LAB5_MAC

This lab is designed to introduce students to system hardening. The students will interact with 2 fundamental technologies used in Linux security; AppArmor and SElinux

PART A - AppArmor

1. Using the SIEM used in the previous lab, explain how are CIS benchmarks checked on an endpoint?
2. Based on a Linux distribution of your choice, fulfill the MAC section of the latest respective CIS benchmark. link: CIS benchmark download
3. Configure a Webapp to serve static files from two directories and configure AppArmor to confine the Webapp to one of the two directories.

i.e Essentially, prove with your setup that an external user is able to access the file within both directories when AppArmor is inactive, and when active, the external user will

4. Briefly explain how AppArmor uses default profiles to secure your services

4. In a situation where your Webapp fails to start or misbehaving after the Apparmor profile has been enforced i.e AppArmor confinement, how would you rectify this? What steps would you take to troubleshoot this?

PART B - SElinux

1. Give a short explanation on SElinux.
2. Deploy a simple webapp or DB on a Linux server.

- Carry out a stress test on the application and verify the performance of the application on the server. The performance can be reviewed using a benchmark such as Spec benchmark. Take note of the results.
- Install and enable SElinux on the same Linux server

- Implement a couple of containment policies for the hosted webapp on the server and perform a similar stress test based on similar benchmarks used earlier.
- Do you observe any difference in performance?

Bonus

Replicate the shellshock attack in a test environment.

- Show how SElinux can be used to stop this.