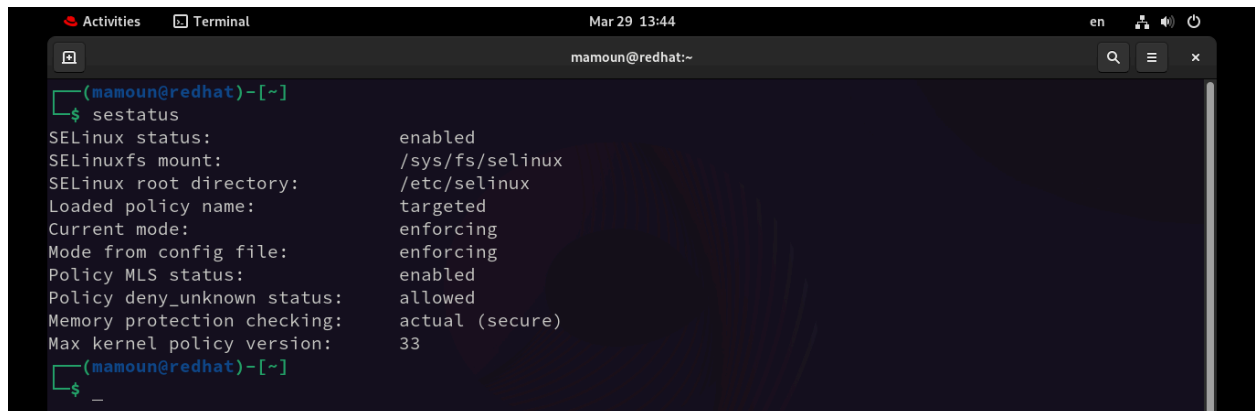


Linux Admin 2 - Lab 5

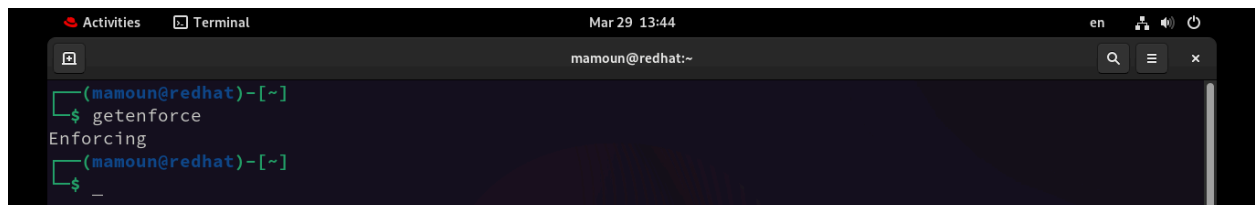
Name: Muhamad Mamoun Elsaid Hassan

1-



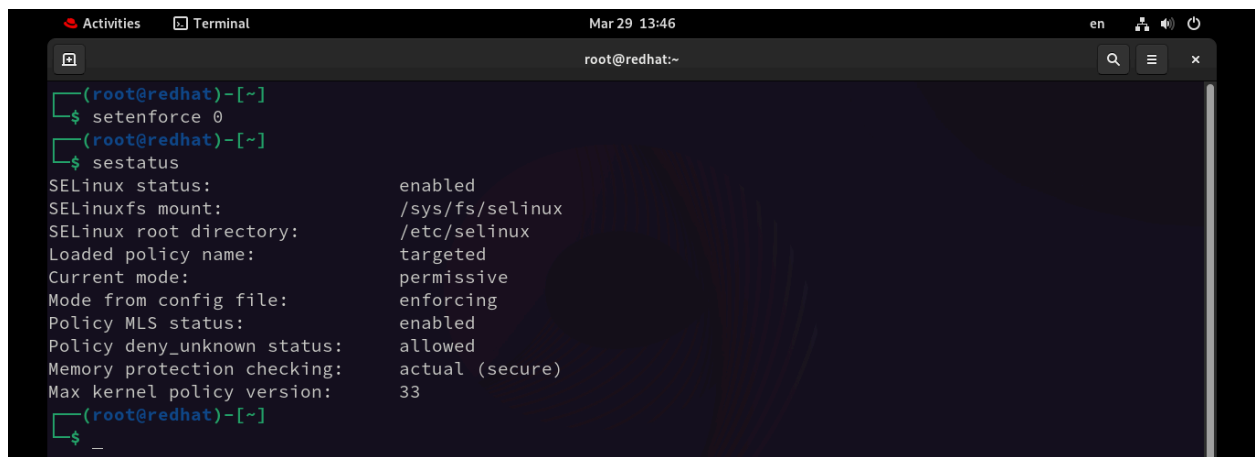
```
mamoun@redhat:~$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:          targeted
Current mode:                enforcing
Mode from config file:      enforcing
Policy MLS status:           enabled
Policy deny_unknown status:  allowed
Memory protection checking:  actual (secure)
Max kernel policy version:   33
mamoun@redhat:~$
```

