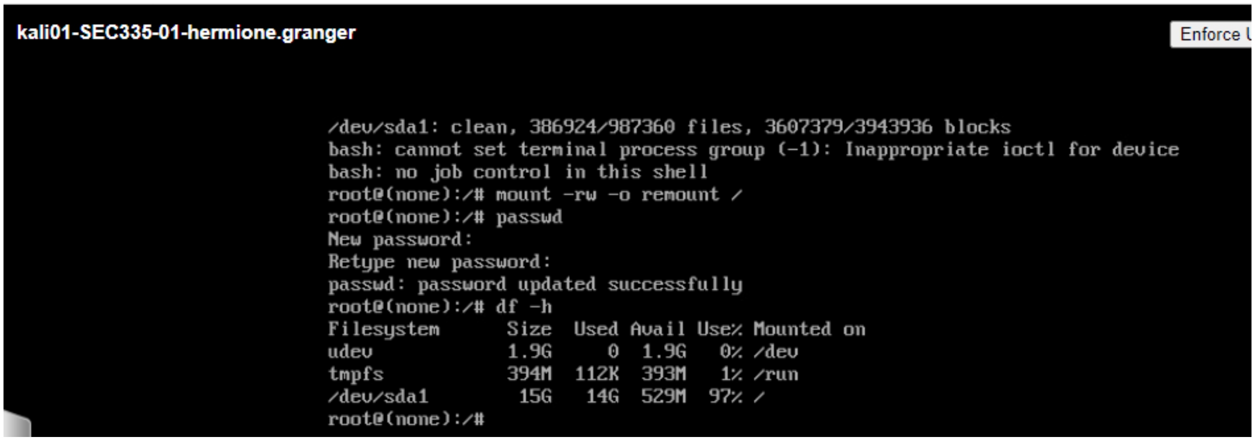
Updated: Feb 16, 2022

Assignment 5.1 - Breaking into Kali

💡Allowing an adversary physical access to a system can quickly lead to system level compromise. Full Disk encryption helps unless the attacker can discern your password through guessing, bruteforce or keylogging.

`Deliverable 1.  Watch this video, and provide a screenshot of your single user mode session where you set the root password for Kali similar to the one below.`



```
/dev/sda1: clean, 386924/987360 files, 3607379/3943936 blocks
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# mount -rw -o remount /
root@(none):/# passwd
New password:
Retype new password:
passwd: password updated successfully
root@(none):/# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  112K  393M   1% /run
/dev/sda1        15G   14G  529M  97% /
root@(none):/#
```

Note, when you are done changing the password issue the following commands

```
sync
umount /
```

then you can power cycle your kali box.

`Deliverable 2.  Document the single user mode hack for debian, provide a link to your journal.`