**Process flow:**

In order to access the Server, we are using 2 levels of authentication and they are (i)LUKS (ii)YUBIKEY **i.e..,**

**1.LUKS-Primary authentication**

**2.YUBIKEY- Secondary authentication.**

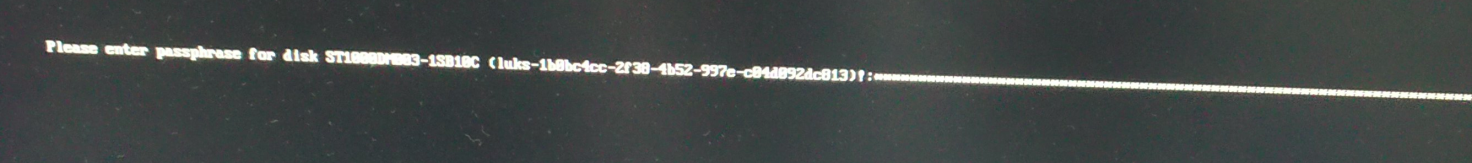
**LUKS-Primary authentication**: To encrypt the server we are using LUKS authentication and in order to access this we need 128 char to finish first level of authentication.

This 128 char is splitted into 2 segments and first 64 segments is handled by LINUX ADMIN and the second 64 segments is handled by SECURITY ADMIN

**YUBIKEY- Secondary authentication:** This YUBIKEY will be kept and handled by MANAGER LEVEL authority. We need to finish the YUBIKEY level of authentication to enable SERVER LOGIN.

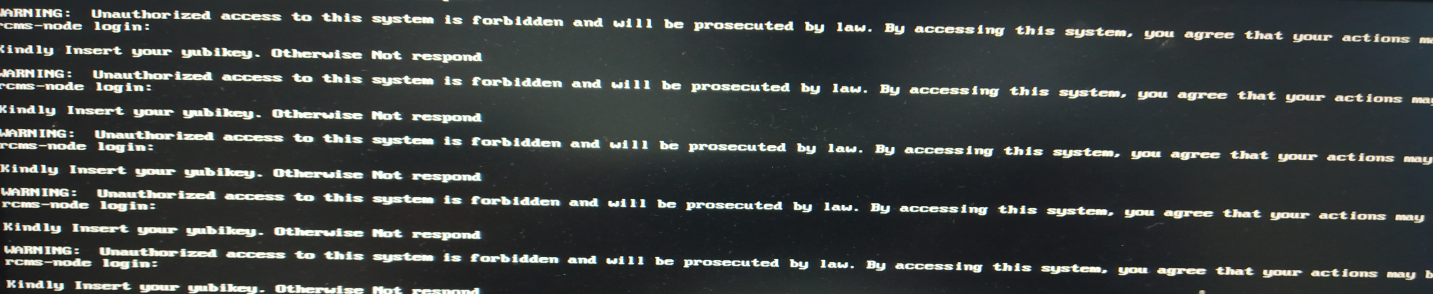
**PROCEDURES TO FOLLOW:**

1. Once LUKS is installed it will be asking for LUKS password in order to Login as it encrypts entire block devices and is therefore well-suited for protecting the contents of mobile devices such as removable storage media or laptop disk drives. The underlying contents of the encrypted block device are arbitrary. This makes it useful for encrypting swap devices. This can also be useful with certain databases that use specially formatted block devices for data storage.



**Luks password 128 characteristics {Linux admin have 64 characteristics + security admin have 64 characteristics)**

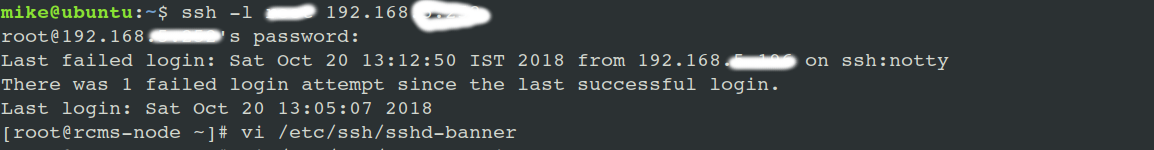
2. The below image represents the after logging in to LUKS and Waiting for Yubikey Access.



3.

Optional for ssh (Remote):

3. Yubikey Access for ssh with Password.



4. If we don’t own YUBI KEY ssh will not get accessed.