2-



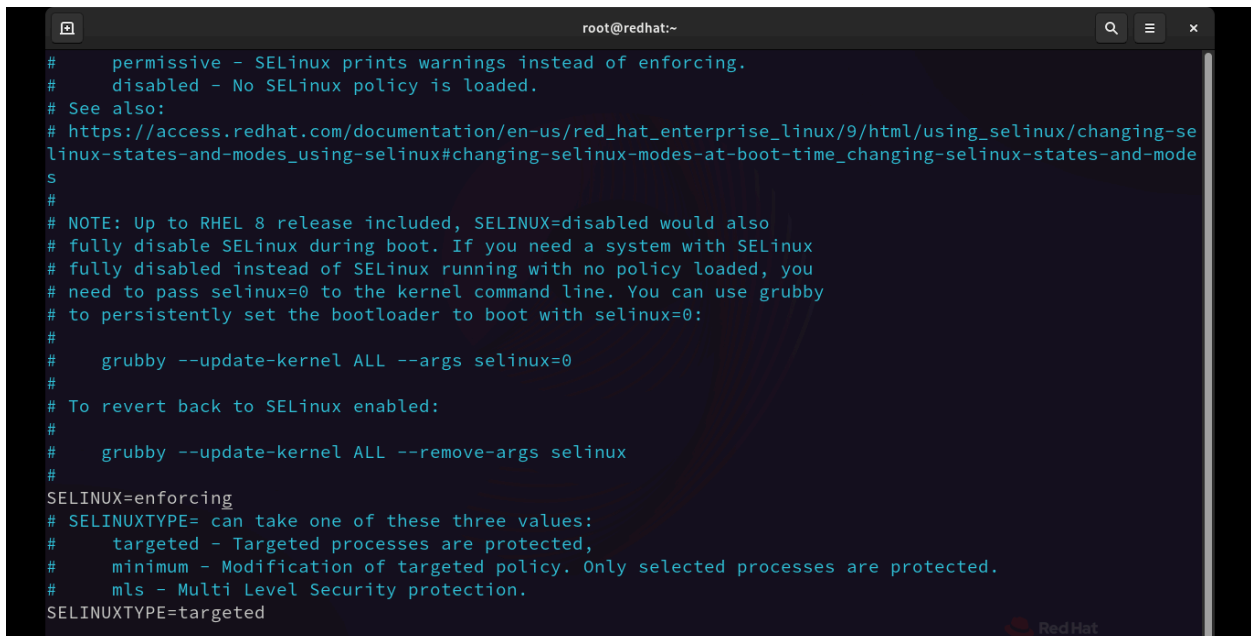
```
mamoun@redhat:~$ getenforce
Enforcing
mamoun@redhat:~$
```

3-



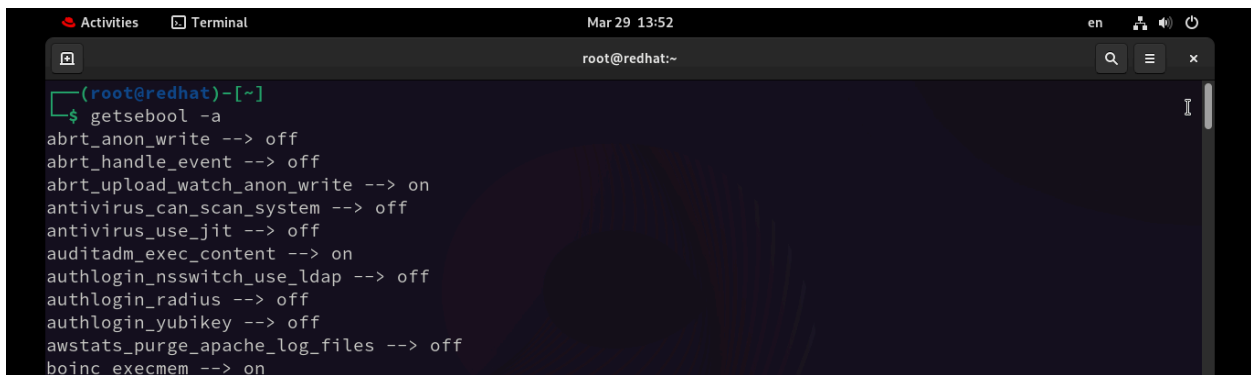
```
root@redhat:~$ setenforce 0
root@redhat:~$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:          targeted
Current mode:                permissive
Mode from config file:      enforcing
Policy MLS status:           enabled
Policy deny_unknown status:  allowed
Memory protection checking:  actual (secure)
Max kernel policy version:   33
root@redhat:~$
```

