**Курс: БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ, MIFIIB, поток 2.**

**ПРАКТИЧЕСКОЕ ЗАДАНИЕ: БЕЗОПАСНОСТЬ ОС LINUX**

**Выполнил: Король В.В.**

1. Разверните виртуальную машину на любом дистрибутиве, основанном на Debian (Ubuntu, Debian…).

Выполните настройку по чек-листу:

2. Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля.

3. Создать нового пользователя с домашней директорией и выдать ему возможность запускать следующие утилиты без требования пароля:

/sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3

usr/bin/systemctl

sbin/ifup, /sbin/ifdown

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

5. Установить на сервер пакеты Java.

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

7. Настроить файервол на блокирование всего входящего и выходящего трафика.

УСЛОВИЯ РЕАЛИЗАЦИИ:

По каждому пункту нужно предоставить:

Команду / набор команд / текст, которыми вы пользовались для выполнения задания.

Скриншот результата работы / получившегося файла.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ:

По пункту 1 предоставьте всё содержимое конфигурационного файла sshd и содержимое файла authorized\_keys.

По пункту 2 предоставьте вывод команды ls в директории home, вывод файла passwd, содержимое файла sudoers.

По пункту 3 самостоятельно найдите информацию по установке минимального пароля. В качестве ответа предоставьте содержимое файла common-passwords.

По пункту 4 предоставьте результат успешной установки Java (последняя доступная версия JRE).

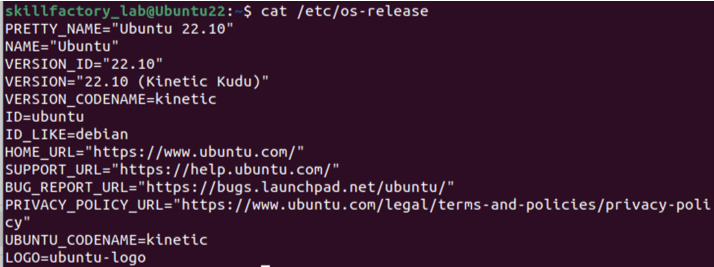
По пункту 5 предоставьте тексты задач cron, содержимое файла crontab (скрипт Bash — пожеланию)

По пункту 6 предоставьте вывод всех цепочек и правил iptables.

Оформите ответ в виде ссылки на облако/Git с файлом формата .docx/.doc внутри.

Выполнение задания.

1. На платформе Virtualbox, создал новую Ubuntu VM, v.22.10:



Размер диска: 32ГБ

Размер памяти: 4ГБ

Сетевые настройки: Bridged

Внешние USB устройства: Отключены

Разбивка диска: default

Установленны Guest Additions.

Обновление свежеустановленной системы:



Установил XFCE десктоп, как менее ресурсоёмкий.

2. Настройка SSH-сервера и подключения по ключам.

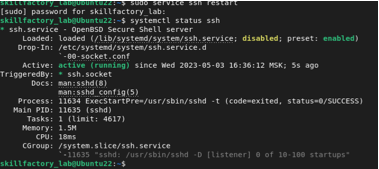
На хостовой машине создал public и private ключи:





Установил openssh server на сервере:





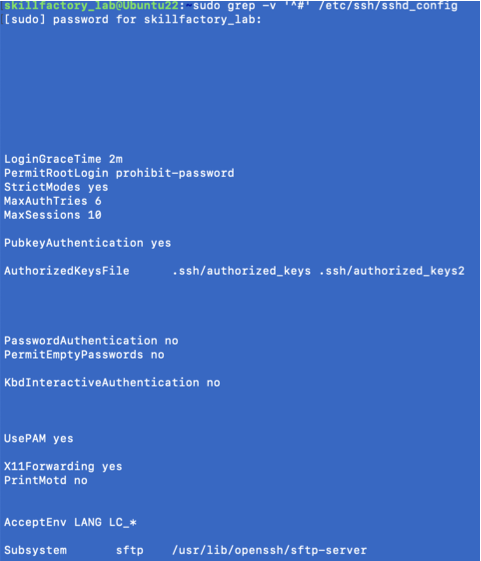
Директория .ssh уже была в системе с правами 0700. Создал файл autorized\_keys, назначил права 0644. На сервере разрешил доступ по паролю, скопировал туда public ключ:



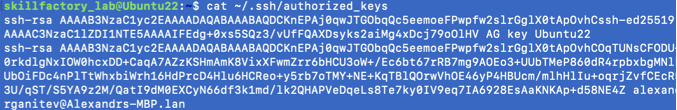
Добавил ключ в authorized\_keys и настроил доступ только по ключу:



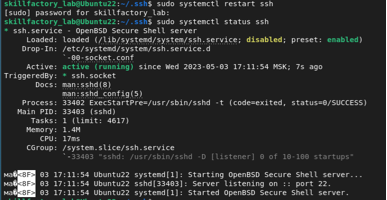
**SSHD:**

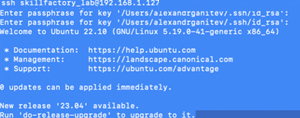


**Authorized\_keys:**



Перезагрузил сервис и подключился по ключу:



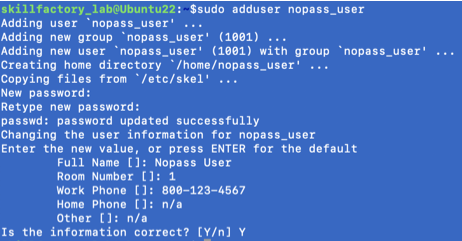


3. Создание нового пользователя с настройками NOPASSWD.

