

**Министерство науки и высшего образования Российской
Федерации**
федеральное государственное автономное образовательное
учреждение высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Отчет

по лабораторной работе
«Первичное конфигурирование хоста ОС Linux»

Авторы:

Кулинич Ярослав Вадимович
Кириллова Надежда Сергеевна

Факультет:

ПИИКТ

Группа:

P3213

Преподаватель:

Береснев Артем Дмитриевич



УНИВЕРСИТЕТ ИТМО

Санкт-Петербург 2020

Цель:

Получить практические навыки работы с дополнительными с инструментальными средствами настройки доступа к хосту в ОС Linux.

Необходимые инструменты:

Установленная на компьютере среда виртуализации ORACLE VirtualBox;
Образы виртуальной машины Linux CentOS 7.

Ход работы:

Часть 1. Проверка конфигурации.

1. В работе используются виртуальные машины, сконфигурированные в предыдущей работе. Запустим системы c7-1 и c7-2 и авторизируемся с правами root.
2. Проверьте доступность хостов по внутренней сети и доступность внешней сети на хосте c7-1.

```
[root@c7-1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d4:dc:c8 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global noprefixroute dynamic enp0s3
        valid_lft 86224sec preferred_lft 86224sec
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:21:ff:0e brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/24 brd 10.0.0.255 scope global noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::c91d:1840:ed01/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
[root@c7-1 ~]# nmap 10.0.0.2

Starting Nmap 6.40 ( http://nmap.org ) at 2020-11-25 20:35 MSK
Nmap scan report for 10.0.0.2
Host is up (0.00042s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:D4:DC:C8 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 6.19 seconds
```

3. Убедитесь, что на c7-2 в качестве шлюза по умолчанию задан адрес c7-1.

```
[root@c7-2 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d4:dc:c8 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.2/24 scope global enp0s3
        valid_lft forever preferred_lft forever
```

Часть 2. Создание пользователей и настройка sshd.

1. На хосте c7-2 создаем пользователя с именем KYUser. Заходим на вторую консоль под вашим пользователем.

```
[root@c7-2 ~]# useradd KYUser
[root@c7-2 ~]# passwd KYUser
Изменяется пароль пользователя KYUser.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@c7-2 ~]# su KYUser
[KYUser@c7-2 root]$_
```

2. По системным журналам определите, когда был создан пользователь и когда, он зашел в систему.

По .bash_logout смотрим когда пользователь был создан

```
[KYUser@c7-2 ~]# stat .bash_logout
  файл: «.bash_logout»
  Размер: 18             Блоков: 8             Блок В/В: 4096    обычный файл
Устройство: 803h/2051d  Inode: 70             Ссылки: 1
Доступ: (0644/-rw-r--r--)  Uid: ( 1000/ KYUser)  Gid: ( 1000/ KYUser)
Контекст: unconfined_u:object_r:user_home_t:s0
Доступ: 2020-12-02 16:39:02.544027049 +0300
Модифицирован: 2020-04-01 05:25:23.000000000 +0300
Изменён: 2020-11-25 20:38:46.860434579 +0300
Создан: -
```

Смотрим когда пользователь последний раз зашел в систему

```
[root@c7-2 ~]# lastlog
Пользователь  Порт  C          Последний раз
root          tty1   C          Ср дек  2 17:50:57 +0300 2020
bin                               **Никогда не входил в систему**
daemon        C          **Никогда не входил в систему**
adm           C          **Никогда не входил в систему**
lp            C          **Никогда не входил в систему**
sync          C          **Никогда не входил в систему**
shutdown      C          **Никогда не входил в систему**
halt          C          **Никогда не входил в систему**
mail          C          **Никогда не входил в систему**
operator      C          **Никогда не входил в систему**
games         C          **Никогда не входил в систему**
ftp           C          **Никогда не входил в систему**
nobody        C          **Никогда не входил в систему**
systemd-network C          **Никогда не входил в систему**
dbus          C          **Никогда не входил в систему**
polkitd       C          **Никогда не входил в систему**
sshd          C          **Никогда не входил в систему**
postfix       C          **Никогда не входил в систему**
chrony        C          **Никогда не входил в систему**
KYUser        tty1   C          Ср дек  2 17:41:06 +0300 2020
```

