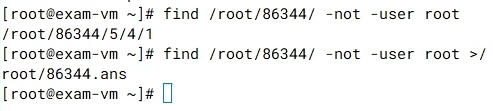
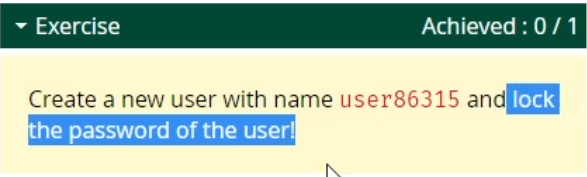
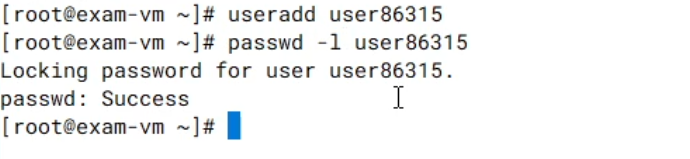


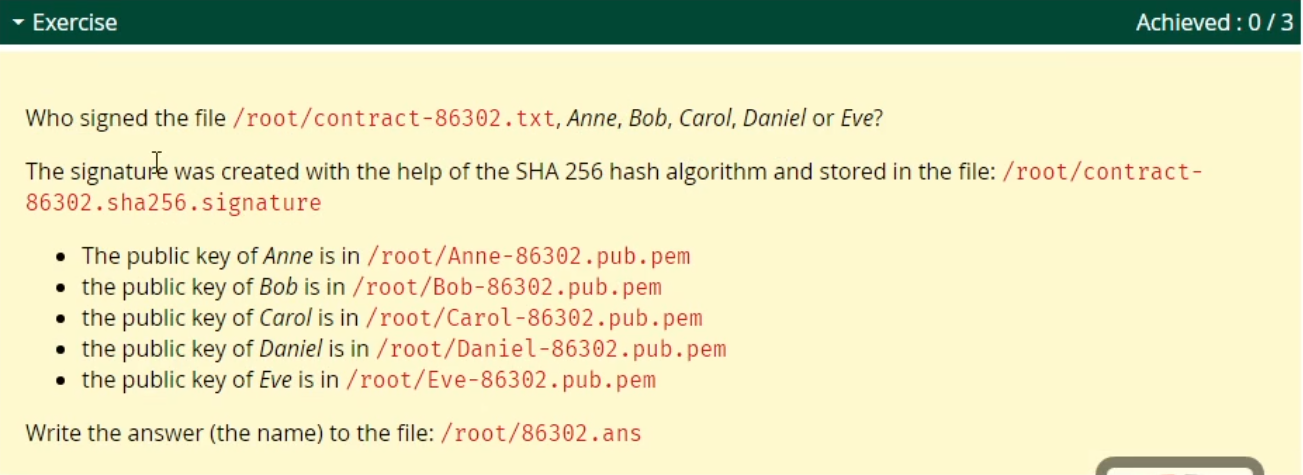
Find the directory | where owner is / is not \* user | write in file



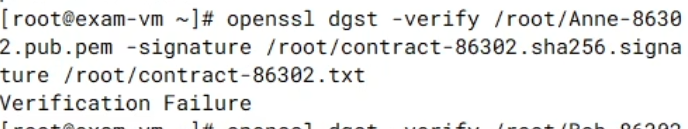


Create a new user | lock password

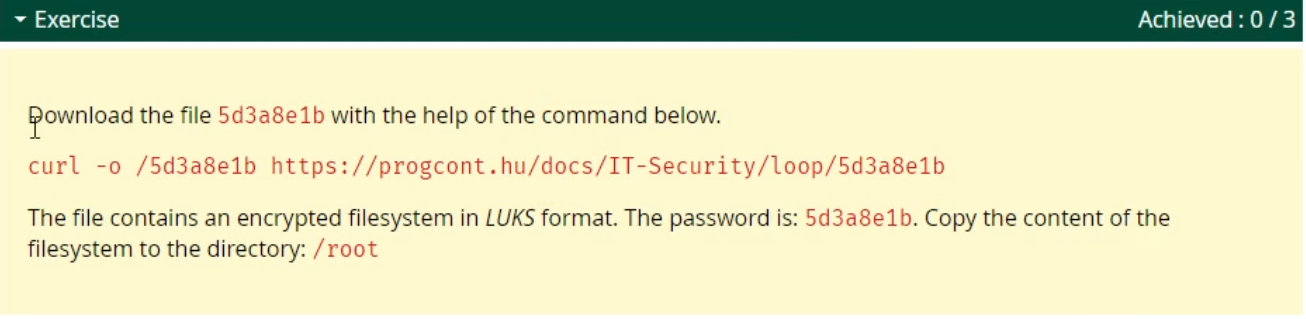




Who signed the file | signature was created with \* | write answer to file







Download the file | encrypted file system | LUKS format

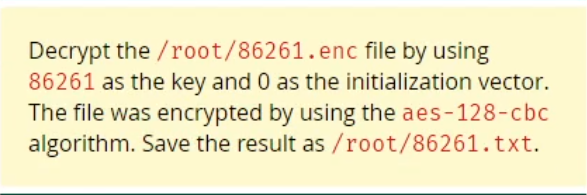
[root@localhost ~]# losetup -f /0cd53a06

