**CONFIGURE OPEN SSH AND SCP IN LINUX CLIENT AND SERVER USING KERBEROS AUTHENTICATION**

**REQUIREMENT SPECIFICATION**

**SOFTWARE REQUIREMENTS**

The Kerberos authentication protocol is an inbuilt feature of various operating

systems. Following are some required operating systems to implement Kerberos

Authentication;

a. VMWare Workstation (preferred latest version)

b. Linux (Debian)

In our project, we use debian10 Version. Below are some required dependencies for

server &client machines;

Sever Machine:

a. krb5-kdc

b. krb5-admin-server

c. krb5-config

Client Machine:

a. krb5-user

b. libpam-krb5

c. libpam-ccreds

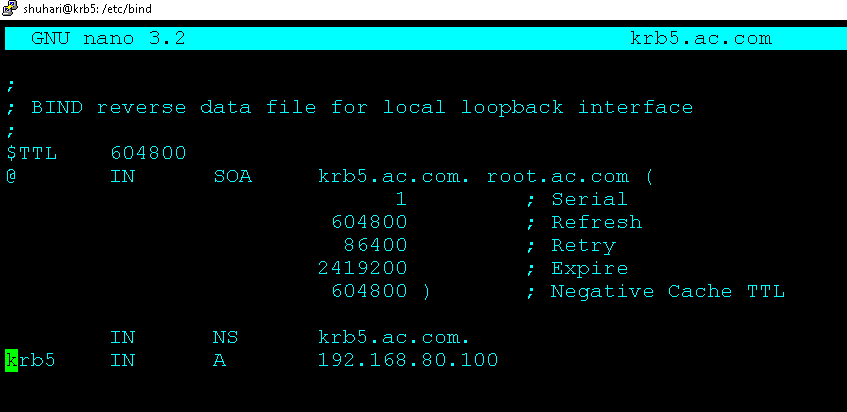
# IMPLEMENTATION

The following are the steps for implementing Kerberos Authentication Protocol;

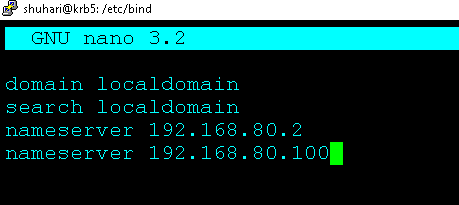
## Server Configuration

#### Step 1: Setting up FQDN ‘krb5.ac.com’

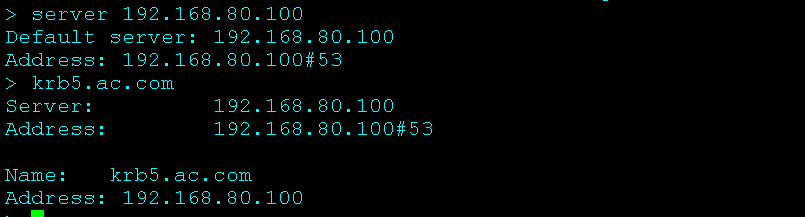
* sudo apt install bind9 bind9utils dnsutils (Install DNS server)
* sudo nano /etc/hosts (Define hosts entry for new domain
  + sudo cp /etc/bind/db.127 /etc/bind/krb5.ac.com (Create backup)
  + sudo nano /etc/bind/krb5.ac.com (Create new file for domain)



* + sudo nano /etc/bind/named.conf.local (Define zone scope for domain
  + sudo nano /etc/resolv.conf (Define DNS nameserver)



