15.9.4 Practice Questions

Candidate: Ethan Bonavida (suborange)
Date: 12/9/2022 12:32:46 am • **Time Spent:** 00:24

Score: 100% Passing Score: 80%

Question 1: ✔ Correct

You have just started protecting your computer while running Firefox using AppArmor. After a short time, employees start to complain that some of the features they use frequently are no longer functioning. After a quick check, you discover that these features should be working and decide not to protect Firefox anymore.

Which of the following is the BEST command to quickly stop protecting Firefox?

- **aa-unconfined**
- **aa-complain /etc/apparmor.d/usr.bin.firefox**
- **aa-disable /etc/apparmor.d/usr.bin.firefox**
- **systemctl stop apparmor**

Explanation

If run with the correct permissions (root or using sudo):

- **aa-disable /etc/apparmor.d/usr.bin.firefox** will disable apparmor from enforcing the rules associated with this application.
- **aa-complain /etc/apparmor.d/usr.bin.firefox** will enable a disabled application, but the application will run in complain mode.
- **aa-unconfined** will display a list of processes with TCP or UDP ports that do not have AppArmor profiles loaded.
- **systemctl stop apparmor** will stop apparmor from protecting your entire system and should not be used to troubleshoot just one application.

References

15.9.2 Application Armor Facts

q_apparmor_lp5_apparmor_01.question.fex

Question 2: ✔ Correct

AppArmor has been installed on your computer.

Which of the following directories contain your AppArmor profiles?

- /etc/
- /home/apparmor/
- /home/apparmor/apparmor.d/
- ➡ /etc/apparmor.d/
- /etc/apparmor/apparmor.d/

Explanation

AppArmor profiles are stored in the /etc/apparmor.d/ directory.

References

15.9.2 Application Armor Facts

q_apparmor_lp5_apparmor_02.question.fex

Question 3: ✔ Correct

You are running AppArmor on your system.

Which of the following commands will show all of the processes from the /proc filesystem with TCP or UDP ports that are not protected by AppArmor profiles?

- **aa-unconfined --with-ss**
- **aa-unconfined --paranoid**
- **aa-unconfined --with-netstat**
- **aa-unconfined**

Explanation

The **aa-unconfined --paranoid** command will show all of the processes from the /proc filesystem with TCP or UDP ports that are not protected by AppArmor profiles

The other three valid **aa-unconfined** commands will only list the processes listening on the network sockets. The only difference between these three commands is that **aa-unconfined** and **aa-unconfined --with-ss** both use the **ss** command to located the desired information, while the **aa-unconfined --with-netstat** use the **netstat** command to located the same information.

References

15.9.2 Application Armor Facts

q_apparmor_lp5_apparmor_03.question.fex

Question 4: ✔ Correct

Your computer is using AppArmor.

Which of the following commands is BEST to use for troubleshooting an AppArmor profile?

- **aa-complain**
- **aa-unconfined**
- **aa-enforce**
- **aa-disable**

Explanation

If a particular application being protected using apparmor is not functioning as you think it should, you should change it to run in the complain mode using the **aa-complain** command. This lets the application run without enforcing the apparmor policy. However, all access violations, as defined in the profile, are logged to the system log, which can then be used to help troubleshoot the desired profile.

The **aa-disable** command will disable apparmor from enforcing the rules associated with this application.

The **aa-unconfined** command will display a list of processes with TCP or UDP ports that do not have AppArmor profiles loaded.

The **aa-enforce** command is used to enable a disabled apparmor profile.

References

15.9.2 Application Armor Facts

q_apparmor_lp5_apparmor_04.question.fex