

## Задание №1

**Потоки ввода/вывода.** Создать файл, используя команду `echo`. Используя команду `cat`, прочитать содержимое каталога `etc`, ошибки перенаправить в отдельный файл.

```
vlad@test-server:~$ echo 1> error.txt
vlad@test-server:~$ ls
error.txt  test
vlad@test-server:~$ cat error.txt

vlad@test-server:~$ cat /etc 2> error.txt
vlad@test-server:~$ cat error.txt
cat: /etc: Is a directory
vlad@test-server:~$
```

## Задание №2

**Конвейер (pipeline).** Использовать команду `cut` на вывод длинного списка каталога, чтобы отобразить только права доступа к файлам. Затем отправить в конвейере этот вывод на `sort` и `uniq`, чтобы отфильтровать все повторяющиеся строки.

[illegible]

## Задание №3

**Управление процессами.** Изменить конфигурационный файл службы SSH: /etc/ssh/sshd\_config, отключив аутентификацию по паролю PasswordAuthentication no. Выполните рестарт службы systemctl restart sshd (service sshd restart), верните аутентификацию по паролю, выполните reload службы systemctl reload sshd (service sshd reload). В чём различие между действиями restart и reload?

```
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication no

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

#allowAgentForwarding yes
#allowTcpForwarding yes
#GatewayPorts no
#X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
```

```
viad@test-server:~$ sudo nano /etc/ssh/sshd_config
viad@test-server:~$ systemctl restart sshd
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'ssh.service'.
Multiple identities can be used for authentication:
 1. viad
 2. Super Duper User,9876548,6484,4 (superuser)
Choose identity to authenticate as (1-2): 1
Password:
==== AUTHENTICATION COMPLETE ====
viad@test-server:~$ sudo nano /etc/ssh/sshd_config
GNU nano 4.8 /etc/ssh/sshd.config
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

#allowAgentForwarding yes
#allowTcpForwarding yes
#GatewayPorts no
#X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
```

```

vlad@test-server:~$ sudo nano /etc/ssh/sshd_config
vlad@test-server:~$ systemctl restart sshd
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units =====
Authentication is required to restart 'ssh.service'.
Multiple identities can be used for authentication:
 1. vlad
 2. Super Duper User,9876548,6484,4 (superuser)
Choose identity to authenticate as (1-2): 1
Password:
===== AUTHENTICATION COMPLETE =====
vlad@test-server:~$ sudo nano /etc/ssh/sshd_config
vlad@test-server:~$ systemctl reload sshd
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units =====
Authentication is required to reload 'ssh.service'.
Multiple identities can be used for authentication:
 1. vlad
 2. Super Duper User,9876548,6484,4 (superuser)
Choose identity to authenticate as (1-2): 1
Password:
===== AUTHENTICATION COMPLETE =====
vlad@test-server:~$

```

**Restart** – перезапускает службу т.е. останавливает и запускает.

**Reload** – перечитывает файлы конфы, без остановки процесса.

## Задание №4

**Сигналы процессам.** Запустите `nc`. Используя `ps`, найдите PID процесса, завершите процесс, передав ему сигнал 9.

```

2127 pts/2      00:00:00 sensible-editor
2150 pts/2      00:00:00 nano
2173 pts/2      00:00:00 ps
vlad@test-server:~$ kill -9 2150

```

```

2150 pts/2      00:00:00 nano <defunct>
2174 pts/2      00:00:00 ps
vlad@test-server:~$

```