HACETTEPE UNIVERSITY
ENGINEERING DEPARTMENT
COMPUTER ENGINEERING

LESSON

BBM 465 INFORMATION SECURITY LAB.

ADVISOR

Yasin Şahin, Işıl Karabey

EXPERIMENT 4

KERBEROS

NAME : Hasan Hüseyin TOPÇU - 212228764

Taha BAŞKAK - 21228104

KERBEROS

Kerberos is a computer network authentication protocol that allows resources communicating over an unsecured network to communicate by proving their identity using ticket logic. [1] Targeting the Kerberos client-server model, it provides a feature that allows users and servers to authenticate each other and uses a symmetric encryption algorithm.

It was developed by MIT to protect the services of the "Athena Project" project, and only versions 1-3 use only MIT. However, the 4th and 5th versions that are still in use now are used in many places. For example ; Windows and Mac OS X. However, version 4 is not very preferred. The reason for this is that there are many open doors and weaknesses in the 4th edition.

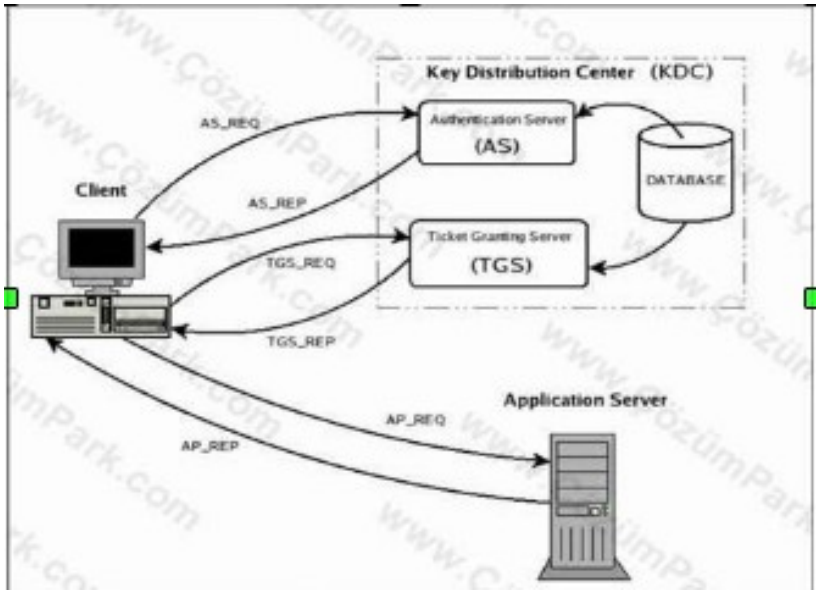
When we come to the content of Kerberos, it contains 3 substructures as the name implies. These;

- Key Distribution Center (KDC)
- Client
- Server

The KDC serves two different services. These services are generally "Authentication Service (AS)" and "Ticket Granting Service (TGS)", which authenticate the user and perform ticket stub service.

With Kerberos protocol, when a user wants to get service from a server for the first time, it goes through 3 basic services.

- Authentication Server (AS)
- Ticket granting Server (TGS)
- Ticket server connection service



When the user wants to connect to the server, they provide credentials to prove that they are the user of the KDC. The KDC checks the submitted information and directs it to the AS to approve and send the user to the TGT by hashing the user with the password without sending TGT (Ticket Granding Ticket) to the user. The user opens the encrypted TGT with the password. The handler then passes the authenticated TGT by the KDC and is required to get the ticket that will go to the server that he really wants to reach. Eline sends the last TGT back to the KDC. This time the KDC sends the TGT from the user to the TGS and the authenticated user arriving at the TGS sends the original ticket to connect to the server. The ticket passed to the user also connects to the server he wants to connect to.

Approve the ticket verified by the KDC, ie TGT, over time. The reason for this is that the TGT does not harm long-term usability when taken over by others. Time-stamp control should not be time-consuming for both the user and the server. In addition, after a certain period of time has elapsed (time out) TGT, the user is not noticed by the session manager renewed, the user provides the service from the server to continue.

Although Kerberos is preferred, there are many disadvantages. One-point crash; Kerberos requests persistent access to the server, and if server access is denied, new users are prevented from accessing it. The time constraint is due to the short duration of the kerberos ticket. This creates a situation where if the Kerberos server and the system time of the users are not set up, it will cause problems in the authentication process. There is a non-standardized administration protocol and these servers may differ. Attack with encryption; Kerberos can do both symmetric encryption and asymmetric encryption. In symmetric cryptography, the capture of this infrastructure may result in severe damage to the attacker by the fake ID because the authentication process is performed by the KDC.

