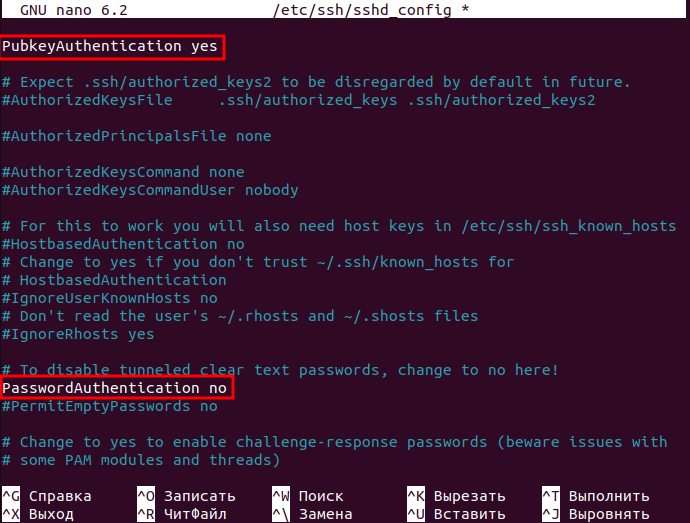
## Установка SSH-сервера

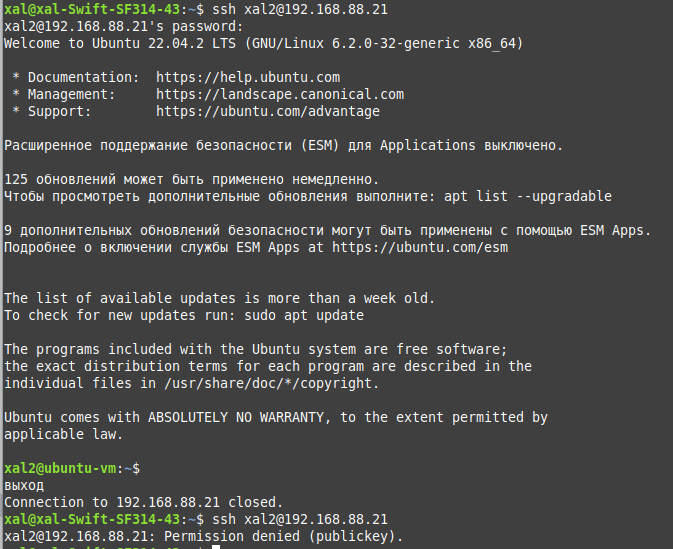


У меня уже установлен ssh-сервер на этапе прохождения лекции, но если бы он не был установлен, то установился бы такой командой «**sudo apt install ssh**». Автозапуск тоже включился при установке, но его можно установить вручную (если по какой-то причине он не настроился) командой «**systemctl enable ssh**».

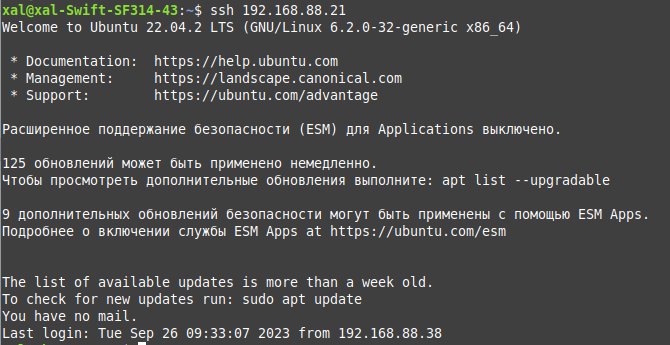
Теперь насторою ssh-сервер на прием соединения только по ключам и отказ по паролю:



