Bulletproof Penguin

Bulletproof Penguin

https://tryhackme.com/room/bppenguin

redis

`vim /etc/redis/redis.conf`

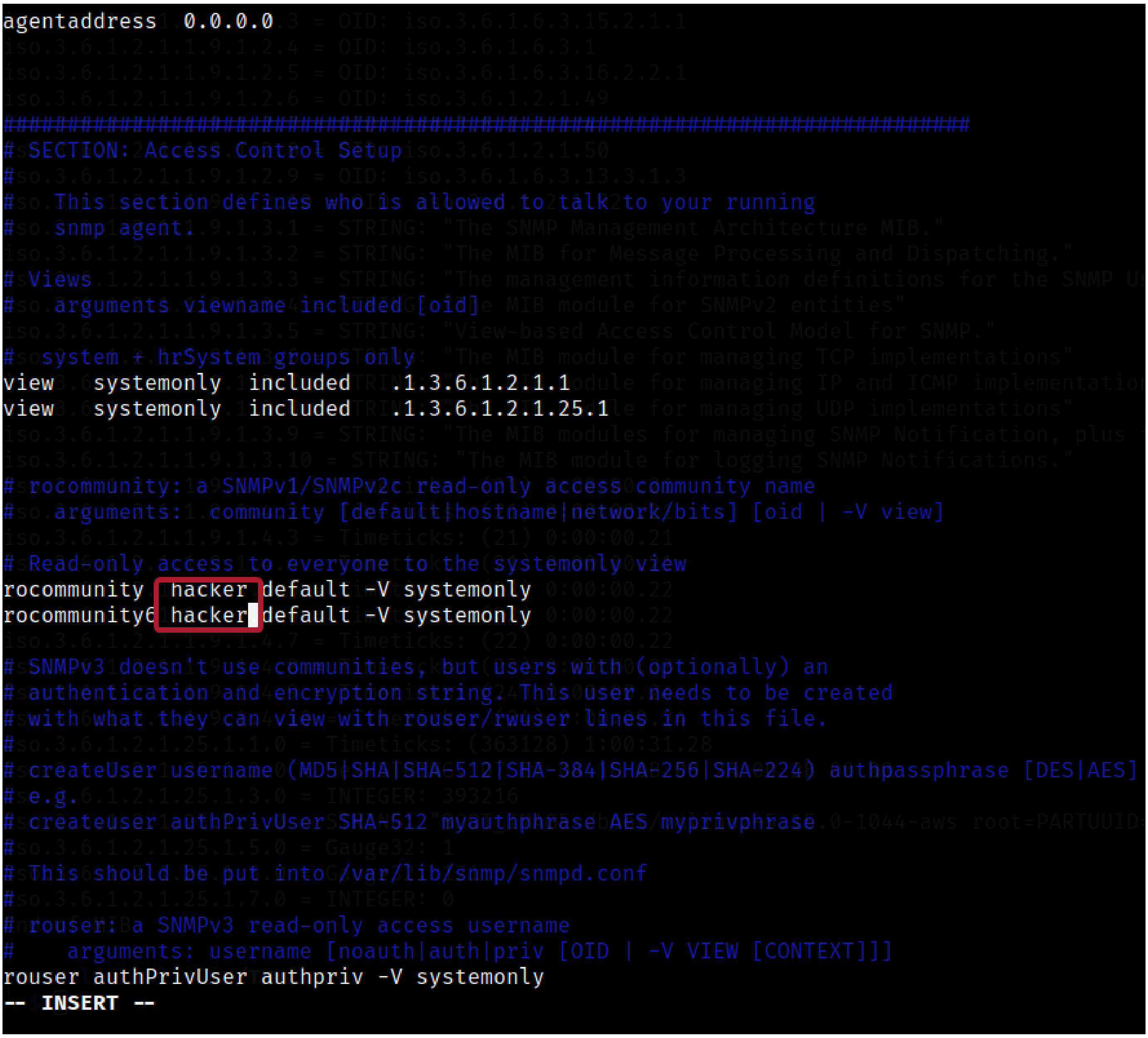
`/\<requirepass\>` (to find in "requirepass" vim)