#### Testing-

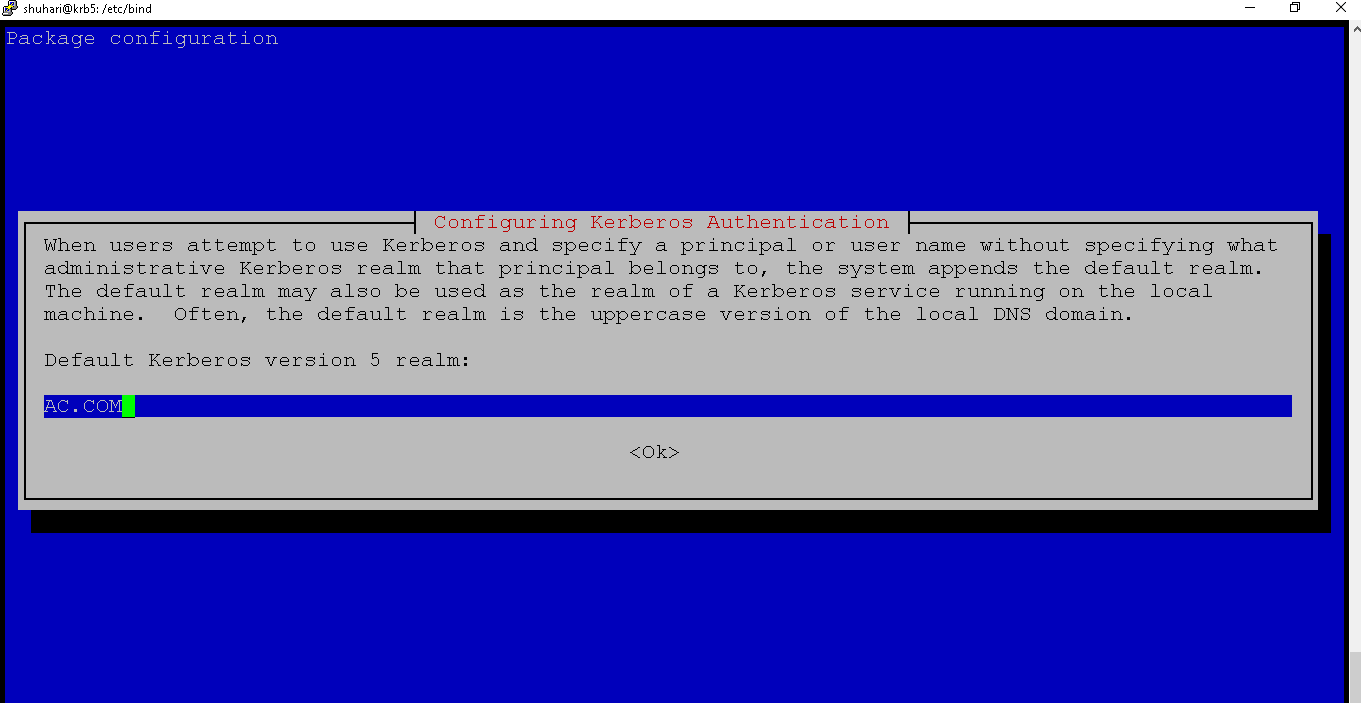


## Step 2: Install KDC Server

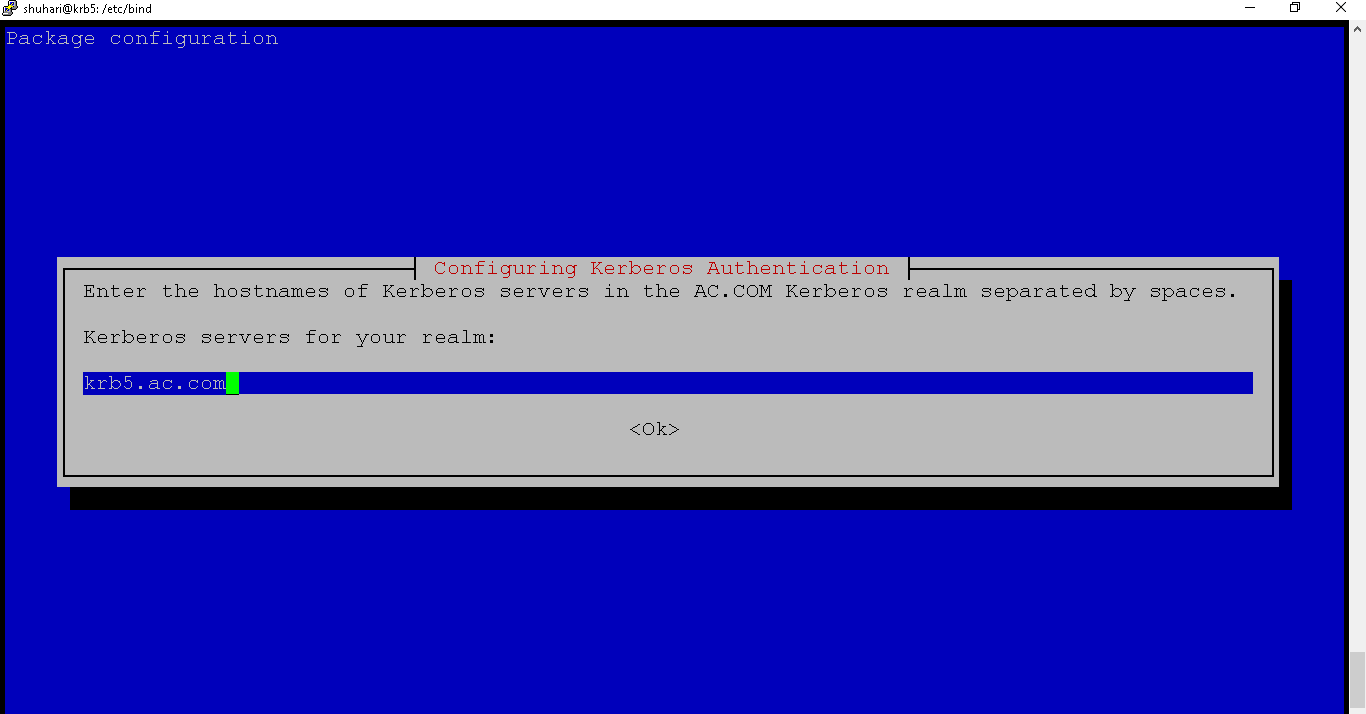
##### **-** sudo apt install krb5-admin-server krb5-config krb5-kdc

* Default Kerberos realm ‘**AC.COM**’

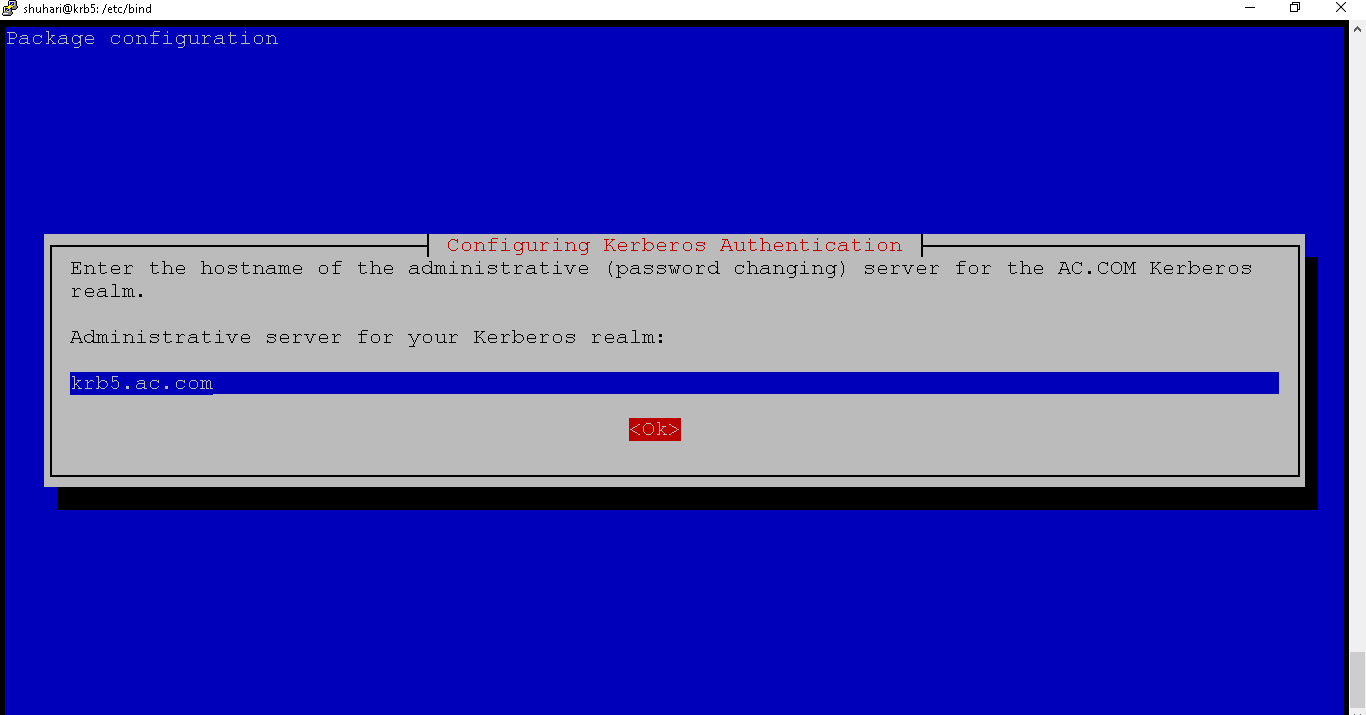
- Kerberos realms are a way of logically grouping resources and identities that use Kerberos



