

Assignments:07

Module:- COSA(OS Hardening) Name:- Prithviraj Nikam

Lab Assignment :-

1.Set the password in GRUB

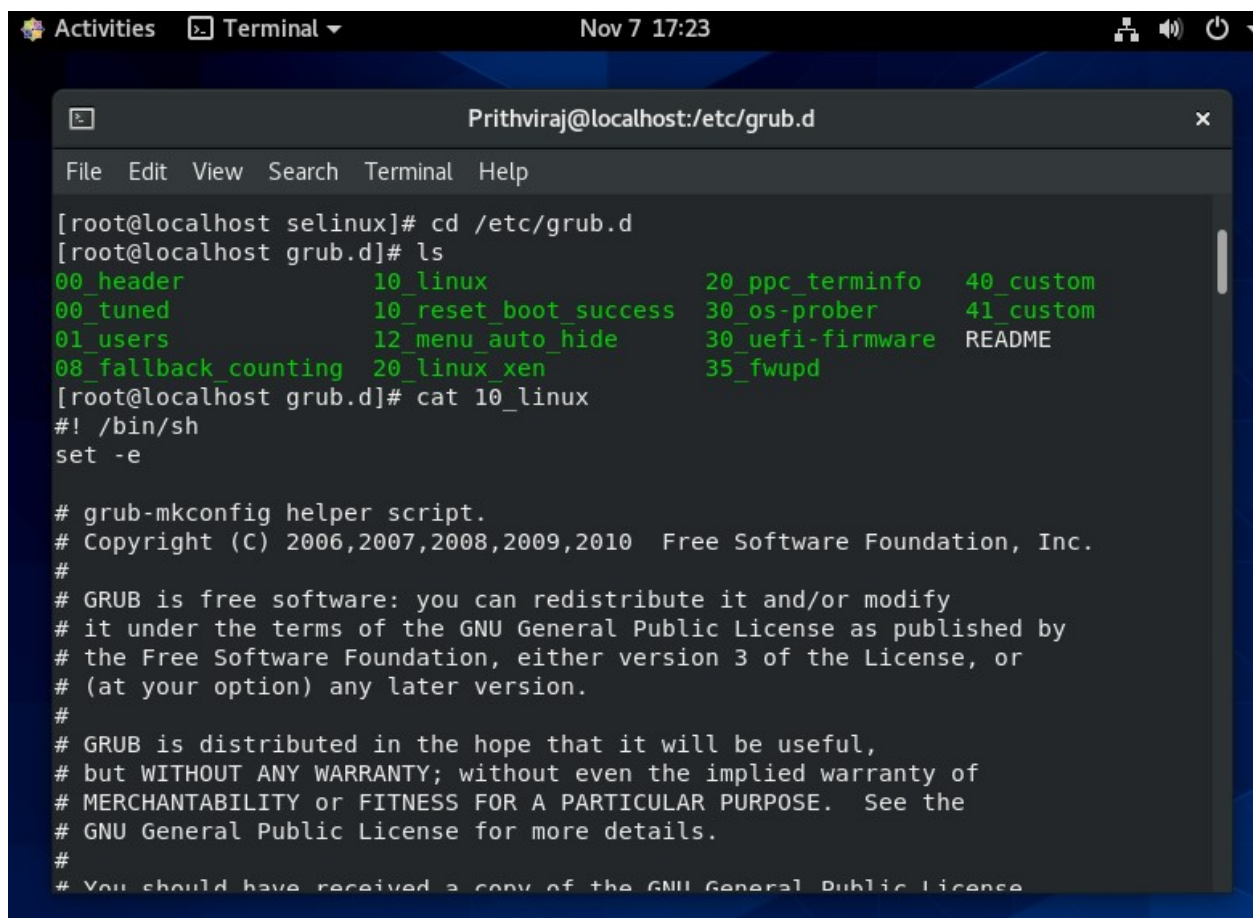
Step-1:- Go to vi Editor

Cmd:- # vi /etc/grub.d/10_Linux

—>Go to Line no.29 and

“remove --unrestricted “

Then save it

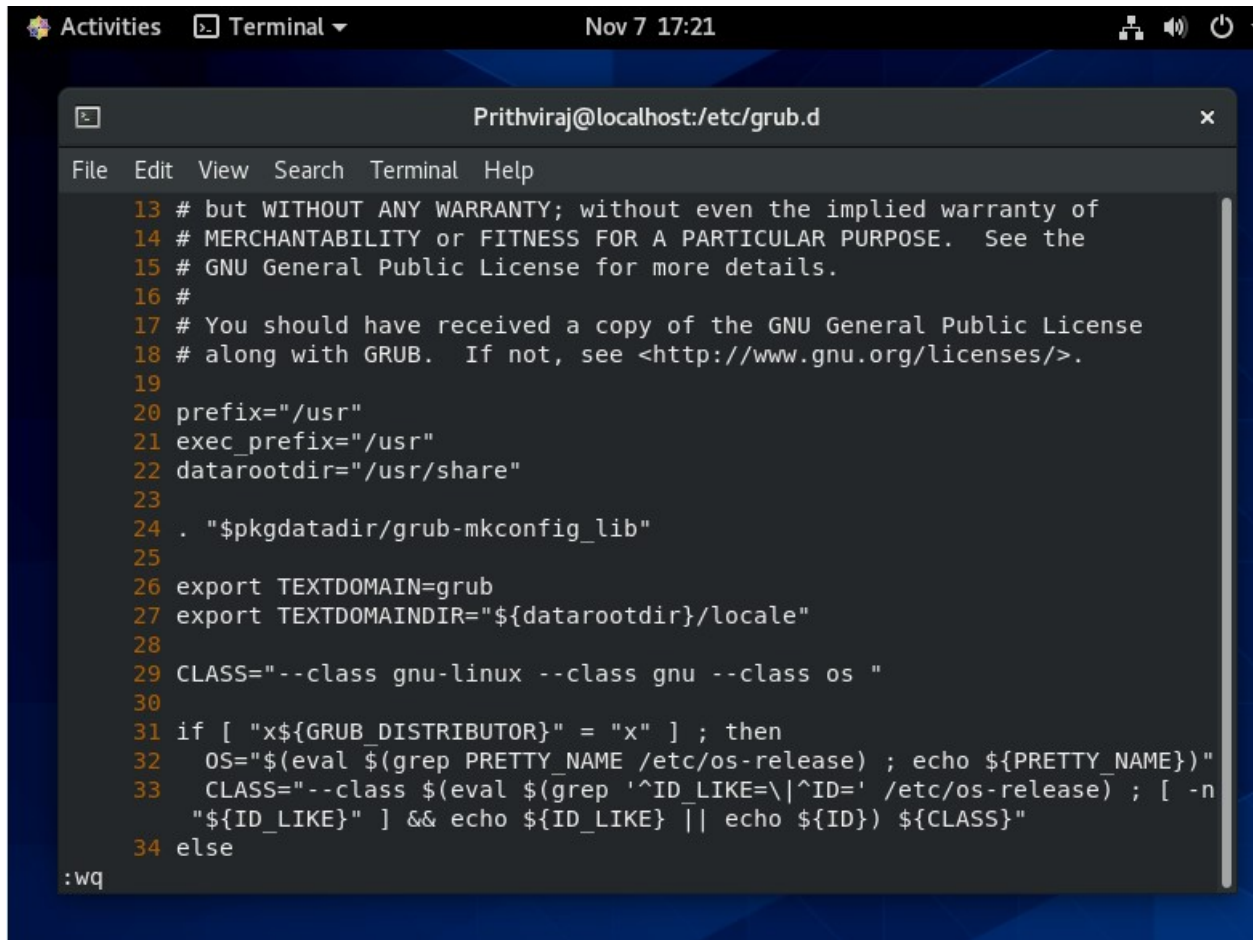


```
Prithviraj@localhost:/etc/grub.d
File Edit View Search Terminal Help

[root@localhost selinux]# cd /etc/grub.d
[root@localhost grub.d]# ls
00_header          10_linux           20_ppc_terminfo    40_custom
00_tuned           10_reset_boot_success 30_os-prober        41_custom
01_users           12_menu_auto_hide   30_uefi-firmware    README
08_fallback_counting 20_linux_xen        35_fwupd

[root@localhost grub.d]# cat 10_linux
#!/bin/sh
set -e

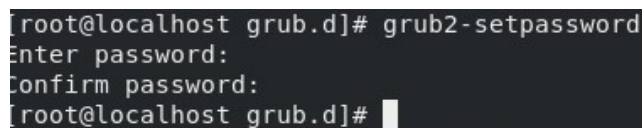
# grub-mkconfig helper script.
# Copyright (C) 2006,2007,2008,2009,2010 Free Software Foundation, Inc.
#
# GRUB is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
#
# GRUB is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
```



```
13 # but WITHOUT ANY WARRANTY; without even the implied warranty of
14 # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
15 # GNU General Public License for more details.
16 #
17 # You should have received a copy of the GNU General Public License
18 # along with GRUB. If not, see <http://www.gnu.org/licenses/>.
19
20 prefix="/usr"
21 exec_prefix="/usr"
22 datarootdir="/usr/share"
23
24 . "$pkgdatadir/grub-mkconfig_lib"
25
26 export TEXTDOMAIN=grub
27 export TEXTDOMAINDIR="${datarootdir}/locale"
28
29 CLASS="--class gnu-linux --class gnu --class os "
30
31 if [ "x${GRUB_DISTRIBUTOR}" = "x" ] ; then
32   OS="$(eval $(grep PRETTY_NAME /etc/os-release) ; echo ${PRETTY_NAME})"
33   CLASS="--class $(eval $(grep '^ID_LIKE=\|^ID=' /etc/os-release) ; [ -n
34     "${ID_LIKE}" ] && echo ${ID_LIKE} || echo ${ID}) ${CLASS}"
35 else
36
```