3. Настройте ssh сервер так, чтобы:
 - a. Пользователю root нельзя было бы входить по ssh
 - b. Количество попыток ввода неверного пароля = 2
 - c. Время ожидания авторизации = 30 секундам.

```
[root@c7-2 ~]# nano /etc/ssh/ssh_config
```

```
LoginGraceTime 30
PermitRootLogin no
MaxAuthTries 2
```

4. После перезапуска выведите на консоль состояние сервиса sshd

```
[root@c7-2 ~]# systemctl status sshd
■ sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Cp 2020-11-25 21:05:26 MSK; 20s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 833 (sshd)
      CGroup: /system.slice/ssh.service
              └─833 /usr/sbin/sshd -D

ноя 25 21:05:26 c7-2 systemd[1]: Starting OpenSSH server daemon...
ноя 25 21:05:26 c7-2 sshd[833]: Server listening on 0.0.0.0 port 22.
ноя 25 21:05:26 c7-2 sshd[833]: Server listening on :: port 22.
ноя 25 21:05:26 c7-2 systemd[1]: Started OpenSSH server daemon.
```

5. С машины c7-1 подключусь к c7-2 по ssh, используя новую учетную запись.

```
[root@c7-1 ~]# ssh -p22 KYUser@10.0.0.2
KYUser@10.0.0.2's password:
Last login: Wed Nov 25 20:53:14 2020
[KYUser@c7-2 ~]$_
```

6. На консоли c7-2 с помощью утилиты su входим на консоль root. Добавьте нового пользователя в группу wheel (группа для работы через sudo).

```
[root@c7-1 ~]# ssh -p22 KYUser@10.0.0.2
KYUser@10.0.0.2's password:
Last login: Wed Nov 25 21:22:12 2020 from 10.0.0.1
[KYUser@c7-2 ~]$_ su
Пароль:
[root@c7-2 KYUser]# sudo usermod -a -G wheel KYUser
[root@c7-2 KYUser]# exit
exit
[KYUser@c7-2 ~]$_
```

Проверим, добавился ли наш пользователь

```
[KYUser@c7-2 ~]$_ groups KYUser
KYUser : KYUser wheel
```

7. Чтобы проверить, действительно ли этот пользователь находится в группе суперпользователей - попробую прочитать содержимое файла shadow

```
[KYUser@c7-2 ~]# sudo cat /etc/shadow

Мы полагаем, что ваш системный администратор изложил вам основы
безопасности. Как правило, всё сводится к трём следующим правилам:

#1) Уважайте частную жизнь других.
#2) Думайте, прежде что-то вводить.
#3) С большой властью приходит большая ответственность.

[sudo] пароль для KYUser:
root:$6$z1KmmaUmT3Deri1x$U8cbzWU4cbq jKiDqwHXqJPx6stkgqwMgd9XNyUgmoVWxuPYpxph91AcTf .hrwFSfYcaQ jZUsPzq
tMzUUP.jTve/::0:99999:7:::
bin:!:18353:0:99999:7:::
daemon:!:18353:0:99999:7:::
adm:!:18353:0:99999:7:::
lp:!:18353:0:99999:7:::
sync:!:18353:0:99999:7:::
shutdown:!:18353:0:99999:7:::
halt:!:18353:0:99999:7:::
mail:!:18353:0:99999:7:::
operator:!:18353:0:99999:7:::
games:!:18353:0:99999:7:::
ftp:!:18353:0:99999:7:::
nobody:!:18353:0:99999:7:::
systemd-network:!!:18498:!!!!:
dbus:!!:18498:!!!!:
polkitd:!!:18498:!!!!:
sshd:!!:18498:!!!!:
postfix:!!:18498:!!!!:
chrony:!!:18498:!!!!:
KYUser:$6$4W0G/g6S$01Xkp4IdaryTH.ymW05C5RY0dA4193xT/AZU jP04e IZLTsEUr6MAkF68XSPTc .Qqd3t879Uqv3P2HyZ5
cgiZv0:18591:0:99999:7:::
```

