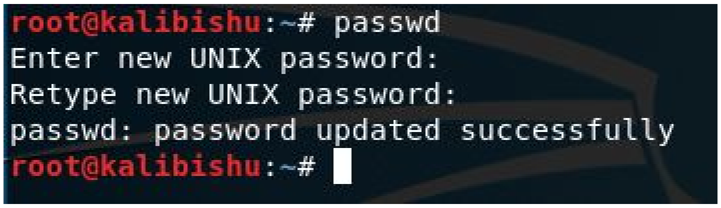
# System Hardening (Kali Linux Gnu) (64-bit OS)

#1 a. Changing Root password

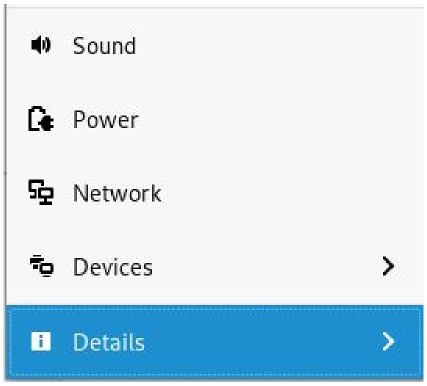
- Login as root.
- Open up the terminal and type the “**passwd**” command.
- Type new password twice.
- Your root password is changed.

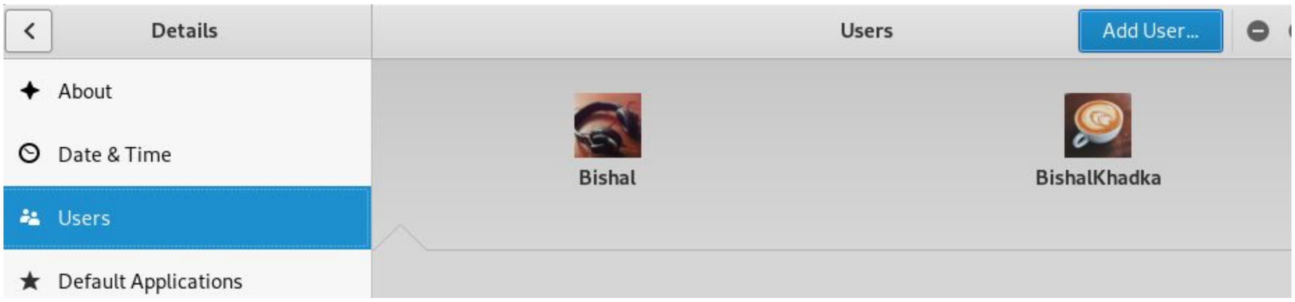


```
root@kalibishu:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kalibishu:~# 
```

#1 b. Creating a new user and changing the password

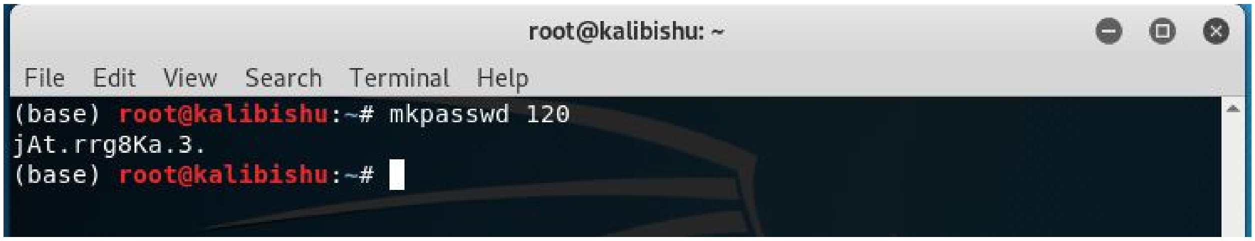
- Go to **settings** => **Users**
- Click on **Add User** which is on the top right corner of the window
- Set the username and password for the user.
- Log out from the root user and login as a regular user.
- Follow #1 a. to change the password for the current user.





### Making a random strong password

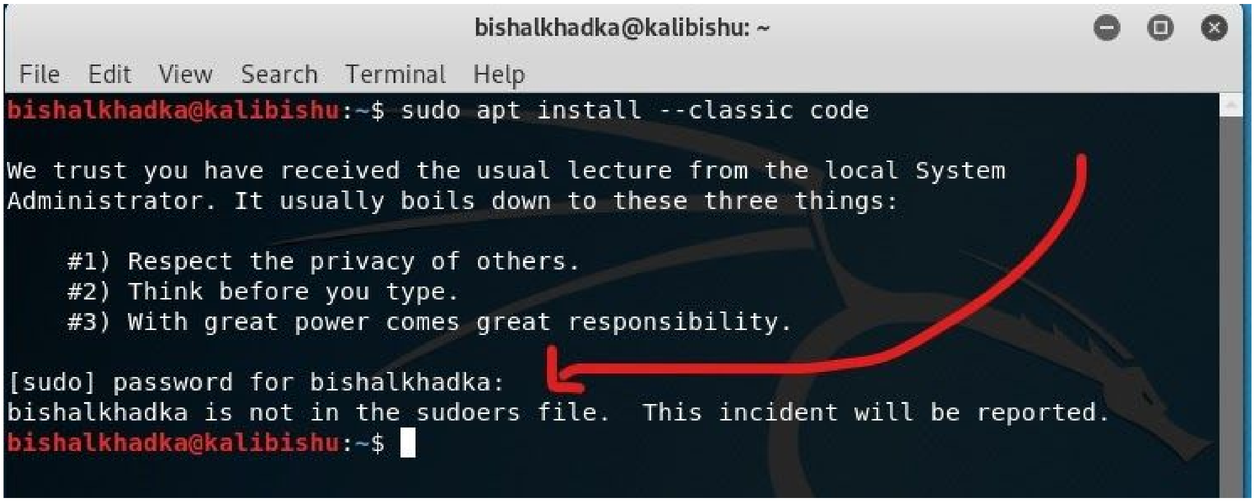
- Type “**mkpasswd numberOfBits**”, where “**mkpasswd 120**” makes a random password of 120 bits.



```
(base) root@kalibishu:~# mkpasswd 120
jAt.rrg8Ka.3.
(base) root@kalibishu:~# 
```