EXPERIMENT PHASES

Server Side
realm = TAHA.KERBEROS.COM

Step 1 : The client and server times were synchronized using system setting on ubuntu and checked via “date” command.

Step 2 : ıfconfig
#Server's ip address is learned using this command and send to client for configuration to client's hosts file as seen as figure 1.

```
Paket listeleri okunuyor... Bitti
taha@taha-X555LB:/etc$ ifconfig -a
enp2s0    Link encap:Ethernet  HWaddr 1c:b7:2c:2f:55:96
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Sunucu
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1562 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1562 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:351850 (351.8 KB)  TX bytes:351850 (351.8 KB)

wlp3s0    Link encap:Ethernet  HWaddr 28:c2:dd:15:d7:ef
          inet addr:10.224.0.101  Bcast:10.224.255.255  Mask:255.255.0.0
          inet6 addr: fe80::2ac2:ddff:fe15:d7ef/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8024 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7558183 (7.5 MB)  TX bytes:1247309 (1.2 MB)
```

Figure 1

Step 3 : sudo service ufw stop
#firewall is closed as seen as figure 2.

Step 4 : ping 10.224.15.145
#ping client to test as seen as figure 2.

```
iptables v1.4.21: no command specified
Try `iptables -h' or 'iptables --help' for more information.
taha@taha-X555LB:/etc$ sudo service ufw stop
taha@taha-X555LB:/etc$ ping 10.244.15.145
PING 10.244.15.145 (10.244.15.145) 56(84) bytes of data.
^C
--- 10.244.15.145 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6048ms

taha@taha-X555LB:/etc$ ping 10.224.15.145
PING 10.224.15.145 (10.224.15.145) 56(84) bytes of data.
64 bytes from 10.224.15.145: icmp_seq=1 ttl=64 time=3.56 ms
64 bytes from 10.224.15.145: icmp_seq=2 ttl=64 time=12.7 ms
^C
--- 10.224.15.145 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 3.565/8.145/12.725/4.580 ms
taha@taha-X555LB:/etc$ sudo apt-get install krb5-kdc krb5-admin-server
```

Figure 2

Step 5 : sudo apt-get install krb5-kdc krb5-admin-server

#installed packages for server as seen as figure3

```
rtt min/avg/max/mdev = 3.503/8.145/12.723/4.580 ms
taha@taha-X555LB:/etc$ sudo apt-get install krb5-kdc krb5-admin-server
Paket listeleri okunuyor... Bitti
Bağımlılık ağacı oluşturuluyor
Durum bilgisi okunuyor... Bitti
Aşağıdaki ek paketler de kurulacak:
  libverto-libevent1 libverto1
Önerilen paketler:
  openbsd-inetd inet-superserver krb5-kdc-ldap
Aşağıdaki YENİ paketler kurulacak:
  krb5-admin-server krb5-kdc libverto-libevent1 libverto1
0 paket yükseltilecek, 4 yeni paket kurulacak, 0 paket kaldırılacak ve 3 paket yükseltilmeyecek.
0 B/270 kB arşiv dosyası indirilecek.
Bu işlem tamamlandıktan sonra 971 kB ek disk alanı kullanılacak.
Devam etmek istiyor musunuz? [E/h] e
Paketler önyapılandırılıyor ...
Daha önce seçili olmayan libverto1:amd64 paketi seçiliyor.
(Veritabanı okunuyor ... 212431 dosya veya dizin kurulu durumda.)
Paket açılacak: .../libverto1_0.2.4-1ubuntu2_amd64.deb ...
Paket açılıyor: libverto1:amd64 (0.2.4-1ubuntu2) ...
Daha önce seçili olmayan libverto-libevent1:amd64 paketi seçiliyor.
Paket açılacak: .../libverto-libevent1_0.2.4-1ubuntu2_amd64.deb ...
Paket açılıyor: libverto-libevent1:amd64 (0.2.4-1ubuntu2) ...
Daha önce seçili olmayan krb5-kdc paketi seçiliyor.
Paket açılacak: .../krb5-kdc_1.13.2+dfsg-2ubuntu0.1_amd64.deb ...
```

Figure 3

Step 6 : Configured "/etc/krb5.conf" file as following and send to client

krb5.conf file contents

```
[libdefaults]
        default_realm = TAHA.KERBEROS.COM

[realms]
        TAHA.KERBEROS.COM = {
                kdc = taha.kerberos.com
                admin_server = taha.kerberos.com
        }

[domain_realm]
        taha.kerberos.com = TAHA.KERBEROS.COM
        .taha.kerberos.com = TAHA.KERBEROS.COM
```