Установил требуемые компоненты посредством команды:



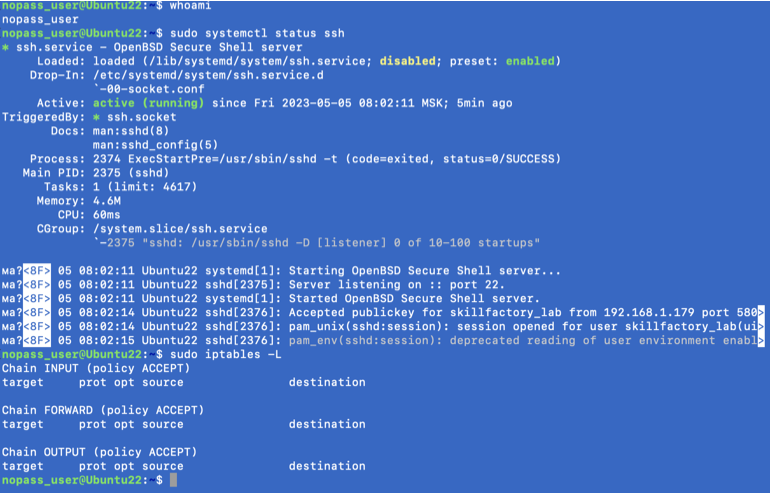
Создание пользователя:



Установил рекомендованные права доступа, перезагрузил систему для вступления прав в силу:



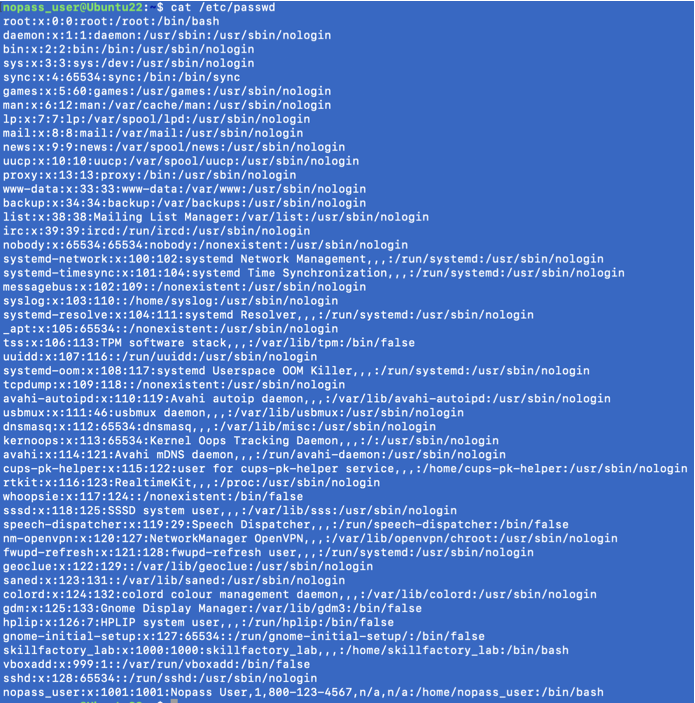
Проверка прав доступа пользователя nopass\_user:



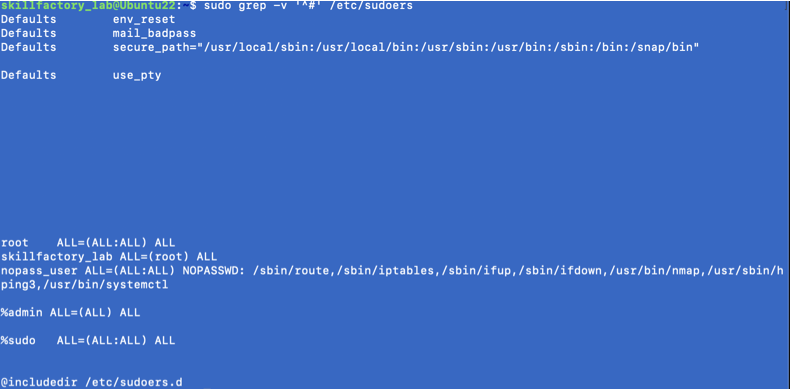
Вывод команды ls:



Вывод файла passwd:

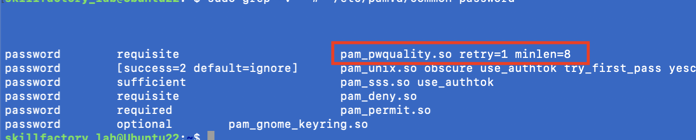


Вывод содержимого файла sudoers:



4 Настройка параметра установки минимальной длины пароля.