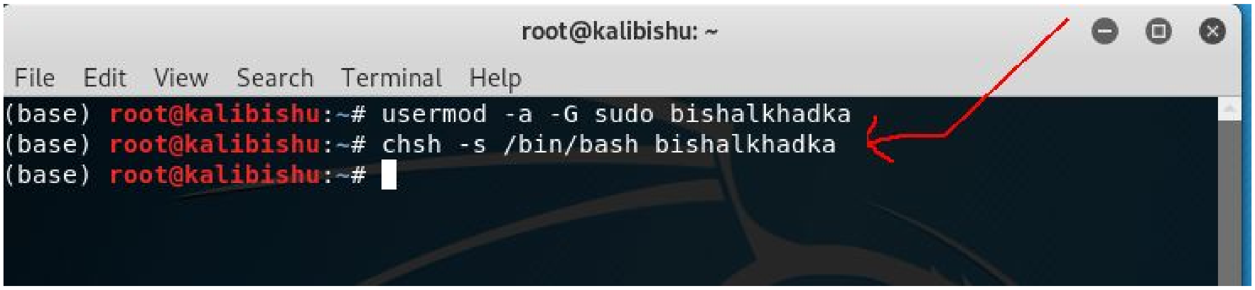
#1 c. Giving permission to regular user as sudoers

- Log out from the root and login as a regular user.
- Unless the root does not give the user permission, the user is not recognized as sudoer, so basically you cannot download or install anything on a system.


bishalkhadka@kalibishu: ~
File Edit View Search Terminal Help

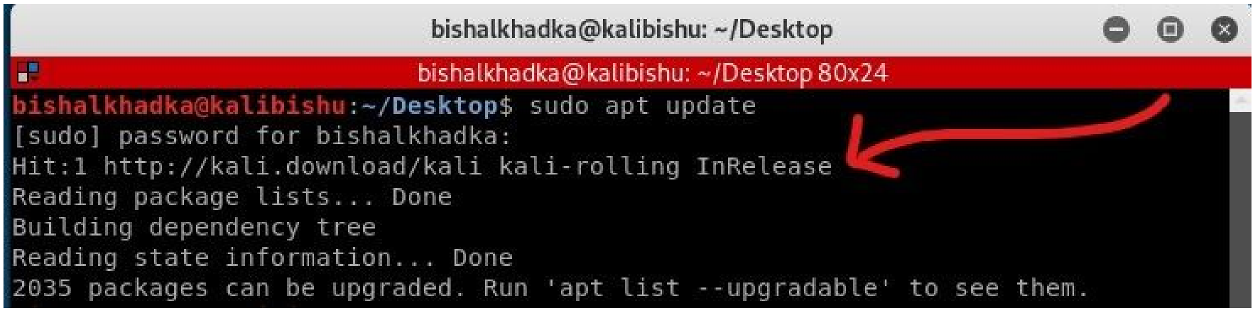
```
bishalkhadka@kalibishu:~$ sudo apt install --classic code

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for bishalkhadka:
bishalkhadka is not in the sudoers file.  This incident will be reported.
bishalkhadka@kalibishu:~$ 
```

- To make the user sudoer,open up the terminal and type “ **usermod -a -G sudo bishalkhadka**” to give sudo permission to the user “bishalkhadka”.
- Specify the shell for the user by typing “**chsh -s /bin/bash bishalkhadka**”.



```
(base) root@kalibishu:~# usermod -a -G sudo bishalkhadka
(base) root@kalibishu:~# chsh -s /bin/bash bishalkhadka
(base) root@kalibishu:~# 
```

- After you perform the above mentioned steps, the user will now have the sudo privilege.

