

BBM 465 INFORMATION SECURITY LAB

EXPERIMENT 4 REPORT

Subject : Kerberos

Group Number : 25

Group Members

EMİN ORÇUN SANCAR 21427306

MUSA ALİŞAR 21426567

KERBEROS

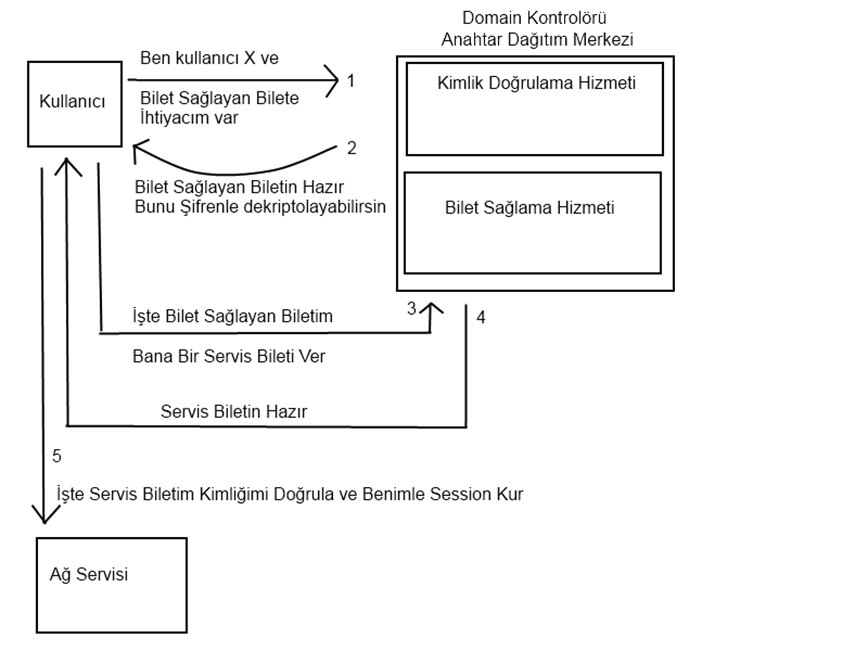
Kerberos is an protocol developed by MIT for identification and authentication. It was developed for UNIX systems. There is an security gap in the network when sending passwords. And kerberos designed for this vulnerability.

Kerberos has 3 main component. Server, client and key distribution service (KDC). Keys and passwords saved in KDC. And it has 2 components, KDC authentication service and ticket granting server. In the network safe connections realized with tickets. In order to increase security tickets use

time stamps. Time synchronization is very important between server and client. And this is realized with network time protocol (NTP).

Kerberos uses asymmetric cryptography. Default one is UDP 88 port. Cryptography algorithm was DES but after update used AES.





NTP (Network Time Protocol)

Time is very important parameter for tickets which is used in kerberos for time stamp. Therefore server and client time must be synchronized.

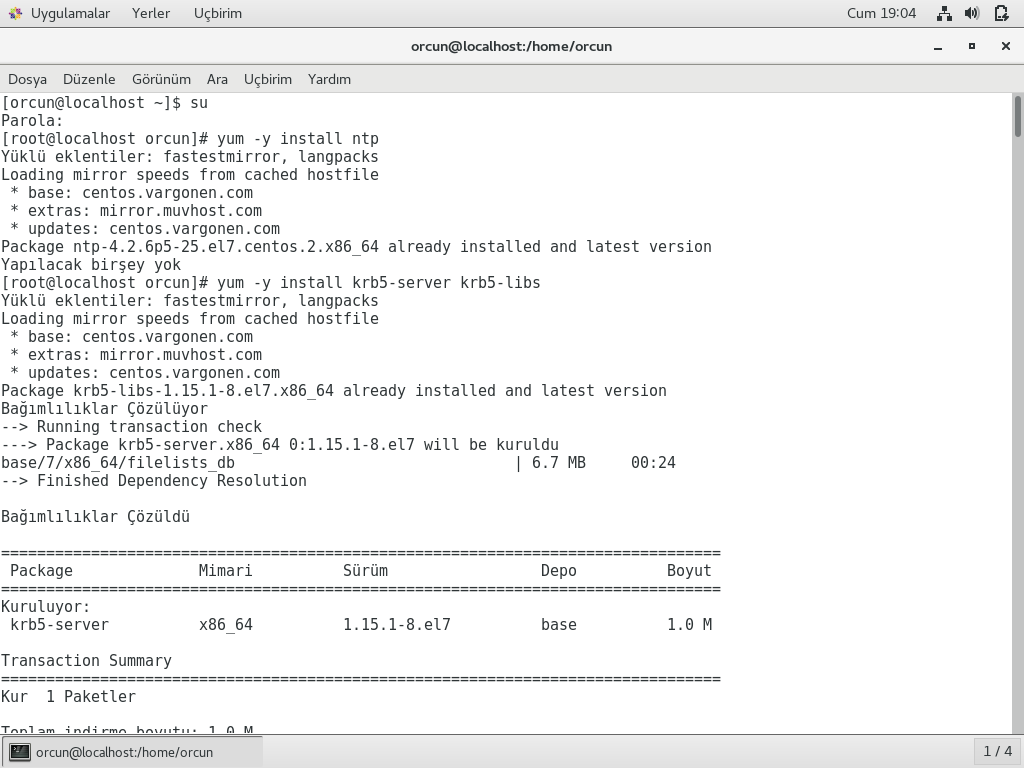
Ntp (network time protocol) is a program for time synchronization in a network.

# yum -y install ntp

# ntpdate -q time.nist.gov

# systemctl start ntpd

# systemctl enable ntpd



Kerberos Server

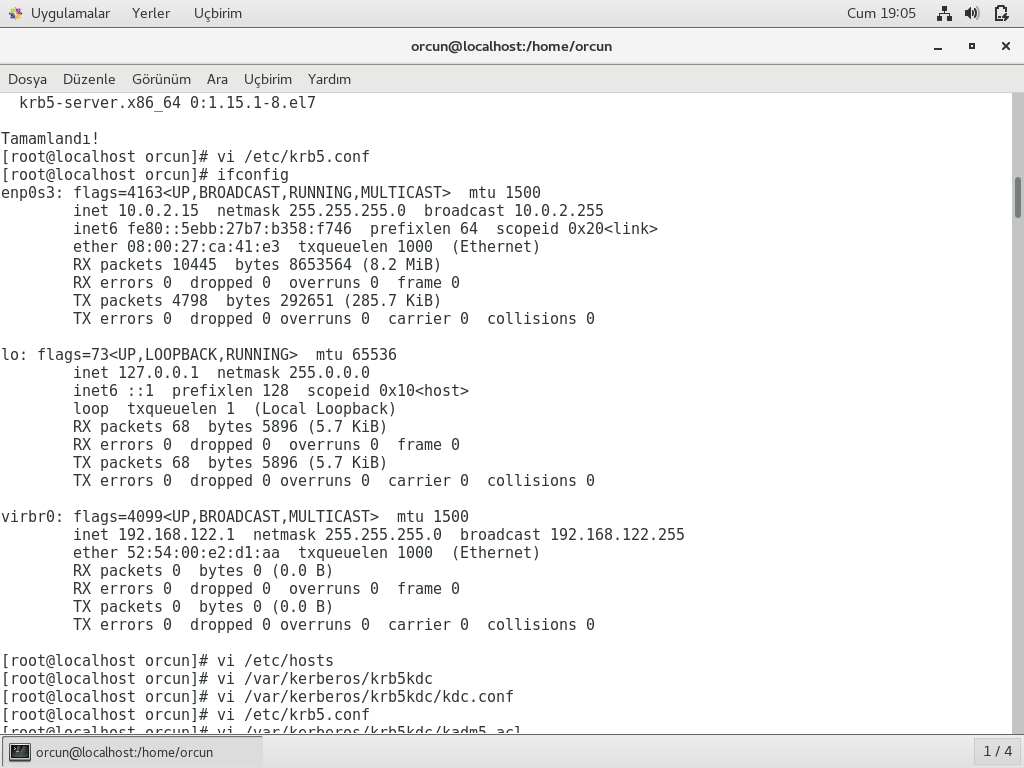
# yum install krb5-server krb5-libs

# vi /etc/krb5.conf

# vi /etc/hosts

# vi /var/kerberos/krb5kdc/kdc.conf

# vi /var/kerberos/krb5kdc/kadm5.acl



Create database and set a password that we can remember.