`sudo systemctl restart redis`

snmp

`vim /etc/snmp/snmpd.conf`

Change names



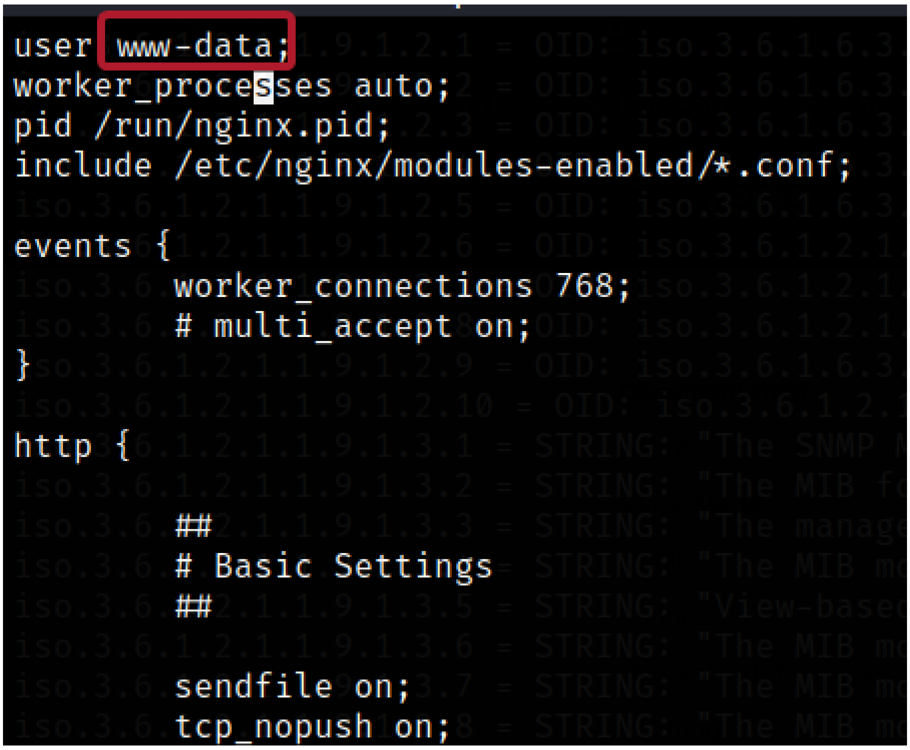
```
agentaddress  0.0.0.0
###########################################################################
# SECTION: Access Control Setup
#
#  This section defines who is allowed to talk to your running
#  snmp agent.

# Views
#  arguments viewname included [oid]

#  system + hrSystem groups only
view   systemonly  included   .1.3.6.1.2.1.1
view   systemonly  included   .1.3.6.1.2.1.25.1

# rocommunity: a SNMPv1/SNMPv2c read-only access community name
#  arguments:  community [default|hostname|network/bits] [oid | -V view]

# Read-only access to everyone to the systemonly view
rocommunity  hacker default -V systemonly
rocommunity6 hacker default -V systemonly

# SNMPv3 doesn't use communities, but users with (optionally) an
# authentication and encryption string. This user needs to be created
# with what they can view with rouser/rwuser lines in this file.
#
# createUser username (MD5|SHA|SHA-512|SHA-384|SHA-256|SHA-224) authpassphrase [DES|AES]
# e.g.
# createuser authPrivUser SHA-512 myauthphrase AES myprivphrase
#
# This should be put into /var/lib/snmp/snmpd.conf
#
# rouser: a SNMPv3 read-only access username
#    arguments: username [noauth|auth|priv [OID | -V VIEW [CONTEXT]]]
rouser authPrivUser authpriv -V systemonly
-- INSERT --
```

`systemctl restart snmpd.service`

nginx

`vim /etc/nginx/nginx.conf`

Change user root to user www-data

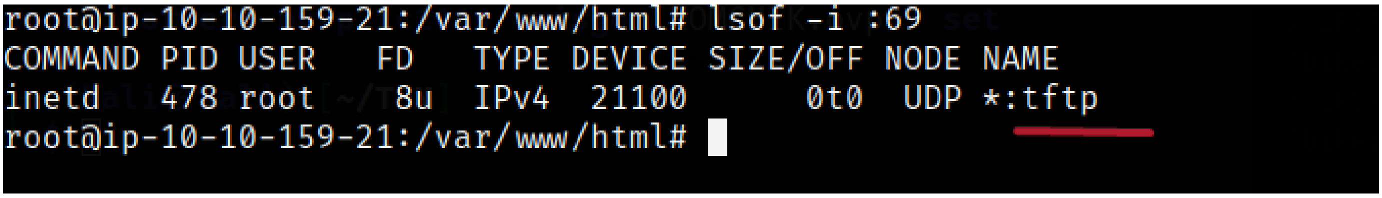


```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
        worker_connections 768;
        # multi_accept on;
}

http {

        ##
        # Basic Settings
        ##

        sendfile on;
        tcp_nopush on;
```