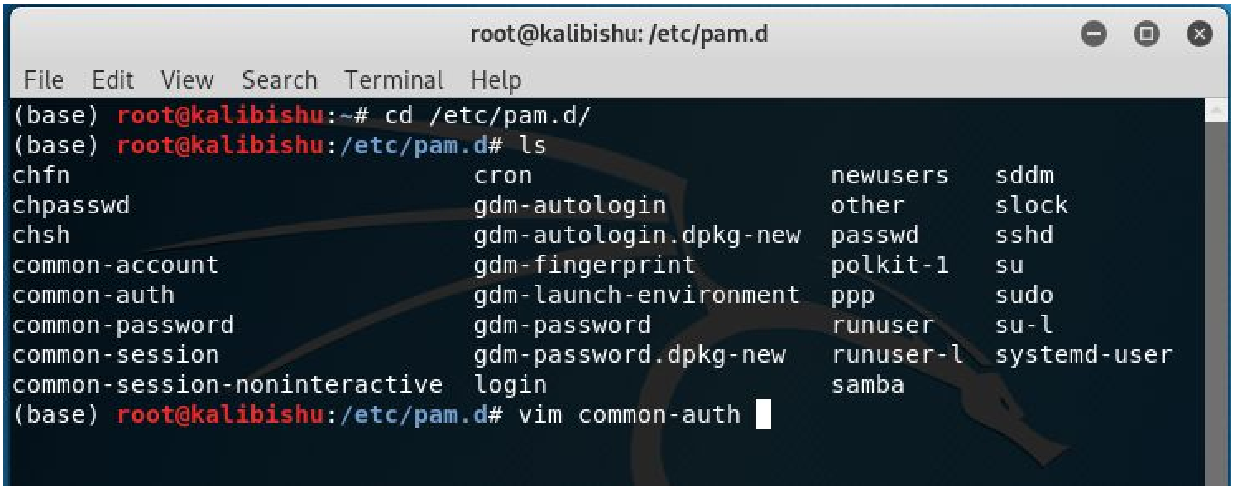


bishalkhadka@kalibishu: ~/Desktop
bishalkhadka@kalibishu: ~/Desktop 80x24

```
bishalkhadka@kalibishu:~/Desktop$ sudo apt update
[sudo] password for bishalkhadka:
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
2035 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

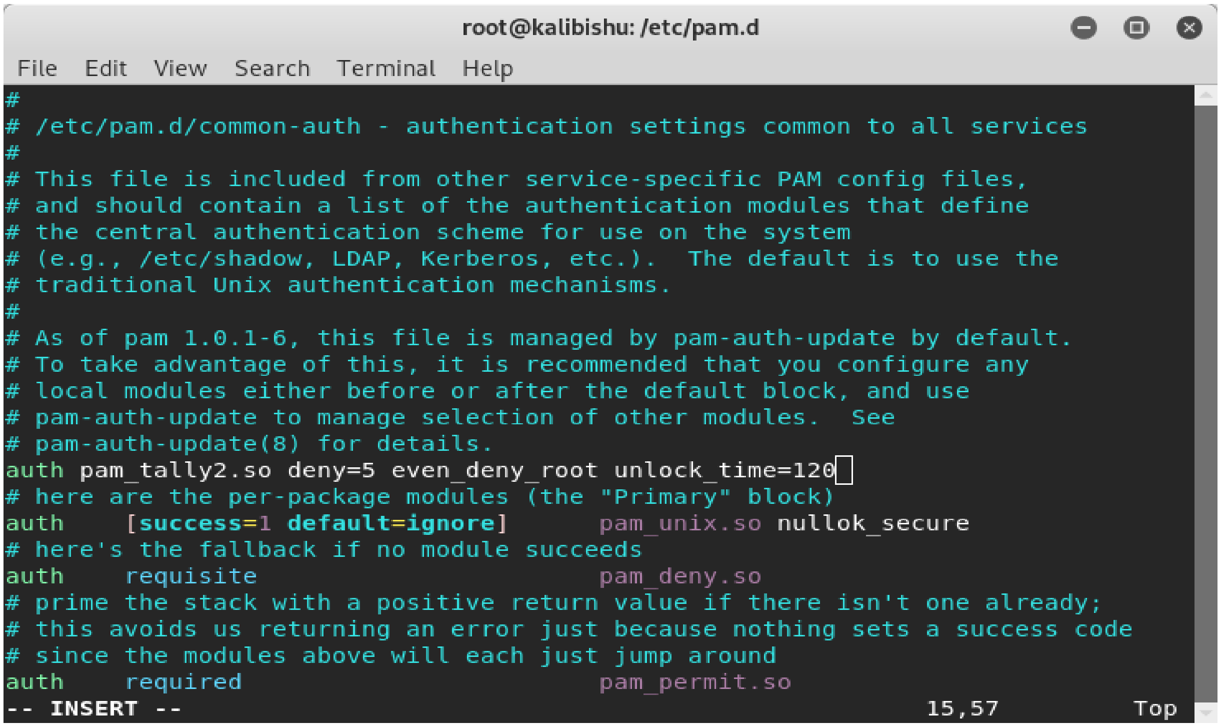
#1 d. Enabling System Lock out after 5 failed attempts

- Open up the terminal and go to /etc/pam.d folder
- Use your favourite command line editor emacs/vim/nano and edit “common-auth” file.
- Add “**auth required pam_tally2.so deny=5 even_deny_root unlock_time=120**” at the beginning of the auth section. Where, **pam_tally2** is used to lock user accounts after certain number of failed ssh login attempts to the system, **deny=5** is for denying access after 5 failed attempts to login, **even_deny_root** is for applying that rule to root users as well, and **unlock_time=120** means you need to wait for 2 mins to log back into the system again.

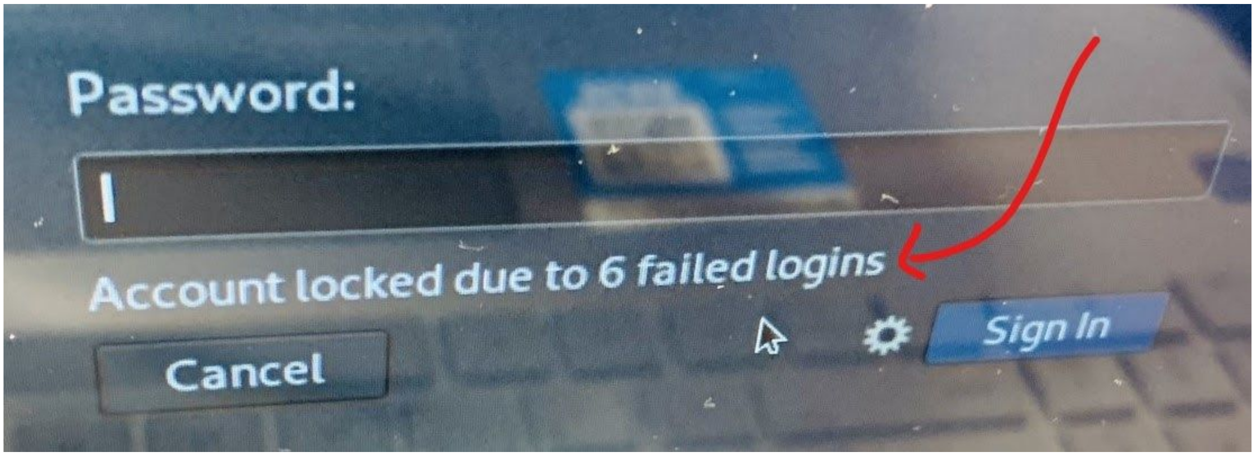


root@kalibishu: /etc/pam.d
File Edit View Search Terminal Help

```
(base) root@kalibishu:~# cd /etc/pam.d/
(base) root@kalibishu:/etc/pam.d# ls
chfn                           cron                      newusers   sddm
chpasswd                       gdm-autologin             other      slock
chsh                           gdm-autologin.dpkg-new    passwd     sshd
common-account                 gdm-fingerprint           polkit-1   su
common-auth                    gdm-launch-environment    ppp        sudo
common-password                gdm-password              runuser    su-l
common-session                 gdm-password.dpkg-new     runuser-l  systemd-user
common-session-noninteractive  login                     samba
(base) root@kalibishu:/etc/pam.d# vim common-auth
```

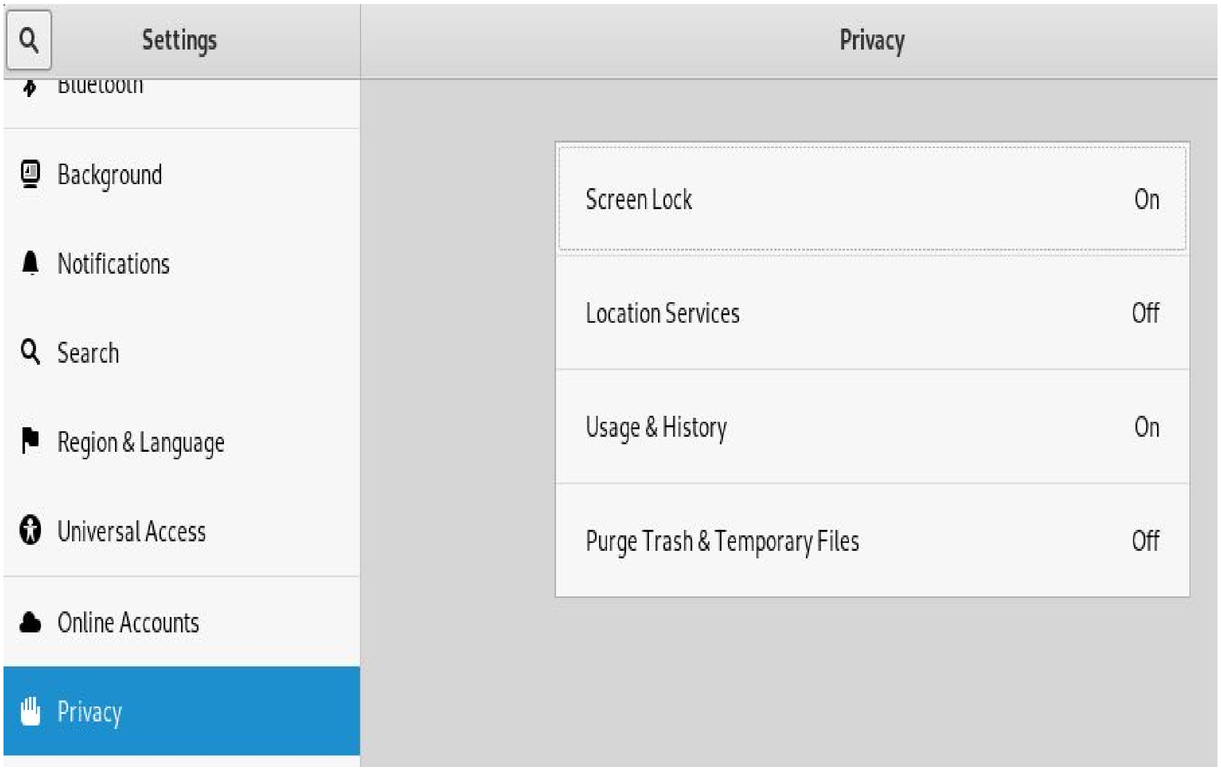

root@kalibishu: /etc/pam.d
File Edit View Search Terminal Help