# kdb5\_util create -r ORCUN.COM -s

Now on the KDC create a admin principal and we add musa user.

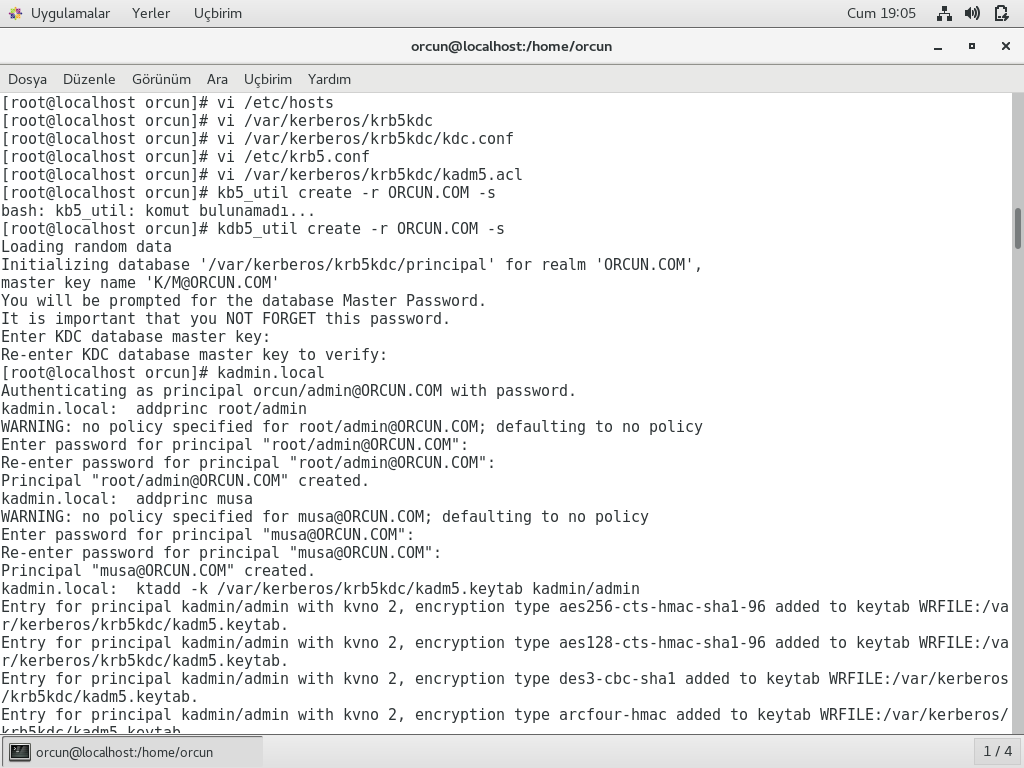
# kadmin.local

# addprinc root/admin

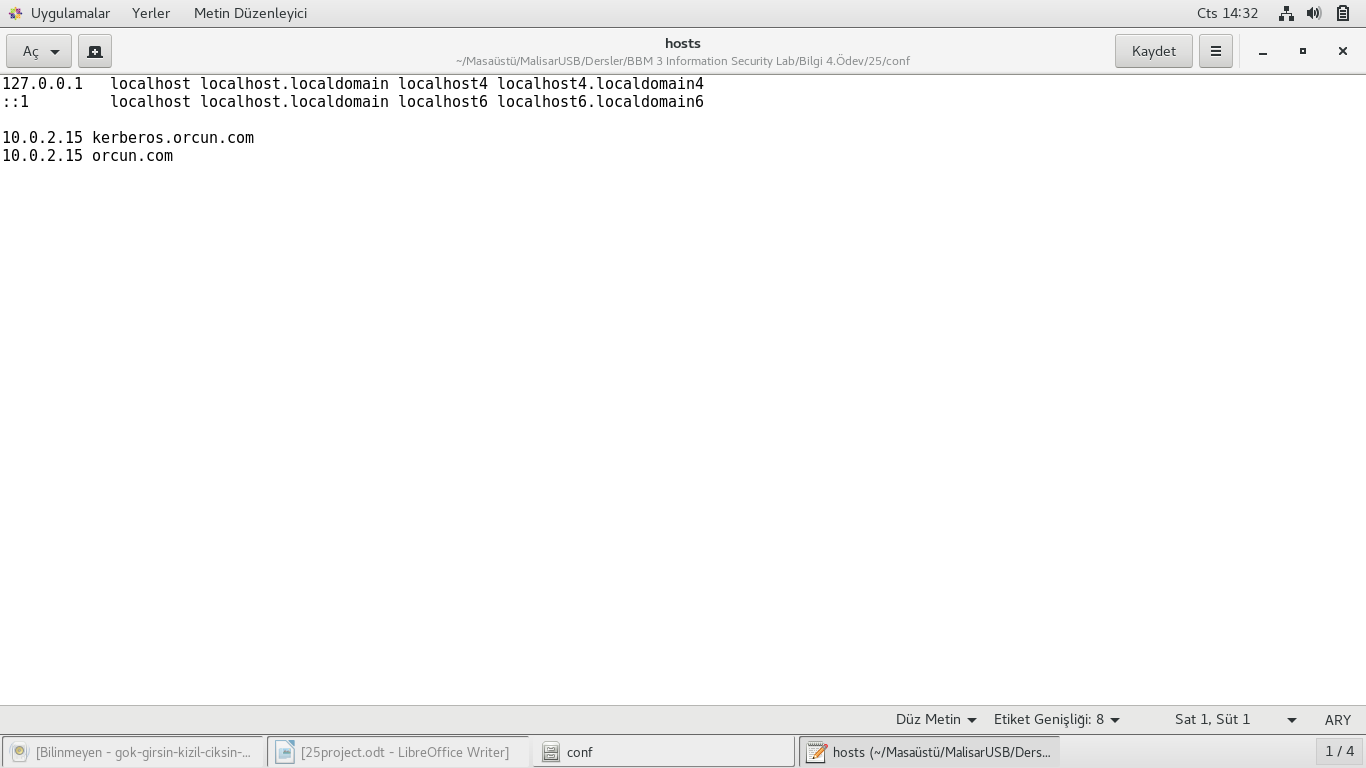
# addprinc musa

# ktadd -k /var/kerberos/krb5kdc/kdb5.keytab kadmin/admin

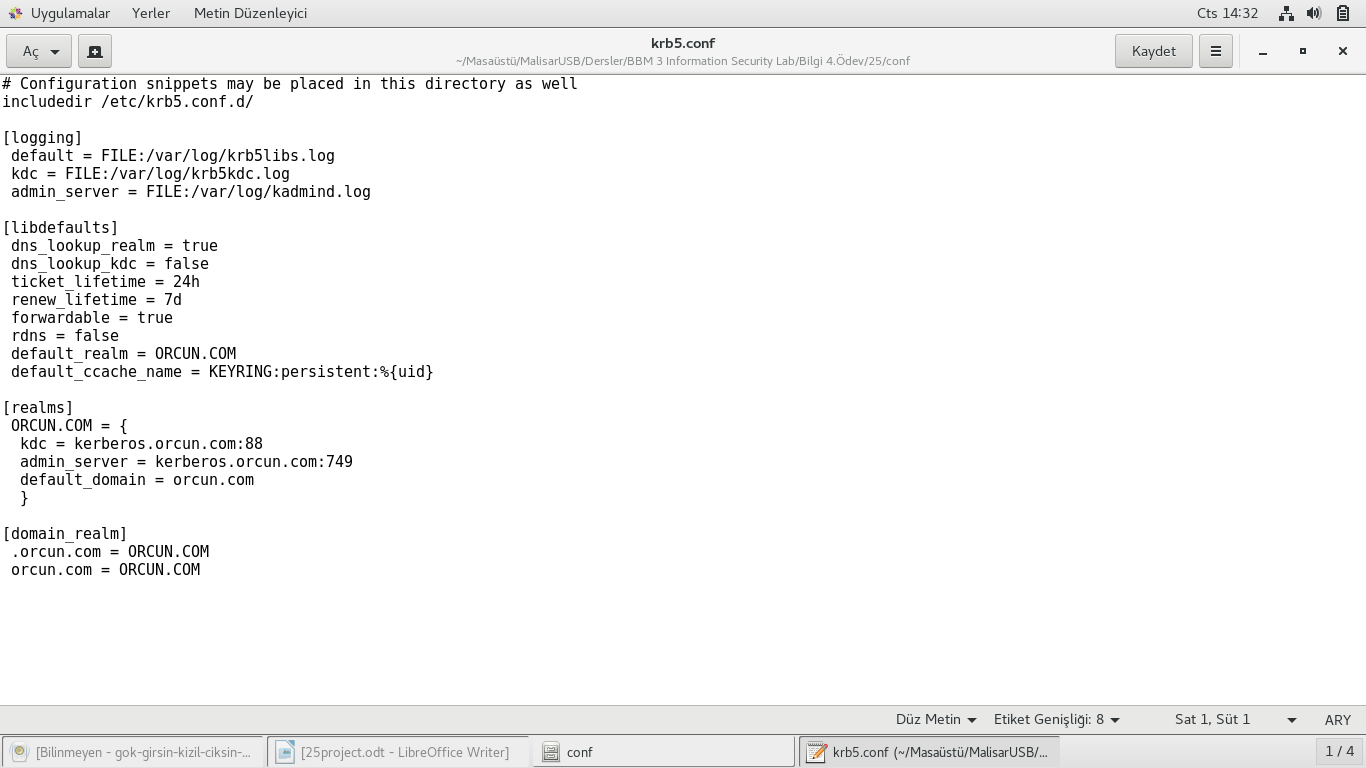
# ktadd -k /var/kerberos/krb5kdc/kdb5.keytab kadmin/changepw