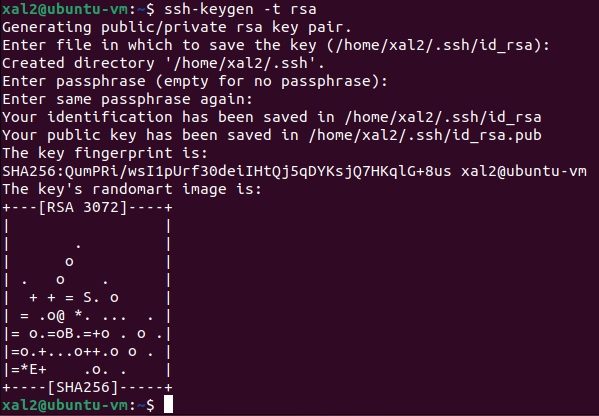
Перед тем, как служба ssh была перезагружена для применения конфига, я проверил, что по паролю пользователя xal2 пускало (про создание пользователя xal2 будет описано в п.2, т.к. в отчете сохранена нумерация ДЗ), а после применения конфига – доступ только по ключу:



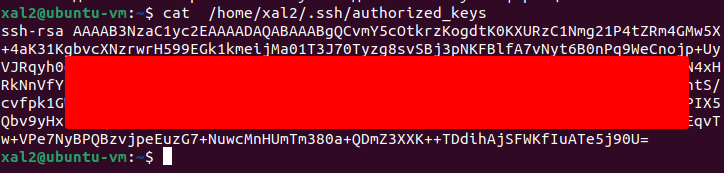
При этом по ключу пускает (ключ пользователя xal я гораздо раньше уже прописал):



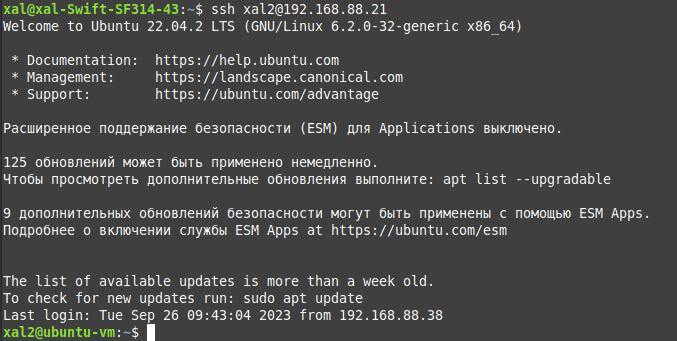
Создаем rsa-ключ для нового пользователя xal2:



После создания ключей, я занес публичный ключ в файл **/home/xal2/.ssh/authorized\_keys**:



потом скопировал приватный ключ (переименовав, чтобы не перепутать его с другими своими ключами) на хостовую машину и проверил, что при помощи нового ключа удается войти:

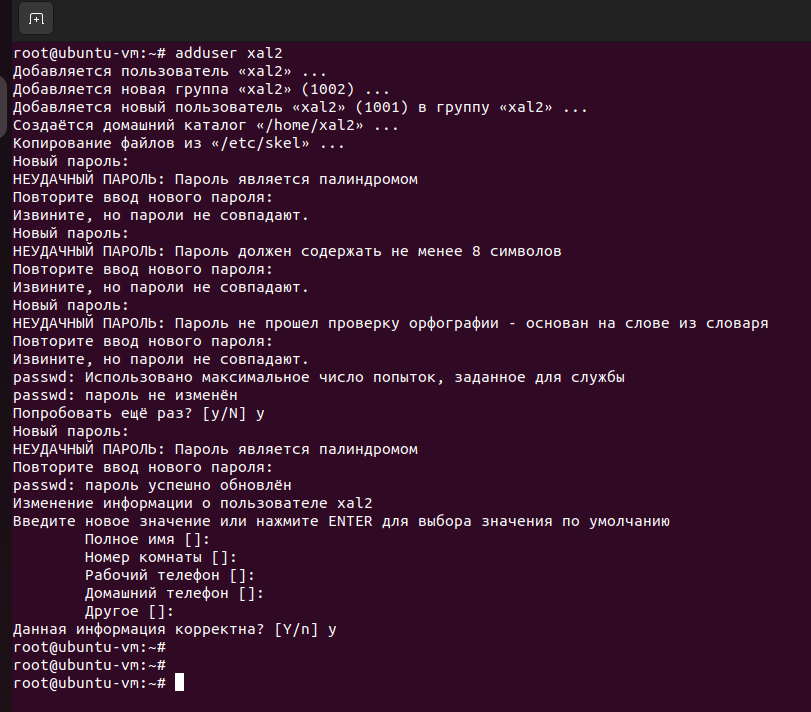


Чтобы новый ключ применялся, я занес информацию об этом в локальный конфиг ssh пользователя на хостовой машине:



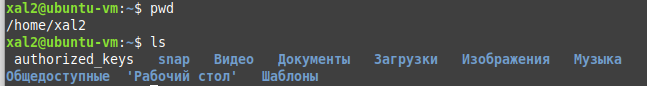
## Создание нового пользователя

Создам нового пользовател при помощи утилиты adduser:

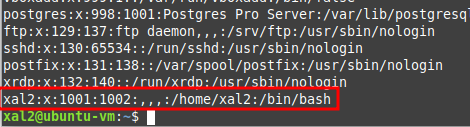


Система поругалась на разные аспекты слабости пароля, но дала ввести пароль из трех цифр (в итоге. На более безопасный пароль смена будет в п.3)

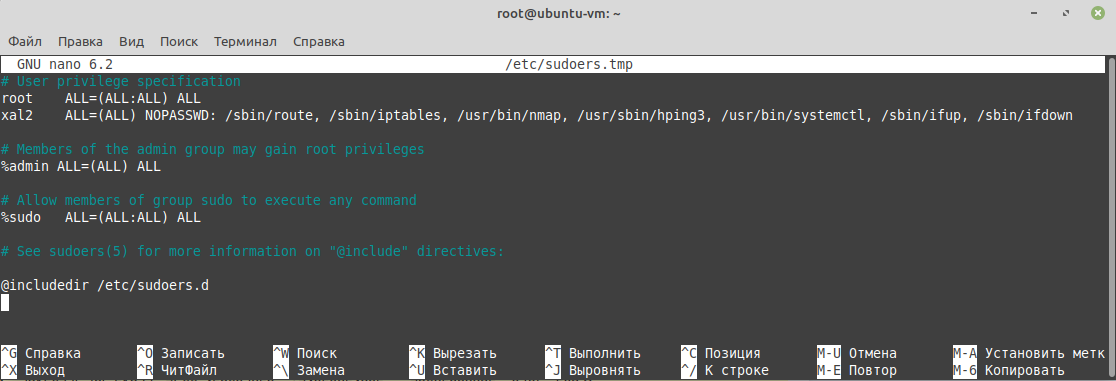
Вот содержимое домашнего каталога:



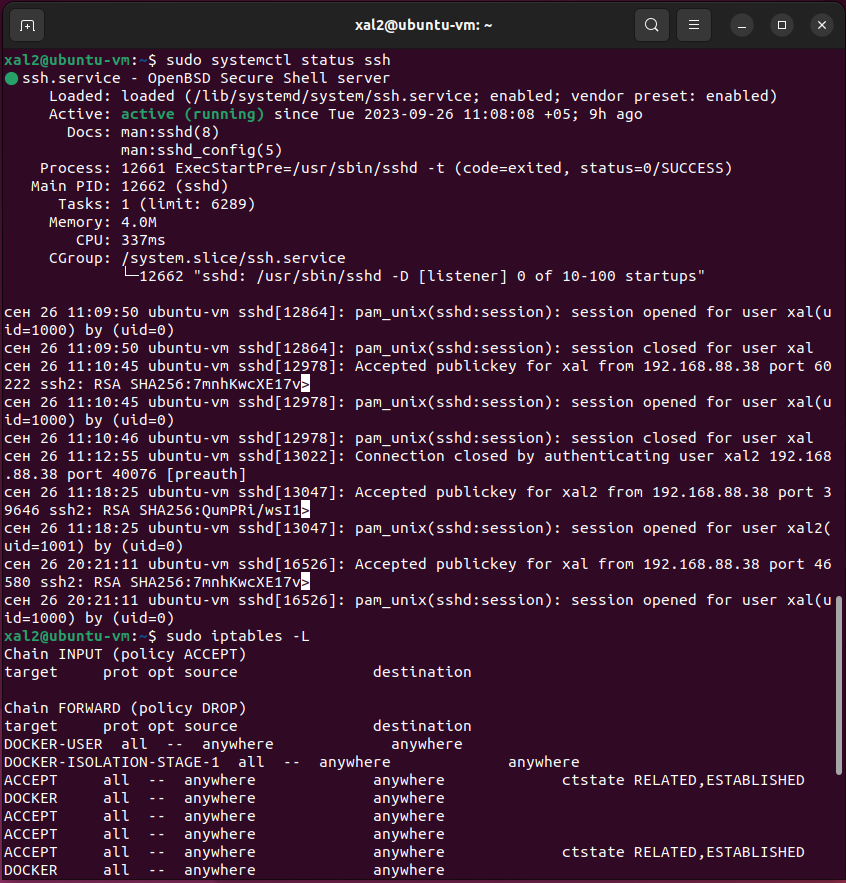
Вот запись в /etc/passwd:



Выдам право запускать часть утилит пользователю xal2 через sudo без пароля (visudo):



Проверю, что настройка сработала:

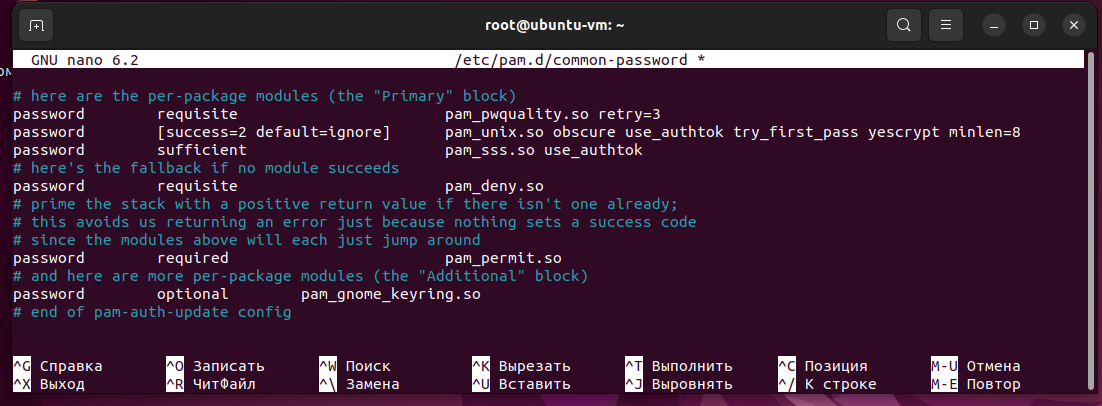


Отмечу, что дополнительно пришлось поставить ряд пакетов:

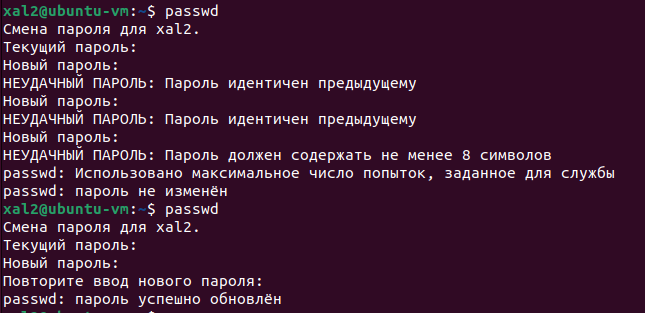
**apt install net-tools nmap ifupdown-ng hping3**

