

Курс: БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ, МИИТ, поток 1.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ: БЕЗОПАСНОСТЬ ОС LINUX

Выполнил: Ганицев А.С.

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

Выполните настройку по чек-листву:

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:

```
skillfactory_lab@Ubuntu22:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.10"
NAME="Ubuntu"
VERSION_ID="22.10"
VERSION="22.10 (Kinetic Kudu)"
VERSION_CODENAME=kinetic
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=kinetic
LOGO=ubuntu-logo
```

Размер диска: 32ГБ

Размер памяти: 4ГБ

Сетевые настройки: Bridged

Внешние USB устройства: Отключены

Разбивка диска: default

Установленны Guest Additions.

Обновление свежеустановленной системы:

```
skillfactory_lab@Ubuntu22:~$ sudo apt update -y && sudo apt upgrade -y
```

Установил XFCE десктоп, как менее ресурсоёмкий.

2. Настройка SSH-сервера и подключения по ключам.

На хостовой машине создал public и private ключи:

```
alexandrganitev@Alexandrs-MBP .ssh % ssh-keygen -b 2048 -t rsa -C AGUBUNTU22KEY
```

```
-rw----- 1 alexandrganitev staff 1876 2 May 16:51 AGUBUNTU22KEY
-rw-r--r-- 1 alexandrganitev staff 395 2 May 16:51 AGUBUNTU22KEY.pub
```

Установил openssh server на сервере:

```
skillfactory_lab@Ubuntu22:~$ sudo apt install -y openssh-server
```

```
skillfactory_lab@Ubuntu22:~$ sudo service ssh restart
[sudo] password for skillfactory_lab:
skillfactory_lab@Ubuntu22:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Drop-In: /etc/systemd/system/ssh.service.d
             └─00-socket.conf
   Active: active (running) since Wed 2023-05-03 16:36:12 MSK; 5s ago
     TriggeredBy: ssh.socket
   Docs: man:sshd(8)
         man:sshd_config(5)
   Process: 11634 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 11635 (sshd)
      Tasks: 1 (limit: 4617)
        Memory: 1.5M
          CPU: 0ms
        CGroup: /system.slice/ssh.service
               └─11635 "/usr/sbin/sshd -D [listener] 0 of 10-100 startups"

skillfactory_lab@Ubuntu22:~$
```

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

```
alexandrganitev@Alexandrs-MBP .ssh % cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABQDCKnEPAjqqwTGOqbQc5eemoeFPwpfw2slrGg1X0t
p0vhCoqTNscF0DU+0rkdlgNxIOW0hcxD+CagA7AzxKShAmkBVixXFwMzr6bHCU30W+/Ec6bt67r
B7mg9AOEo3+UUbTMeP860dR4rpbxgbMN1LUbOiFDc4nP1TtWhxbiWrh16HdPrcD4Hlu6HCReo+y5rb7
TMY+NE+KqTB1QOrw+hOE46yP4HBUCm/mlhH1Iu+oqrjZvfCecR53U/qST/S5Y9z2M/Qat19dM0EXCy
66df3k1nd/lk2QHAPVeDqels8Te7ky0IV9eq7IA6928EsAaKNKA�+d5BNE4Z alexandrganitev@Al
```

Добавил ключ в authorized_keys и настроил доступ только по ключу:

```
alexandrganitev@Alexandrs-MBP .ssh % ssh-copy-id skillfactory_lab@192.168.1.127
```

SSHD:

```
skillfactory_lab@Ubuntu22: sudo grep -v '^#' /etc/ssh/sshd_config
[sudo] password for skillfactory_lab:

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

PubkeyAuthentication yes

AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

PasswordAuthentication no
PermitEmptyPasswords no

KbdInteractiveAuthentication no

UsePAM yes

X11Forwarding yes
PrintMotd no

AcceptEnv LANG LC_*

Subsystem      sftp      /usr/lib/openssh/sftp-server
```

