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»

по дисциплине «**Современные инструменты анализа данных**»

Выполнила:
Пастухова А. А.
Факультет: БИТ
Группа: N3253
Преподаватель:
Береснев А.Д.

Санкт-Петербург, 2021

Часть 1. Проверка конфигурации.

1. В работе используются виртуальные машины, сконфигурированные в предыдущей работе.
2. Запустите системы c7-1 и c7-2, авторизуйтесь с правами root.
3. Проверьте доступность хостов по внутренней сети и доступность внешней сети на хосте c7-1.
4. Убедитесь, что на c7-2 в качестве шлюза по умолчанию задан адрес c7-1.

Часть 2. Создание пользователей и настройка sshd.

1. На хосте c7-2 создайте пользователя с именем FIOuser, где FIO – ваши инициалы**(!)**.

```
[root@c7-2 ~]# adduser AAPuser
[root@c7-2 ~]# who
root     tty1         2021-11-06 08:10
[root@c7-2 ~]# compgen -u
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
operator
games
ftp
nobody
systemd-network
dbus
polkitd
sshd
postfix
chrony
artem
AAPuser
[root@c7-2 ~]#
```

2. Зайдите на вторую консоль под вашим пользователем.

```
[root@c7-2 ~]# ssh AAPuser@10.0.0.2
AAPuser@10.0.0.2's password:
Last failed login: Sat Nov  6 08:37:55 EDT 2021 from c7-2 on ssh:notty
There was 1 failed login attempt since the last successful login.
[AAPuser@c7-2 ~]$
```

По системным журналам определите, когда был создан пользователь и когда, он зашел в систему. **(!)**.

```
[AAPuser@c7-2 ~]$ last -4
AAPuser  pts/0        c7-2             Sat Nov  6 08:47   still logged in
root     tty1                          Sat Nov  6 08:10   still logged in
reboot   system boot  3.10.0-1160.41.1 Sat Nov  6 08:10 - 08:50  (00:39)
root     pts/0        c7-2             Fri Nov  5 18:16 - down   (03:31)

wtmp begins Tue Sep 29 15:18:34 2020
[AAPuser@c7-2 ~]$
```

```
[AAPuser@c7-2 ~]$ sudo cat /var/log/messages | grep AAPuser
[sudo] password for AAPuser:
Nov 23 09:43:07 c7-2 systemd: Removed slice User Slice of AAPuser.
Nov 23 09:49:00 c7-2 systemd: Created slice User Slice of AAPuser.
Nov 23 09:49:00 c7-2 systemd: Started Session 4 of user AAPuser.
Nov 23 09:49:00 c7-2 systemd-logind: New session 4 of user AAPuser.
```

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.

Изменить строки в каталоге /etc/ssh/sshd_config

```
# Authentication:

LoginGraceTime 30
PermitRootLogin no
#StrictModes yes
MaxAuthTries 2
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys
-- INSERT --
```

4. После перезапуска выведите на консоль состояние сервиса sshd и его журнал средствами systemd **(!)**.

```
[MBYuser@c7-2 ~]$ systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-11-23 08:18:50 EST; 3min 55s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 935 (sshd)
   CGroup: /system.slice/sshd.service
           └─935 /usr/sbin/sshd -D

Nov 23 08:18:50 c7-2 systemd[1]: Starting OpenSSH server daemon...
Nov 23 08:18:50 c7-2 sshd[935]: Server listening on 0.0.0.0 port 22.
Nov 23 08:18:50 c7-2 sshd[935]: Server listening on :: port 22.
Nov 23 08:18:50 c7-2 systemd[1]: Started OpenSSH server daemon.
```

5. С машины c7-1 подключитесь к c7-2 по ssh, используя новую учетную запись.
6. На консоли c7-2 с помощью утилиты su войдите на консоль root.

```
[AAPuser@c7-2 ~]$ su root
Password:
[root@c7-2 AAPuser]# _
```