## Установка мимнимальной длины пароля в 8 символов

Теперь поменяю парольную политику (допишу параметр минимальной длины пароля «minlen=8»):

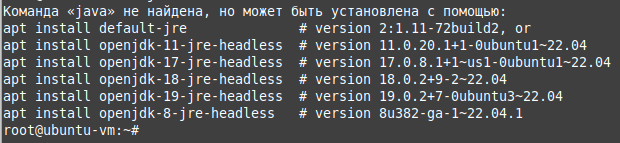


И теперь попробуем сменить пароль пользователя xal2:



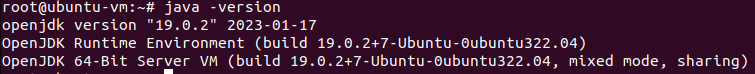
## Установить на сервер пакеты Java

Проверяю наличие JRE:



Установлю последнюю версию JRE командой «apt install openjdk-19-jre-headless»

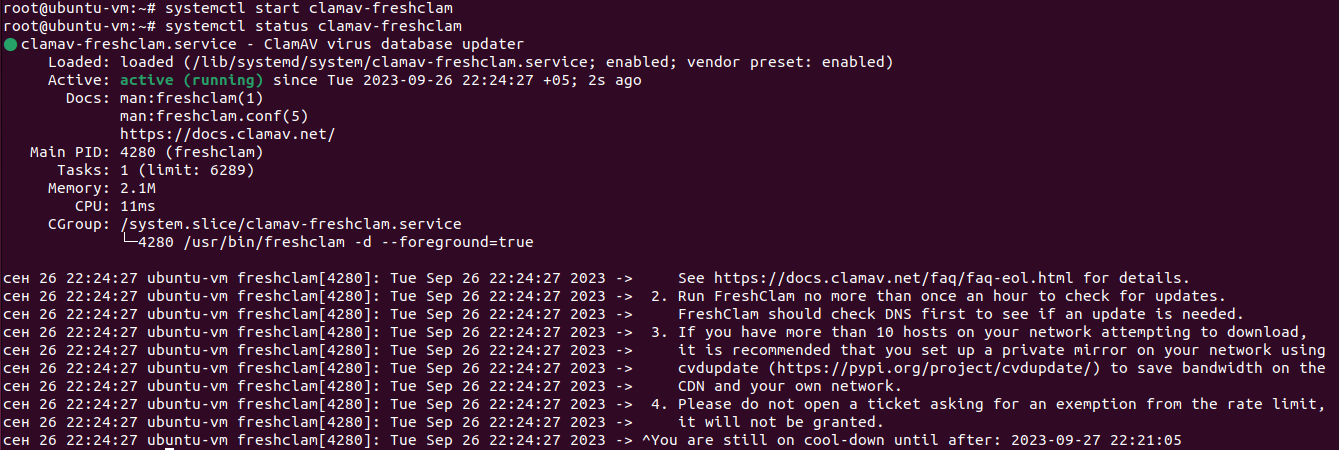
Результат:



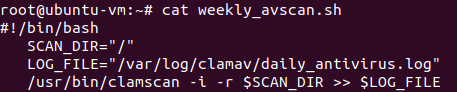
## Настроить автоматическое сканирование антивирусом всей ОС

Установка антивируса:

# **apt install clamav clamav-daemon clamav-freshclam**



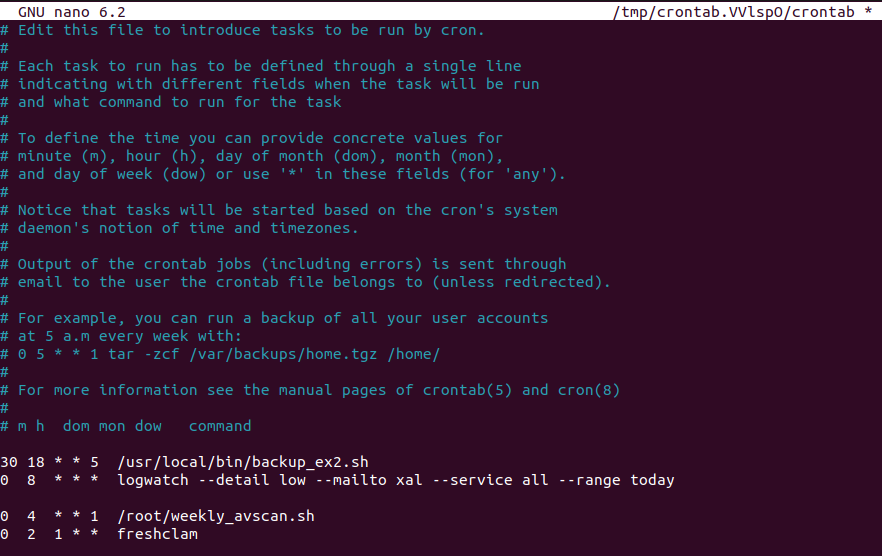
Создам скрипт еженедельной проверки:



Дадим право на исполнение:

# **chmod +x weekly\_avscan.sh**

Напишем правила для cron на запуск и обновление АВ:



## Настроить файервол на блокирование всего входящего и выходящего трафика

Т.к. у нас нет никаких правил в цепочках INPUT и OUTPUT, то для закрытия всего входящего и исходящего трафика необходимо изменить политику этих цепочек по-умолчанию на "DROP":

# **iptables -P INPUT DROP**

# **iptables -P OUTPUT DROP**



Все дополнительные материалы в приложениях. Для удобства навигации вот оглавление:

[1. Установка SSH-сервера 1](#__RefHeading___1)

[2. Создание нового пользователя 4](#__RefHeading___2)

[3. Установка мимнимальной длины пароля в 8 символов 6](#__RefHeading___3)

[4. Установить на сервер пакеты Java 6](#__RefHeading___4)

[5. Настроить автоматическое сканирование антивирусом всей ОС 7](#__RefHeading___5)

[6. Настроить файервол на блокирование всего входящего и выходящего трафика 8](#__RefHeading___6)

[Дополнительно: 9](#__RefHeading___7)

[/etc/ssh/ssh\_config 9](#__RefHeading___8)

[/home/xal2/.ssh# cat authorized\_keys 11](#__RefHeading___9)

[/etc/passwd 11](#__RefHeading___10)

[/etc/sudoers 12](#__RefHeading___11)

[/etc/pam.d/common-password 13](#__RefHeading___12)

[iptables -L 13](#__RefHeading___13)

[crontab 14](#__RefHeading___14)

# Дополнительно:

## /etc/ssh/ssh\_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/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd\_config shipped with