Authorized_keys:

```
skillfactory_lab@Ubuntu22: $ cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDCKnEPAj0qwJTGObqQc5eemoeFPwpfw2slrGglX0tApOvhCssh-ed25519
AAAAC3NzaC1zD1NTE5AAAIFdg+0xs5Sz3/vUfQAXDsYks2aiMg4x0cj79o0lHV AG key Ubuntu22
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDCKnEPAj0qwJTGObqQc5eemoeFPwpfw2slrGglX0tApOvhCqTUNsCFODU
0rkdlgNxI0W0hcxDd+CaqA7AZzKSHmAmK8VixFwmZrr6bHCU3oW+/Ec6bt67rRB7mg9AOEo3+UUbTMeP860dR4rpbxbgMNL
Ub0iFdc4nPlttWhxiWrh16HdPrcD4Hu6HCReo+ysrb7oTMY+NE+KqTB1QOrwVh0E4yP4HBUCm/m1hH1iu+qrjZvfCcER
3U/qST/S5YAz2M/QatI9dM0EXCyN6df3k1md/lk2QHAPVeDqeLs8Te7ky0IV9eq7IA6928EsAaKNKAp+d58NE4Z alexan
rganitev@Alexandrs-MBP.lan
```

Перезагрузил сервис и подключился по ключу:

```
skillfactory_lab@Ubuntu22: ~ $ sudo systemctl restart ssh
[sudo] password for skillfactory_lab:
skillfactory_lab@Ubuntu22: ~ $ sudo systemctl status ssh
 * ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Drop-In: /etc/systemd/system/ssh.service.d
             '--socket.conf'
     Active: active (running) since Wed 2023-05-03 17:11:54 MSK; 7s ago
   TriggeredBy: * ssh.socket
   Docs: man:ssh(8)
           man:ssh(5)
           man:ssh_config(5)
 Process: 33402 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 33403 (sshd)
   Tasks: 1 (limit: 4617)
  Memory: 1.4M
    CPU: 17ms
   CGroup: /system.slice/ssh.service
           `--33403 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 03 17:11:54 Ubuntu22 systemctl[1]: Starting OpenBSD Secure Shell server...
May 03 17:11:54 Ubuntu22 sshd[33403]: Server listening on : port 22.
May 03 17:11:54 Ubuntu22 systemctl[1]: Started OpenBSD Secure Shell server.
```

```
alexandrganitev@Alexandrs-MBP .ssh % ssh skillfactory_lab@192.168.1.127
Enter passphrase for key '/Users/alexandrganitev/.ssh/id_rsa':
Enter passphrase for key '/Users/alexandrganitev/.ssh/id_rsa':
Welcome to Ubuntu 22.10 (GNU/Linux 5.19.0-41-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

0 updates can be applied immediately.

New release '23.04' available.
Run 'do-release-upgrade' to upgrade to it.
```

3. Создание нового пользователя с настройками NOPASSWD.

Установил требуемые компоненты посредством команды:

```
skillfactory_lab@Ubuntu22: $ sudo apt install net-tools iptables ifupdown nmap hping3
```

Создание пользователя:

```
skillfactory_lab@Ubuntu22: $ sudo adduser nopass_user
Adding user `nopass_user' ...
Adding new group `nopass_user' (1001) ...
Adding new user `nopass_user' (1001) with group `nopass_user' ...
Creating home directory `/home/nopass_user' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for nopass_user
Enter the new value, or press ENTER for the default
  Full Name []: Nopass User
  Room Number []: 1
  Work Phone []: 800-123-4567
  Home Phone []: n/a
  Other []: n/a
Is the information correct? [Y/n] Y
```

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

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
skillfactory_lab ALL=(root) ALL
nopass_user ALL=(ALL:ALL) NOPASSWD: /sbin/route,/sbin/iptables,/sbin/ifup,/sbin/ifdown,/usr/bin/nmap,/usr/sbin/hping3,/usr/bin/systemctl
```

Проверка прав доступа пользователя nopass_user:

```
nopass_user@Ubuntu22: $ whoami
nopass_user
nopass_user@Ubuntu22: $ sudo systemctl status ssh
* ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: enabled)
  Drop-In: /etc/systemd/system/ssh.service.d
            '-00-socket.conf'
  Active: active (running) since Fri 2023-05-05 08:02:11 MSK; 5min ago
TriggeredBy: * ssh.socket
  Docs: man:sshd(8)
        man:sshd_config(5)
  Process: 2374 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 2375 (sshd)
   Tasks: 1 (limit: 4617)
  Memory: 4.6M
    CPU: 60ms
   CGroup: /system.slice/ssh.service
           `--2375 "sshd: /usr/sbin/sshd -D [listener] 0 of 10~100 startups"

 ма?<8F> 05 08:02:11 Ubuntu22 systemd[1]: Starting OpenBSD Secure Shell server...
 ма?<8F> 05 08:02:11 Ubuntu22 sshd[2375]: Server listening on :: port 22.
 ма?<8F> 05 08:02:11 Ubuntu22 systemd[1]: Started OpenBSD Secure Shell server.
 ма?<8F> 05 08:02:14 Ubuntu22 sshd[2376]: Accepted publickey for skillfactory_lab from 192.168.1.179 port 586
 ма?<8F> 05 08:02:14 Ubuntu22 sshd[2376]: pam_unix(sshd:session): session opened for user skillfactory_lab(uid)
 ма?<8F> 05 08:02:15 Ubuntu22 sshd[2376]: pam_env(sshd:session): deprecated reading of user environment enabled
nopass_user@Ubuntu22: $ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
nopass_user@Ubuntu22: $
```

Вывод команды ls:

```
nopass_user@Ubuntu22:/home$ ls
nopass_user  skillfactory_lab
```

Вывод файла passwd:

```
nopass_user@Ubuntu22: ~ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:68:games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:101:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:109:/:/nonexistent:/usr/sbin/nologin
syslog:x:103:110:/:/home/syslog:/usr/sbin/nologin
systemd-resolve:x:104:111:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
_apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin
tss:x:106:113:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:116:/:/run/uuidd:/usr/sbin/nologin
systemd-oom:x:108:117:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:109:118:/:/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124:/:/nonexistent:/bin/false
sssd:x:118:125:SSSD system user,,,:/var/lib/sssd:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
nm-openvpn:x:120:127:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
fwupd-refresh:x:121:128:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
geoclue:x:122:129:/:/var/lib/geoclue:/usr/sbin/nologin
saned:x:123:131:/:/var/lib/saned:/usr/sbin/nologin
colord:x:124:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
gdm:x:125:133:GNOME Display Manager:/var/lib/gdm3:/bin/false
hplip:x:126:7:HPLIP system user,,,:/run/hplip:/bin/false
gnome-initial-setup:x:127:65534:/:/run/gnome-initial-setup:/bin/false
skillfactory_lab:x:1000:1000:skillfactory_lab,,,:/home/skillfactory_lab:/bin/bash
vboxadd:x:999:1:/:/var/run/vboxadd:/bin/false
sshd:x:128:65534:/:/run/sshd:/usr/sbin/nologin
nopass_user:x:1001:1001:Nopass User,1,800-123-4567,n/a,n/a:/home/nopass_user:/bin/bash
```

Вывод содержимого файла sudoers:

```
skillfactory_lab@Ubuntu22: ~ sudo grep -v '^#' /etc/sudoers
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
Defaults        use_pty

root    ALL=(ALL:ALL) ALL
skillfactory_lab ALL=(root) ALL
nopass_user ALL=(ALL:ALL) NOPASSWD: /sbin/route,/sbin/iptables,/sbin/ifup,/sbin/ifdown,/usr/bin/nmap,/usr/sbin/hping3,/usr/bin/systemctl

%admin  ALL=(ALL) ALL
%sudo   ALL=(ALL:ALL) ALL

@includedir /etc/sudoers.d
```

4 Настройка параметра установки минимальной длины пароля.

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