* Enter the Kerberos Server realm ‘**krb5.ac.com**’



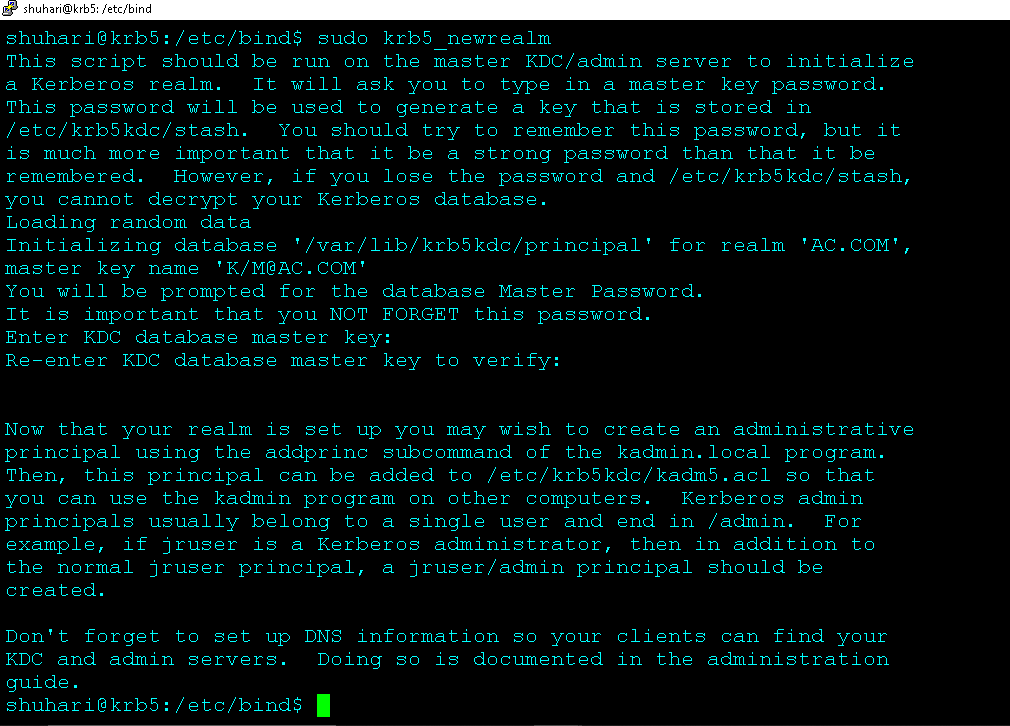
* + Enter the administrative server for Kerberos realm **‘krb5.ac.com’.**



## Step 3: Configure KDC Kerberos Server

- sudo krb5\_newrealm (Used to create new kerberos realm)

- give password as master key for KDC server



Run ‘**kadmin.local**’ CLI interface for kerberos-

* sudo kadmin.local
  + kadmin.local: addprinc root/admin

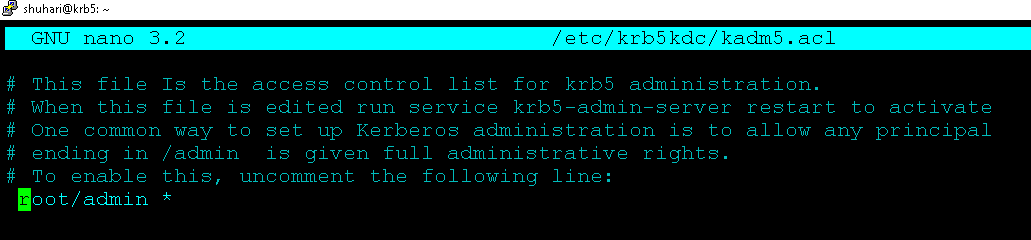
- give passsword

* + kadmin.local: addprinc -randkey host/krb5.ac.com

kadmin.local: ktadd host/krb5ac.com

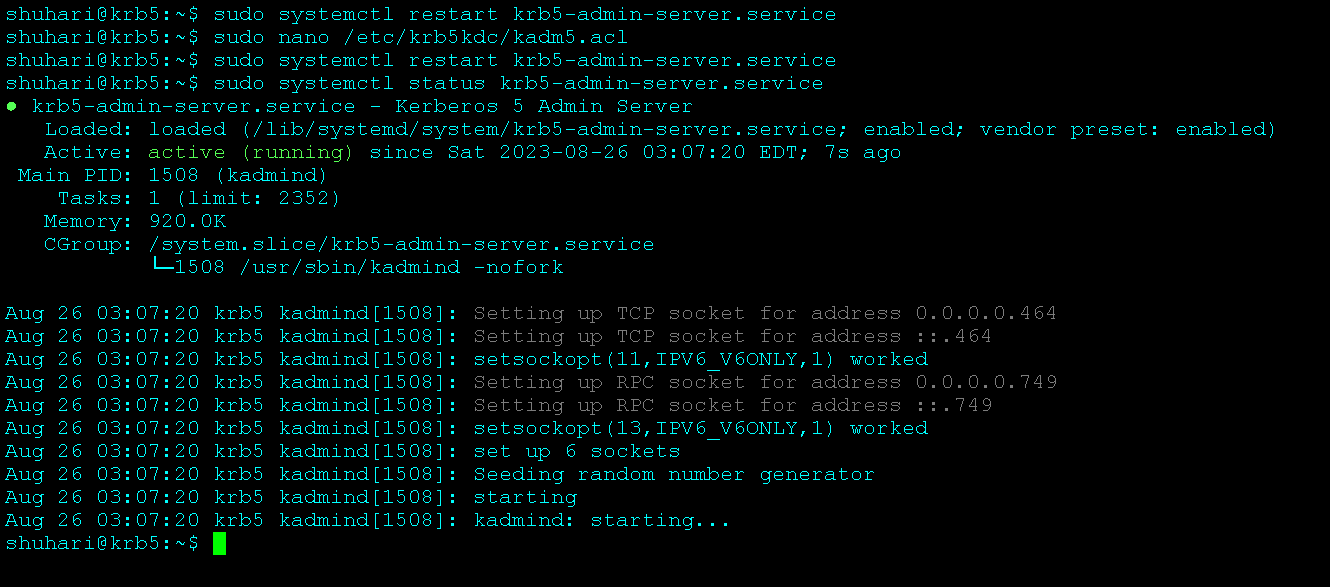
## Adding ‘root’ admin principal to the access control list-

