

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

**ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №9**  
**«Обеспечение безопасности в среде операционной системы GNU Linux»**

Практическая работа  
по дисциплине «Системное программное обеспечение»  
студента 3 курса группы ИВТ-б-о-222(1)  
Гоголева Виктора Григорьевича

09.03.01 « Информатика и вычислительная техника»

Симферополь, 2025  
Ход Работы

1. Определить для обычного пользователя возможность для запуска команды tcpdump через команду 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]
$

```

Рисунок – попытка запуска утилиты требующей sudo или root

```

(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..

```

Рисунок – успешная попытка после добавления пользователя в группу sudo

2. Установить пароль 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
```

Рисунок – выполнении утилиты для ввода пароля и генерации хеша для него

```
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
```

Рисунок – редактирование конфига, добавление имя пользователя и хеш пароля

```
(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
```

Рисунок - обновление конфигурации grub командой update-grub

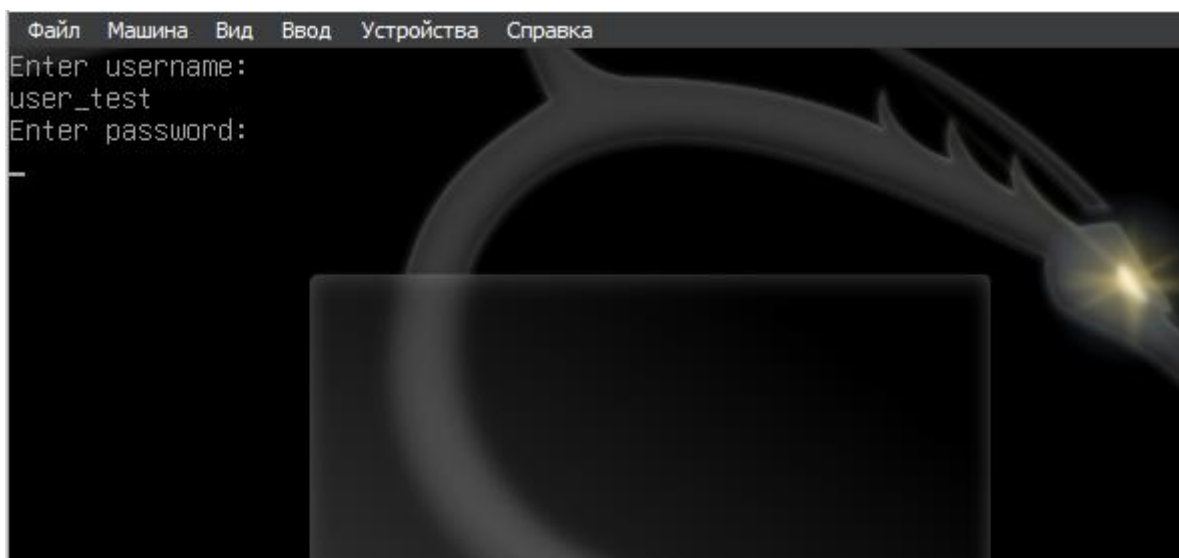


Рисунок – перезапуск системы и проверка что задание выполнено

3. Настроить ограничения для работы программы ssh путем редактирования файла конфигурации. Запретить удаленный доступ к системе суперпользователю, изменить порт для подключения с 22 на иной (например 6622).



Рисунок – редактирование конфига sshd



```

(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)-[~]
$

```

Рисунок – перезапуск демона, чтобы конфиг применился

```

(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.

```

Рисунок – попытка подключения

Получаем уведомление что требуется пара ключей.

4. Настроить аутентификацию программы SSH по ключевой паре вместо паролей.

```

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

```

Рисунок - Изменения конфига

```

(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+O.+o.     |
| o + =.* o         |
| . * S =           |
| + o o .           |
| o o               |
| .                 |
+--[SHA256]--+

```

Рисунок – генерация публичного и приватного ключ

```
(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.
$ █
```

Рисунок – копирование публичного ключа с хоста на сервер и проверка доступа