4- vim /etc/selinux/config



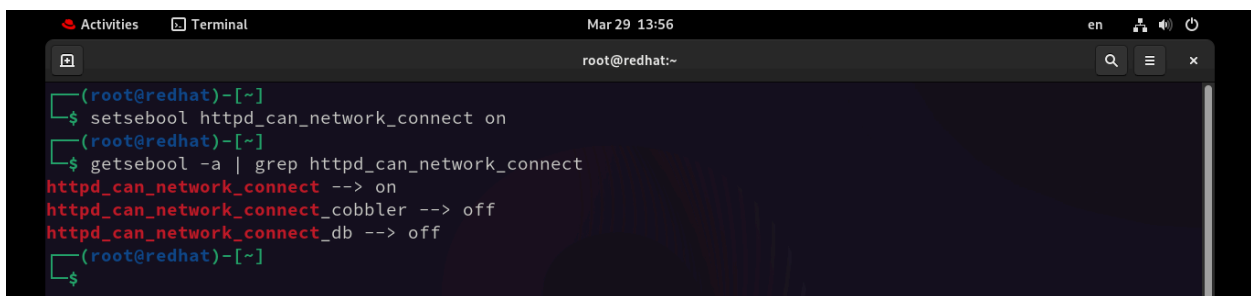
```
root@redhat:~
# permissive - SELinux prints warnings instead of enforcing.
# disabled - No SELinux policy is loaded.
# See also:
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing-selinux-states-and-modes_using-selinux#changing-selinux-modes-at-boot-time_changing-selinux-states-and-modes
#
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
# grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
# grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

5-



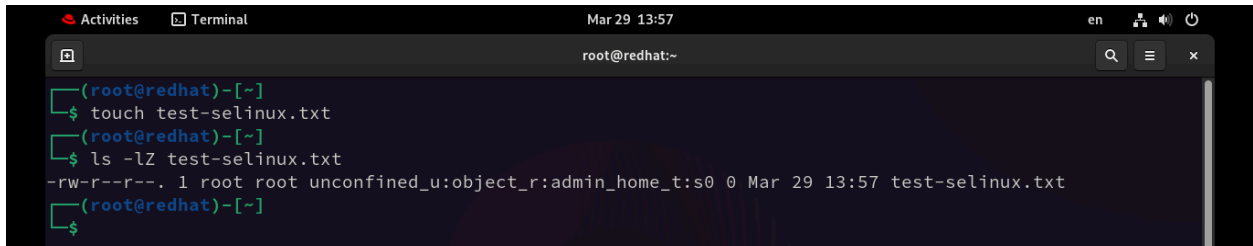
```
Activities Terminal Mar 29 13:52 en
root@redhat:~
(root@redhat)~[~]
$ getsebool -a
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
antivirus_use_jit --> off
auditadm_exec_content --> on
authlogin_nsswitch_use_ldap --> off
authlogin_radius --> off
authlogin_yubikey --> off
awstats_purge_apache_log_files --> off
boinc_execmem --> on
```

6-



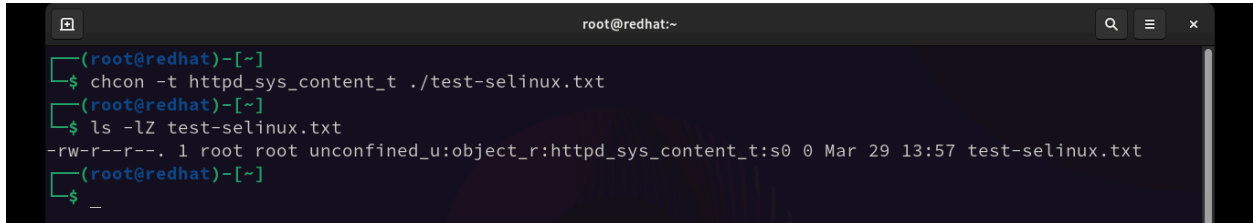
```
Activities Terminal Mar 29 13:56 en
root@redhat:~
(root@redhat)~[~]
$ setsebool httpd_can_network_connect on
(root@redhat)~[~]
$ getsebool -a | grep httpd_can_network_connect
httpd_can_network_connect --> on
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
(root@redhat)~[~]
$
```

7-

A terminal window titled 'root@redhat:~' showing the execution of 'touch test-selinux.txt' and 'ls -lZ test-selinux.txt'. The output of the ls command shows the file permissions as -rw-r--r-- and the SELinux context as unconfined_u:object_r:admin_home_t:s0.