# OpenSSH is to specify options with their default value where

# possible, but leave them commented. Uncommented options override the

# default value.

Include /etc/ssh/sshd\_config.d/\*.conf

#Port 22

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

#HostKey /etc/ssh/ssh\_host\_rsa\_key

#HostKey /etc/ssh/ssh\_host\_ecdsa\_key

#HostKey /etc/ssh/ssh\_host\_ed25519\_key

# Ciphers and keying

#RekeyLimit default none

# Logging

#SyslogFacility AUTH

#LogLevel INFO

# Authentication:

#LoginGraceTime 2m

#PermitRootLogin prohibit-password

#StrictModes yes

#MaxAuthTries 6

#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 no

#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with

# some PAM modules and threads)

KbdInteractiveAuthentication no

# Kerberos options

#KerberosAuthentication no

#KerberosOrLocalPasswd yes

#KerberosTicketCleanup yes

#KerberosGetAFSToken no

# GSSAPI options

#GSSAPIAuthentication no

#GSSAPICleanupCredentials yes

#GSSAPIStrictAcceptorCheck yes

#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,

# and session processing. If this is enabled, PAM authentication will

# be allowed through the KbdInteractiveAuthentication and

# PasswordAuthentication. Depending on your PAM configuration,

# PAM authentication via KbdInteractiveAuthentication may bypass

# the setting of "PermitRootLogin without-password".

# If you just want the PAM account and session checks to run without

# PAM authentication, then enable this but set PasswordAuthentication

# and KbdInteractiveAuthentication to 'no'.

UsePAM yes

#AllowAgentForwarding yes

#AllowTcpForwarding yes

#GatewayPorts no

X11Forwarding yes

#X11DisplayOffset 10

#X11UseLocalhost yes

#PermitTTY yes

PrintMotd no

#PrintLastLog yes

#TCPKeepAlive yes

#PermitUserEnvironment no

#Compression delayed

#ClientAliveInterval 0

#ClientAliveCountMax 3

#UseDNS no

#PidFile /run/sshd.pid

#MaxStartups 10:30:100

#PermitTunnel no

#ChrootDirectory none

#VersionAddendum none

# no default banner path

#Banner none

# Allow client to pass locale environment variables

AcceptEnv LANG LC\_\*

# override default of no subsystems

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

# Example of overriding settings on a per-user basis

#Match User anoncvs

# X11Forwarding no

# AllowTcpForwarding no

# PermitTTY no

# ForceCommand cvs server

## /home/xal2/.ssh# cat authorized\_keys

ssh-rsa 

## /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:/bin/sync

games:x:5:60:games:/usr/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:/bin:/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

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/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-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

messagebus:x:102:105::/nonexistent:/usr/sbin/nologin

systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin

syslog:x:104:111::/home/syslog:/usr/sbin/nologin

\_apt:x:105:65534::/nonexistent:/usr/sbin/nologin

tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false

uuidd:x:107:115::/run/uuidd:/usr/sbin/nologin

systemd-oom:x:108:116:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin

tcpdump:x:109:117::/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/sss:/usr/sbin/nologin

speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false

fwupd-refresh:x:120:126:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin

nm-openvpn:x:121:127:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin

saned:x:122:129::/var/lib/saned:/usr/sbin/nologin

colord:x:123:130:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin

geoclue:x:124:131::/var/lib/geoclue:/usr/sbin/nologin

pulse:x:125:132:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin

gnome-initial-setup:x:126:65534::/run/gnome-initial-setup/:/bin/false

hplip:x:127:7:HPLIP system user,,,:/run/hplip:/bin/false

gdm:x:128:134:Gnome Display Manager:/var/lib/gdm3:/bin/false

xal:x:1000:1000:xal,,,:/home/xal:/bin/bash

vboxadd:x:999:1::/var/run/vboxadd:/bin/false

postgres:x:998:1001:Postgres Pro Server:/var/lib/postgresql:/bin/bash

ftp:x:129:137:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin

sshd:x:130:65534::/run/sshd:/usr/sbin/nologin

postfix:x:131:138::/var/spool/postfix:/usr/sbin/nologin

xrdp:x:132:140::/run/xrdp:/usr/sbin/nologin

xal2:x:1001:1002:,,,:/home/xal2:/bin/bash

## /etc/sudoers

#

# This file MUST be edited with the 'visudo' command as root.

#

# Please consider adding local content in /etc/sudoers.d/ instead of

# directly modifying this file.

#

# See the man page for details on how to write a sudoers file.

#

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

# This preserves proxy settings from user environments of root

# equivalent users (group sudo)

#Defaults:%sudo env\_keep += "http\_proxy https\_proxy ftp\_proxy all\_proxy no\_proxy"

# This allows running arbitrary commands, but so does ALL, and it means

# different sudoers have their choice of editor respected.

#Defaults:%sudo env\_keep += "EDITOR"

# Completely harmless preservation of a user preference.

#Defaults:%sudo env\_keep += "GREP\_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper

#Defaults:%sudo env\_keep += "GIT\_AUTHOR\_\* GIT\_COMMITTER\_\*"

