**Практическое задание: Безопасность OC Linux**

1. Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля. Предоставьте всё содержимое конфигурационного файла sshd и содержимое файла authorized\_keys.

**Команды:**

Установка SSH-сервера - sudo apt-get install ssh, - sudo systemctl restart sshd,   
- sudo systemctl status sshd. Далее для SSH-подключения Windows-Linux cкачал и установил [Putty](https://putty.org/). В PuTTYgen выбрал параметр **SSH-1 (RSA) и ключ длиной 2048 и нажал** Generate. Сохранил public и private key с именами test.pub и test.ppk. Далее через общую папку перебросил публичный ключ на сервер и записал его содержимое в файл /home/.ssh/authorized\_keys. Далее указал путь до сгенерированного приватного ключа и подключился к серверу

**- authorized\_keys.txt**

**- sshd\_config.txt**

1. Создать нового пользователя с домашней директорией и выдать ему возможность запускать утилиты без требования пароля. Предоставьте вывод команды ls в директории home, вывод файла passwd, содержимое файла sudoers.

**Команды:**

Создание нового пользователя - sudo adduser nsdm-test.

Выдача разрешений для утилит без требования пароля - sudo visudo

В файле sudoers добавил строку *nsdm ALL=(ALL) NOPASSWD: /sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3, /usr/bin/systemctl, /sbin/ifup, /sbin/ifdown,* чтобы разрешить запуск указанных утилит без пароля для нового пользователя.

*-* ***Вывод директории home.png (скриншот)***

* ***Вывод passwd.png (скриншот)***
* ***Вывод passwd.txt***
* ***Содержание файла sudoers.txt***

1. Установить минимальную длину пароля для пользователя в 8 символов.

*Первый вариант:* открыл файл */etc/pam.d/common-password* в текстовом редакторе командой *- sudo nano /etc/pam.d/common-password. Внутри файла внес строку password requisite pam\_cracklib.so и добавил в нее параметр minlen=8*

* ***common-passwords.txt***

*Второй вариант: для установки минимальной длины пароля для нового пользователя «nsdm-test» в 8 символов я изменил настройки файла /etc/login.defs. В строке, начинающейся с PASS\_MIN\_LEN, которая отвечает за минимальную длину пароля я изменил ее значение на PASS\_MIN\_LEN 8.*

***- etclogindefs.txt***

1. Установить на сервер пакеты Java. Предоставьте результат успешной установки Java (последняя доступная версия JRE).

**Команды:** для установки пакета default-jre, который предоставляет последнюю доступную версию JRE (Java Runtime Environment) использовал команду - sudo apt install default-jre

Первый вариант проверки результата: после установки ввел команду - java -version

Второй вариант проверки результата: создал файл HelloWorld.java со следующим кодом:

*public class HelloWorld {*

*public static void main(String[] args) {*

*System.out.println("Hello, World!");*

*}*

*}*

Далее в терминале выполнил команду - javac HelloWorld.java

Затем выполнил команду для запуска скомпилированного кода - java HelloWorld

**- Java.png (скриншот)**

**- JRE.png (скриншот)**

1. Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.

**Команды:** чтобы отредактировать файл cron выполнил команду - crontab -e

В открывшемся файле cron добавил следующую строку для автоматического сканирования 0 4 \* \* 1 /home/nsdm/daily\_antivirus.sh

Для обновления базы данных CLAMAV раз в месяц, добавил еще одну строку в файл cron - 0 0 1 \* \* sudo freshclam

* **CLAMAV.png (скриншот задач в cron);**
* **daily\_antivirus.txt (bash скрипт)**

1. Настроить файервол на блокирование всего входящего и выходящего трафика. Предоставьте вывод всех цепочек и правил iptables.

**Команды:** установка FirewallD - sudo apt install firewalld, после установки выполнил команду для его включения - sudo systemctl enable firewalld и - sudo systemctl start firewalld

Для блокировки входящих и исходящих соединений выполнил команду

- sudo firewall-cmd --panic-on

Чтобы отключить этот запрет, выполниk команду

- sudo firewall-cmd --panic-off

Командами - sudo iptables -P INPUT DROP и - sudo iptables -P OUTPUT DROP изменил политику цепочек INPUT и OUTPUT с ACCEPT на DROP.

**- IPTABLES.png**