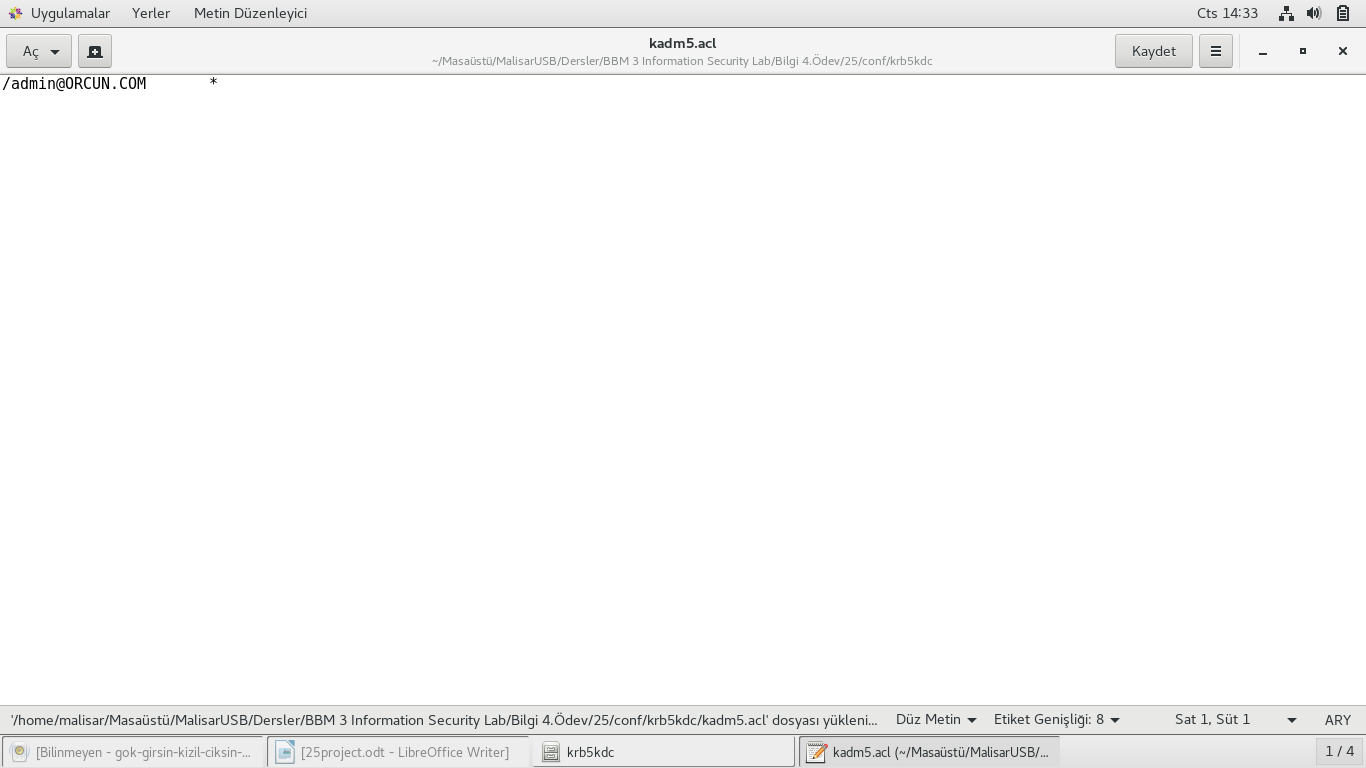
hosts



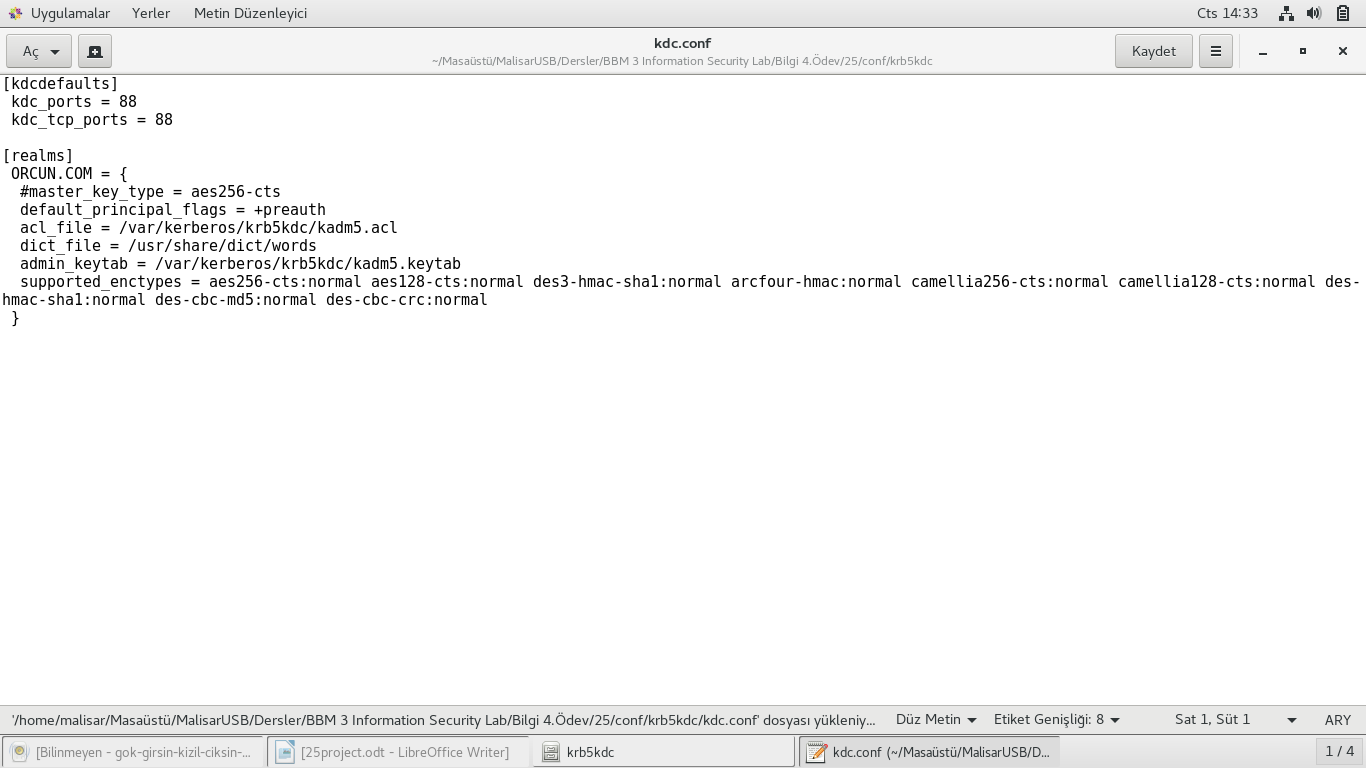
krb5.conf



kadm5.acl



kdc.conf



We start Kerberos KDC and kadmin daemons.

# systemctl start krb5kdc.service

# systemctl start kadmin.service

# systemctl enable krb5kdc.service

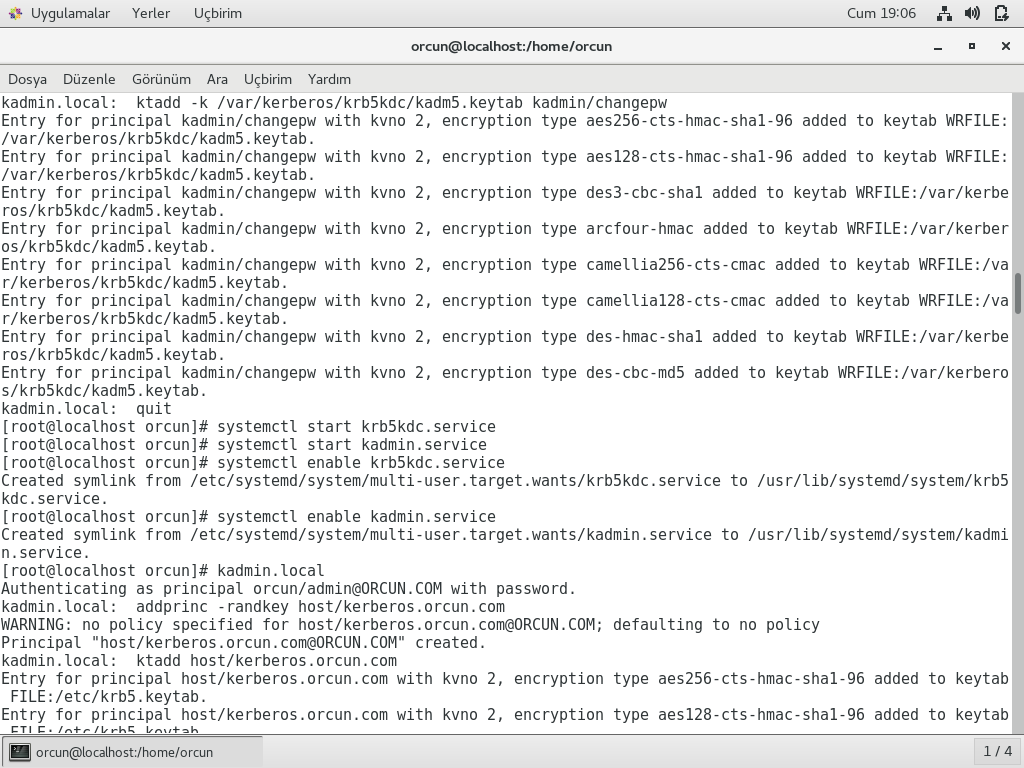
# systemctl enable kadmin.service

Then we create principal for our KDC server and stick it in it's keytab.