# 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

xal2 ALL=(ALL) NOPASSWD: /sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3, /usr/bin/systemctl, /sbin/ifup, /sbin/ifdown

# Members of the admin group may gain root privileges

%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command

%sudo ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d

## /etc/pam.d/common-password

#

# /etc/pam.d/common-password - password-related modules common to all services

#

# This file is included from other service-specific PAM config files,

# and should contain a list of modules that define the services to be

# used to change user passwords. The default is pam\_unix.

# Explanation of pam\_unix options:

# The "yescrypt" option enables

#hashed passwords using the yescrypt algorithm, introduced in Debian

#11. Without this option, the default is Unix crypt. Prior releases

#used the option "sha512"; if a shadow password hash will be shared

#between Debian 11 and older releases replace "yescrypt" with "sha512"

#for compatibility . The "obscure" option replaces the old

#`OBSCURE\_CHECKS\_ENAB' option in login.defs. See the pam\_unix manpage

#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.

# To take advantage of this, it is recommended that you configure any

# local modules either before or after the default block, and use

# pam-auth-update to manage selection of other modules. See

# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)

password requisite pam\_pwquality.so retry=3

password [success=2 default=ignore] pam\_unix.so obscure use\_authtok try\_first\_pass yescrypt minlen=8

password sufficient pam\_sss.so use\_authtok

# here's the fallback if no module succeeds

password requisite pam\_deny.so

# prime the stack with a positive return value if there isn't one already;

# this avoids us returning an error just because nothing sets a success code

# since the modules above will each just jump around

password required pam\_permit.so

# and here are more per-package modules (the "Additional" block)

password optional pam\_gnome\_keyring.so

# end of pam-auth-update config

## iptables -L

Chain INPUT (policy DROP)

target prot opt source destination

Chain FORWARD (policy DROP)

target prot opt source destination

DOCKER-USER all -- anywhere anywhere

DOCKER-ISOLATION-STAGE-1 all -- anywhere anywhere

ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED

DOCKER all -- anywhere anywhere

ACCEPT all -- anywhere anywhere

ACCEPT all -- anywhere anywhere

ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED

DOCKER all -- anywhere anywhere

ACCEPT all -- anywhere anywhere

ACCEPT all -- anywhere anywhere

Chain OUTPUT (policy DROP)

target prot opt source destination

Chain DOCKER (2 references)

target prot opt source destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)

target prot opt source destination

DOCKER-ISOLATION-STAGE-2 all -- anywhere anywhere

DOCKER-ISOLATION-STAGE-2 all -- anywhere anywhere

RETURN all -- anywhere anywhere

Chain DOCKER-ISOLATION-STAGE-2 (2 references)

target prot opt source destination

DROP all -- anywhere anywhere

DROP all -- anywhere anywhere

RETURN all -- anywhere anywhere

Chain DOCKER-USER (1 references)

target prot opt source destination

RETURN all -- anywhere anywhere

## crontab

# Edit this file to introduce tasks to be run by cron.

#

# Each task to run has to be defined through a single line

# indicating with different fields when the task will be run

# and what command to run for the task

#

# To define the time you can provide concrete values for

# minute (m), hour (h), day of month (dom), month (mon),

# and day of week (dow) or use '\*' in these fields (for 'any').

#

# Notice that tasks will be started based on the cron's system

# daemon's notion of time and timezones.

#

# Output of the crontab jobs (including errors) is sent through

# email to the user the crontab file belongs to (unless redirected).

#

# For example, you can run a backup of all your user accounts

# at 5 a.m every week with:

# 0 5 \* \* 1 tar -zcf /var/backups/home.tgz /home/

#

# For more information see the manual pages of crontab(5) and cron(8)

#

# m h dom mon dow command

30 18 \* \* 5 /usr/local/bin/backup\_ex2.sh

0 8 \* \* \* logwatch --detail low --mailto xal --service all --range today

0 4 \* \* 1 /root/weekly\_avscan.sh

0 2 1 \* \* freshclam