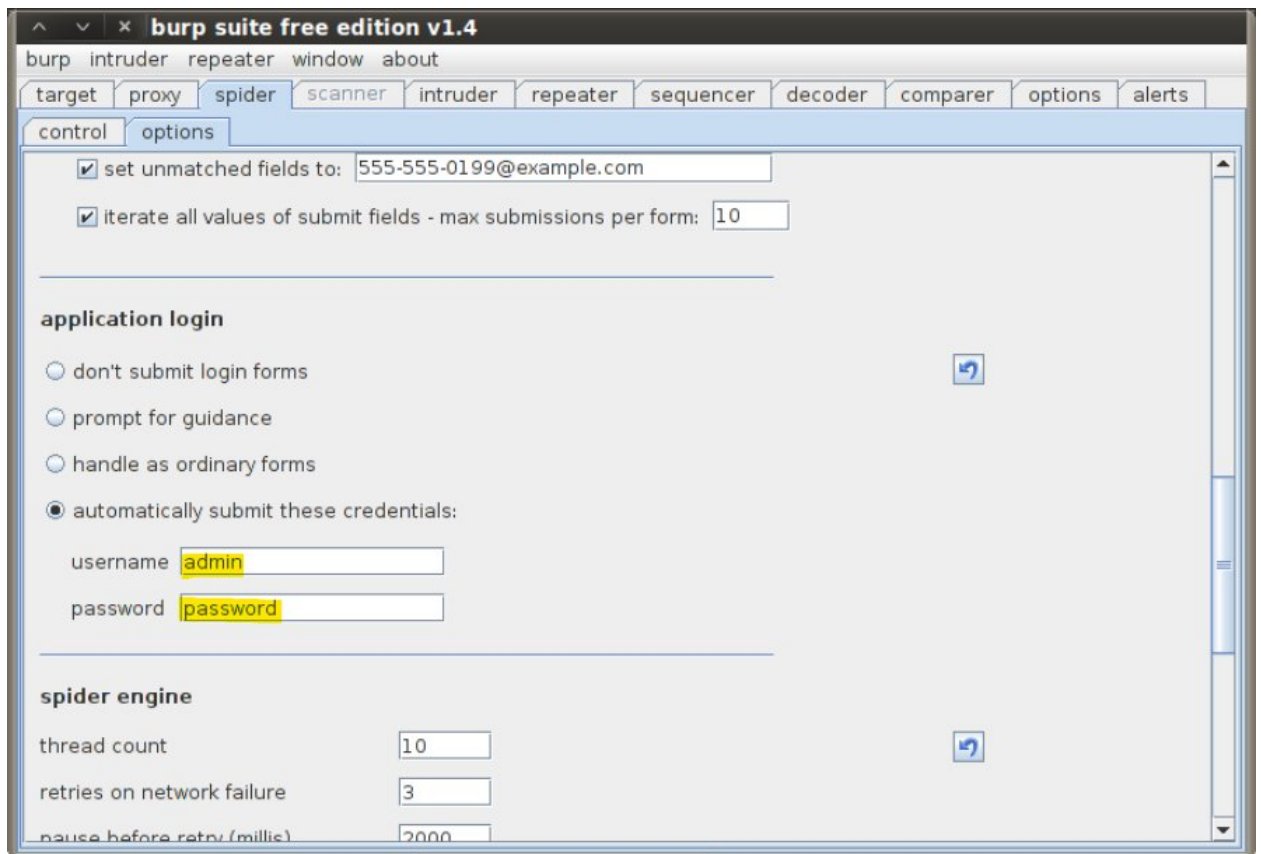
<http://IPADDRESS/dvwa/login.php> (Замените IPADDRESS на ваш ip-адрес)