##### sudo nano /etc/krb5kdc/kadm5.acl



## Now, restart Kerberos Service and check the status.

* + - * sudo systemctl restart krb5-admin-server.service (Restart)
      * sudo systemctl status krb5-admin-server.service (Status)

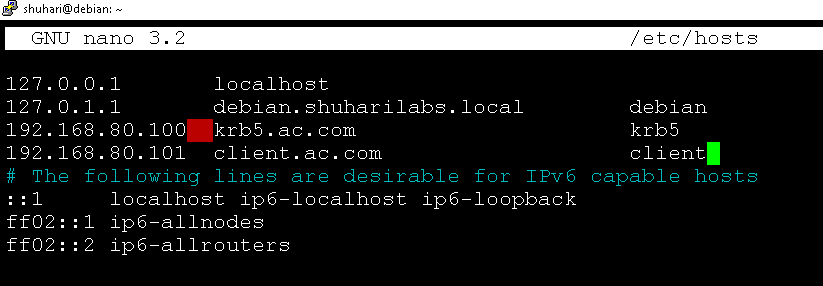


## Client Configuration

#### Step 4: Installing and configuring Kerberos Client

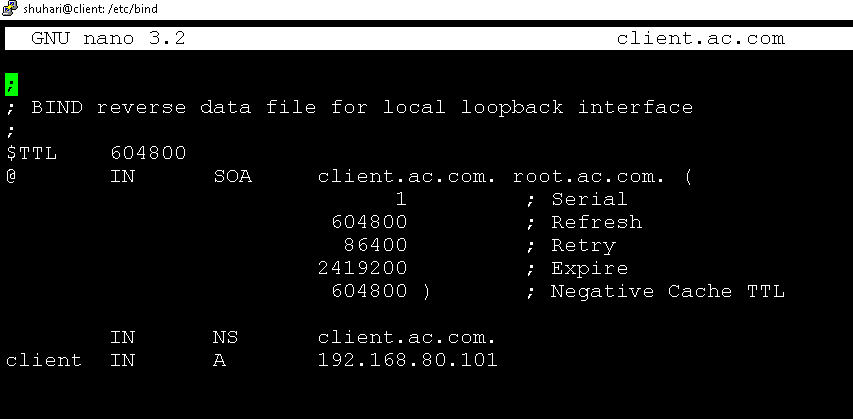
Configure FQDN ‘client.ac.com’

* + sudo apt install bind9 bind9utils dnsutils (Install DNS server)
  + sudo nano /etc/hosts (Define hosts entry for new domain)

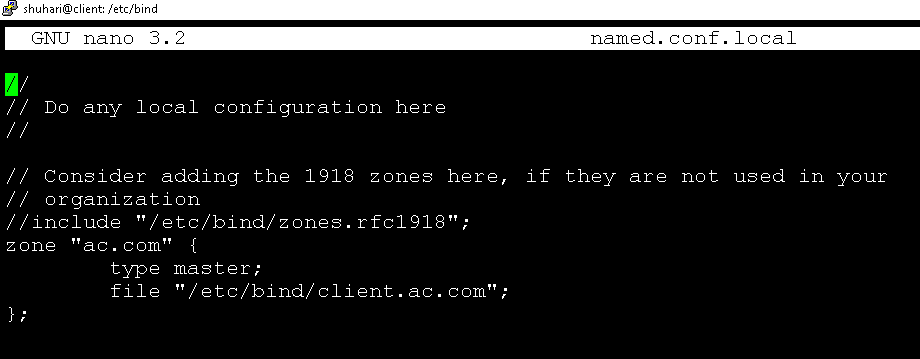


-sudo cp /etc/bind/db.127 /etc/bind/client.ac.com (Create backup)

-sudo nano /etc/bind/client.ac.com (Create new file for domain)



-sudo nano /etc/bind/named.conf.local (Define zone scope for domain)



