Assignment 4 - Linux Penetration Testing

You may find the Kali GUI accessible via browser helpful.
It is at: http://(your-email)-kali.vpn.daviscybersec.org:8444
KasmVNC Username:Password - kali:password
You still have to authenticate using your user account creds (kali:kali).

You have been contracted to perform a penetration test of a Linux server located at ***10.X.10.123***. The system has been newly commissioned and was set up by a team of amateur security engineers, so we would like you to conduct a penetration test. Your goals are thus:

1) Find all vulnerabilities and document them in detail. Include steps to replicate the exploits, and possible remediations.
2) Leave no trace after you are done. Refrain from taking any action that would cause damage or disruption to the services running on the service; document exploits used, their effects, and clean up of any artifacts you leave on the server.

To help you avoid going down large amounts of rabbit holes, the instructors have deliberately inserted the following quantities of vulnerabilities:

- 2 different methods of achieving shell access on the server
- 2 + 1 methods of escalating access to root
    - 2 methods minimum to score full points
    - 1 extra method worth extra credit

If you find more vulnerabilities and properly document them, you may receive extra credit!