

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение  
высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»  
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

**Обеспечение безопасности в среде операционной системы Linux**

Отчет по лабораторной работе 9

по дисциплине «**Системное программное обеспечение**»

студента 3 курса группы ИВТ-б-о-202

Шор Константина Александровича

Направления подготовки 09.03.01 «Информатика и вычислительная техника»

Симферополь, 2023

## Лабораторная работа №9. Обеспечение безопасности в среде операционной системы Linux

Цель работы: Получение навыков конфигурации параметров безопасности

### 1. Добавления пользователя в sudo

```
user_test@kali: /home
File Actions Edit View Help
(kali@kali)-[/home]
$ su user_test
Password:
$ /bin/bash
(user_test@kali)-[/home]
$ tcpdump
tcpdump: eth0: You don't have permission to perform this capture on that device
(socket: Operation not permitted)

(user_test@kali)-[/home]
$ sudo tcpdump
[sudo] password for user_test:
user_test is not in the sudoers file.

(user_test@kali)-[/home]
$
```

```
root@kali: /home
File Actions Edit View Help
GNU nano 7.2 /etc/sudoers
# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

```
(kali㉿kali)-[/home]
$ sudo usermod -a -G sudo user_test

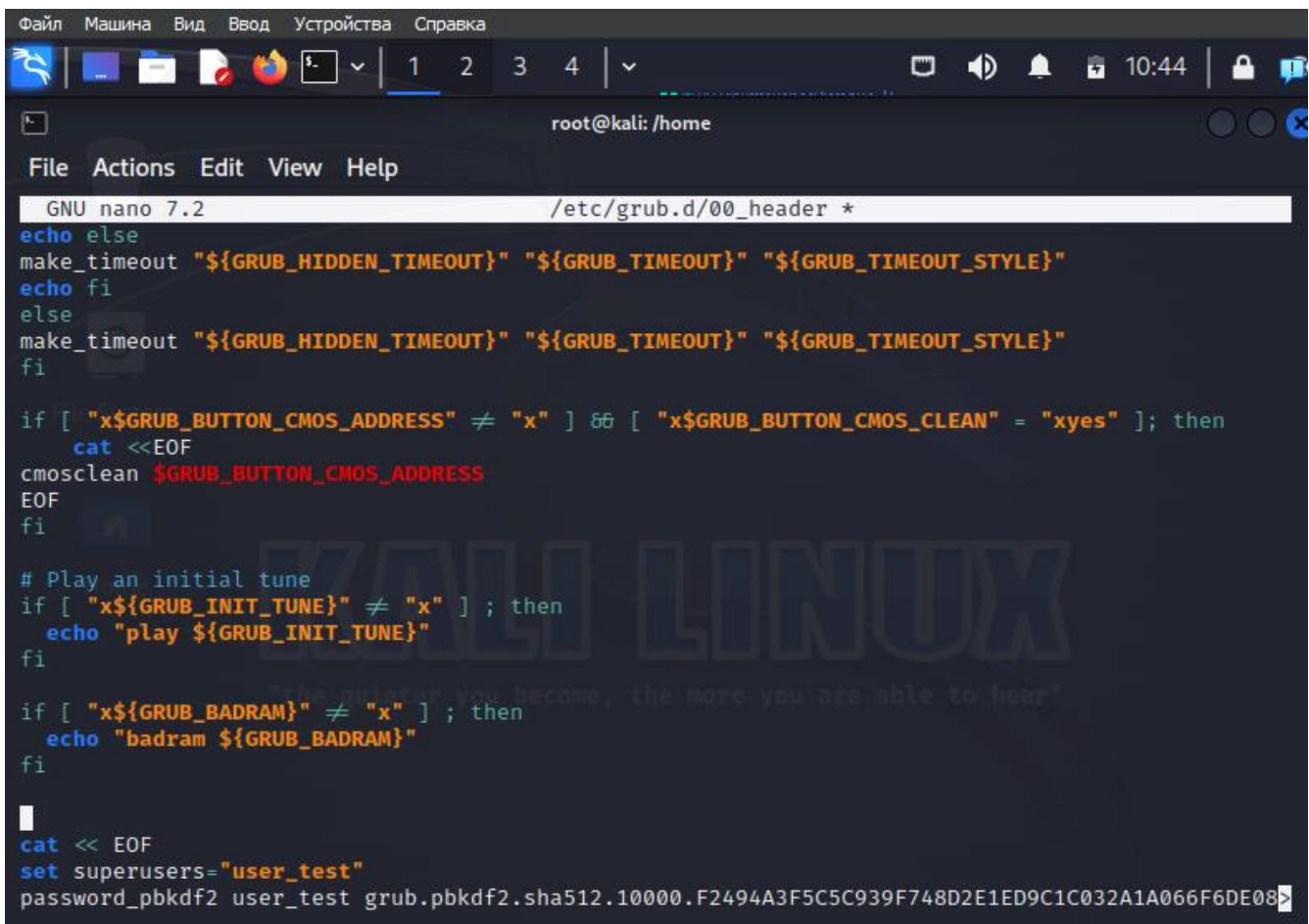
(kali㉿kali)-[/home]
$ su user_test
Password:
$ /bin/bash
(user_test㉿kali)-[/home]
$ sudo tcpdump
[sudo] password for user_test:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^[[A^[[A^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