```
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# 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.
auth pam_tally2.so deny=5 even_deny_root unlock_time=120
# here are the per-package modules (the "Primary" block)
auth    [success=1 default=ignore]      pam_unix.so nullok_secure
# here's the fallback if no module succeeds
auth    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
auth    required                        pam_permit.so
-- INSERT --                                                15,57         Top
```



#1 e. Locking User Screen After 15 Minutes of Inactivity

- Go to settings and click on “**privacy**”
- Click on the “**Screen Lock**” option and set it to your desired time.
- Close the window after setting the time limit.



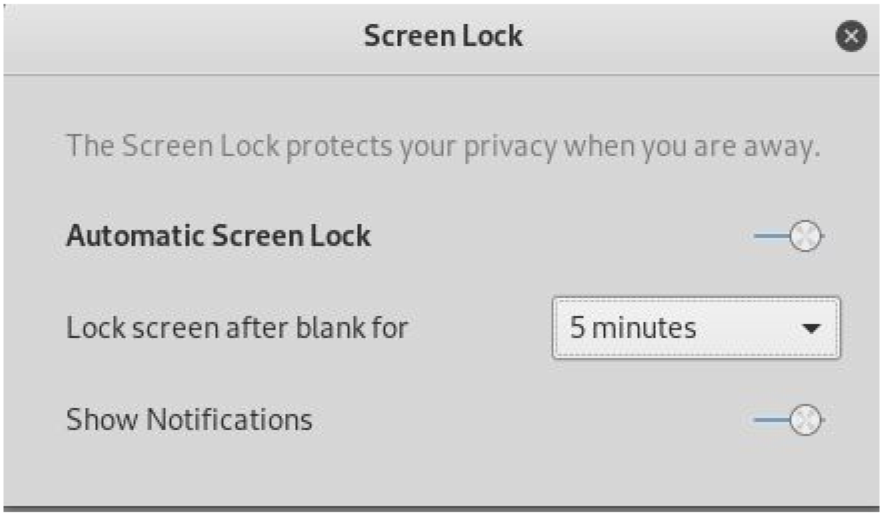
Privacy

Screen Lock On

Location Services Off

Usage & History On

Purge Trash & Temporary Files Off



Screen Lock

The Screen Lock protects your privacy when you are away.

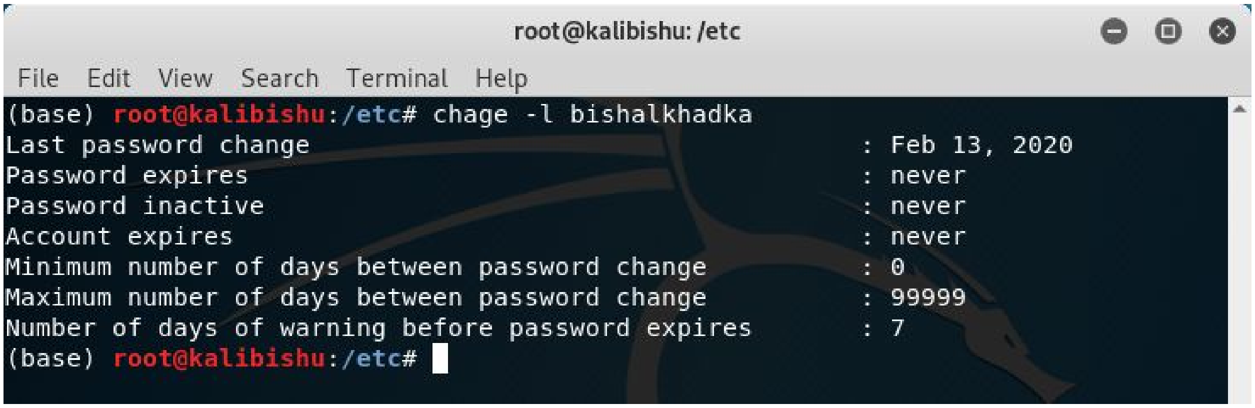
Automatic Screen Lock

Lock screen after blank for 5 minutes

Show Notifications

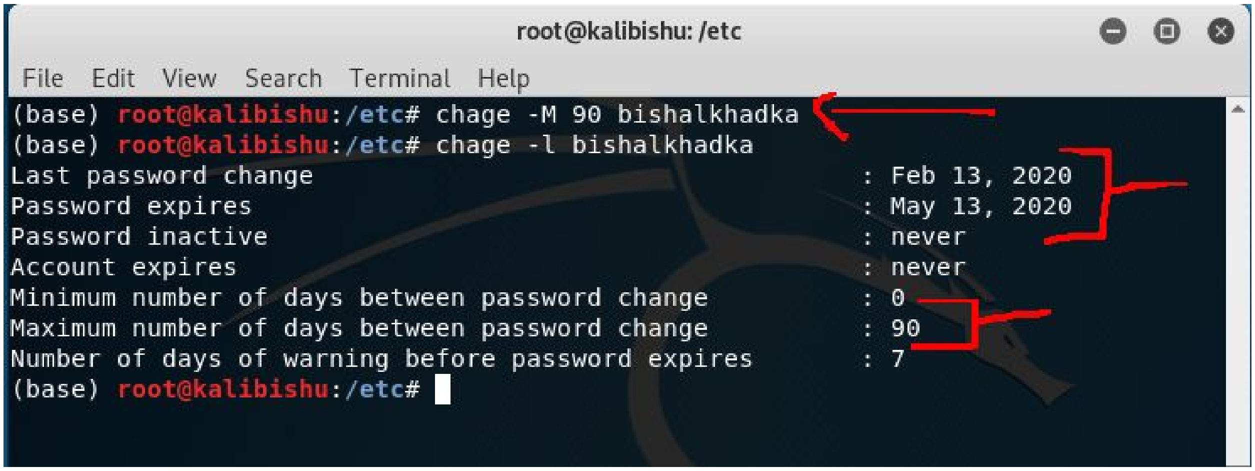
#1 f. Locking User Screen After 15 Minutes of Inactivity

- I have used **chage** command to change the age of the password.
- Type “**chage -l username**” to display the status of the password.



