Exam Report: 15.8.5 Practice Questions

Date: 4/4/28 6:52:20 pm
Time Spent: 0:10

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 75%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

▼ **Question 1:** Correct

You are a network administrator for your company. A user calls to complain that his Firefox browser is not working as it did the day before. Knowing that you recently updated the SELinux profile for Firefox, you suspect the change you made is causing the issue. You want to troubleshoot the issue by switching the profile to permissive mode.

Which of the following is the BEST command to use in this situation?

○ **getenforce**

○ **setsebool**

➡ ◉ **setenforce**

○ **sestatus**

Explanation

setenforce switches between permissive and enforcing mode. The command syntax is **setenforce mode value**.

setsebool changes the current state of an SELinux boolean.

sestatus displays the status of a system running SELinux.

getenforce displays the current SELinux mode (Enforcing, Permissive, or Disabled).

References

Linux Pro - 15.8 Security-Enhanced Linux (SELinux)
[e_s_selinux_lp5.exam.xml Q_SELINUX_LP5_SETENFORCE]

▼ **Question 2:** Correct

You were recently asked to manage the SELinux implementation at your company. Since you are still coming up to speed on this technology, you have not yet mastered the process of creating or making major changes to SELinux policies.

However, an employee has just called you complaining that they don't seem to be able to accomplish a task with a particular application. After scanning through the SELinux policy for that application, you notice that there is a method that can be used to enable the desired function.

Which of the following is the BEST command for enabling that feature without editing the policy?

➡ ◉ **setsebool**

○ **setenforce**

○ **ls -Z *application_name***

○

○ **sestatus**

○ **getenforce**

Explanation

setsebool changes the current state of an SELinux boolean. This command is used to make the change immediately. But unless the**-P** switch is used, at the next boot, it will revert back to the defaults.

setenforce switches between permissive and enforcing mode. The command syntax is **setenforce mode value**.

sestatus displays the status of a system running SELinux.

getenforce displays the current SELinux mode (Enforcing, Permissive, or Disabled).

ls -Z *application_name* displays the SELinux context for a specified file by using the **-Z** parameter.

References

Linux Pro - 15.8 Security-Enhanced Linux (SELinux)
[e_s_selinux_lp5.exam.xml Q_SELINUX_LP5_SETSEBOOL]

▼ Question 3: Correct

As the network administrator, one of your responsibilities is to analyze and troubleshoot SELinux context violations.

In which directory are the SELinux violations recorded?

○ /var/log/firewalld

○ /var/log

○ /var/log/secure

➡ ● /var/log/audit

Explanation

/var/log/audit is the directory where SELinux violations are recorded as Access Vector Cache (AVC) event errors. The entries are stored in the audit.log files.

/var/log/secure contains information related to authentication and authorization privileges.

/var/log/firewalld contains information related to the local firewall.

/var/log is the main folder where logs are stored.

References

Linux Pro - 15.8 Security-Enhanced Linux (SELinux)
[e_s_selinux_lp5.exam.xml Q_SELINUX_LP5_AVC]

▼ Question 4: Incorrect

Which of the following is the BEST command for viewing SELinux errors?

➡ ○ **sealert**

● ~~**getsebool**~~

○ **getenforce**

○ **semanage**

Explanation

sealert is used to view SELinux errors. If not run from the GUI interface, you would run sealer -a /var/log/audit/audit.log.

semanage is used to configure certain elements of SELinux policy without requiring modification to or

recompilation from policy sources.
getenforce displays the current SELinux mode (Enforcing, Permissive, or Disabled).

getsebool displays a list of booleans. Booleans allow you to change part of the SELinux policy at run time without reloading or recompiling the SELinux policy.

References

Linux Pro - 15.8 Security-Enhanced Linux (SELinux)
[e_s_selinux_lp5.exam.xml Q_SELINUX_LP5_SEALERT]