(user_test㉿kali)-[/home]
$ sudo tcpdump -A
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
09:53:41.763110 IP 10.0.2.15.51955 > 192.168.1.1.domain: 53918+ A? contile.services.mozilla.com.
(46)
E..JD9@.@.(.
.....5.6.....contile.services.mozilla.com.....
09:53:41.763145 IP 10.0.2.15.51955 > 192.168.1.1.domain: 41368+ AAAA? contile.services.mozilla.c
om. (46)
E..JD:@.@.(.
.....5.6.....contile.services.mozilla.com.....
09:53:41.767792 IP 192.168.1.1.domain > 10.0.2.15.51955: 53918 1/13/13 A 34.117.237.239 (494)
E..
5 @
```

## 2. Установка пароля на grub

```
(root@kali)-[/home]
# grub-mkpasswd-pbkdf2
Enter password:
Reenter password:
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.F2494A3F5C5C93
6DE086AF7C5B5A907797960228D9139AE67172B19368ABEDFE821FCAF988C49D7B25CD6
185DDBA2BB4F680D7EB02BF452D5C159B54BEC7BDD2605B6A309A05791F7294AFB8E13A
9F29757E9AE26F665D0FA1243A
```

### Test



```
Файл  Машина  Вид  Ввод  Устройства  Справка
root@kali: /home
File  Actions  Edit  View  Help
GNU nano 7.2 /etc/grub.d/00_header *
echo else
make_timeout "${GRUB_HIDDEN_TIMEOUT}" "${GRUB_TIMEOUT}" "${GRUB_TIMEOUT_STYLE}"
echo fi
else
make_timeout "${GRUB_HIDDEN_TIMEOUT}" "${GRUB_TIMEOUT}" "${GRUB_TIMEOUT_STYLE}"
fi

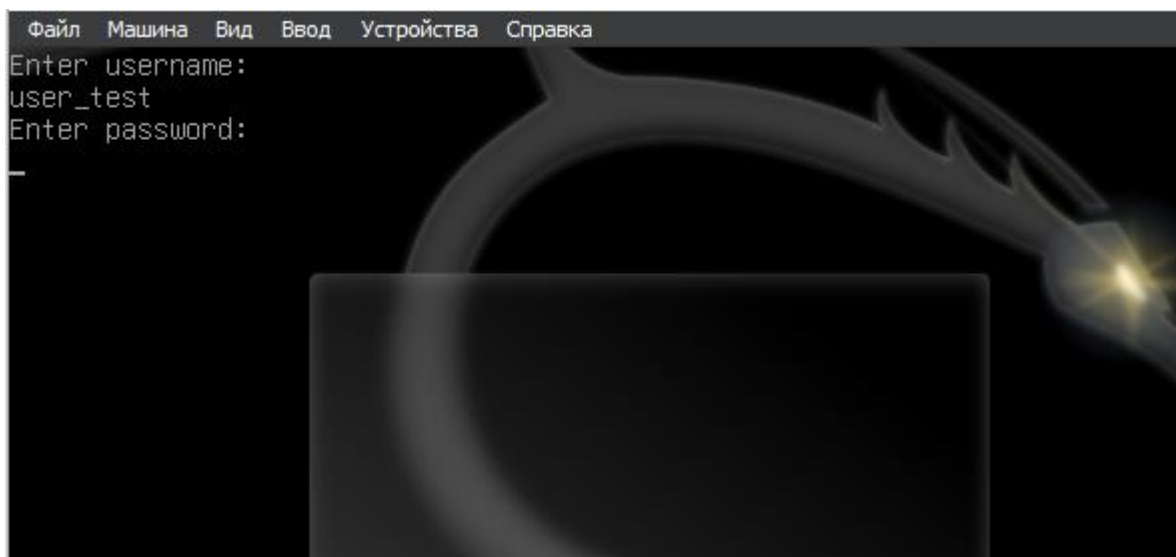
if [ "x${GRUB_BUTTON_CMOS_ADDRESS}" != "x" ] && [ "x${GRUB_BUTTON_CMOS_CLEAN}" = "xyes" ]; then
    cat <<EOF
cmosclean ${GRUB_BUTTON_CMOS_ADDRESS}
EOF
fi