# kadmin.local

# addprinc -randkey host/kerberos.orcun.com

# ktadd host/kerberos.orcun.com



We use listprincs command to see our users in server

Kerberos Client

We configure our client by installing krb5-workstation

And add musa user in our server

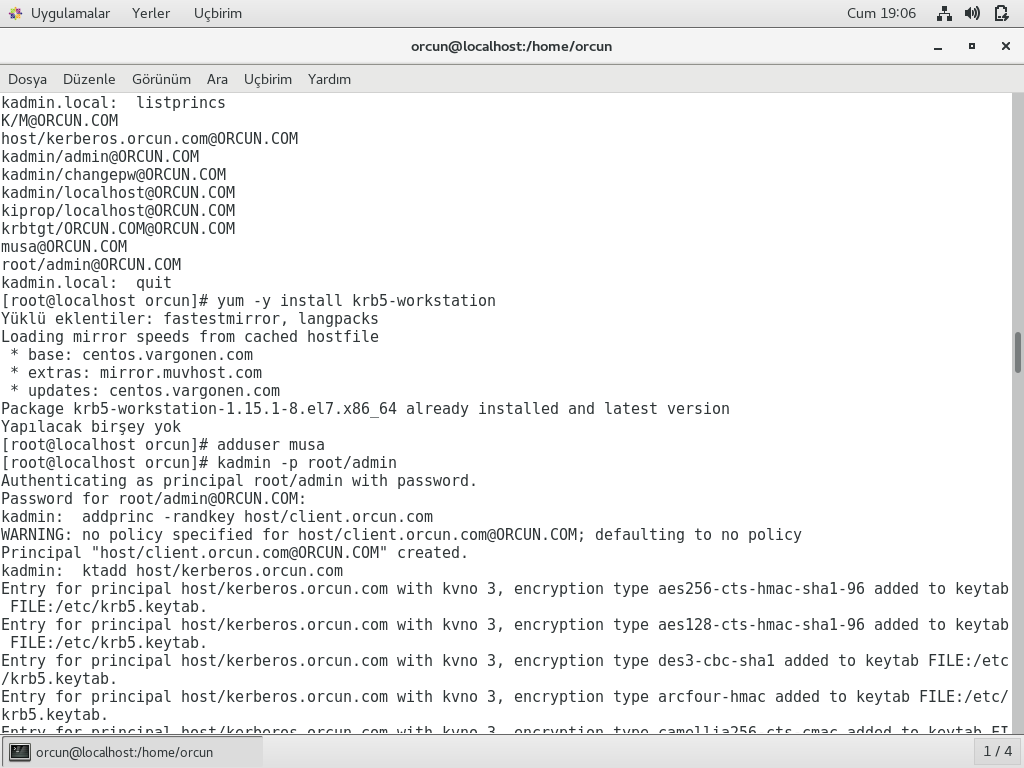
# yum –y install krb5-workstation

# yum install krb5-workstation

# kadmin -p root/admin

# addprinc -randkey host/kerberos.orcun.com

# ktadd host/kerberos.orcun.com



We confgure our sshd server and ssh client files

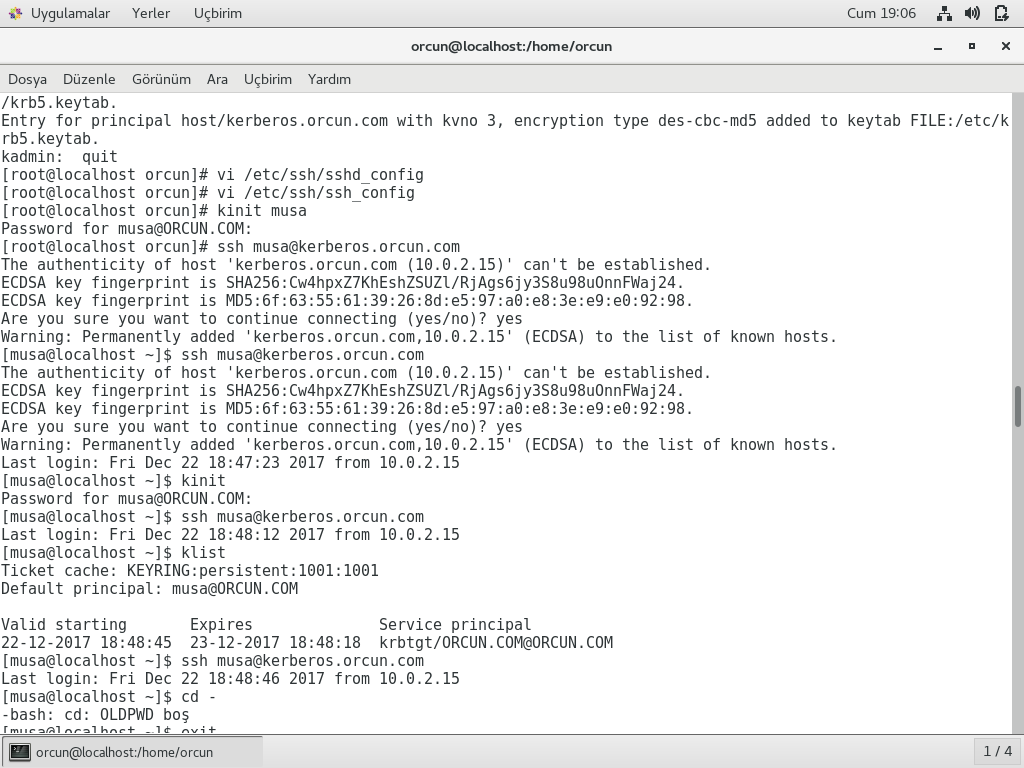
Then enter ssh by typing this

**#ssh musa@kerberos.orcun.com**

We enter kinit command to enter server and we enter klist command to check our ticket information

**#kinit**

**#klist**



 Then we authenticate 3 users to our server orcun we add kerem and nurlan as a new users and so on we have 3 users to authenticate(musa,kerem,nurlan)