[root@localhost ~]# cryptsetup luksOpen /dev/loop0 a

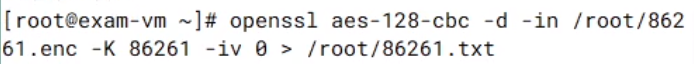
[root@localhost ~]# mount /dev/mapper/a /mnt

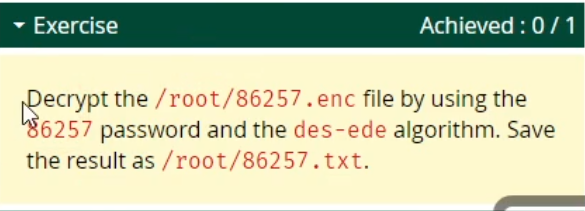
[root@localhost ~]# cp -r /mnt/\* /root/





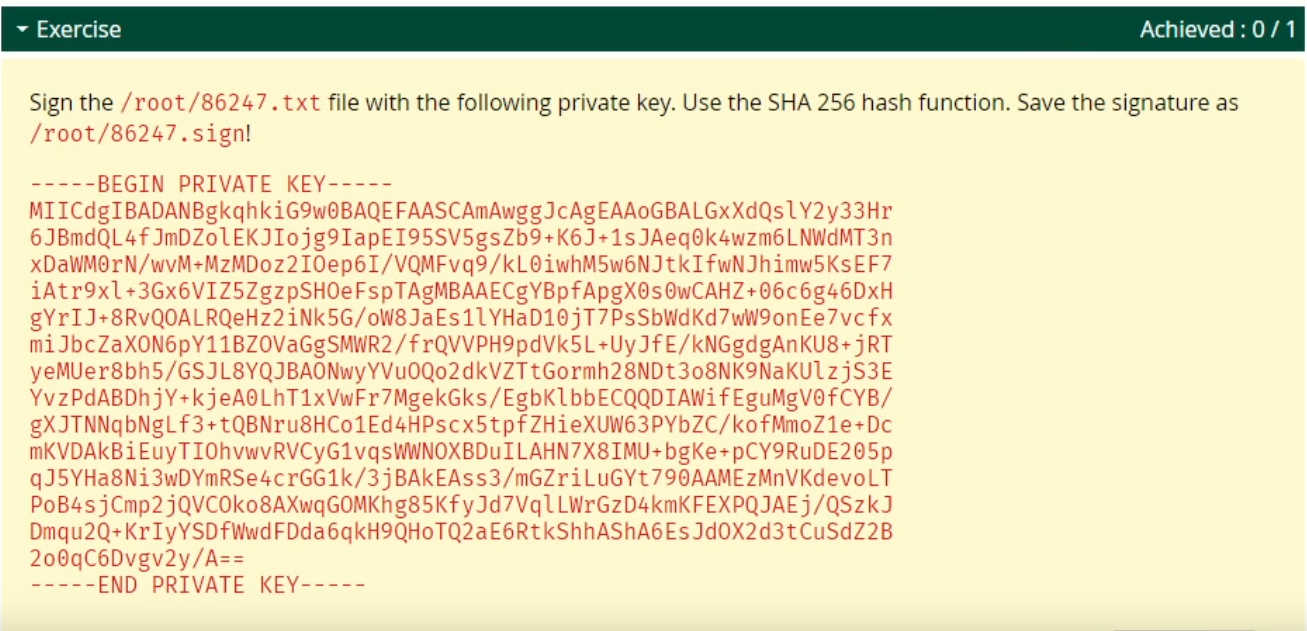
Decrypt | The file was encrypted by using aes-128-cbc