# Play an initial tune
if [ "x${GRUB_INIT_TUNE}" != "x" ] ; then
    echo "play ${GRUB_INIT_TUNE}"
fi

if [ "x${GRUB_BADRAM}" != "x" ] ; then
    echo "badram ${GRUB_BADRAM}"
fi

cat << EOF
set superusers="user_test"
password_pbkdf2 user_test grub.pbkdf2.sha512.10000.F2494A3F5C5C939F748D2E1ED9C1C032A1A066F6DE08
```

```
(root@kali)-[/home]
# update-grub
Generating grub configuration file ...
Found theme: /boot/grub/themes/kali/theme.txt
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.1.0-kali5-amd64
Found initrd image: /boot/initrd.img-6.1.0-kali5-amd64
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
```



### 3. Selinux

#### Скачивание

```
root@kali: /home
File Actions Edit View Help
(root@kali)-[/home]
# apt update
Hit:1 http://fastmirror.pp.ua/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
561 packages can be upgraded. Run 'apt list --upgradable' to see them.

(root@kali)-[/home]
# apt install policycoreutils selinux-utils selinux-basics
```



## Активация

```
(root@kali)-[/home]
# sestatus
SELinux status:                disabled

(root@kali)-[/home]
# selinux-activate
Activating SE Linux
Generating grub configuration file ...
Found theme: /boot/grub/themes/kali/theme.txt
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.1.0-kali5-amd64
Found initrd image: /boot/initrd.img-6.1.0-kali5-amd64
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
SE Linux is activated.  You may need to reboot now.
```

```
(kali@kali)-[~]
$ sestatus
SELinux status:                enabled
SELinuxfs mount:               /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            default
Current mode:                  permissive
Mode from config file:         permissive
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
```

User	Role	Domain	X Window System	su or sudo	Execute in home directory and /tmp (default)	Networking
sysadm_u	sysadm_r	sysadm_t	yes	su and sudo	yes	yes
staff_u	staff_r	staff_t	yes	only sudo	yes	yes
user_u	user_r	user_t	yes	no	yes	yes
guest_u	guest_r	guest_t	no	no	yes	no
xguest_u	xguest_r	xguest_t	yes	no	yes	Firefox only

## Создание пользователя и добавление в selinux

```
(kali㉿kali)-[~]
$ sudo useradd -Z user_u user
[libsemanage]: user sddm not in password file

(kali㉿kali)-[~]
$ passwd user
passwd: You may not view or modify password information for user.

(kali㉿kali)-[~]
$ sudo passwd user
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~]
$ sudo semanage login -l
```

Login Name	SELinux User	MLS/MCS Range	Service
__default__	unconfined_u	s0-s0:c0.c1023	*
root	unconfined_u	s0-s0:c0.c1023	*
sddm	xdm	s0-s0	*
user	user_u	s0	*

```
(kali㉿kali)-[~]
$
```

## Настройка доступа

```
(kali㉿kali)-[~]
$ ls -Z /home/kali/test_file.txt
unconfined_u:object_r:user_home_t:s0 /home/kali/test_file.txt

(kali㉿kali)-[~]
$ sudo chcon -t samba_share_t /home/kali/test_file.txt
[sudo] password for kali:

(kali㉿kali)-[~]
$ ls -Z /home/kali/test_file.txt
unconfined_u:object_r:samba_share_t:s0 /home/kali/test_file.txt
```



Доступ к файлу ограничен

```
(kali㉿kali)-[~]  
$ su user_test  
Password:  
$ /bin/bash  
(user_test㉿kali)-[/home/kali]  
$ ls  
ls: cannot open directory '.': Permission denied  
  
(user_test㉿kali)-[/home/kali]  
$
```

Восстановление

```
(kali㉿kali)-[~]  
$ ls -Z /home/kali/test_file.txt  
unconfined_u:object_r:samba_share_t:s0 /home/kali/test_file.txt  
  