Часть 3. Настройка шлюза

1. Включим на хосте c7-1 пересылку пакетов через ядро с помощью утилиты sysctl. Для этого меняем конфиг:

```
# nano /etc/sysctl.conf
```

```
[root@c7-1 ~]# cat /etc/sysctl.conf
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv6.conf.all.disable_ipv6=1
net.ipv4.ip_forward=1
```

2. С помощью утилиты firewall-cmd настроим с7-1. Для начала посмотрим изначальные настройки:

```
[root@c7-1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- a. Запросы от с7-2 транслировались во внешнюю сеть

```
[root@c7-1 ~]# firewall-cmd --zone=public --add-masquerade
success
```

- b. На порту с номером 55022 внешнего сетевого интерфейса с7-1 был опубликован порт 22 на хосте с7-2

```
[root@c7-1 ~]# firewall-cmd --add-forward-port=port=55022:proto=tcp:toport=22:toaddr=10.0.0.2
success
```

Проверим конфигурацию после изменений:

```
[root@c7-1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: yes
  forward-ports: port=55022:proto=tcp:toport=22:toaddr=10.0.0.2
  source-ports:
  icmp-blocks:
  rich rules:
```


3. Подключитесь к серверу c7-2 с вашей реальной операционной системы (используйте публикацию портов в NAT в VirtualBox или Сетевой Мост).

Настроим проброс портов:

Правила проброса портов					
Имя	Протокол	Адрес хоста	Порт хоста	Адрес гостя	Порт гостя
ssh	TCP		48022	10.0.0.1	22
file	TCP		48100	10.0.0.1	55022

Подключаемся по ssh:

```
C:\Users\Yaroslav>ssh -p 48100 KYVuser@127.0.0.1
The authenticity of host '[127.0.0.1]:48100 ([127.0.0.1]:48100)' can't be established.
ECDSA key fingerprint is SHA256:NfZMxCHdSLMhq0n3eipUKuIHnMTcLOI9KS01LcKxeqo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[127.0.0.1]:48100' (ECDSA) to the list of known hosts.
KYVuser@127.0.0.1's password:
Last login: Wed Dec  2 16:31:36 2020 from 10.0.0.1
Last login: Wed Dec  2 16:31:36 2020 from 10.0.0.1
[KYVuser@c7-2 ~]$
```

4. С помощью команды who выведем список пользователей на хосте c7-2.

```
[KYVuser@c7-2 ~]$ who
root      tty1          2020-12-02 16:26
KYVuser   pts/0         2020-12-02 17:13 (10.0.0.1)
```

Часть 4. Управление процессами

5. На машине c7-2 от имени созданного пользователя запустите редактор vi.

```
[root@c7-2 ~]# su KYVuser
[KYVuser@c7-2 root]# vi test
```

6. На другой консоли, работая от пользователя root определите PID и PPID процесса vi.

```
[root@c7-2 ~]# ps aux | grep vi
root      1205  0.0  0.1  7336  1544 tty1      T   17:14   0:00 vi wow_vi
KYVuser   1248  0.0  0.1  7336  1540 tty1      S+  17:16   0:00 vi test
root      1264  0.0  0.0  6248   940 pts/0    R+  17:18   0:00 grep --color=auto vi
```

7. Завершите процесс используя сигнал безусловного завершения (сигнал KILL).

```
[root@c7-2 ~]# kill -9 1248
```


8. Убедитесь в завершении процесса.

```
[root@c7-2 ~]# ps aux | grep vi
root      1205  0.0  0.1  7336  1544 tty1    T   17:14   0:00 vi wow_vi
root      1266  0.0  0.0   6248   936 pts/0    R+  17:20   0:00 grep --color=auto vi
```

```
disdsd
Убито
[KYUuser@c7-2 root]$_
```

Часть 5. Передача файлов

Передаем тестовый файл

```
[root@c7-1 ~]# scp -p22 I_KILLED_PROCESS KYUuser@10.0.0.2:~/
KYUuser@10.0.0.2's password:
I_KILLED_PROCESS                                100%   0   0.0KB/s   00:00
```

Проверим что он дошел:

```
[KYUuser@c7-2 ~]$_ ls
I_KILLED_PROCESS
```