Seif Hendawy
RHCSA II Day 5

1. What command would you use to check the current status of SELinux?

```
seif@172:~$ 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
seif@172:~$
```

2. How can you view the SELinux mode (enforcing, permissive, or disabled)?

```
seif@172:~$ getenforce
Enforcing
seif@172:~$
```

3. What command would you use to temporarily set SELinux to permissive mode?

```
seif@172:~$ setenforce 0
setenforce:  security_setenforce() failed:  Permission denied
seif@172:~$ sudo setenforce 0
seif@172:~$ getenforce
Permissive
seif@172:~$
```

4. How do you permanently set SELinux to enforcing mode by editing the configuration file?

Already set to enforcing inside the /etc/selinux/config file

```
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

5. What command would you use to list all SELinux booleans?

```
seif@172:~$ sudo getsebool -a
abrt_anon_write --> off
abrt_handle_event --> on
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
cdrecord_read_content --> off
cluster_can_network_connect --> off
cluster_manage_all_files --> off
cluster_use_execmem --> off
cobbler_anon_write --> off
cobbler_can_network_connect --> off
cobbler_use_cifs --> off
cobbler_use_nfs --> off
collectd_tcp_network_connect --> off
colord_use_nfs --> off
condor_tcp_network_connect --> off
conman_can_network --> off
```

6. How can you enable a specific SELinux boolean (e.g., httpd_can_network_connect)?

```
seif@172:~$ sudo setsebool -P httpd_can_network_connect on
[sudo] password for seif:
seif@172:~$ sudo getsebool -a | grep httpd_can_network_connect
httpd_can_network_connect --> on
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
seif@172:~$
```

7. What command would you use to check the SELinux context of a file?

```
seif@172:~$ ls -Z tmrw.txt
unconfined_u:object_r:user_home_t:s0 tmrw.txt
seif@172:~$
```

8. How can you change the SELinux context of a file to a specific type (e.g., httpd_sys_content_t)?

```
seif@172:~$ sudo chcon -t httpd_sys_content_t tmrw.txt
seif@172:~$ ls -Z tmrw.txt
unconfined_u:object_r:httpd_sys_content_t:s0 tmrw.txt
seif@172:~$
```

9. What command can be used to restore the default SELinux context of files in a Directory?

```
seif@172:~$ sudo restorecon -Rv tmrw.txt
Relabeled /home/seif/tmrw.txt from unconfined_u:object_r:httpd_sys_content_t:s0 to unconfined_u:object_r:user_home_t:s0
seif@172:~$ ls -Z tmrw.txt
unconfined_u:object_r:user_home_t:s0 tmrw.txt
seif@172:~$
```

10. How do you list all active zones in firewalld?

```
seif@172:~$ sudo firewall-cmd --get-active-zones
public (default)
  interfaces: ens160
seif@172:~$
```

11. What command would you use to view the current rules in the public zone?

```
seif@172:~$ sudo firewall-cmd --zone=public --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

12. How can you add a new service (e.g., HTTP) to the public zone?

```
seif@172:~$ sudo firewall-cmd --zone=public --add-service=http
success
seif@172:~$ sudo firewall-cmd --zone=public --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client http ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

13. What command removes a service (e.g., HTTPS) from the public zone?

```
seif@172:~$ sudo firewall-cmd --zone=public --remove-service=http
success
seif@172:~$ sudo firewall-cmd --zone=public --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
seif@172:~$
```

14. How do you allow a specific port (e.g., 8080) in the public zone?

```
seif@172:~$ sudo firewall-cmd --zone=public --add-port=8080/tcp
success
seif@172:~$ sudo firewall-cmd --zone=public --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client ssh
  ports: 8080/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

15. How can you view the default zone used by firewalld?

```
seif@172:~$ sudo firewall-cmd --get-default-zone
public
seif@172:~$
```

16. How to change the GRUB timeout value? How to set the default boot entry in GRUB?

```
  GNU nano 8.1                                  /etc/default/grub
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release
GRUB_DEFAULT=saved
```

```
  GNU nano 8.1                                  /etc/default/grub
GRUB_TIMEOUT=10
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-rel
GRUB_DEFAULT=0
```

17. How to regenerate the GRUB configuration file after modifying /etc/default/grub?

```
seif@172:~$ sudo nano /etc/default/grub
seif@172:~$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
Generating grub configuration file ...
File descriptor 3 (pipe:[64237]) leaked on vgs invocation. Parent PID 7793: grub2-probe
File descriptor 9 (pipe:[64260]) leaked on vgs invocation. Parent PID 7793: grub2-probe
File descriptor 3 (pipe:[64237]) leaked on vgs invocation. Parent PID 7793: grub2-probe
File descriptor 9 (pipe:[64260]) leaked on vgs invocation. Parent PID 7793: grub2-probe
Adding boot menu entry for UEFI Firmware Settings ...
done
seif@172:~$
```