Assignment 5 - Linux defense

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).

A new homelab operator has contracted you to secure their Linux server, located at ***10.X.10.43***. Unfortunately, they didn't use best security practices and messed with things they shouldn't have. To make matters worse, there's a chance hackers have gotten in before...

The server can be accessed over SSH; you may log in as the user **debian**, which has the password **debian**. All other accounts on the system have **abc123** as their password. All services on the system use the default credentials for the given service.

The server operates as a Web server (HTTP). Your goals are as follows:

1) Patch holes in the server to prevent random people (including malicious users) from modifying the website or gaining remote access.
2) Keep Web and SSH access available.

For each vulnerability you resolve, explain why the original setting constitutes a vulnerability.

For this assignment, **20%** of your score will be based on the results of simulated attacks, which will be run after the submission window closes. You must ensure that the system is not vulnerable to these attacks ***and*** that SSH and HTTP are running and accessible.

Note that anything you can access from Kali (or your laptop on the VPN) can be accessed by users (malicious or otherwise).

Extra Credit:

1. [15%] Set up a logging service on the system. SSH and Web logs should be aggregated to this service. Demonstrate that warnings appear in the log system.
2. [25%] Set up a firewall on the system. The firewall should adhere to the principle of least privilege. **Please be incredibly wary of accidentally locking yourself out of the system. You can request us to reset your system, but that will clear all of your progress, so proceed with caution.**