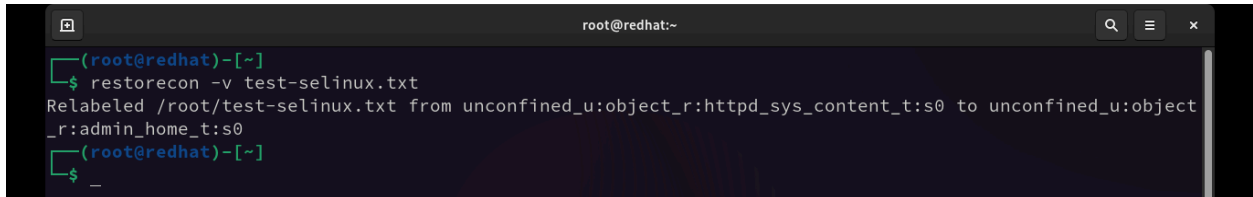
```
(root@redhat)~[~]
$ touch test-selinux.txt
(root@redhat)~[~]
$ ls -lZ test-selinux.txt
-rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0 0 Mar 29 13:57 test-selinux.txt
(root@redhat)~[~]
$
```

8-

A terminal window titled 'root@redhat:~' showing the execution of 'chcon -t httpd_sys_content_t ./test-selinux.txt' and 'ls -lZ test-selinux.txt'. The output of the ls command shows the SELinux context updated to httpd_sys_content_t:s0.

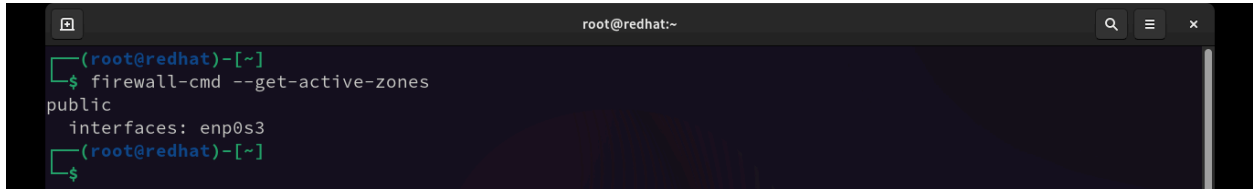
```
(root@redhat)~[~]
$ chcon -t httpd_sys_content_t ./test-selinux.txt
(root@redhat)~[~]
$ ls -lZ test-selinux.txt
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 0 Mar 29 13:57 test-selinux.txt
(root@redhat)~[~]
$
```

9-

A terminal window titled 'root@redhat:~' showing the execution of 'restorecon -v test-selinux.txt'. The output indicates the file was relabeled from httpd_sys_content_t:s0 back to admin_home_t:s0.

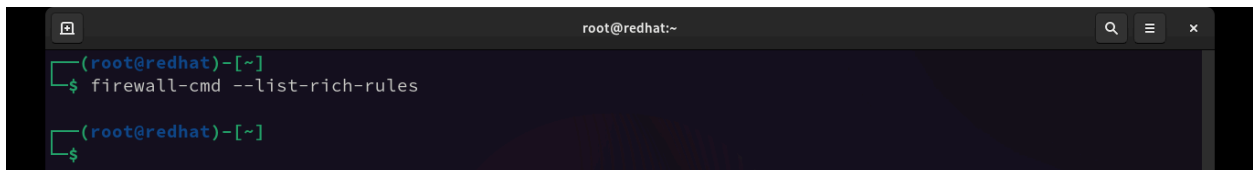
```
(root@redhat)~[~]
$ restorecon -v test-selinux.txt
Relabeled /root/test-selinux.txt from unconfined_u:object_r:httpd_sys_content_t:s0 to unconfined_u:object_r:admin_home_t:s0
(root@redhat)~[~]
$
```

10-

A terminal window titled 'root@redhat:~' showing the execution of 'firewall-cmd --get-active-zones'. The output shows the 'public' zone is active on the 'enp0s3' interface.