1. Нацельтесь на хост
 - а. Выберите Targetàsite map

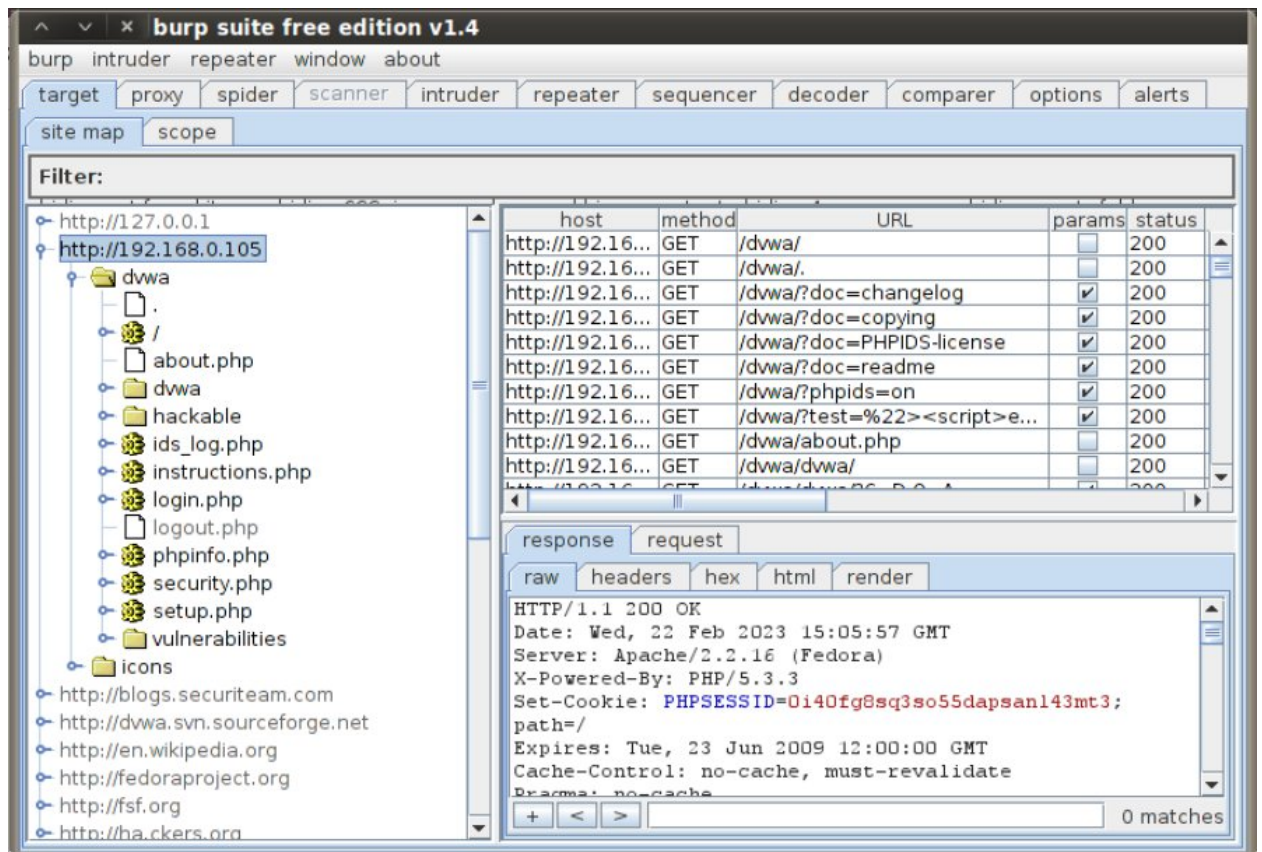


Замечания:

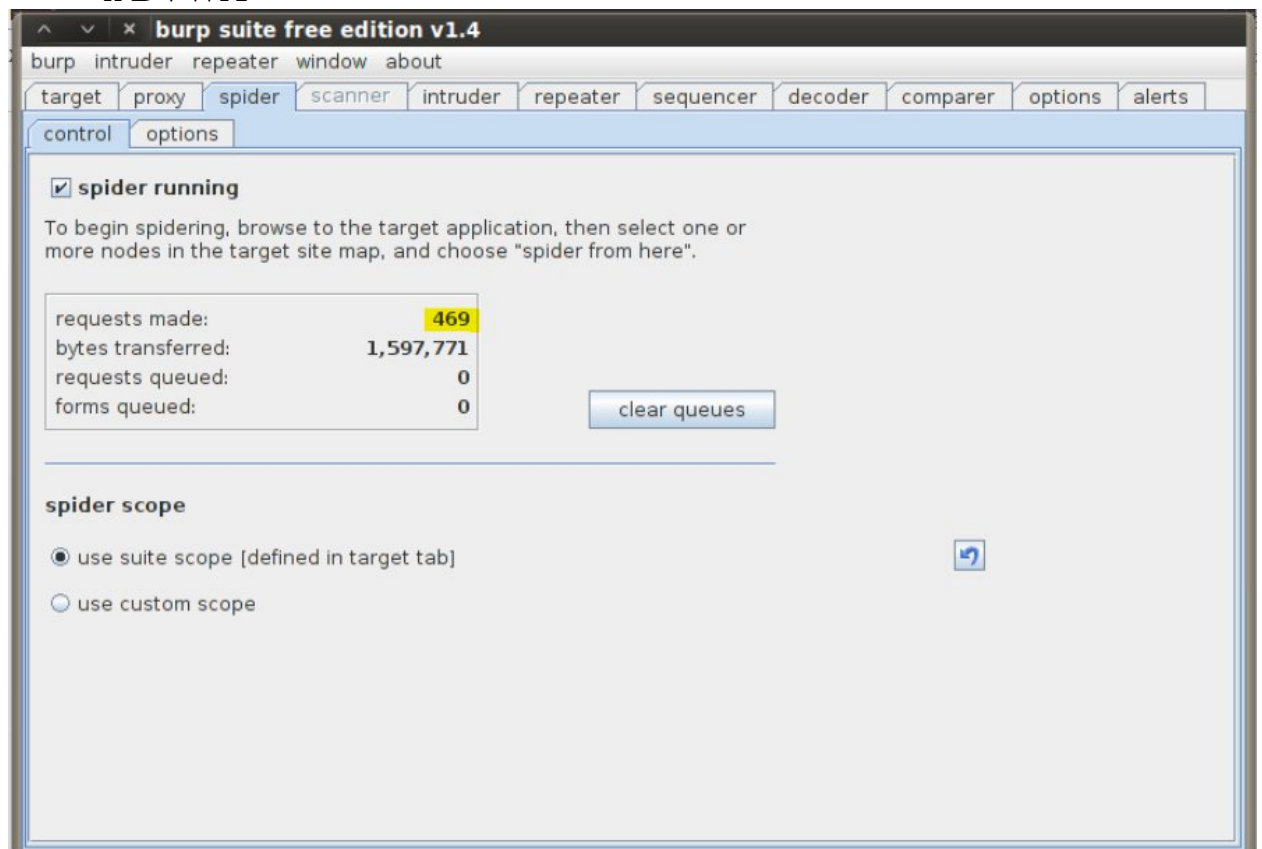
1. Несмотря на то, что перехват отключен, вы можете видеть запросы. Вдобавок, вы можете видеть поля GET-запросов, в том числе PHPSESSID для /dvwa/login.php. Также обратите внимание на создание структуры DVWA для страницы логина
2. Настройте паука
 - a. Выберите spider→options
 - b. Выберите “automatically submit these credentials
 - c. Нажмите “request”
 - d. username: admin
 - e. password: password



3. Исследуйте хост с помощью паука
 - a. Выберите target->site map
 - b. Выберите DVWA IP Address, затем правым кликом мыши вызовите подменю
 - c. Выберите "spider this host"