`systemctl restart nginx`

telnet

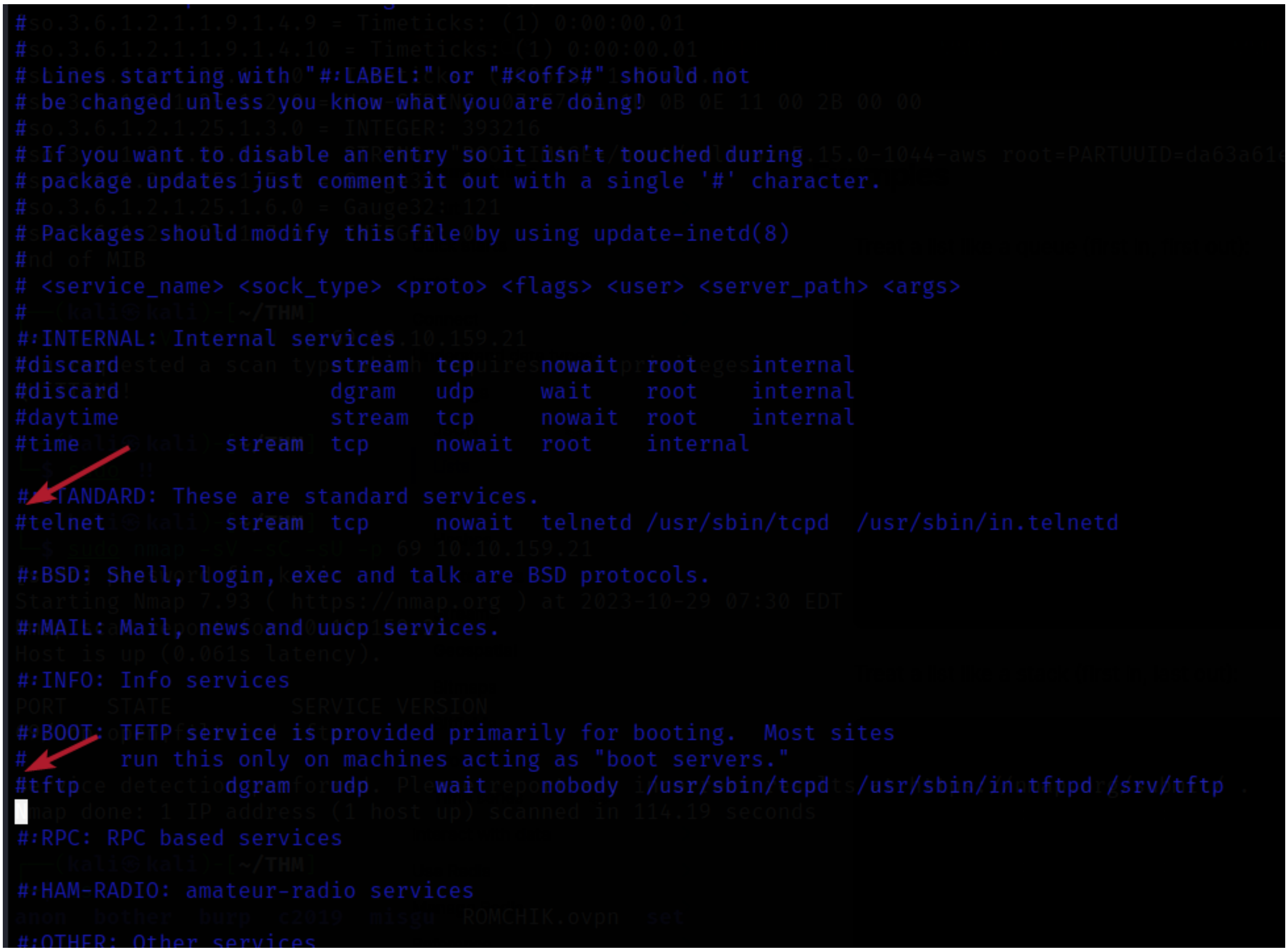
`lsof -i :69`



```
root@ip-10-10-159-21:/var/www/html# lsof -i :69
COMMAND PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
inetd   478 root    8u  IPv4  21100      0t0  UDP *:tftp
root@ip-10-10-159-21:/var/www/html#
```