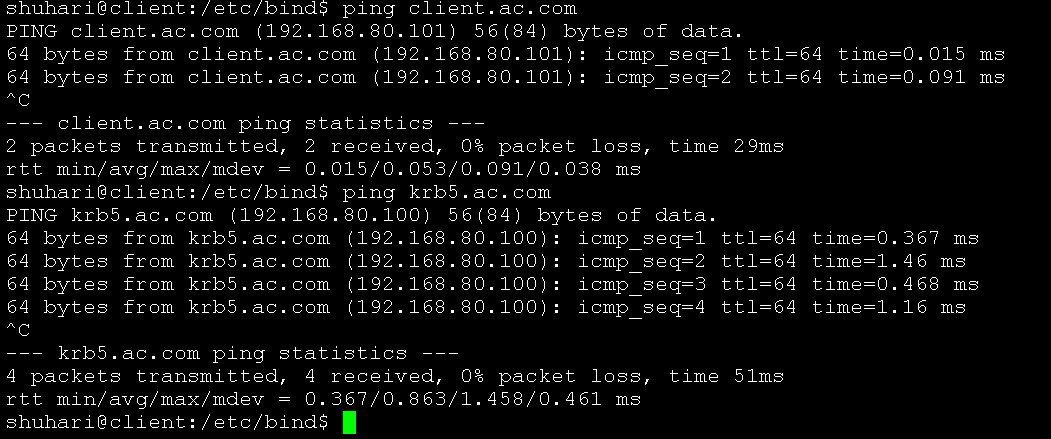
##### sudo nano /etc/resolv.conf

put nameserver as DNS nameserver IP -> **192.168.80.100**



## Testing-

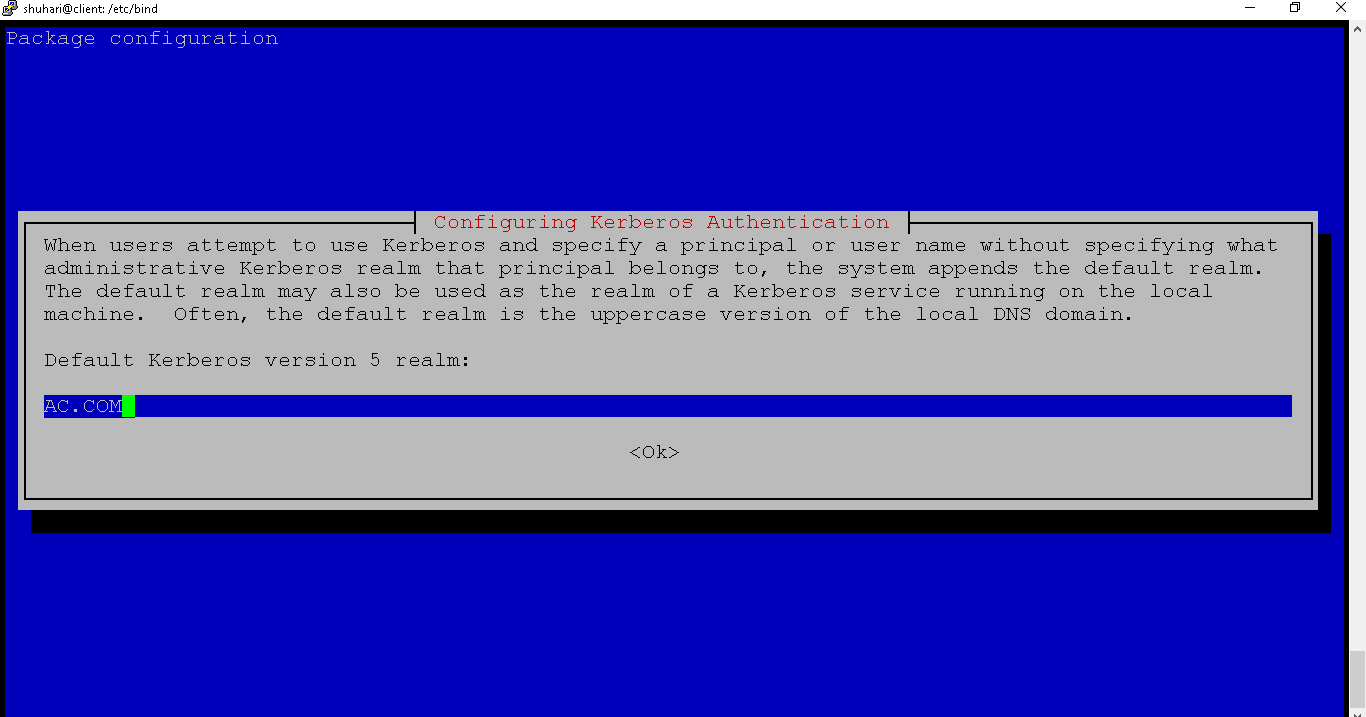
##### Try to ping to ‘client.ac.com’ and ‘krb5.ac.com’