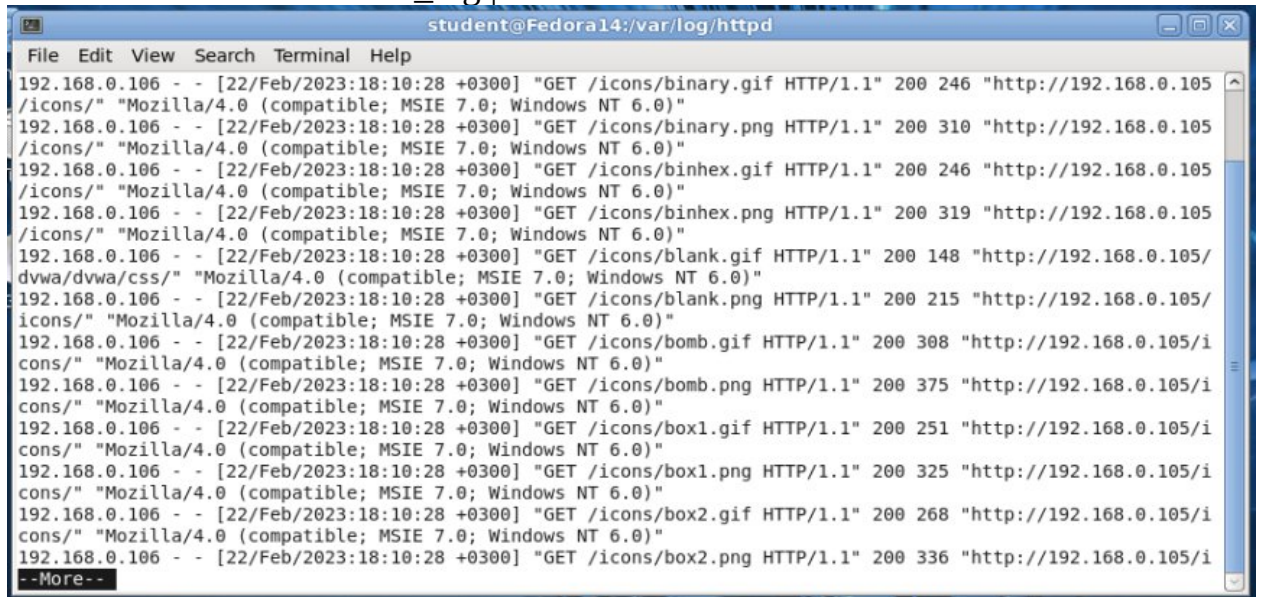


4. Изучите результаты исследования
 - а. Обратите внимание на полную карту сайта DVWA
 - б. Выберите spideràcontrol
 - с. Обратите внимание, было совершено более 460 запросов к DVWA



Раздел 10. Отображение результатов сканирования на веб-сервере

1. Просмотрите журнал доступа Apache'a
 - a. Переключитесь на Fedora 14
 - b. Активируйте консоль
 - c. `su – root`
 - d. `cd /var/log/httpd`
 - e. `tail -400 access_log | more`




```
student@Fedora14:/var/log/httpd
File Edit View Search Terminal Help
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/binary.gif HTTP/1.1" 200 246 "http://192.168.0.105
/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/binary.png HTTP/1.1" 200 310 "http://192.168.0.105
/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/binhex.gif HTTP/1.1" 200 246 "http://192.168.0.105
/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/binhex.png HTTP/1.1" 200 319 "http://192.168.0.105
/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/blank.gif HTTP/1.1" 200 148 "http://192.168.0.105/
dvwa/dvwa/css/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/blank.png HTTP/1.1" 200 215 "http://192.168.0.105/
icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/bomb.gif HTTP/1.1" 200 308 "http://192.168.0.105/i
cons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/bomb.png HTTP/1.1" 200 375 "http://192.168.0.105/i
cons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/box1.gif HTTP/1.1" 200 251 "http://192.168.0.105/i
cons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/box1.png HTTP/1.1" 200 325 "http://192.168.0.105/i
cons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/box2.gif HTTP/1.1" 200 268 "http://192.168.0.105/i
cons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.0.106 - - [22/Feb/2023:18:10:28 +0300] "GET /icons/box2.png HTTP/1.1" 200 336 "http://192.168.0.105/i
cons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
--More--
```

Замечания:

- `tail -400` отображает последние 400 записей журнала доступа
- `more` позволяет удобно просмотреть вывод на экране

2. Просмотрите журнал ошибок Apache'a
 - a. `cd /var/log/httpd`
 - b. `grep `date +%a %b %d` error_log | head`



```
[root@Fedora14 httpd]# grep `date +%a %b %d` error_log | head
grep: Feb: No such file or directory
grep: 22: No such file or directory
error_log:[Wed Feb 22 13:21:55 2023] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
error_log:[Wed Feb 22 13:21:55 2023] [notice] Digest: generating secret for digest authentication ...
error_log:[Wed Feb 22 13:21:55 2023] [notice] Digest: done
error_log:[Wed Feb 22 13:21:55 2023] [notice] Apache/2.2.16 (Unix) DAV/2 PHP/5.3.3 configured -- resuming norm
al operations
error_log:[Wed Feb 22 13:21:55 2023] [warn] ./mod_dnssd.c: No services found to register
error_log:[Wed Feb 22 13:30:57 2023] [error] [client 192.168.0.106] File does not exist: /var/www/html/favicon
.ico
error_log:[Wed Feb 22 13:30:57 2023] [error] [client 192.168.0.106] File does not exist: /var/www/html/favicon
.ico
error_log:[Wed Feb 22 16:15:29 2023] [error] [client 192.168.0.108] File does not exist: /var/www/html/favicon
.ico
error_log:[Wed Feb 22 16:15:29 2023] [error] [client 192.168.0.108] File does not exist: /var/www/html/favicon
.ico
error_log:[Wed Feb 22 18:00:23 2023] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[root@Fedora14 httpd]#
```

Замечания:

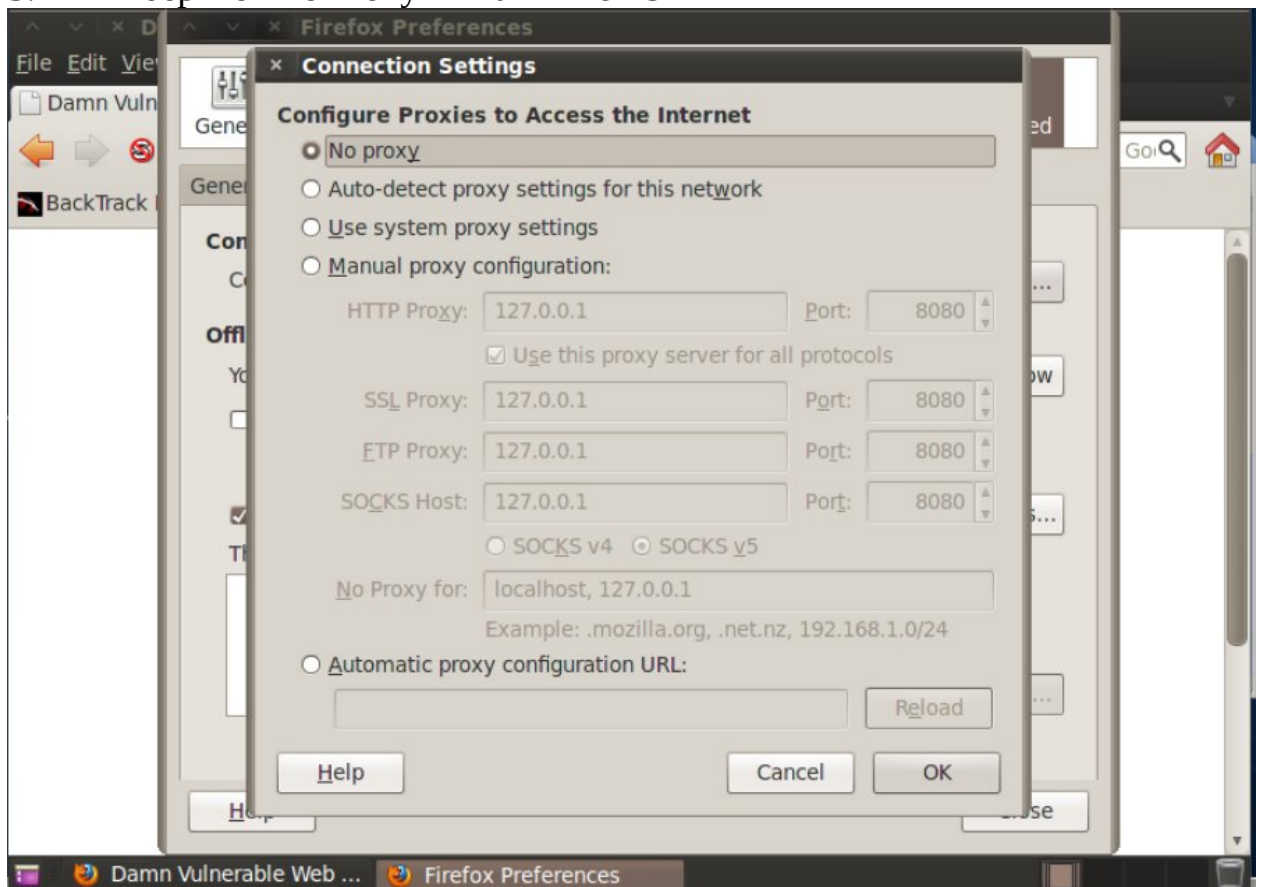
- Важно – ` - апостроф, вводится клавишей ~
- `grep` ищет и выводит строки, соответствующие шаблону
- ``date +%a %b %d`` отображает текущую дату

- error_log – журнал ошибок. данные попадают сюда, когда люди/пауки ищут несуществующие данные либо отправляют в форму подозрительные/бессмысленные инструкции
- head выводит первые 10 строк

3. Обратите внимание, как паук burpsuite ищет несуществующие команды

Раздел 11. Удаление Proxy в BackTrack

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



Раздел 12. Отчет о работе

1. В Backtrack откройте консоль и выполните:
 - a. `cd /var/log/httpd`
 - b. `grep 'date '+%d/%b/%Y'' access_log | wc -l`
wc -l считает, сколько строк нашел grep с сегодняшней датой в журнале доступа
 - c. `date`

```
student@Fedora14:/var/log/httpd
File Edit View Search Terminal Help
[student@Fedora14 ~]$ su root
Password:
[root@Fedora14 student]# cd /var/log/httpd/
[root@Fedora14 httpd]# grep 'date '+%d/%b/%Y' access_log | wc -l
585
[root@Fedora14 httpd]# date
Wed Feb 22 18:22:38 MSK 2023
```