```
(root@redhat)~[~]
$ firewall-cmd --get-active-zones
public
interfaces: enp0s3
(root@redhat)~[~]
$
```

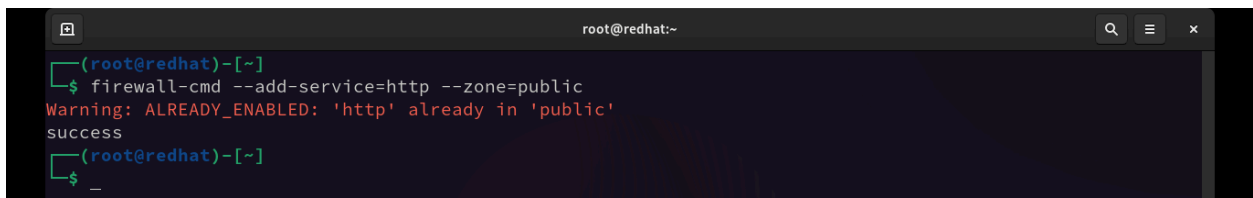
11-

A terminal window titled 'root@redhat:~' showing the execution of 'firewall-cmd --list-rich-rules'. The output is empty, indicating no rich rules are currently defined.

```
(root@redhat)~[~]
$ firewall-cmd --list-rich-rules

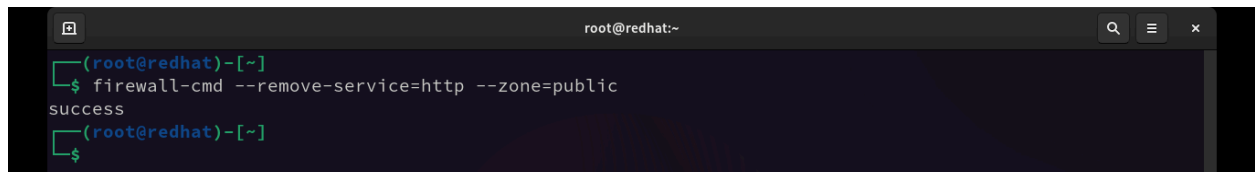
(root@redhat)~[~]
$
```

12-

A terminal window titled 'root@redhat:~' showing the execution of 'firewall-cmd --add-service=http --zone=public'. The output shows a warning that the service is already enabled in the public zone, followed by a success message.

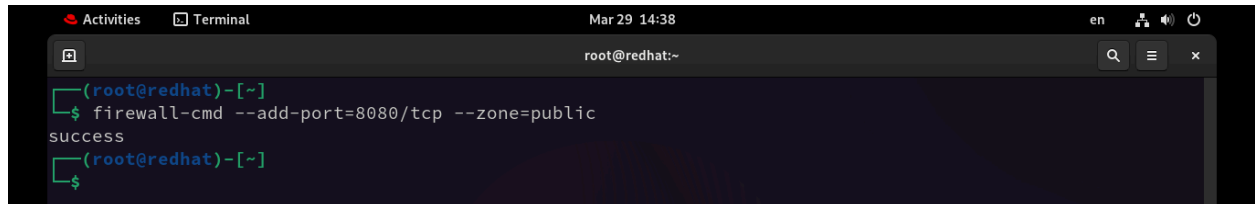
```
(root@redhat)~[~]
$ firewall-cmd --add-service=http --zone=public
Warning: ALREADY_ENABLED: 'http' already in 'public'
success
(root@redhat)~[~]
$
```

13-



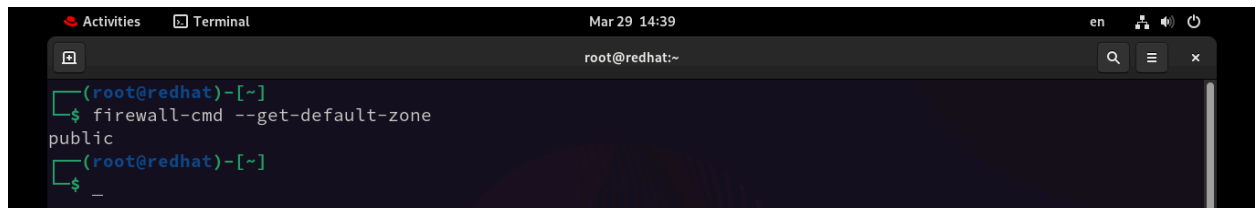
```
root@redhat:~  
(root@redhat)-[~]  
$ firewall-cmd --remove-service=http --zone=public  
success  
(root@redhat)-[~]  
$
```

14-



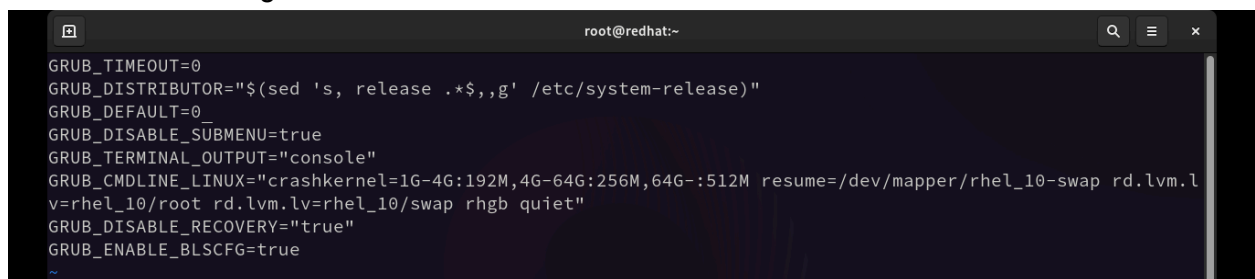