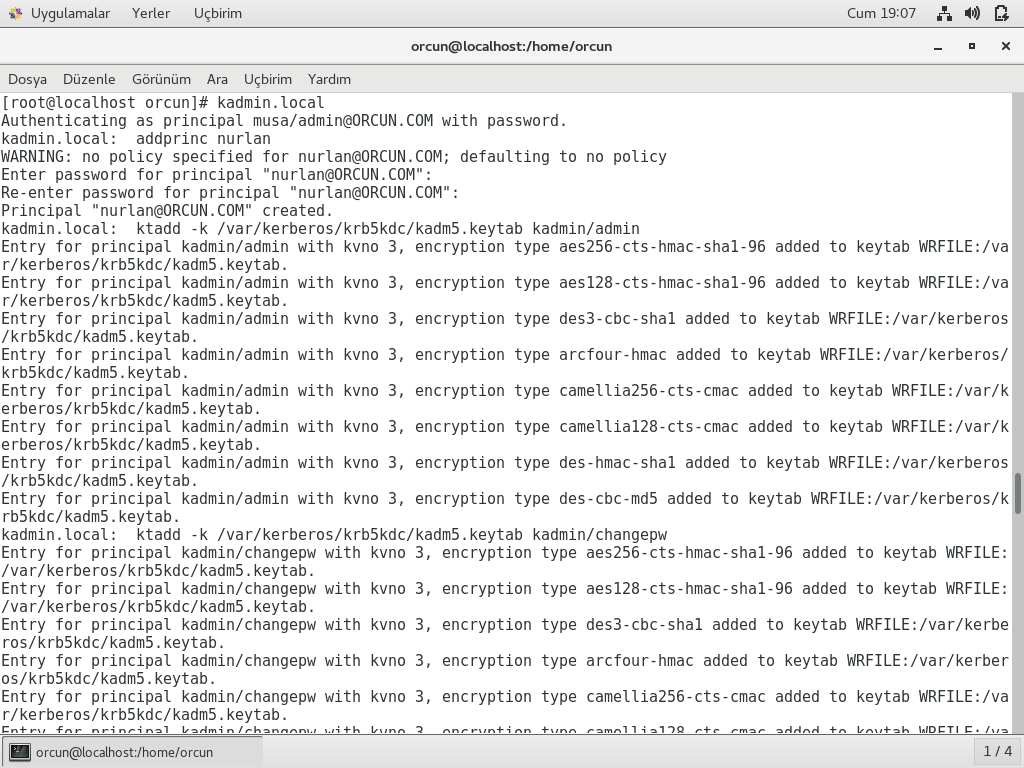
**#addprinc nurlan**

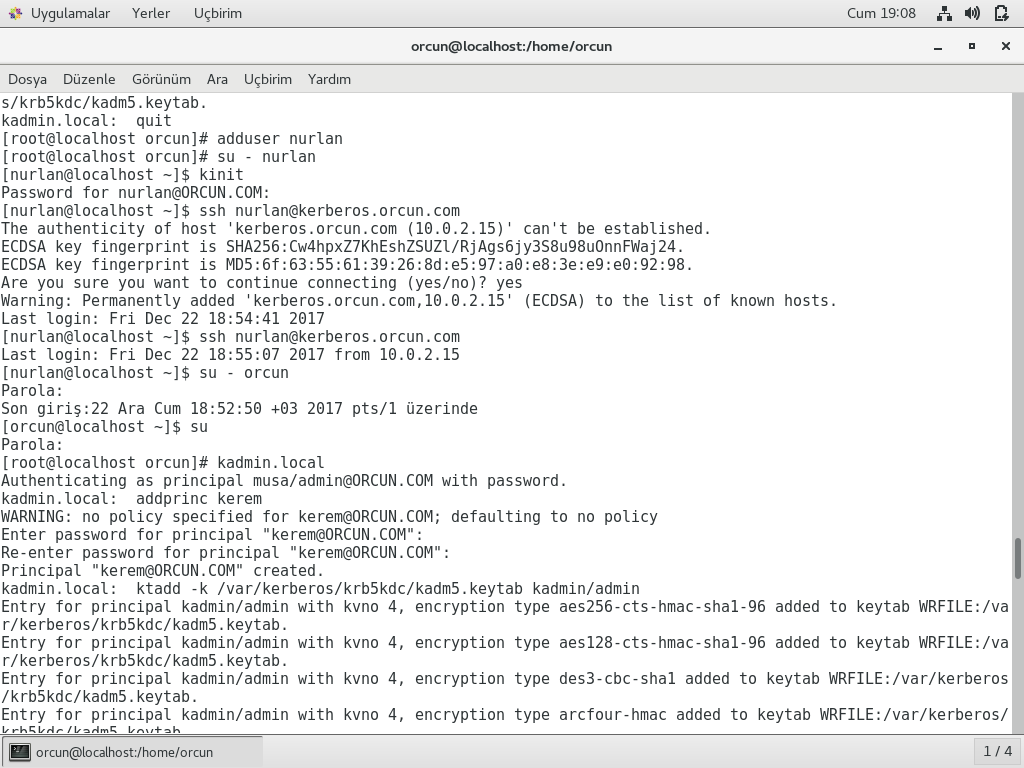
# ktadd -k /var/kerberos/krb5kdc/kdb5.keytab kadmin/admin

# ktadd -k /var/kerberos/krb5kdc/kdb5.keytab kadmin/changepw

#klist

#kinit





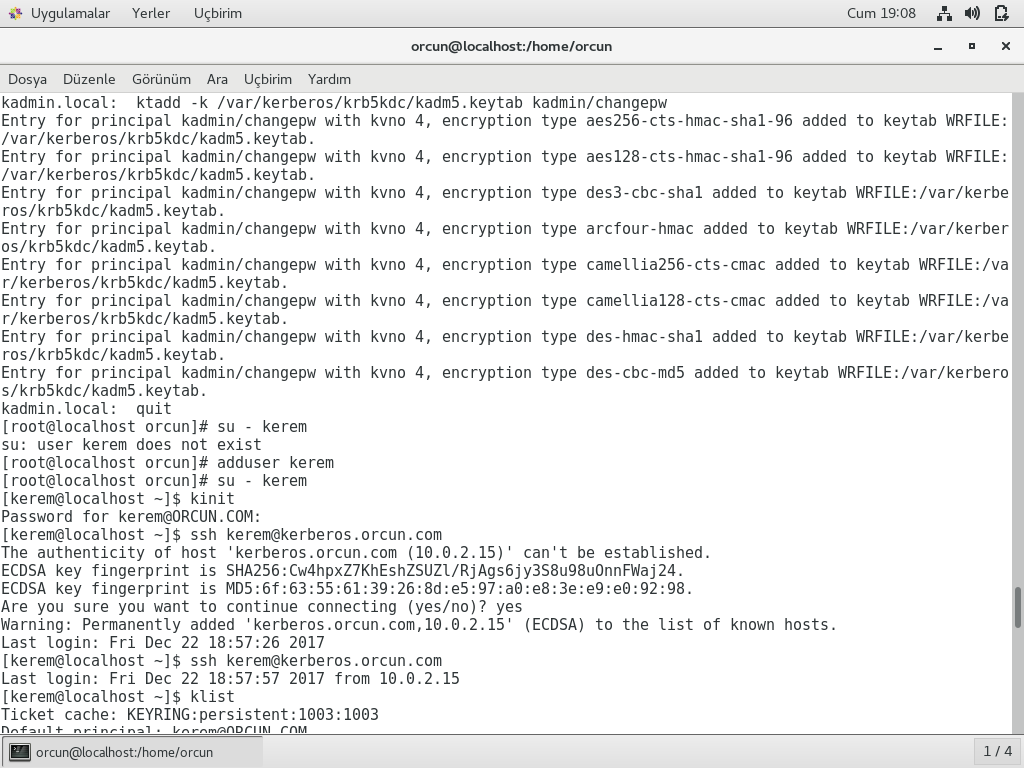
**#addprinc kerem**

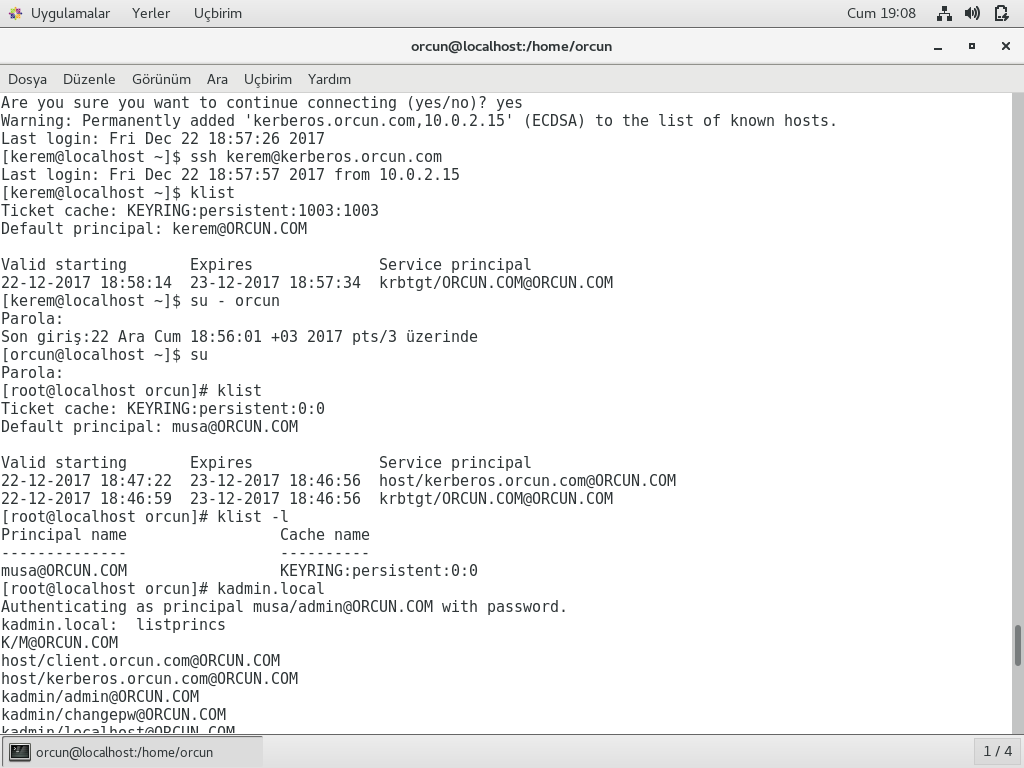
# ktadd -k /var/kerberos/krb5kdc/kdb5.keytab kadmin/admin