`vim /etc/inetd.conf`

comment this 2 services

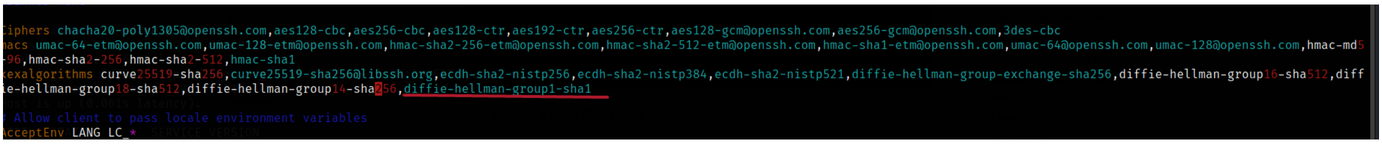


```
#
#
# Lines starting with "#:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# If you want to disable an entry so it isn't touched during
# package updates just comment it out with a single '#' character.
#
# Packages should modify this file by using update-inetd(8)
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
#:INTERNAL: Internal services
#discard                stream  tcp     nowait  root    internal
#discard                dgram   udp     wait    root    internal
#daytime                stream  tcp     nowait  root    internal
#time           stream  tcp     nowait  root    internal

#:STANDARD: These are standard services.
#telnet         stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd

#:BSD: Shell, login, exec and talk are BSD protocols.

#:MAIL: Mail, news and uucp services.

#:INFO: Info services

#:BOOT: TFTP service is provided primarily for booting.  Most sites
#       run this only on machines acting as "boot servers."
#tftp           dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd /srv/tftp

#:RPC: RPC based services

#:HAM-RADIO: amateur-radio services

#:OTHER: Other services
```

`systemctl restart inetd.service`

ssh

remove this



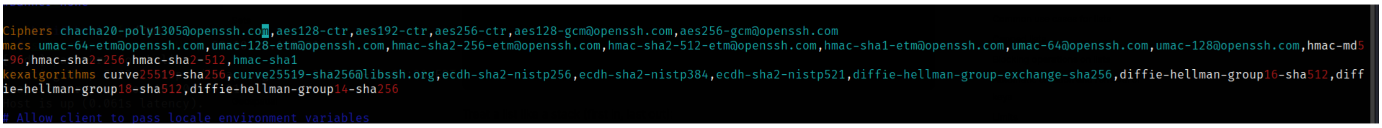
```
Ciphers chacha20-poly1305@openssh.com,aes128-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,3des-cbc
macs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-md5
-96,hmac-sha2-256,hmac-sha2-512,hmac-sha1
kexalgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diff
ie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group1-sha1

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*
```

and this:

3des-cbc

aes128-cbc

aes256-cbc



```
Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
macs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-md5
-96,hmac-sha2-256,hmac-sha2-512,hmac-sha1
kexalgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diff
ie-hellman-group18-sha512,diffie-hellman-group14-sha256

# Allow client to pass locale environment variables
```