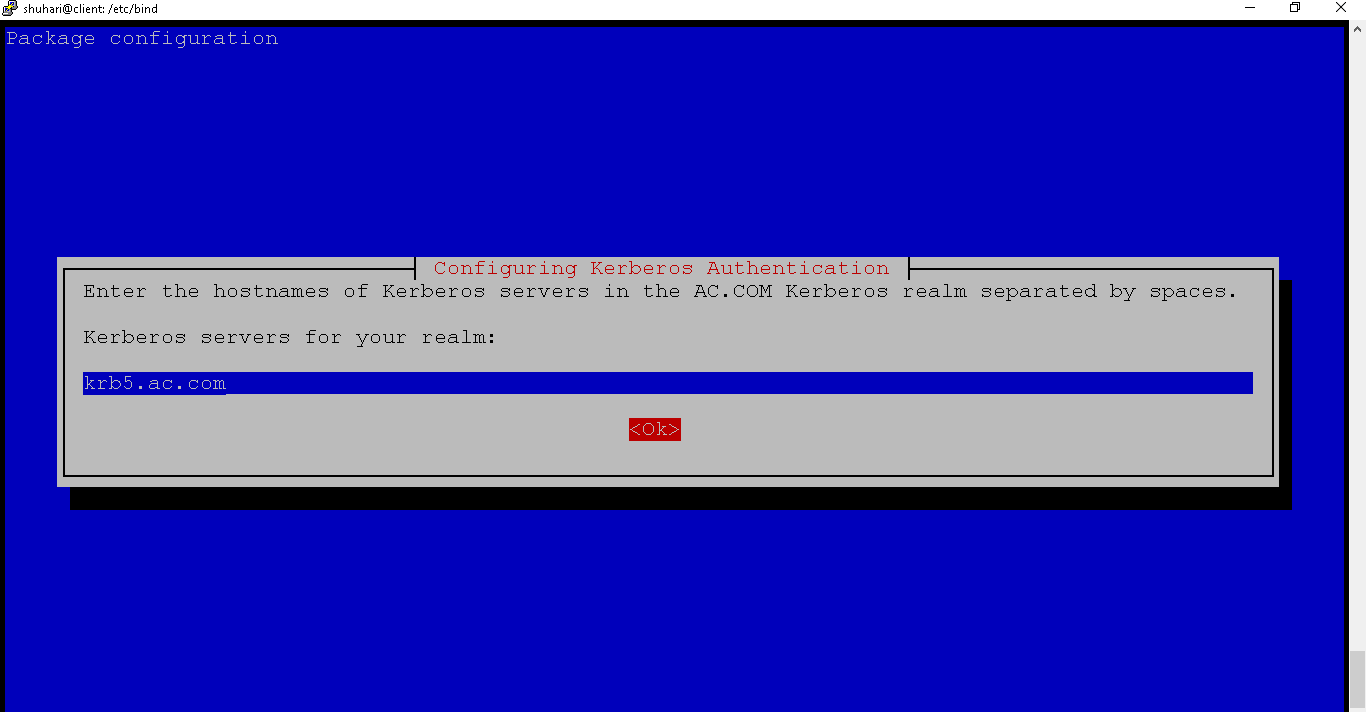
## Install Kerberos client-

##### - sudo apt install –y krb5-user libpam-krb5 libpam-ccreds

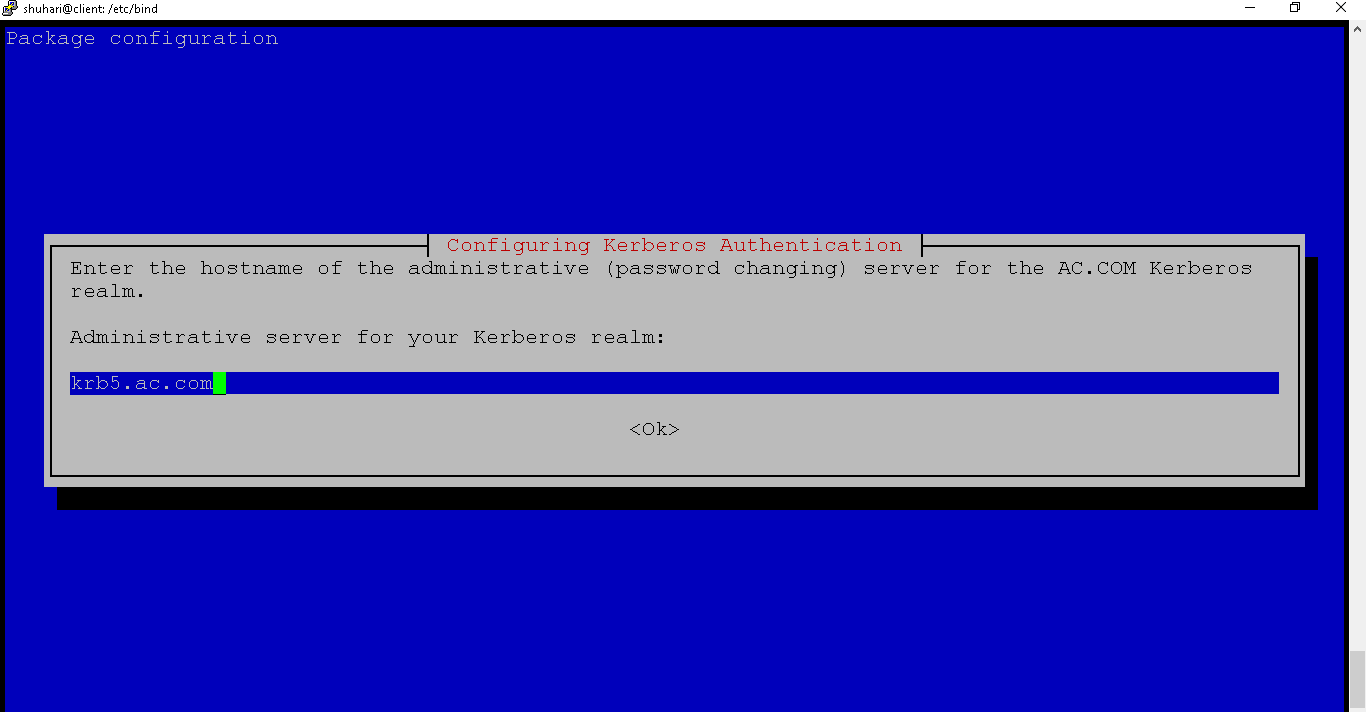
**Check for Kerberos server domain name as realm ‘AC.COM’-**



#### Enter the Kerberos server ‘krb5.ac.com’-



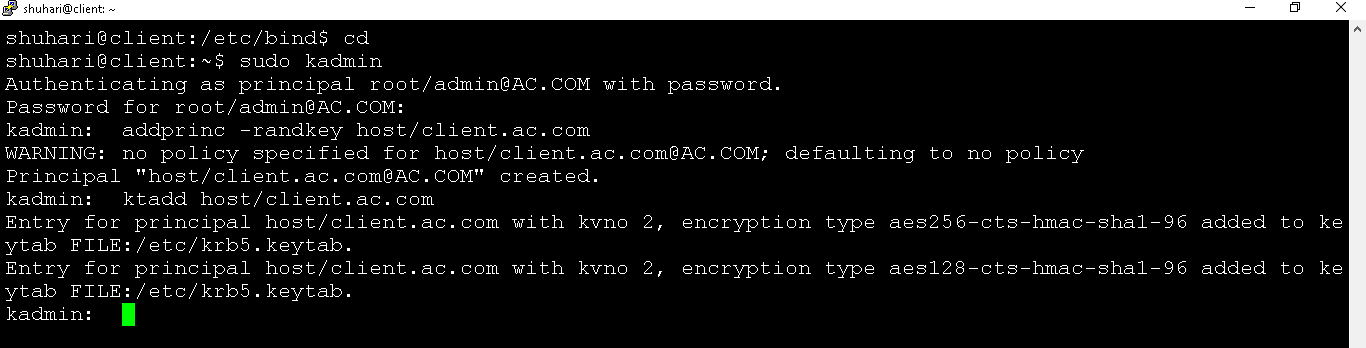
**Enter the admin server name as the Kerberos server name ‘krb5.ac.com’-**