```
password      requisite          pam_pwquality.so retry=1 minlen=8
password      [success=2 default=ignore]  pam_unix.so obscure use_authtok try_first_pass yes
password      sufficient        pam_sss.so use_authtok
password      requisite          pam_deny.so
password      required          pam_permit.so
password      optional           pam_gnome_keyring.so
```

Проверка изменений введённых выше:

```
skillfactory_lab@Ubuntu22:~$ sudo passwd nopass_user
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
```

```
skillfactory_lab@Ubuntu22:~$ sudo passwd nopass_user
New password:
Retype new password:
passwd: password updated successfully
```

5. Установка пакетов Java.

```
skillfactory_lab@Ubuntu22:~$ sudo apt install default-jre
skillfactory_lab@Ubuntu22:~$ java --version
openjdk 11.0.18 2023-01-17
OpenJDK Runtime Environment (build 11.0.18+10-post-Ubuntu-0ubuntu122.10)
OpenJDK 64-Bit Server VM (build 11.0.18+10-post-Ubuntu-0ubuntu122.10, mixed mode, sharing)
```

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.

```
skillfactory_lab@Ubuntu22:~$ sudo apt install clamav clamav-daemon clamav-freshclam
[sudo] password for skillfactory_lab:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  clamav-base clamdscan libclamav9 libtfm1
skillfactory_lab@Ubuntu22:~$ clamscan -V
ClamAV 0.103.8
```

К сожалению, я потратил около двух дней на тестирование разных VPN, затем совершил покупку VPN на Timeweb спольским IP, но попытки обновить ClamAV приводили всё время кбану моего IP адреса.

```

skillfactory_lab@Ubuntu22:~$ sudo systemctl status clamav-freshclam
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; preset: enabled)
   Active: failed (Result: exit-code) since Fri 2023-05-05 10:02:13 MSK; 1min 53s ago
     Duration: 3.446s
       Docs: man:freshclam(1)
              man:freshclam.conf(5)
              https://docs.clamav.net/
   Process: 3480 ExecStart=/usr/bin/freshclam -d --foreground=true (code=exited, status=17)
    Main PID: 3480 (code=exited, status=17)
      CPU: 57ms

May  5 10:02:13 Ubuntu22 freshclam[3480]: Fri May  5 10:02:13 2023 ->      c. If you have checked (a) and (b), ple>
May  5 10:02:13 Ubuntu22 freshclam[3480]: Fri May  5 10:02:13 2023 ->      https://github.com/Cisco-Talos/clama>
May  5 10:02:13 Ubuntu22 freshclam[3480]: Fri May  5 10:02:13 2023 ->      and we will investigate why your net>
May  5 10:02:13 Ubuntu22 freshclam[3480]: Fri May  5 10:02:13 2023 -> ^You are on cool-down until after: 2023-05->
May  5 10:02:13 Ubuntu22 freshclam[3480]: Fri May  5 10:02:13 2023 -> !Database update process failed: Forbidden>
May  5 10:02:13 Ubuntu22 freshclam[3480]: Fri May  5 10:02:13 2023 -> !Update failed.
May  5 10:02:13 Ubuntu22 freshclam[3480]: Fri May  5 10:02:13 2023 -> ^FreshClam was forbidden from downloading >
May  5 10:02:13 Ubuntu22 freshclam[3480]: Fri May  5 10:02:13 2023 -> "This is fatal. Retrying later won't help.>
May  5 10:02:13 Ubuntu22 systemd[1]: clamav-freshclam.service: Main process exited, code=exited, status=17/n/a
May  5 10:02:13 Ubuntu22 systemd[1]: clamav-freshclam.service: Failed with result 'exit-code'.
skillfactory_lab@Ubuntu22:~$ sudo freshclam
Fri May  5 10:08:21 2023 -> ClamAV update process started at Fri May  5 10:08:21 2023
Fri May  5 10:08:21 2023 -> ^FreshClam previously received error code 429 or 403 from the ClamAV Content Delivery Network (CDN).
Fri May  5 10:08:21 2023 -> This means that you have been rate limited or blocked by the CDN.
Fri May  5 10:08:21 2023 -> 1. Verify that you're running a supported ClamAV version.
Fri May  5 10:08:21 2023 ->     See https://docs.clamav.net/faq/faq-eol.html for details.
Fri May  5 10:08:21 2023 -> 2. Run FreshClam no more than once an hour to check for updates.
Fri May  5 10:08:21 2023 ->     FreshClam should check DNS first to see if an update is needed.
Fri May  5 10:08:21 2023 -> 3. If you have more than 10 hosts on your network attempting to download,
Fri May  5 10:08:21 2023 ->     it is recommended that you set up a private mirror on your network using
Fri May  5 10:08:21 2023 ->     cvdupdate (https://pypi.org/project/cvdupdate/) to save bandwidth on the
Fri May  5 10:08:21 2023 ->     CDN and your own network.
Fri May  5 10:08:21 2023 -> 4. Please do not open a ticket asking for an exemption from the rate limit,
Fri May  5 10:08:21 2023 ->     it will not be granted.
Fri May  5 10:08:21 2023 -> ^You are still on cool-down until after: 2023-05-06 10:02:13

```

Содал задачу в Cron:

```

# m h  dom mon dow   command
0 4 * * * /usr/bin/clamscan -r /           # Full scan with ClamAV
# 0 0 1 * * /usr/bin/freshscan               # Updating the ClamAV DB

```

Добавил исключения на две директории, которые считаю необходимыми к исключению. Хотя я сторонник полного сканирования всей системы.

```

skillfactory_lab@Ubuntu22:~$ sudo nano /etc/clamav/clamd.conf

```

```

# Don't scan files and directories matching regex
# This directive can be used multiple times
# Default: scan all
ExcludePath ^/proc/
ExcludePath ^/sys/

```

7. Блокирование всего трафика при помощи iptables.

Выводим все доступные цепочки:

```

skillfactory_lab@Ubuntu22:~$ sudo iptables -v -L
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target  prot opt in     out     source          destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target  prot opt in     out     source          destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 . . .
skillfactory_lab@Ubuntu22:~$ sudo su
root@Ubuntu22:/home/skillfactory_lab# iptables -P INPUT DROP
root@Ubuntu22:/home/skillfactory_lab# iptables -P OUTPUT DROP
root@Ubuntu22:/home/skillfactory_lab# /sbin/iptables-save
# Generated by iptables-save v1.8.7 on Fri May  5 11:26:23 2023
*filter
:INPUT DROP [25:5481]
:FORWARD ACCEPT [0:0]
:OUTPUT DROP [221:18852]
COMMIT
# Completed on Fri May  5 11:26:23 2023
root@Ubuntu22:/home/skillfactory_lab#

```

Блокирование трафика:

```
root@Ubuntu22:/home/skillfactory_lab# ping google.ca
ping: google.ca: Temporary failure in name resolution
root@Ubuntu22:/home/skillfactory_lab#
```

```
alexandrganitev@Alexandrs-MBP ~ % ssh skillfactory_lab@192.168.1.127
ssh: connect to host 192.168.1.127 port 22: Operation timed out
```

```
alexandrganitev@Alexandrs-MBP ~ % ping 192.168.1.127
PING 192.168.1.127 (192.168.1.127): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
```

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

```
root@Ubuntu22:/home/skillfactory_lab# iptables -P OUTPUT ACCEPT
root@Ubuntu22:/home/skillfactory_lab# iptables -P INPUT ACCEPT
root@Ubuntu22:/home/skillfactory_lab# /sbin/iptables-save
# Generated by iptables-save v1.8.7 on Fri May  5 11:32:23 2023
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT
# Completed on Fri May  5 11:32:23 2023
root@Ubuntu22:/home/skillfactory_lab# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@Ubuntu22:/home/skillfactory_lab#
```