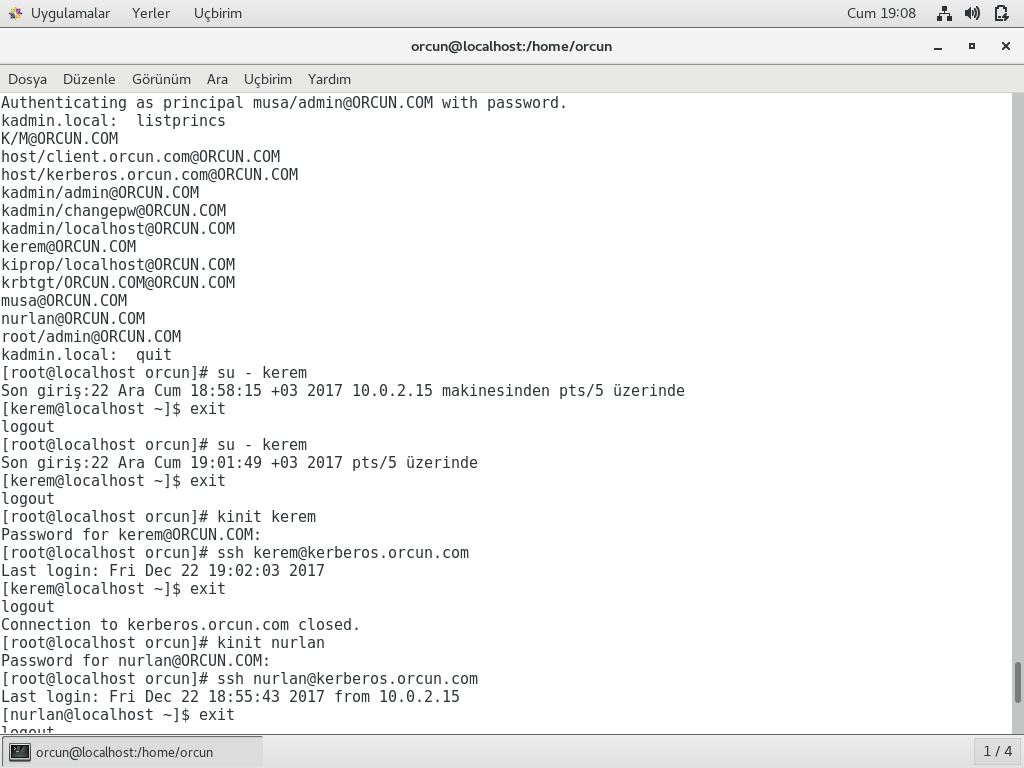
# ktadd -k /var/kerberos/krb5kdc/kdb5.keytab kadmin/changepw