###### Configure Kerberos Client & add Kerberos client to the Kerberos database and addthe keytab file for the client.

###### Configure Kerberos Client & add Kerberos client to the Kerberos database and addthe keytab file for the client.

- sudo kadmin



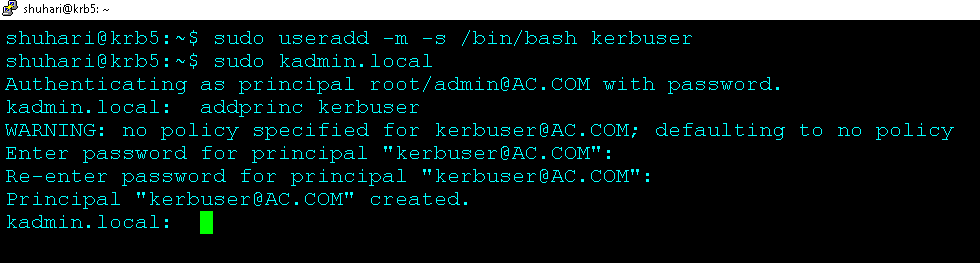
#### *Step 5: Testing the configurations*

* + Setup ‘krb5.ac.com’ Server

- Creating a new user to the system & adding a new principal for the user

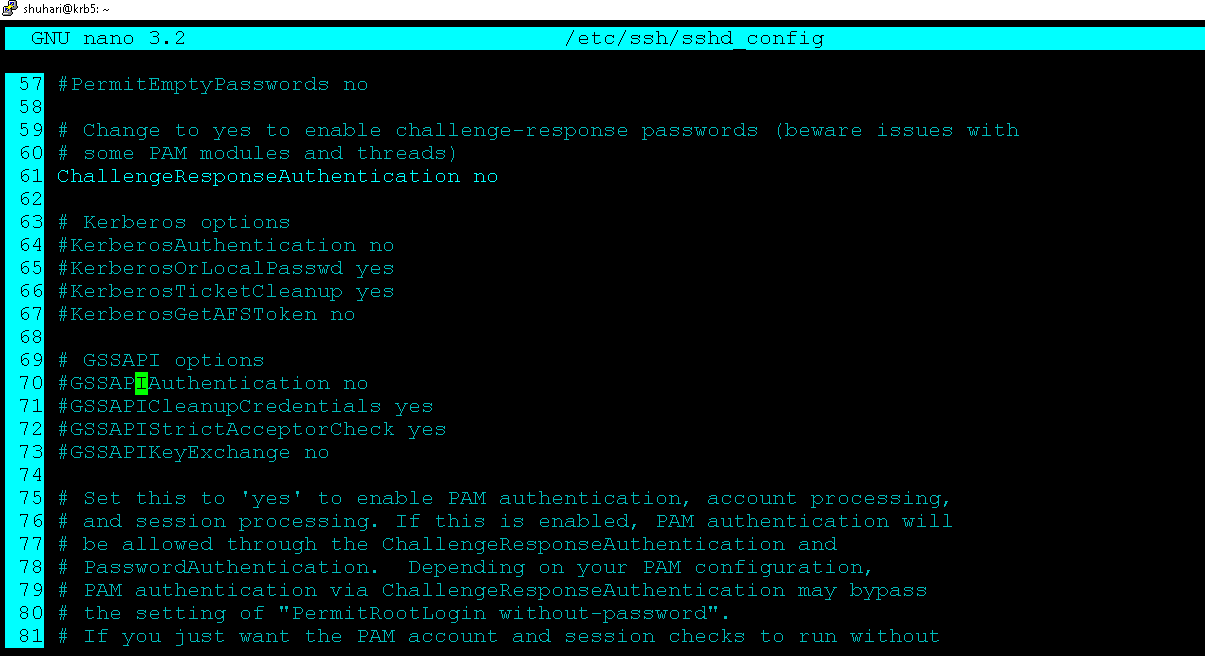
- sudo useradd -m -s /bin/bash **kerbuser**

**-** sudo kadmin.local



* Edit ssh configuration ‘/etc/ssh/sshd\_config’ & uncomment the ‘GSSAPIAuthentication’ and enable it by changing the value to **‘yes’**