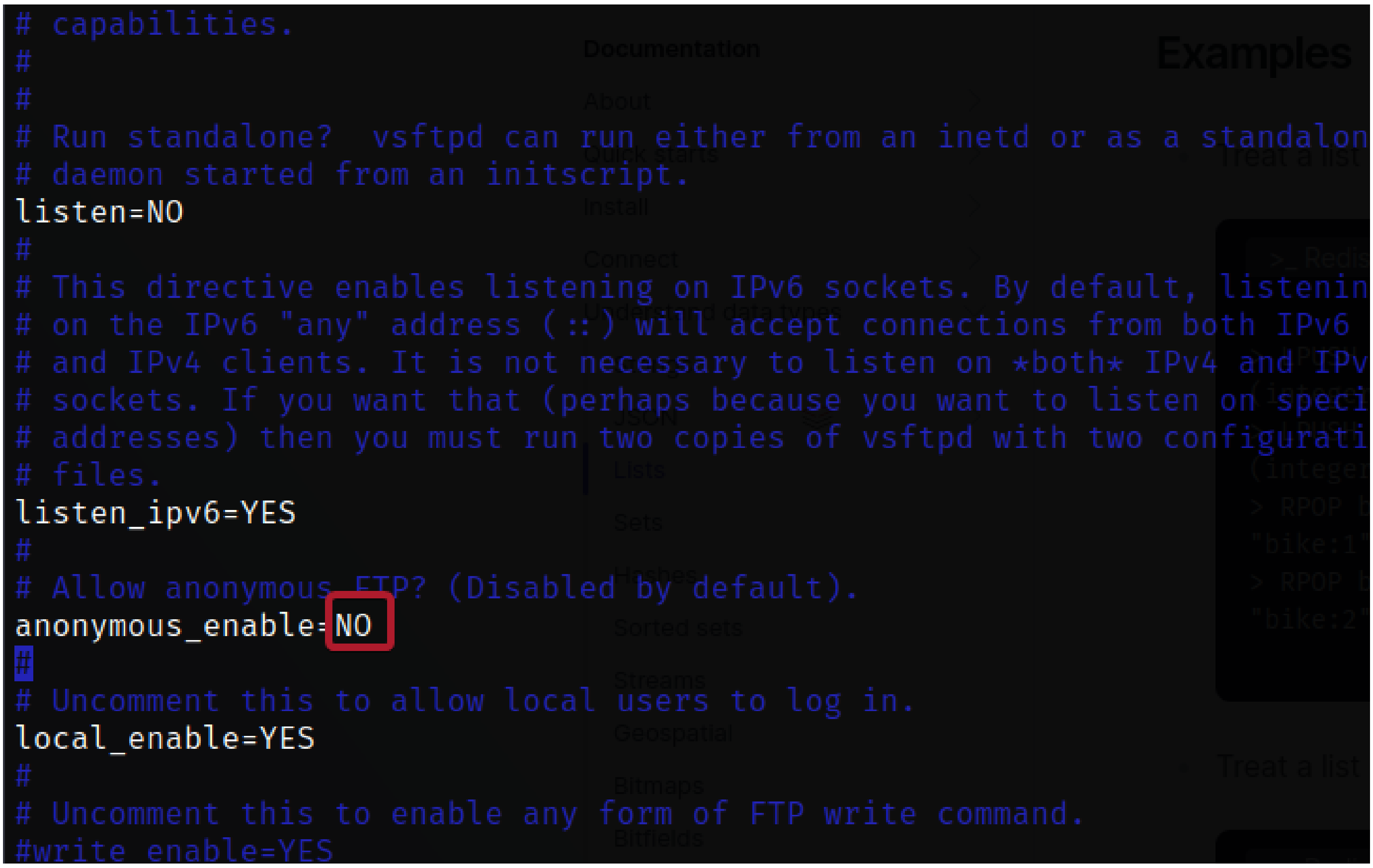
and this:

hmac-md5-96

FTP

`vim /etc/vsftpd.conf`

change "anonymous_enable=YES" to "anonymous_enable=NO"



```
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalon
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listenin
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv
# sockets. If you want that (perhaps because you want to listen on speci
# addresses) then you must run two copies of vsftpd with two configurati
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
#write_enable=YES
```

`systemctl restart vsftpd.service`

weak passwords

`userdel joseph`

`userdel test1`

`passwd munra`(write hard password)

`passwd mary`(write hard password)