```
Activities Terminal Mar 29 14:38 en [system icons]  
root@redhat:~  
(root@redhat)-[~]  
$ firewall-cmd --add-port=8080/tcp --zone=public  
success  
(root@redhat)-[~]  
$
```

15-



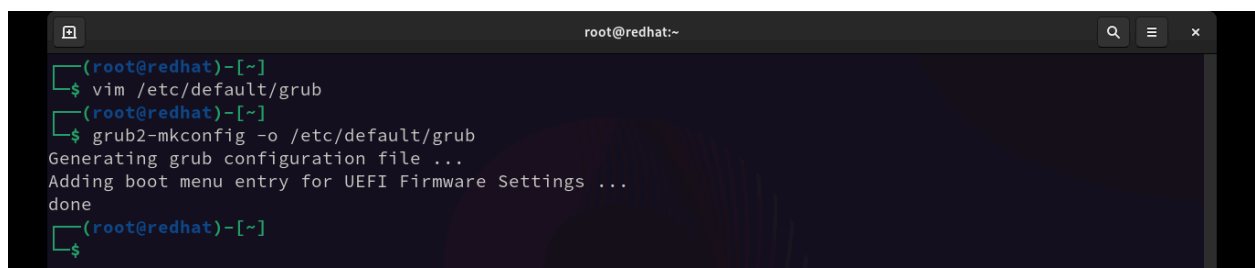
```
Activities Terminal Mar 29 14:39 en [system icons]  
root@redhat:~  
(root@redhat)-[~]  
$ firewall-cmd --get-default-zone  
public  
(root@redhat)-[~]  
$
```

16- vim /etc/default/grub



```
root@redhat:~  
GRUB_TIMEOUT=0  
GRUB_DISTRIBUTOR="$(sed 's, release .*,g' /etc/system-release)"  
GRUB_DEFAULT=0  
GRUB_DISABLE_SUBMENU=true  
GRUB_TERMINAL_OUTPUT="console"  
GRUB_CMDLINE_LINUX="crashkernel=1G-4G:192M,4G-64G:256M,64G-:512M resume=/dev/mapper/rhel_10-swap rd.lvm.lv=rhel_10/root rd.lvm.lv=rhel_10/swap rhgb quiet"  
GRUB_DISABLE_RECOVERY="true"  
GRUB_ENABLE_BLSCFG=true  
~
```

17-



```
root@redhat:~  
(root@redhat)-[~]  
$ vim /etc/default/grub  
(root@redhat)-[~]  
$ grub2-mkconfig -o /etc/default/grub  
Generating grub configuration file ...  
Adding boot menu entry for UEFI Firmware Settings ...  
done  
(root@redhat)-[~]  
$
```