```
(base) root@kalibishu:/etc# chage -l bishalkhadka
Last password change                                    : Feb 13, 2020
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
(base) root@kalibishu:/etc#
```

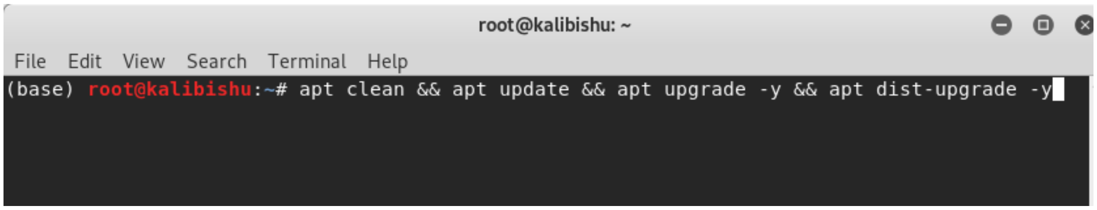
- In order to make your password expire after 90 days, type "**chage -M noOfDays Username**"



```
(base) root@kalibishu:/etc# chage -M 90 bishalkhadka
(base) root@kalibishu:/etc# chage -l bishalkhadka
Last password change                                    : Feb 13, 2020
Password expires                                        : May 13, 2020
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 7
(base) root@kalibishu:/etc#
```

#2 Update and Upgrade System

- Type "**sudo apt clean && sudo apt update && sudo apt upgrade -y && sudo apt dist-upgrade -y**" to clean, update, and upgrade your system in the terminal .



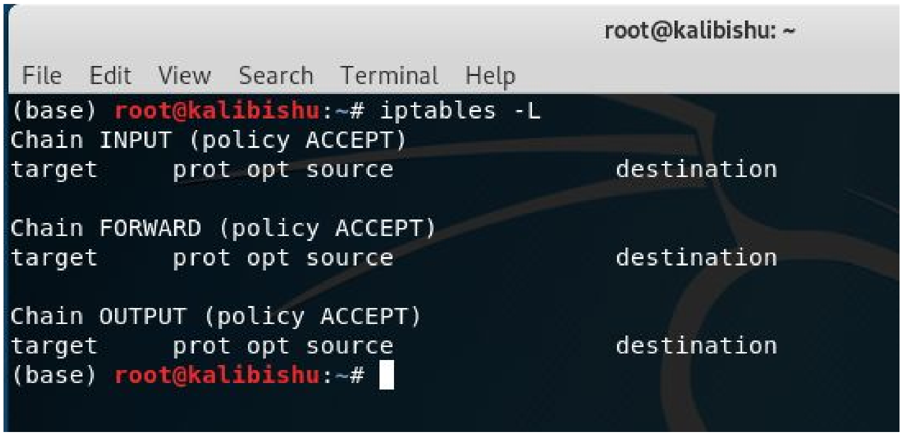
```
(base) root@kalibishu:~# apt clean && apt update && apt upgrade -y && apt dist-upgrade -y
```

#3 Step to see all the firewall rules using IPTABLES

- Iptable is the user-utility program to display all the firewall rules.

Using Command Line:

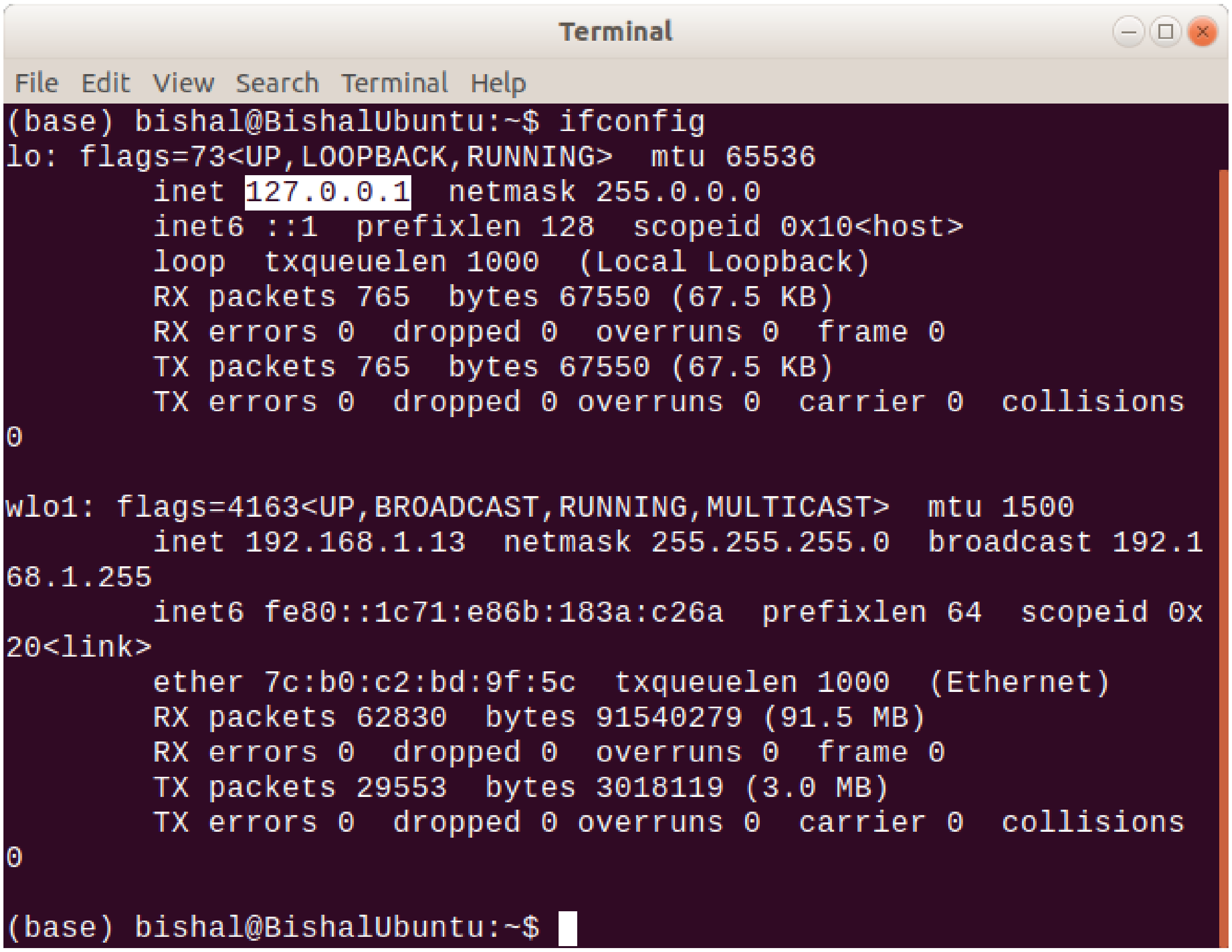
- Open up terminal and type “**iptables -L**” and it will list INPUT, OUTPUT, and FORWARD rules.
- To add a rule, type “**iptables -A INPUT/OUTPUT/FORWARD**”