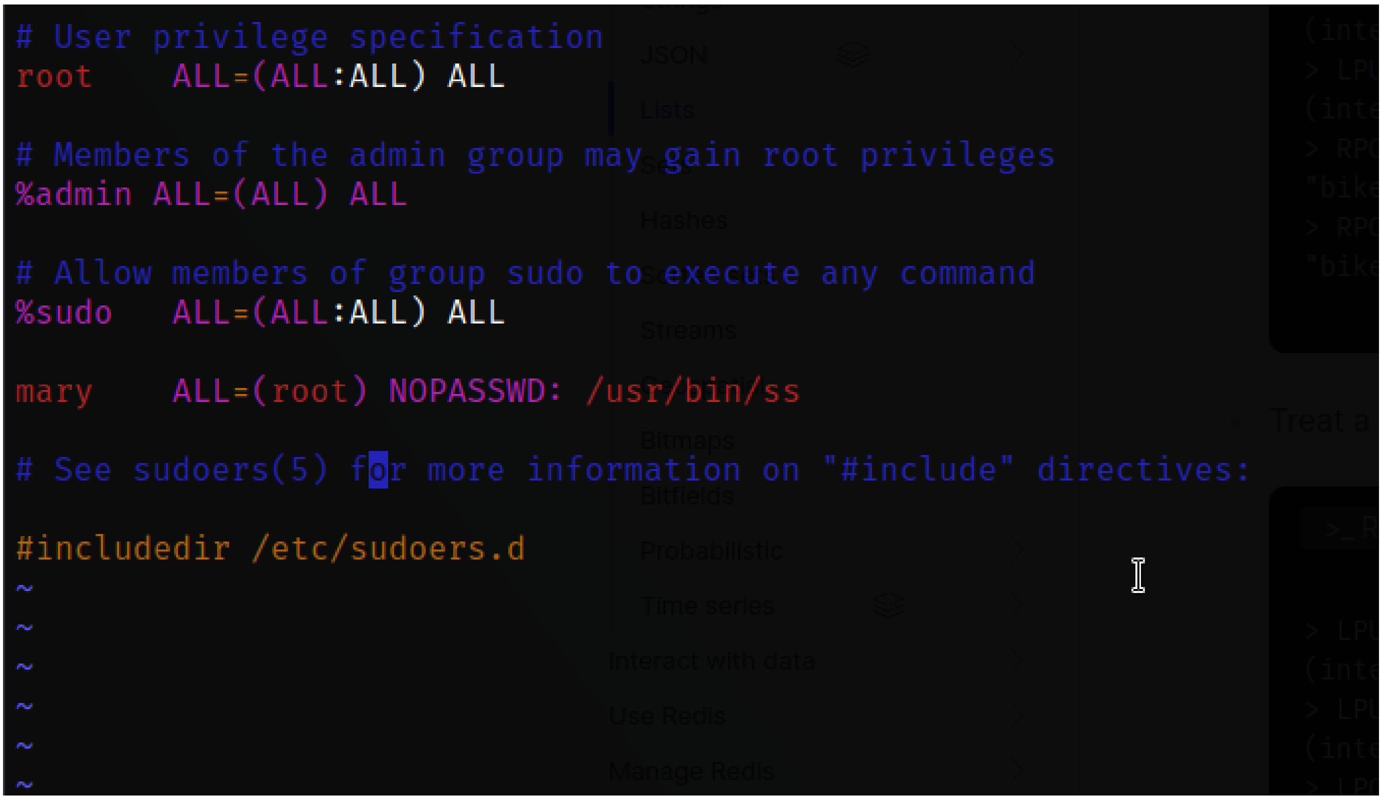
sudo

`vim /etc/sudoers`

delete user munra from this file

add rules for user mary:

```
mary ALL=(root) NOPASSWD: /usr/bin/ss
```

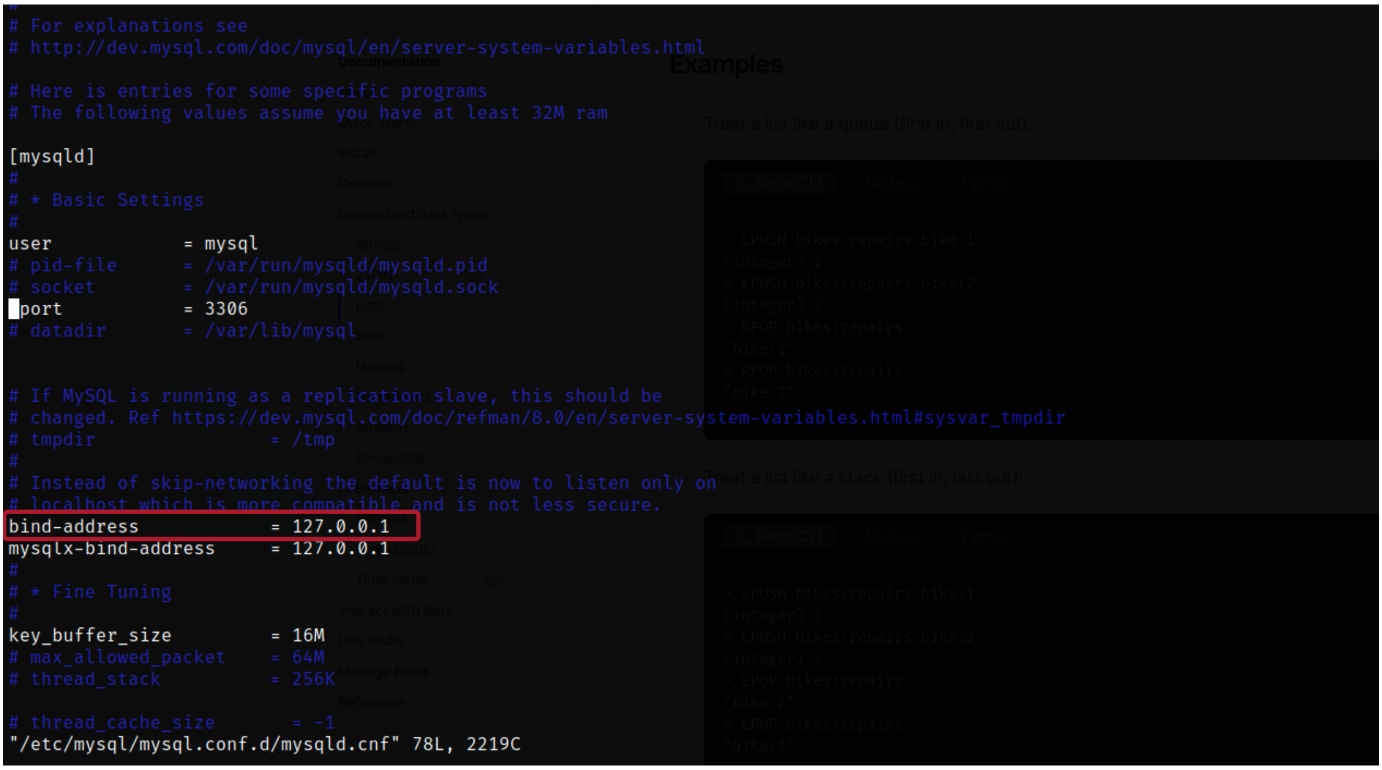


```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# 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

mary    ALL=(root) NOPASSWD: /usr/bin/ss

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

#includedir /etc/sudoers.d
~
~
~
~
~
~
```