#### Before-

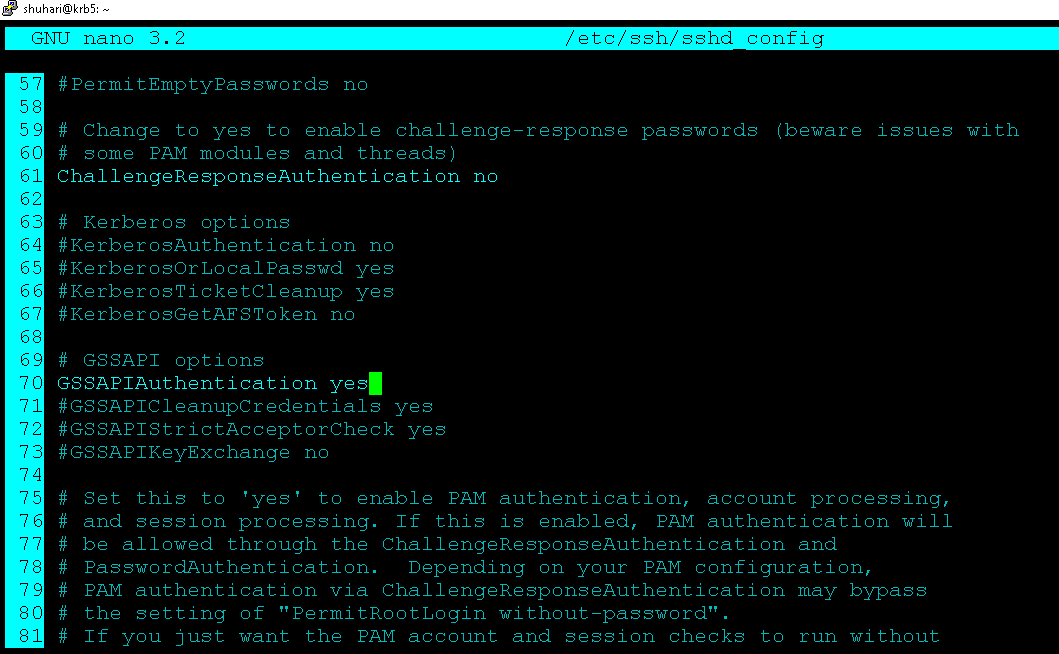


-sudo nano /etc/ssh/sshd\_config

#### After-

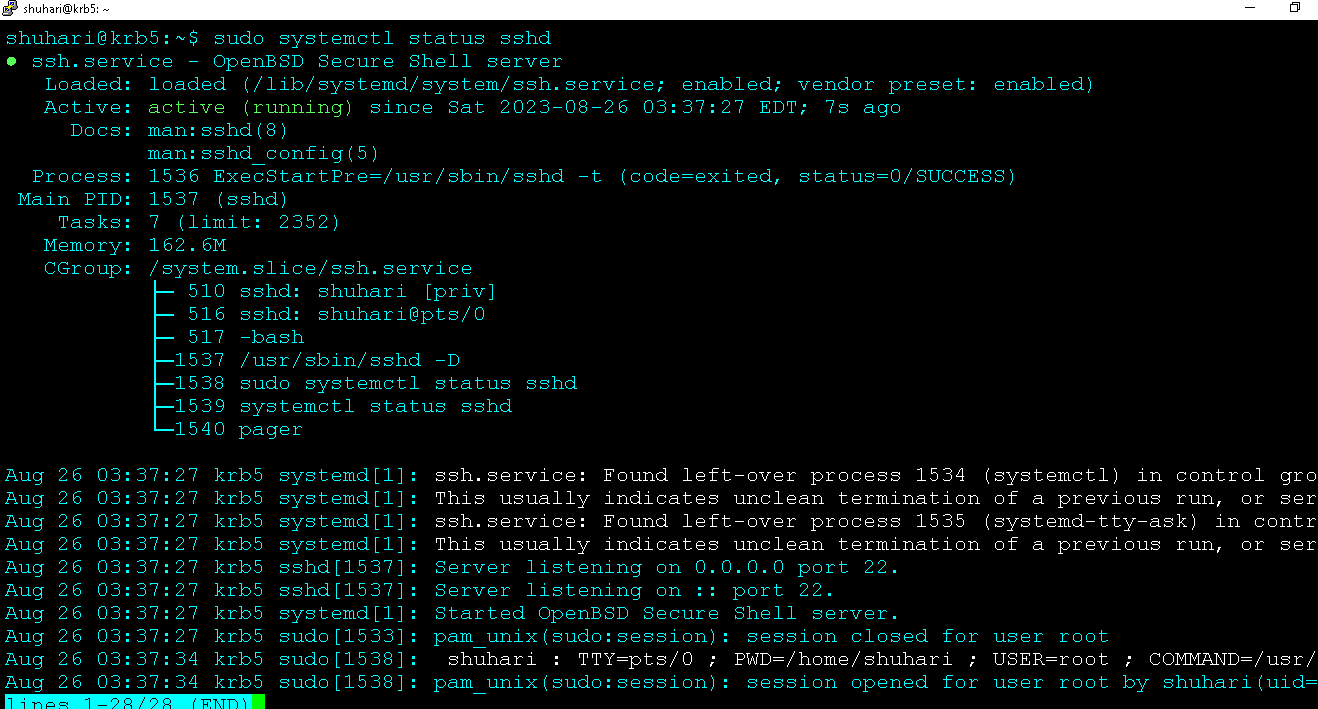
#### sudo nano /etc/ssh/sshd\_config

-> GSSAPIAuthentication yes



#### Restart sshd service-

* sudo systemctl restart sshd
* sudo systemctl status sshd



#### Setup ‘client.ac.com’ machine

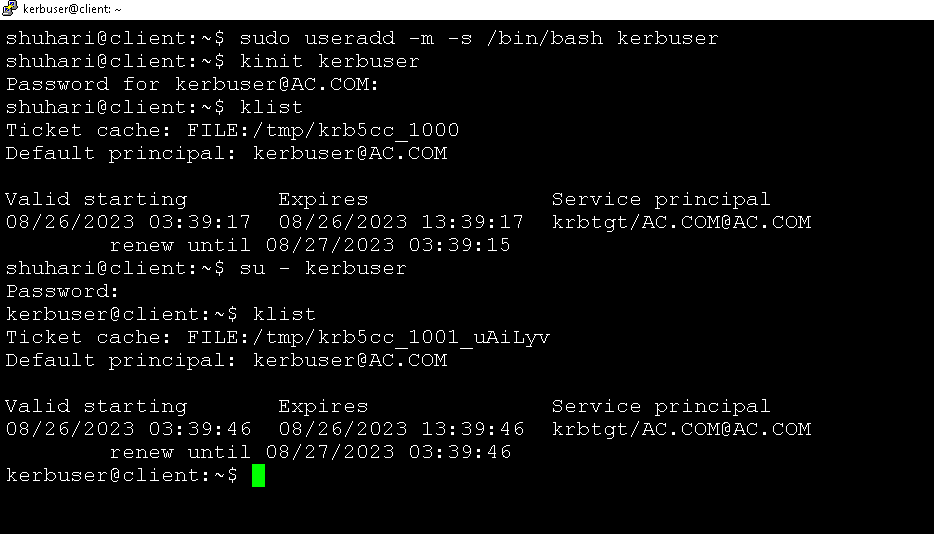
* + Add a new user to the client and login into it.
  + Initialize the user-principal
  + Then check the ticket list
* sudo useradd -m -s /bin/bash kerbuser
* kinit kerbuser
* klist

###### -Run kinit kerbuser:

1. Enter the password for the kerbuser principal.
2. If the password is correct and the Kerberos server approves, you'll receive a ticket.

###### -Run klist:

**Testing - SSH**



**Now connect the server ‘krb5.ac.com’ using SSH Kerberos authentication-**

**-** ssh krb5.ac.com

**Testing - SSH**

**Now connect the server ‘krb5.ac.com’ using SSH Kerberos authentication-**

**-** ssh krb5.ac.com



**Testing - SCP**

Now send files from client to server and server to the client using SCP Kerberos authentication.

- sudo scp test.txt [shuhari@192.168.80.100:/home/shu](mailto:shuhari@192.168.80.100:/home/shu)