```
(base) root@kalibishu:~# 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
(base) root@kalibishu:~#
```

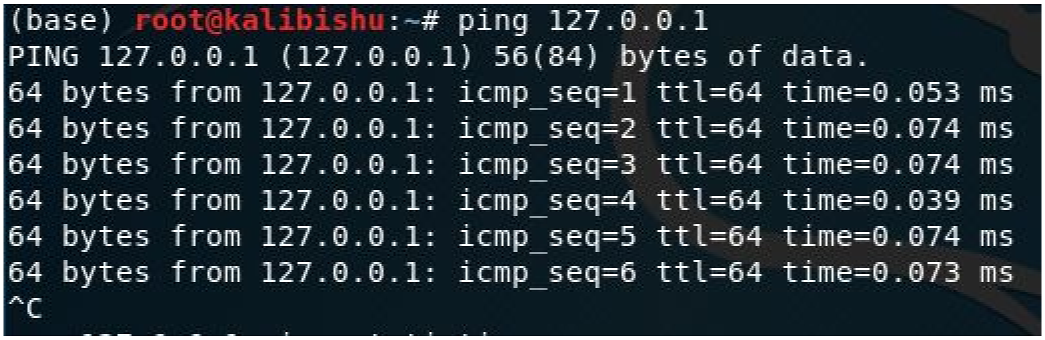
#4 Stop ping from a particular ip address

- First find the ip address of the device you want to block.



```
(base) bishal@BishalUbuntu:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 765  bytes 67550 (67.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 765  bytes 67550 (67.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.13  netmask 255.255.255.0  broadcast 192.1
68.1.255
        inet6 fe80::1c71:e86b:183a:c26a  prefixlen 64  scopeid 0x
20<link>
        ether 7c:b0:c2:bd:9f:5c  txqueuelen 1000  (Ethernet)
        RX packets 62830  bytes 91540279 (91.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29553  bytes 3018119 (3.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

(base) bishal@BishalUbuntu:~$
```

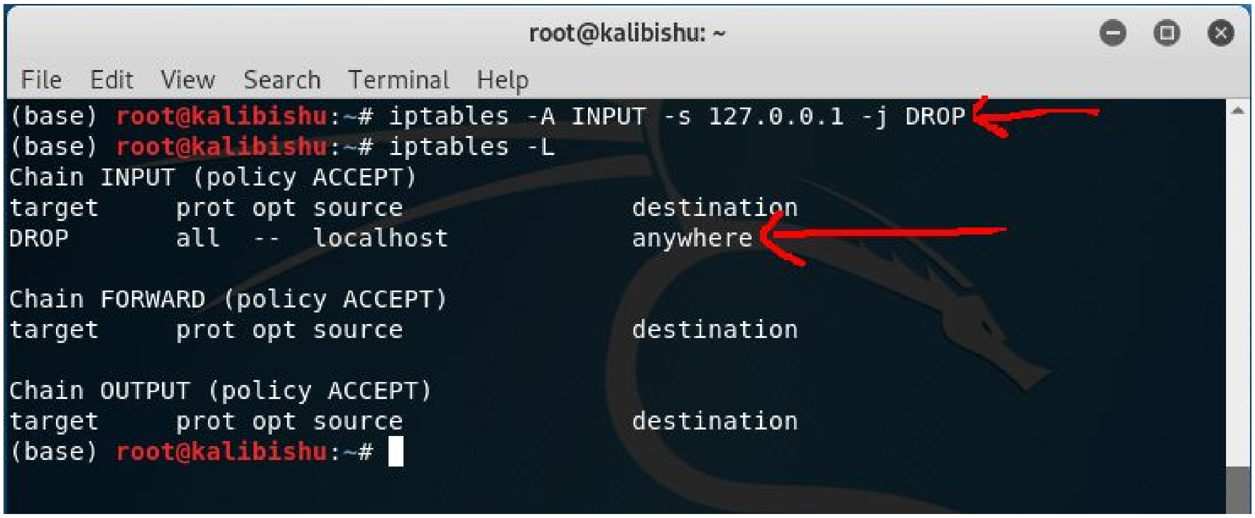
#4 a. Before Blocking



```
(base) root@kalibishu:~# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.073 ms
^C
```

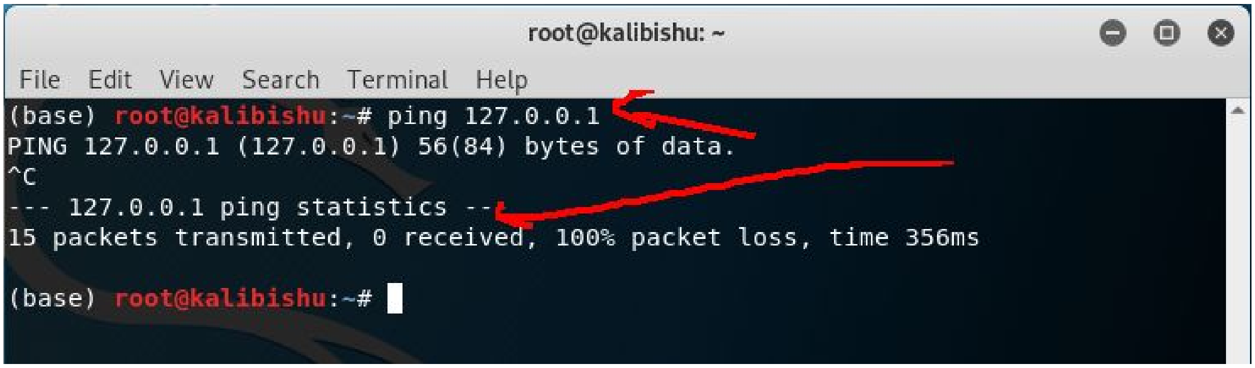
#4 b. To Block

In order to block the ip address type the following command.
“**Iptables -A INPUT -s ip address -j DROP**”