databases

```
vim /etc/mysql/mysql.conf.d/mysqld.cnf
```

Change rules for SQL (only localhost listening)

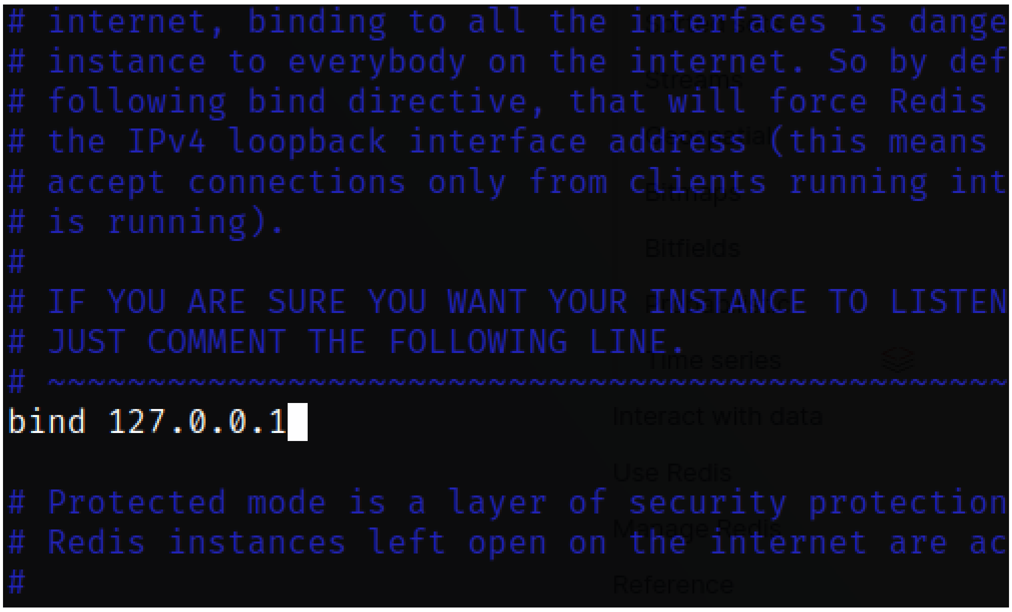


```
# For explanations see
# http://dev.mysql.com/doc/mysql/en/server-system-variables.html

# Here is entries for some specific programs
# The following values assume you have at least 32M ram

[mysqld]
#
# * Basic Settings
#
user            = mysql
# pid-file      = /var/run/mysqld/mysqld.pid
# socket        = /var/run/mysqld/mysqld.sock
port            = 3306
# datadir       = /var/lib/mysql


# If MySQL is running as a replication slave, this should be
# changed. Ref https://dev.mysql.com/doc/refman/8.0/en/server-system-variables.html#sysvar_tmpdir
# tmpdir                = /tmp
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 127.0.0.1
mysqlx-bind-address     = 127.0.0.1
#
# * Fine Tuning
#
key_buffer_size         = 16M
# max_allowed_packet    = 64M
# thread_stack          = 256K

# thread_cache_size       = -1
"/etc/mysql/mysql.conf.d/mysqld.cnf" 78L, 2219C
```

```
systemctl restart mysql.service
```

```
vim /etc/redis/redis.conf
```