(kali㉿kali)-[~]  
$ sudo restorecon -v /home/kali/test_file.txt  
Relabeled /home/kali/test_file.txt from unconfined_u:object_r:samba_share_t:s0 to unconfined_u:object_r:user_home_t:s0  
  
(kali㉿kali)-[~]  
$ ls -Z /home/kali/test_file.txt  
unconfined_u:object_r:user_home_t:s0 /home/kali/test_file.txt
```

#### 4. Logwatch

```
(kali㉿kali)-[~]  
$ sudo cp /usr/share/logwatch/dist.conf/logwatch.conf /etc/logwatch/conf  
[sudo] password for kali:
```

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/logwatch/conf/logwatch.conf  
mailer = "/usr/sbin/sendmail -t"  
TmpDir = /tmp  
Encode = none  
MailFrom = root  
Detail = High  
MailTo = test_mailos@mail.ru  
MailFrom = Logwatch-myservername  
Archives = Yes  
Range = yesterday  
Print = No  
Service = All
```

```
(kali㉿kali)-[~]  
$ cat /etc/cron.daily/*logwatch  
#!/bin/bash  
  
#Check if removed-but-not-purged  
test -x /usr/share/logwatch/scripts/logwatch.pl || exit 0  
  
#execute  
/usr/sbin/logwatch --mailto test_mailos@mail.ru  
  
#Note: It's possible to force the recipient in above command  
#Just pass --mailto address@a.com instead of --output mail
```

```
(kali㉿kali)-[~]  
$ ls -al /etc/cron.daily | grep logwatch  
-rwxr-xr-x. 1 root root 283 May 29 14:54 00logwatch
```

```
(kali㉿kali)-[~]  
$ /usr/sbin/logwatch
```

```
##### Logwatch 7.7 (07/22/22) #####
```

```
Processing Initiated: Mon May 29 15:09:20 2023
```

```
Date Range Processed: yesterday  
                      ( 2023-May-28 )  
                      Period is day.
```

```
Detail Level of Output: 10
```

```
Type of Output/Format: stdout / text
```

```
Logfiles for Host: kali
```

```
#####
```

```
----- Disk Space Begin -----
```

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	79G	14G	61G	18%	/

```
----- Disk Space End -----
```

```
----- lm_sensors output Begin -----
```

```
BAT0-acpi-0  
Adapter: ACPI interface  
in0:      10.00 V
```

```
----- lm_sensors output End -----
```

```
##### Logwatch End #####
```

```
(kali㉿kali)-[~]
$ sudo dpkg-reconfigure postfix logwatch /etc/cron.daily/00logwatch
setting synchronous mail queue updates: false

mailname is not a fully qualified domain name. Not changing /etc/mailname.
setting destinations: kali, kali, localhost.localdomain, , localhost
setting relayhost:
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
setting mailbox_size_limit: 0
setting recipient_delimiter: +
setting inet_interfaces: all
setting inet_protocols: all
WARNING: /etc/aliases exists, but does not have a root alias.

Postfix (main.cf) is now set up with the changes above. If you need to make
changes, edit /etc/postfix/main.cf (and others) as needed. To view Postfix
configuration values, see postconf(1).

After modifying main.cf, be sure to run 'systemctl reload postfix'.

Running newaliases
postfix.service is a disabled or a static unit, not starting it.
dpkg-query: error: --status needs a valid package name but '/etc/cron.daily/00logwatch' is not:
illegal package name in specifier '/etc/cron.daily/00logwatch': must start with an alphanumeric
character

Use --help for help about querying packages.
/usr/sbin/dpkg-reconfigure: /etc/cron.daily/00logwatch is not installed
```

## 5. SSH

```
GNU nano 7.2 /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr
# The strategy used for options in the default sshd_config shipped w
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override t
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 6622
PermitRootLogin no
```

```

(kali㉿kali)-[~]
$ sudo systemctl restart ssh.service

(kali㉿kali)-[~]
$ sudo systemctl status ssh.service
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Tue 2023-05-30 02:45:11 EDT; 8s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 4094 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 4095 (sshd)
    Tasks: 1 (limit: 2271)
   Memory: 2.8M
      CPU: 31ms
   CGroup: /system.slice/ssh.service
           └─4095 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 30 02:45:11 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
May 30 02:45:11 kali sshd[4095]: Server listening on 0.0.0.0 port 6622.
May 30 02:45:11 kali sshd[4095]: Server listening on :: port 6622.
May 30 02:45:11 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

(kali㉿kali)-[~]
$ sudo systemctl enable ssh.service
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-insta
ll.
Executing: /lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ss
h.service.

(kali㉿kali)-[~]
$ █