```
(base) root@kalibishu:~# iptables -A INPUT -s 127.0.0.1 -j DROP
(base) root@kalibishu:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  localhost            anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
(base) root@kalibishu:~# 
```

#4 c. After Blocking

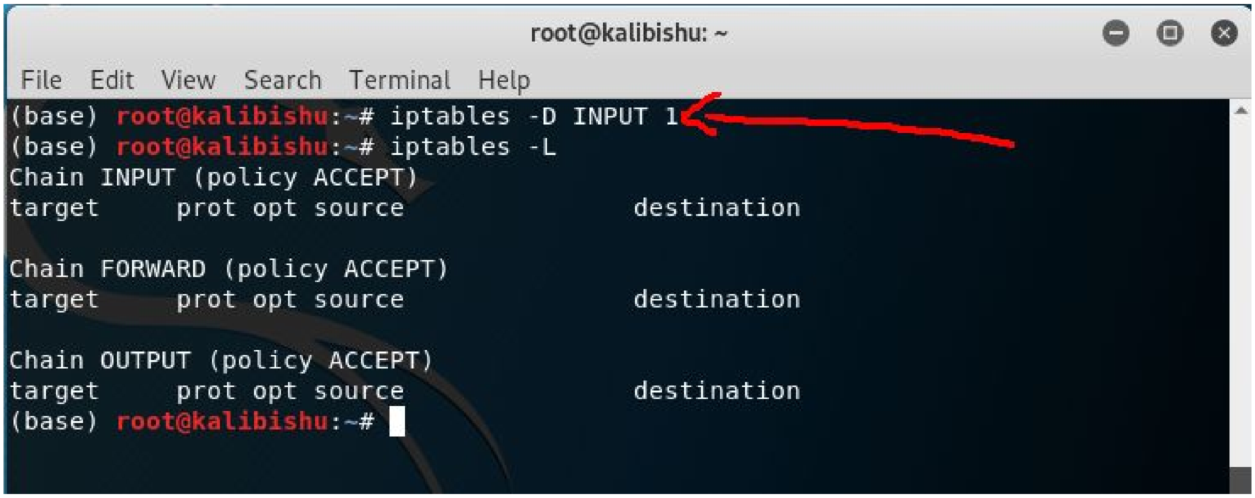


```
(base) root@kalibishu:~# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
^C
--- 127.0.0.1 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 356ms