Step-2:- Now Set Grub password

Cmd:- # grub-setpassword



```
[root@localhost grub.d]# grub2-setpassword
Enter password:
Confirm password:
[root@localhost grub.d]#
```

Step-3:- Password where saved

Cmd:- # cat /boot/grub2/user.cfg

```
[root@localhost grub.d]# cat /boot/grub2/user.cfg
GRUB2_PASSWORD=grub.pbkdf2.sha512.10000.070D717E641254ABF093A80922D79057495B3A34
F85A18BE69F734BE35789B6AA50ECDCA0B655BF05FA034114439BBE1368DBE65A827A81DA2FD0D4
819FE2A1.CE9E563837A70F71AAC17C837F56D63ABCEDD6A5934736A2D44CD806260E00855E60D85
F8EF099F71C1B44828DACA067033295B0394C4CFB3B2A0FEAFF90AC59
[root@localhost grub.d]#
```

Step-4:- Regenerate the grub.cfg file after set the password

Cmd:- #cd /boot/grub2/

#ls

#grub2-mkconfig-0 /boot/grub2/grub.cfg

Then Reboot

```
[root@localhost grub.d]# cd /boot/grub2/
[root@localhost grub2]# ls
device.map  fonts  grub.cfg  grubenv  i386-pc  user.cfg
[root@localhost grub2]#
```

```
[root@localhost grub2]# grub2-mkconfig -o /boot/grub2/grub.cfg
Generating grub configuration file ...
/etc/grub.d/10_linux: line 1: et!: command not found
done
[root@localhost grub2]#
```

```
Enter username:
root
Enter password:
```

```
load_video
set gfx_payload=keep
insmod gzio
linux ($root)/vmlinuz-4.18.0-383.el8.x86_64 root=UUID=63228cbf-7d31-4bb5-a6b9-443e5edc7954 ro resume=UUID=862891c9-3bd3-4130-af6a-02d7539252ee rhgb quiet
initrd ($root)/initramfs-4.18.0-383.el8.x86_64.img $tuned_initrd
```

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to discard edits and return to the menu. Pressing Tab lists possible completions.

Step-5:- And then boot our machine with these new parameter by pressing “ctrl+x .After booting it goes into single user mode by default we enter into the root use password

```
Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.

switch_root:/# _
```

Step-6:- root file system mounted on sysroot so that it have read only permission so we need to mount in read and write mode

Cmd:-`#mount -o remount,rw /sysroot`

`#mount |grep sysroot`

To changes in the file “chrooting”

`##chroot /sysroot`

```
Entering emergency mode. Exit the shell to continue.  
Type "journalctl" to view system logs.  
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot  
after mounting them and attach it to a bug report.
```

```
switch_root:/# mount -o remount,rw /sysroot
```

```
switch_root:/# mount -o remount,rw /sysroot  
switch_root:/# mount |grep sysroot  
/dev/mapper/cs-root on /sysroot type xfs (rw,relatime,attr2,inode64,logbufs=8,logbsize=32k,noquota)  
switch_root:/# chroot /sysroot  
sh-4.4# _
```

```
sh-4.4# passwd  
Changing password for user root.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
sh-4.4# _
```

Step-7:- SELinux relabeling before rebooting Reset SELinux context

Cmd:-#touch /.autorelabel

Then Rebooting

```
sh-4.4# passwd  
Changing password for user root.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
sh-4.4# touch /.autorelabel  
sh-4.4# _
```