7. Добавьте нового пользователя в группу wheel (группа для работы через sudo). **(!)**.

```
[root@c7-2 ~]# gpasswd -a AAPuser wheel
Adding user AAPuser to group wheel
[root@c7-2 ~]#
```

8. Выйдете из консоли root. От имени нового пользователя проверьте доступность по чтению файла с паролями пользователей без использования утилиты sudo и с ней.

```
[AAPuser@c7-2 ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
[AAPuser@c7-2 ~]$ sudo cat /etc/shadow
root:$6$at1iBpPUi/Khm02c$jecHS/qjLHKegsITQ89jlV8UVRV/T0bHdCeamjRuHqQzvXeXAWsTOpHOCyU4Iu
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:!!:18534::::::
dbus:!!:18534::::::
polkitd:!!:18534::::::
sshd:!!:18534::::::
postfix:!!:18534::::::
chrony:!!:18534::::::
artem:$6$7z4Fuc.04n/6M$Qs.vEk5bJGayU4ZM6M0FGT.Dg2rTGcCDf6ZJxUG6Vf95/4StsGNbBtuArroLil4Z
AAPuser:$6$ORAXOKN9$31eXwonj/kKsmPZP5Nb8ywNU13th0UPe4O.0CQ/2.rYrPC1kxk5GgNiAxF8Waipp8ul
[AAPuser@c7-2 ~]$
```

Часть 3. Настройка шлюза

Цель этой части – настроить хост c7-1 как шлюз доступа к хосту c7-2. **(!)**.

1. Включите на хосте c7-1 пересылку пакетов через ядро с помощью утилиты sysctl. **(!)**

```
[root@c7-1 ~]# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[root@c7-1 ~]#
```

2. С помощью утилиты firewall-cmd настройте c7-1 так, чтобы:
    a. Запросы от c7-2 транслировались во внешнюю сеть
    b. На порту с номером 55022 внешнего сетевого интерфейса c7-1 был опубликован порт 22 на хосте c7-2.

```
[root@c7-1 ~]# firewall-cmd --zone=internal --add-interface=enp38
success
[root@c7-1 ~]# firewall-cmd --get-active-zones
internal
  interfaces: enp38
public
  interfaces: enp0s3 enp0s8 enp33
[root@c7-1 ~]#
```

3. Подключитесь к серверу c7-2 с вашей реальной операционной

системы (используйте публикацию портов в NAT в VirtualBox или Сетевой Мост).

```
C:\Users\caxarok>ssh -p 48023 AAPuser@127.0.0.4
AAPuser@127.0.0.4's password:
Last login: Tue Nov 23 10:03:35 2021 from c7-2
[AAPuser@c7-2 ~]$ who
root     tty1         2021-11-23 09:57
AAPuser  pts/0        2021-11-23 10:03 (c7-2)
AAPuser  pts/1        2021-11-23 10:24 (10.0.2.2)
[AAPuser@c7-2 ~]$
```

4. С помощью команды who выведите список пользователей на хосте c7-2. **(!)**

Часть 4. Управление процессами

1. На машине c7-2 от имени созданного пользователя запустите редактор vi.
2. На другой консоли, работая от пользователя root определите PID и PPID процесса vi. **(!)**

   ps -eF | grep vi (PID – 2, PPID – 3)
3. Завершите процесс используя сигнал безусловного завершения (сигнал KILL). **(!)**
4. Убедитесь в завершении процесса.

Часть 5. Передача файлов

1. Используя SSH передайте на машину c7-2 любой файл. Это можно сделать с помощью утилиты scp на Linux и утилиты pscp из комплекта утилиты Putty на Windows **(!).**

   pscp -P 55022 lil.txt AAPuser@10.0.0.2:/ home/AAPuser/

Вопросы и задания:

1. Опишите, как вы проверили доступность машин в части 1.

2. Напишите конвейер команд, или команду или скрипт, позволяющий создать пользователя, сразу указав его пароль.
3. Поясните результаты выполнения п.9 Части 2.
4. В части 4 вы завершили процесс сигналом KILL. Почему это плохой способ завершения процесса?