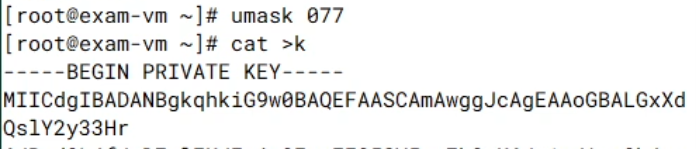


Decrypt | using des-ede algorithm

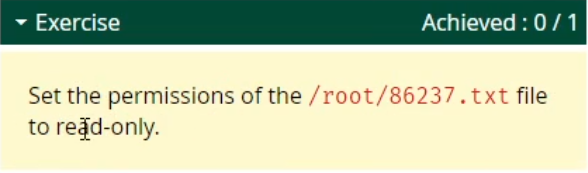




Sign the file with private key | Use SHA 256 hash function | save the signature

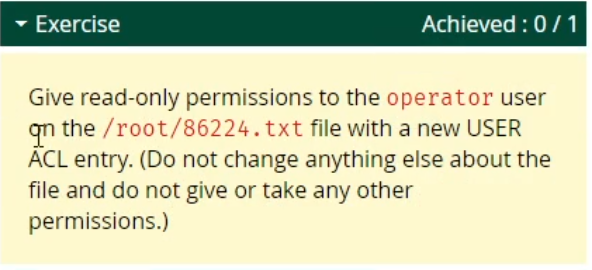






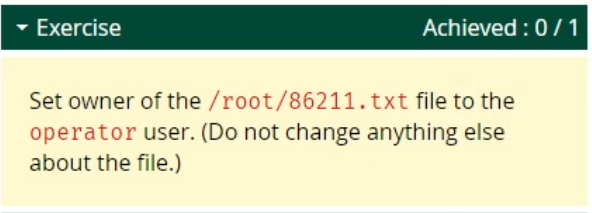
Set the permission | read-only





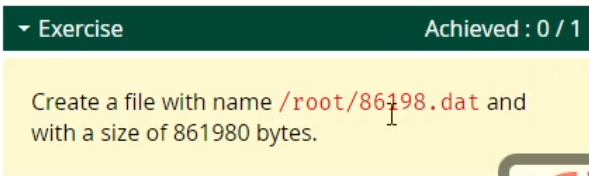
Give read-only permission to \* | new USER ACL entry





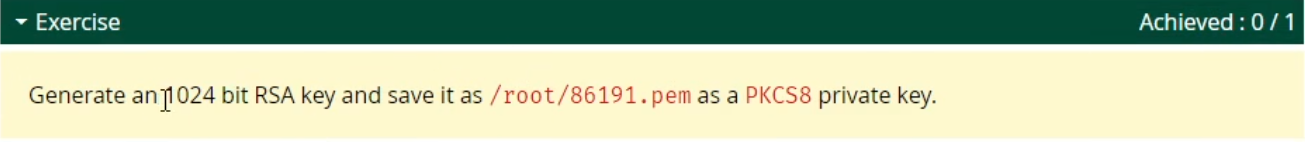
Set owner of a file





Create a file with a size of x bytes



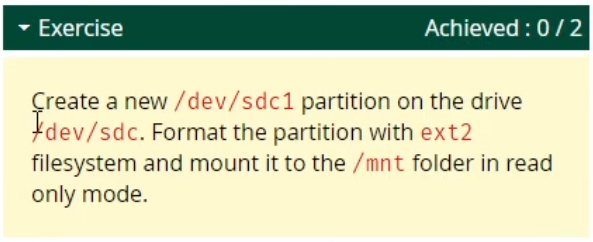


Generate a 1024 bit RSA key | save as PKCS8 private key









Create a new partition | Format it with ext2 | mount to \* in read only mode



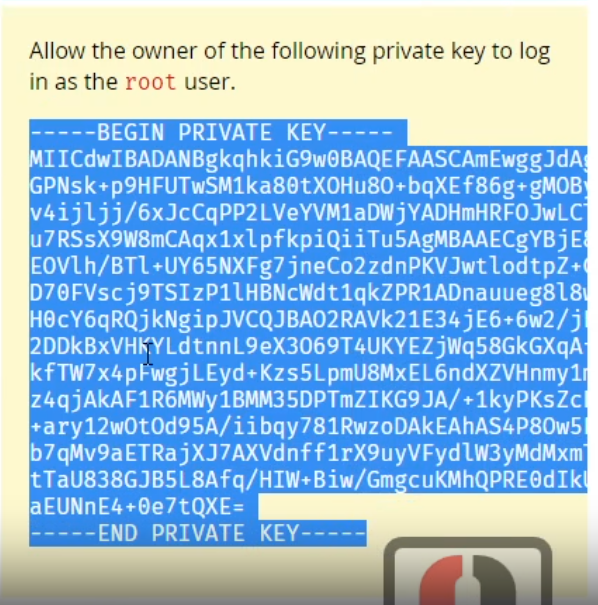












Allow the owner of the private key to log in as \*