(base) root@kalibishu:~# 
```

#4 d. Remove Blocking

In order to accept packets from that ip address, you need to remove the DROPPED ip address from the iptables by typing the following command.

“**Iptables -D INPUT rule#**”



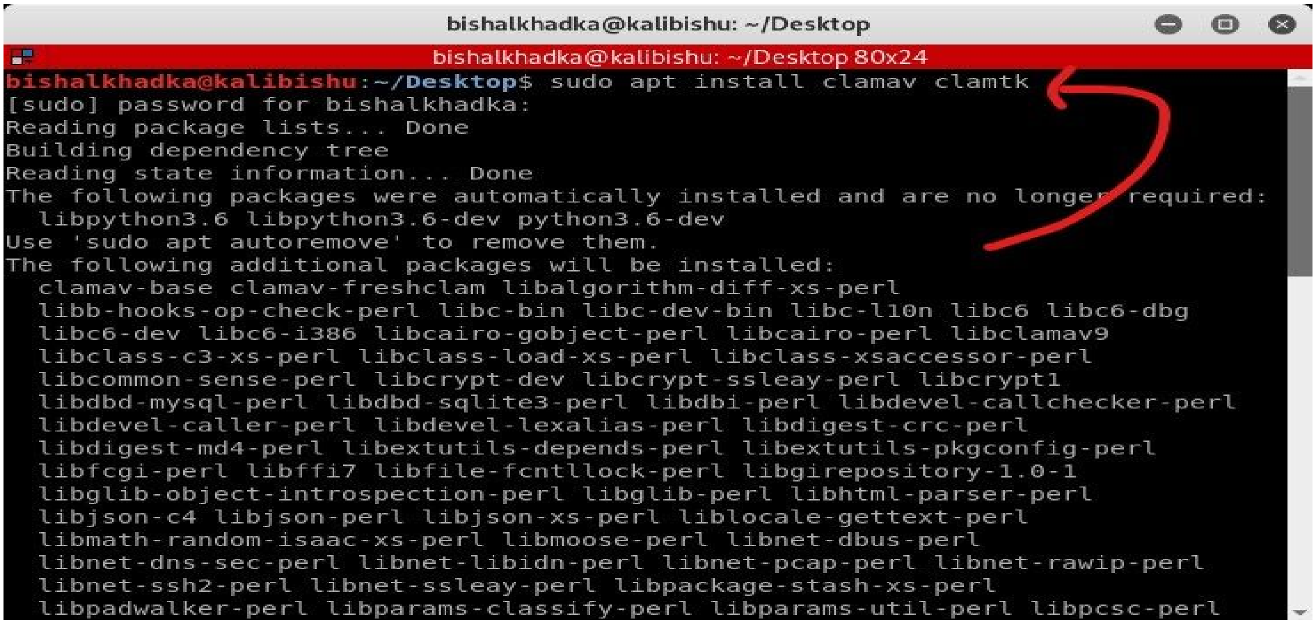
```
(base) root@kalibishu:~# iptables -D INPUT 1
(base) root@kalibishu:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
(base) root@kalibishu:~#
```

Now you can ping that ip address again that you have blocked before.

#5 Installing Anti-virus

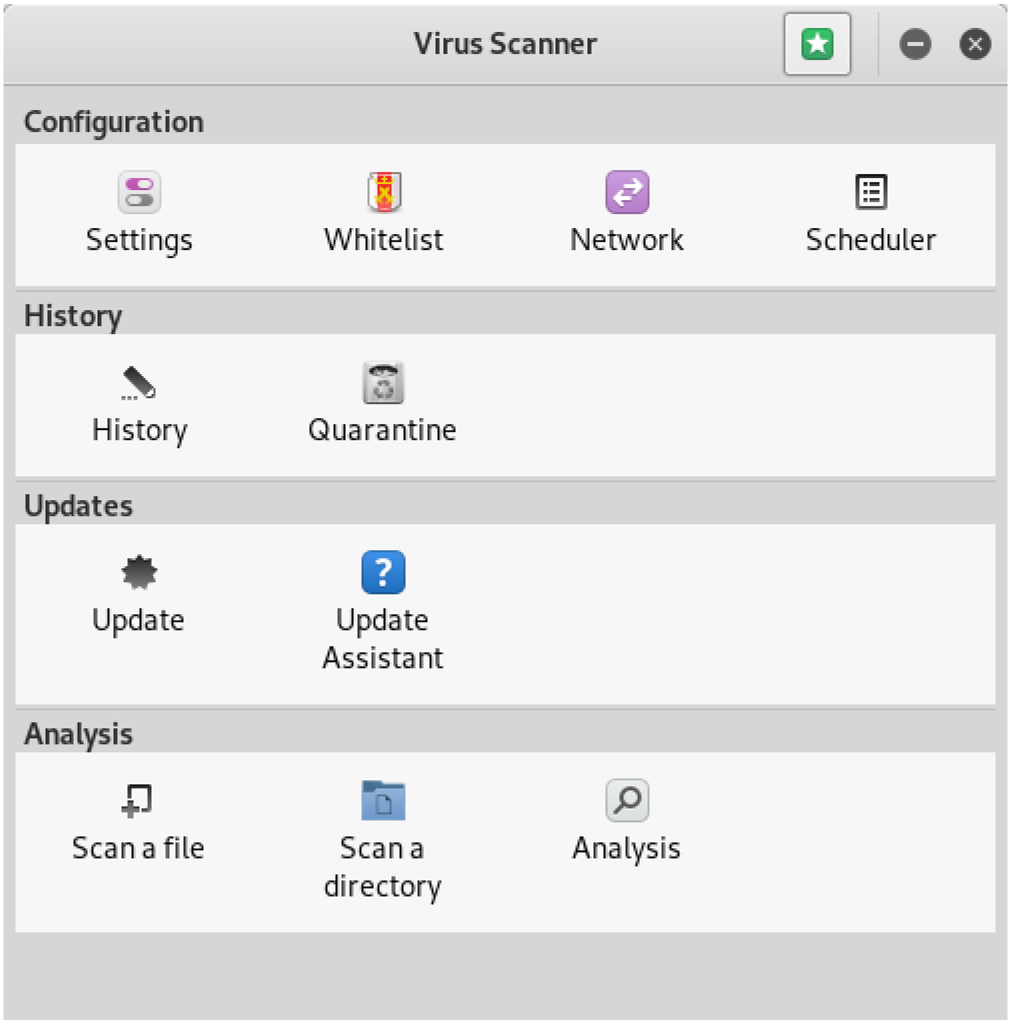
Installing ClamAV Antivirus in Kali Linux:

- Type in the command “**sudo apt install clamav clamtk**” to install clamAV Antivirus in your system.


bishalkhadka@kalibishu: ~/Desktop
bishalkhadka@kalibishu: ~/Desktop 80x24

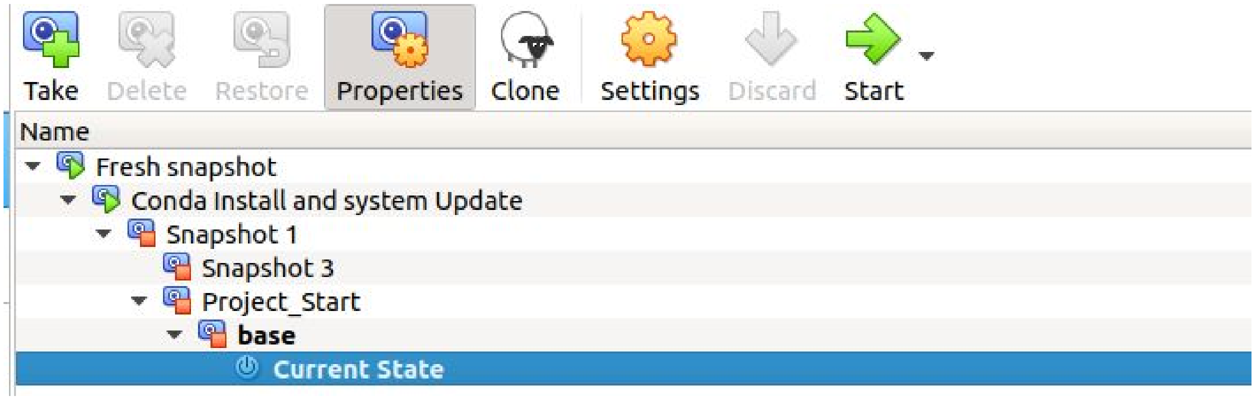
```
bishalkhadka@kalibishu:~/Desktop$ sudo apt install clamav clamtk
[sudo] password for bishalkhadka:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libpython3.6 libpython3.6-dev python3.6-dev
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  clamav-base clamav-freshclam libalgorithm-diff-xs-perl
  libb-hooks-op-check-perl libc-bin libc-dev-bin libc-l10n libc6 libc6-dbg
  libc6-dev libc6-i386 libcairo-gobject-perl libcairo-perl libclamav9
  libclass-c3-xs-perl libclass-load-xs-perl libclass-xsaccessor-perl
  libcommon-sense-perl libcrypt-dev libcrypt-ssleay-perl libcrypt1
  libdbd-mysql-perl libdbd-sqlite3-perl libdbi-perl libdevel-callchecker-perl
  libdevel-caller-perl libdevel-lexalias-perl libdigest-crc-perl
  libdigest-md4-perl libextutils-depends-perl libextutils-pkgconfig-perl
  libfcgi-perl libffi7 libfile-fcntllock-perl libgirepository-1.0-1
  libglib-object-introspection-perl libglib-perl libhtml-parser-perl
  libjson-c4 libjson-perl libjson-xs-perl liblocale-gettext-perl
  libmath-random-isaac-xs-perl libmoose-perl libnet-dbus-perl
  libnet-dns-sec-perl libnet-libidn-perl libnet-pcap-perl libnet-rawip-perl
  libnet-ssh2-perl libnet-ssleay-perl libpackage-stash-xs-perl
  libpadwalker-perl libparams-classify-perl libparams-util-perl libpcsc-perl
```

- Type “**clamtk**” to open the GUI version of clamAV antivirus.
- You can update and scan directory/files in your system.



#5 Screenshot of the current running kali system

- For virtualbox, power off your vm.
- Click on take with a small camera icon on the top bar of vbox.
- Give the name of the current snapshot and click ok.


Take
Delete
Restore
Properties
Clone
Settings
Discard
Start
Name
Fresh snapshot
Conda Install and system Update
Snapshot 1
Snapshot 3
Project_Start
base
Current State