```

```

(kali㉿kali)-[~]
$ sudo systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: disabled)
   Active: active (running) since Tue 2023-05-30 02:45:11 EDT; 59s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 4095 (sshd)
    Tasks: 1 (limit: 2271)
   Memory: 2.8M
      CPU: 31ms
   CGroup: /system.slice/ssh.service
           └─4095 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 30 02:45:11 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
May 30 02:45:11 kali sshd[4095]: Server listening on 0.0.0.0 port 6622.
May 30 02:45:11 kali sshd[4095]: Server listening on :: port 6622.
May 30 02:45:11 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

```



```
(kali㉿kali)-[~]  
$ ssh 127.0.0.1 -p 6622  
The authenticity of host '[127.0.0.1]:6622 ([127.0.0.1]:6622)' can't be established.  
ED25519 key fingerprint is SHA256:t/dfgPNKQrQtJ/Vhf51LZLnrXi0l/f2lry8rHVPizM4.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '[127.0.0.1]:6622' (ED25519) to the list of known hosts.  
kali@127.0.0.1's password:  
Linux kali 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23) x86_64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
(kali㉿kali)-[~]  
$ exit  
Connection to 127.0.0.1 closed.
```

## 6. Ключ ssh

```
GNU nano 7.2 /etc/ssh/sshd_config *
#MaxSessions 10

PubkeyAuthentication yes

# 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 yes
```

### Создание ключа

```
(kali㉿kali)-[~]
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:nSNK3lYFQ4oK2NM1f3JBnCNS1oNVioVOAaQ1P2pJp8Q kali㉿kali
The key's randomart image is:
+--[RSA 3072]--+
|   .Bo+X0o.   |
| o . =.B=+*=  |
| . + o E+0.+o. |
|   o + =.* o   |
|   . * S =     |
|   + o o .     |
|   o o         |
|   .           |
+--[SHA256]--+
```

## Перенос ключа

```
(kali㉿kali)-[~]
$ ssh-copy-id -p 6622 user_test@127.0.0.1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/kali/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to
install the new keys
user_test@127.0.0.1's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -p '6622' 'user_test@127.0.0.1'"
and check to make sure that only the key(s) you wanted were added.

(kali㉿kali)-[~]
$ ssh user_test@127.0.0.1 -p 6622
Linux kali 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ █
```

## Просмотр ключа

```
$ cd ~/.ssh/
$ ls
authorized_keys
$ nano authorized_keys
$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDe1jJkoNC2FemaRljQX/sLflBWuPkntyShbJNknVchPM6HFmZfKzGqY5pu
/g/dwRWUoh3FPpTfTjv7gJtElH11suD0W6JkcRnJejV+MPsdLToI7/YyzvWpJsic7+oAf8IXdtgfXnVxS3pSUu/uibVH7nuE
w2wV6mhQLeK6mbDckJBpbG/wucDy7Jj5asw6E58kWqCojW7buhwbFPRnI153R9rpp1mNHeoRFPhgrexrqpc4UmKG1YCMtXWQ
nRDmjxAZX4+aaJLjNChUI3T1rq80mgZYCdb8Rt9EH3r5MaZ3z/OUT9m5o9bvTJrbHpZyNmWUh1mraFSM11oSgXe6/090/o9B
45GJwb4/Rwfi0BsHpQoNpV+xLnK3ICNsL+7t7E1wactoLjxDsA+rz0oqKHwXuDn0GqmYwLBDLscsOs0BmwGKEp9BVhIKL96
1iJ1PDsH7q/C/xCSGyIwtHal2WS6+w/na1tAqIv9+3odFxi2sujKhkAZh3yiCjy6MLBTVSc= kali@kali
$ █
```

Вывод: В ходе данной лабораторной работе я добавил пользователя в sudo, тем самым дал ему право на использование sudo. Поставил на загрузчик grub логин и пароль, для обеспечения ещё одного уровня безопасности. Скачал и настроил SELinux, который используется для обеспечения безопасности на уровне прав доступа. Настроил оповещения logwatch. А также научился настраивать ssh: менять порт подключения, запрещать подключения рута, создавать и пробрасывать приватный и публичный ключ подключения