Change "bind" from 0.0.0.0 to 127.0.0.1

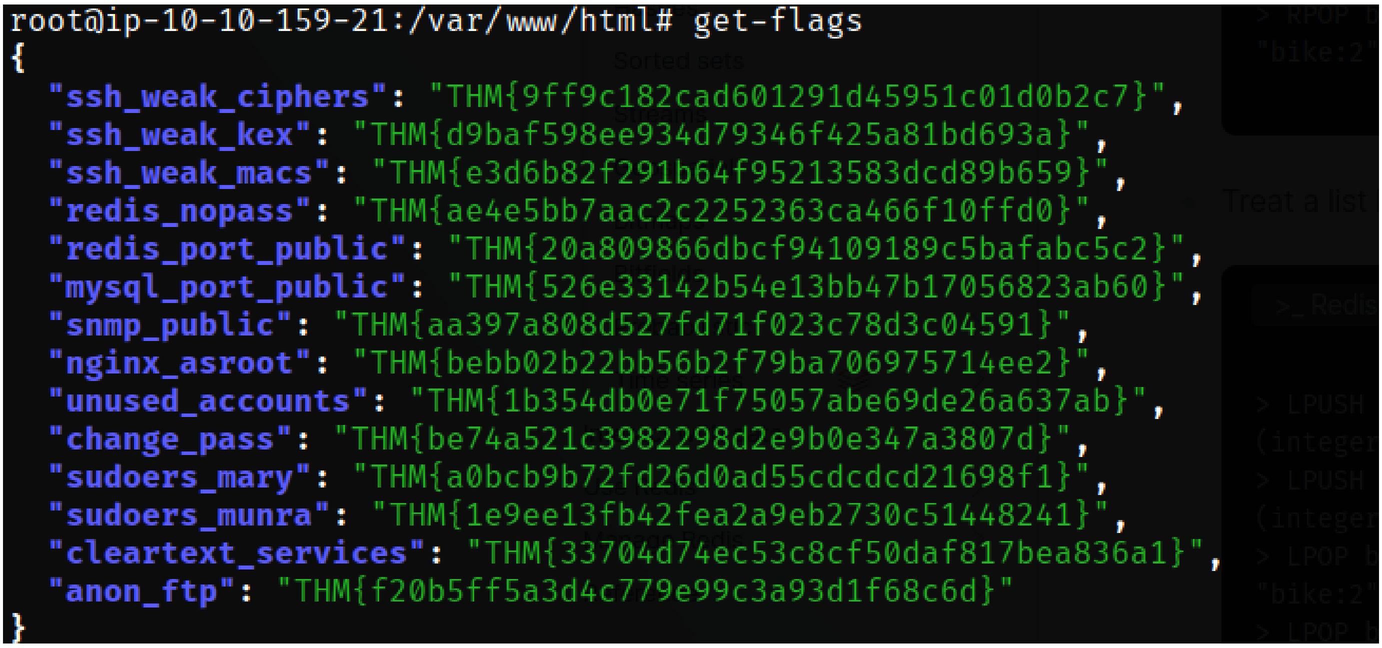


```
# internet, binding to all the interfaces is dange
# instance to everybody on the internet. So by def
# following bind directive, that will force Redis
# the IPv4 loopback interface address (this means
# accept connections only from clients running int
# is running).
#
# IF YOU ARE SURE YOU WANT YOUR INSTANCE TO LISTEN
# JUST COMMENT THE FOLLOWING LINE.
# ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
bind 127.0.0.1

# Protected mode is a layer of security protection
# Redis instances left open on the internet are ac
#
```

`systemctl restart redis`

finish

`get-flags`



```
root@ip-10-10-159-21:/var/www/html# get-flags
{
  "ssh_weak_ciphers": "THM{9ff9c182cad601291d45951c01d0b2c7}",
  "ssh_weak_kex": "THM{d9baf598ee934d79346f425a81bd693a}",
  "ssh_weak_macs": "THM{e3d6b82f291b64f95213583dcd89b659}",
  "redis_nopass": "THM{ae4e5bb7aac2c2252363ca466f10ffd0}",
  "redis_port_public": "THM{20a809866dbcf94109189c5bafabc5c2}",
  "mysql_port_public": "THM{526e33142b54e13bb47b17056823ab60}",
  "snmp_public": "THM{aa397a808d527fd71f023c78d3c04591}",
  "nginx_asroot": "THM{bebb02b22bb56b2f79ba706975714ee2}",
  "unused_accounts": "THM{1b354db0e71f75057abe69de26a637ab}",
  "change_pass": "THM{be74a521c3982298d2e9b0e347a3807d}",
  "sudoers_mary": "THM{a0bcb9b72fd26d0ad55cdcdcd21698f1}",
  "sudoers_munra": "THM{1e9ee13fb42fea2a9eb2730c51448241}",
  "cleartext_services": "THM{33704d74ec53c8cf50daf817bea836a1}",
  "anon_ftp": "THM{f20b5ff5a3d4c779e99c3a93d1f68c6d}"
}
```