В модуле PAM, модифицируем файл /etc/pam.d/common-password, добавляем minlen=8, опционально я изменил retry=1:



Проверка изменений введённых выше:





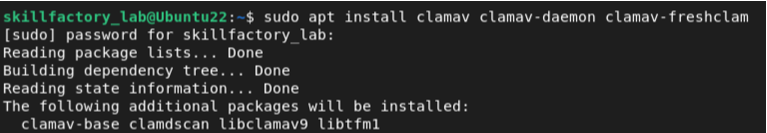
5. Установка пакетов Java.





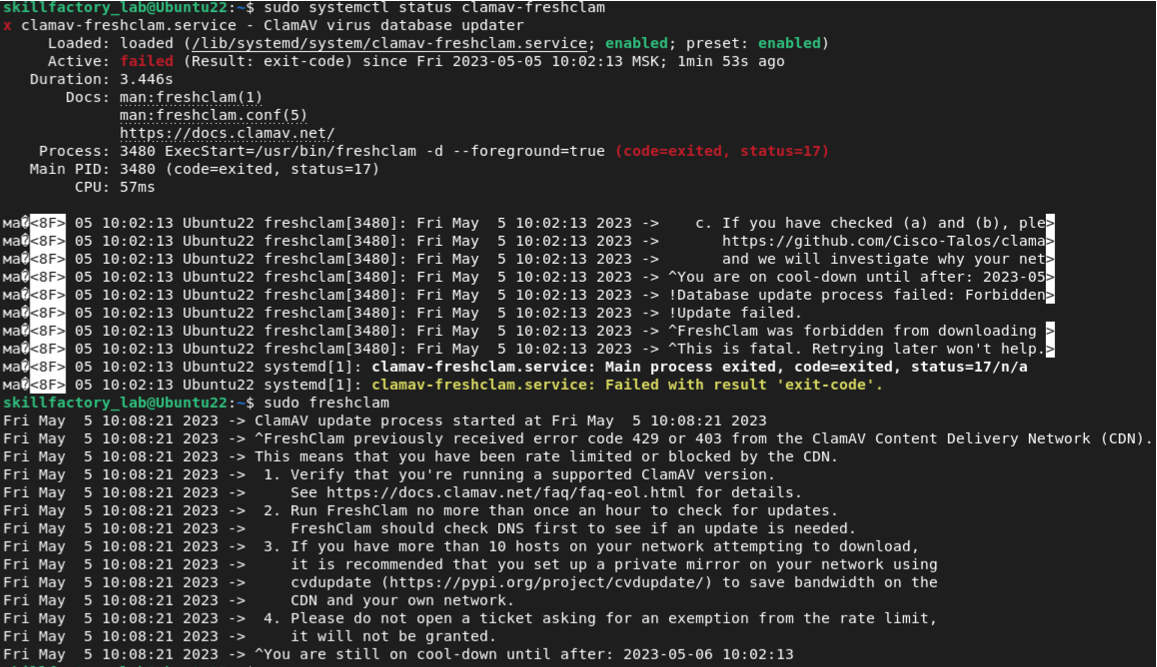
6. Настройка cron задачи для сканирования системы антивирусом.

Переключаемся с Bridged на Nat, для того, чтобы VM имела тот же IP, что и хостовая система под VPN, SSH не доступен, работаем из виртуальной машины.





К сожалению, я потратил около двух дней на тестирование разных VPN, затем совершил покупку VPS на Timeweb с польским IP, но попытки обновить ClamAV приводили всё время к бану моего IP адреса.

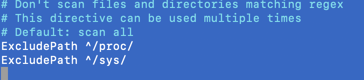


Создал задачу в Cron:



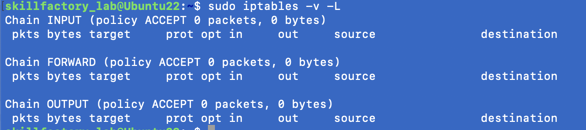
Добавил исключения на две директории. Хотя я сторонник полного сканирования всей системы.



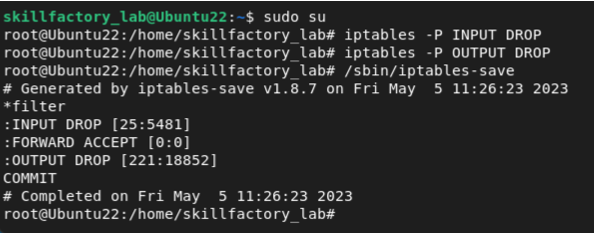


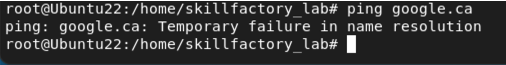
7. Блокирование всего трафика при помощи iptables.

Выводим все доступные цепочки:



Блокирование трафика:









Возвращаем всё на свои места, мне же нужно заходить по SSH и выходить в интернет с этой VM!