#klist

**#kinit**

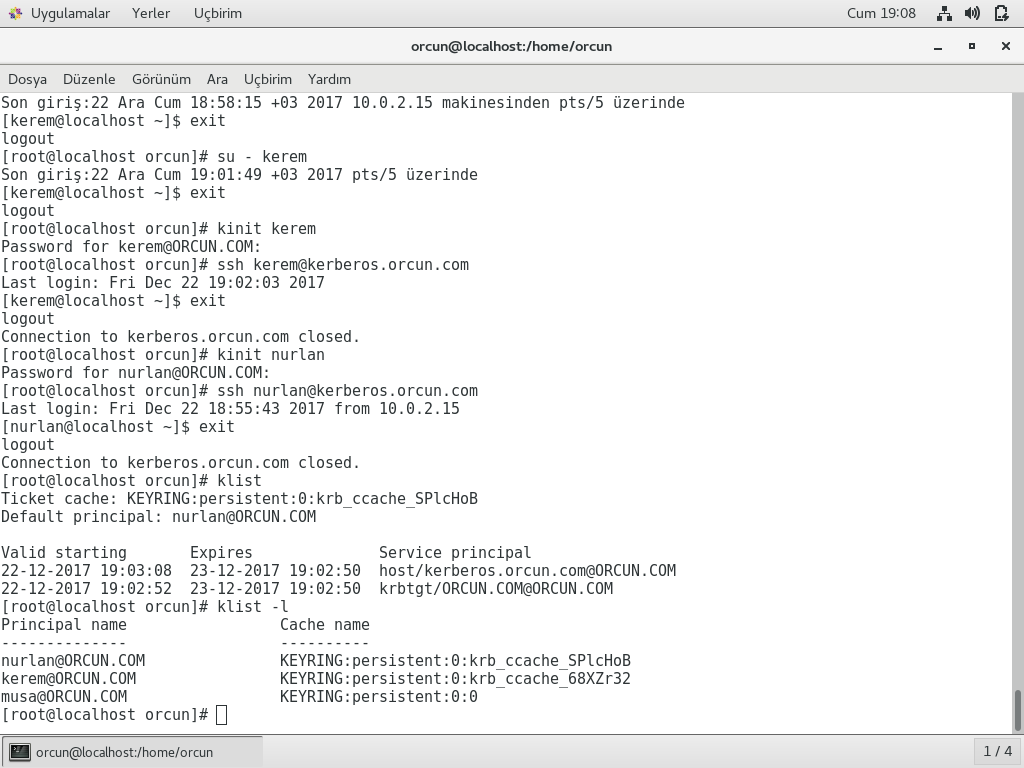




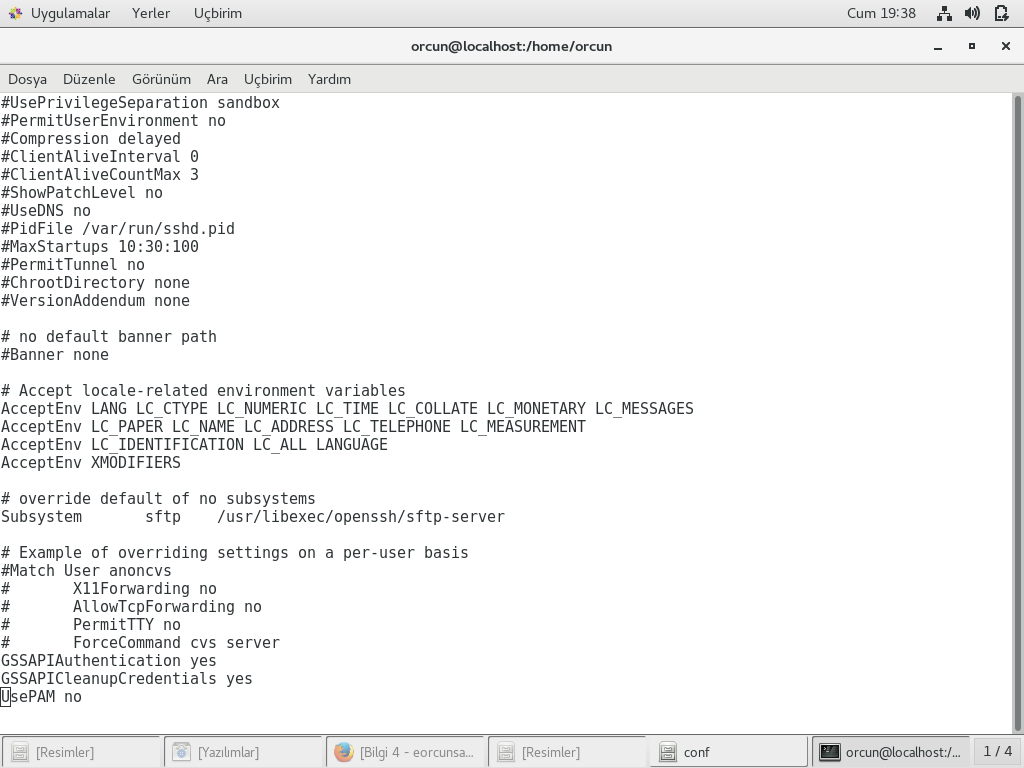


We see our authenticated clients by typing this command

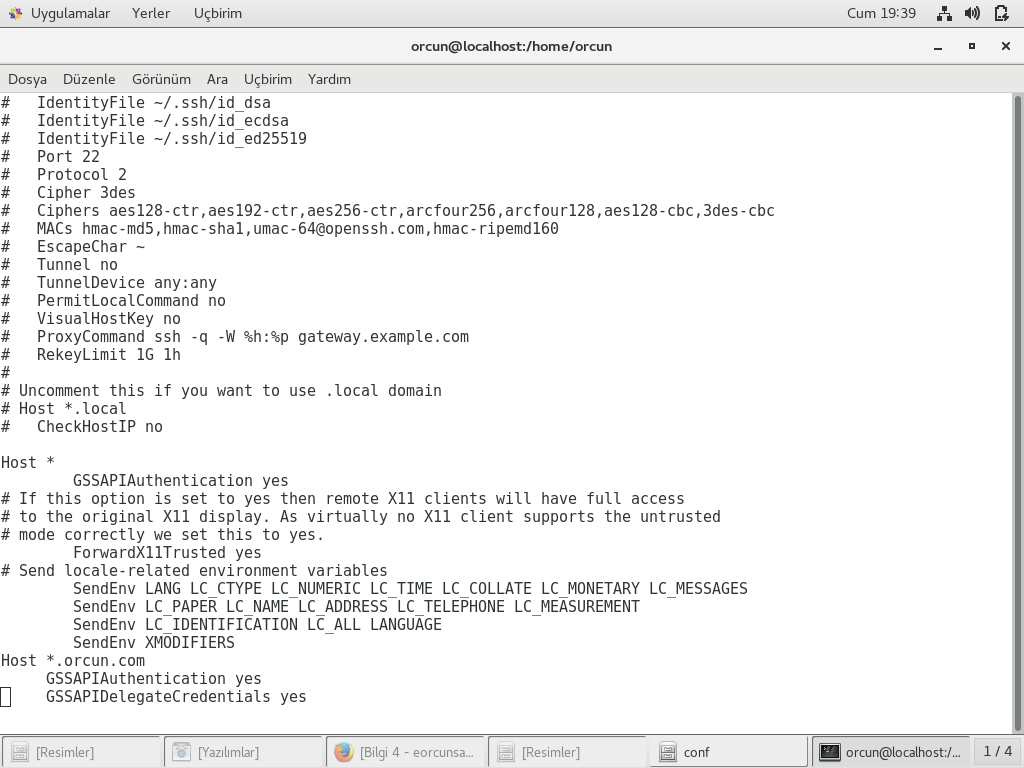
#klist -l



SSHD

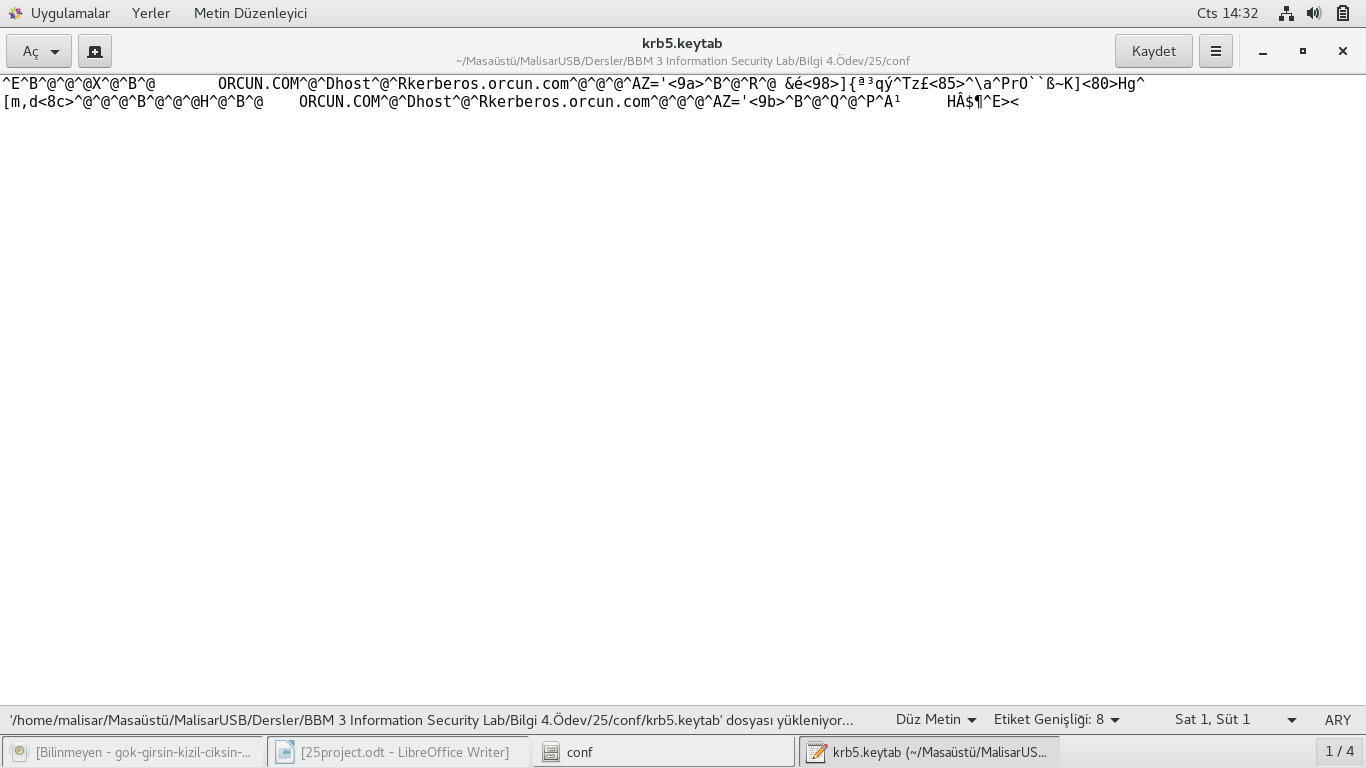


**SSH**



Our keyfile in /etc/krb5.keytab

krb5.keytab



REFERENCES

* <https://www.youtube.com/watch?v=7Q-Xx0I8PXc&t=199s>
* <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/managing_smart_cards/configuring_a_kerberos_5_server>
* <https://www.theurbanpenguin.com/configuring-a-centos-7-kerberos-kdc/>
* <https://www.centos.org/docs/5/html/5.1/Deployment_Guide/s1-kerberos-server.html>
* <https://gist.github.com/ashrithr/4767927948eca70845db>