Step 7 : Configured "/etc/krb5kdc/kdc.conf" file as following and send to client

kdc.conf file contents

```
[kdcdefaults]
   kdc_ports = 750,88

[realms]
   TAHA.KERBEROS.COM = {
      database_name = /var/lib/krb5kdc/principal
      admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
      acl_file = /etc/krb5kdc/kadm5.acl
      key_stash_file = /etc/krb5kdc/stash
      kdc_ports = 750,88
      max_life = 10h 0m 0s
      max_renewable_life = 7d 0h 0m 0s
      master_key_type = des3-hmac-sha1
      supported_enctypes = aes256-cts:normal arcfour-hmac:normal des3-hmac-sha1:normal
des-cbc-crc:normal des:normal des:v4 des:norealm des:onlyrealm des:afs3
      default_principal_flags = +preauth
   }
```

Step 8 : Added this line in "/etc/krb5kdc/kadm5.acl" file

```
*/admin@TAHA.KERBEROS.COM *
```

Step 9 : krb5_newrealm
#Executed this command for creating the kerberos database as seen as figure 4

Step 10 : kadmin_local
#entered kadmin_local tool and runned following command on this interfeace as seen as figure 4.

```
addprincipal hasan   #added pricipal hasan so client
listprincs           #listed pricipals to check
q                    #quit or exit
```

Step 11 : service krb5-kdc restart
Step 12 : service krb5-admin-server restart
#restart kerberos service as seen as figure 4.

```
root@taha-X555LB:/etc# krb5_newrealm
This script should be run on the master KDC/admin server to initialize
a Kerberos realm.  It will ask you to type in a master key password.
This password will be used to generate a key that is stored in
/etc/krb5kdc/stash.  You should try to remember this password, but it
is much more important that it be a strong password than that it be
remembered.  However, if you lose the password and /etc/krb5kdc/stash,
you cannot decrypt your Kerberos database.
Loading random data
Initializing database '/var/lib/krb5kdc/principal' for realm 'TAHA.KERBEROS.COM',
master key name 'K/M@TAHA.KERBEROS.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:


Now that your realm is set up you may wish to create an administrative
```

```
Now that your realm is set up you may wish to create an administrative
principal using the addprinc subcommand of the kadmin.local program.
Then, this principal can be added to /etc/krb5kdc/kadm5.acl so that
you can use the kadmin program on other computers.  Kerberos admin
principals usually belong to a single user and end in /admin.  For
example, if jruser is a Kerberos administrator, then in addition to
the normal jruser principal, a jruser/admin principal should be
created.

Don't forget to set up DNS information so your clients can find your
KDC and admin servers.  Doing so is documented in the administration
guide.
root@taha-X555LB:/etc# kadmin.local
Authenticating as principal root/admin@TAHA.KERBEROS.COM with password.
kadmin.local:  addprinc hasan
WARNING: no policy specified for hasan@TAHA.KERBEROS.COM; defaulting to no policy
Enter password for principal "hasan@TAHA.KERBEROS.COM":
Re-enter password for principal "hasan@TAHA.KERBEROS.COM":
Principal "hasan@TAHA.KERBEROS.COM" created.
kadmin.local:  listprincs
K/M@TAHA.KERBEROS.COM
hasan@TAHA.KERBEROS.COM
kadmin/admin@TAHA.KERBEROS.COM
kadmin/changepw@TAHA.KERBEROS.COM
kadmin/taha-x555lb@TAHA.KERBEROS.COM
kiprop/taha-x555lb@TAHA.KERBEROS.COM
krbtgt/TAHA.KERBEROS.COM@TAHA.KERBEROS.COM
kadmin.local:  q
root@taha-X555LB:/etc# service krb5-kdc restart
root@taha-X555LB:/etc# service krb5-kadmin-server restart
Failed to restart krb5-kadmin-server.service: Unit krb5-kadmin-server.service failed to load: No such file or directory.
root@taha-X555LB:/etc# service krb5-admin-server restart
root@taha-X555LB:/etc# cp krb5.conf /home/taha/MasaÜstÜ/
```

Figure 4

Client Side
principal = hasan@TAHA.KERBEROS.COM

Step 1 : The client and server times were synchronized using system setting on ubuntu and checked via “date” command.

Step 2 : The following line has been added to the “/etc/hosts” file as seen as figure 1.

10.224.0.101 taha.kerberos.com

Step 3 : ping taha.kerberos.com
#pinged to taha.kerberos.com to check connection as seen as figure 1.

Step 4 : sudo service ufw stop
#firewall is closed

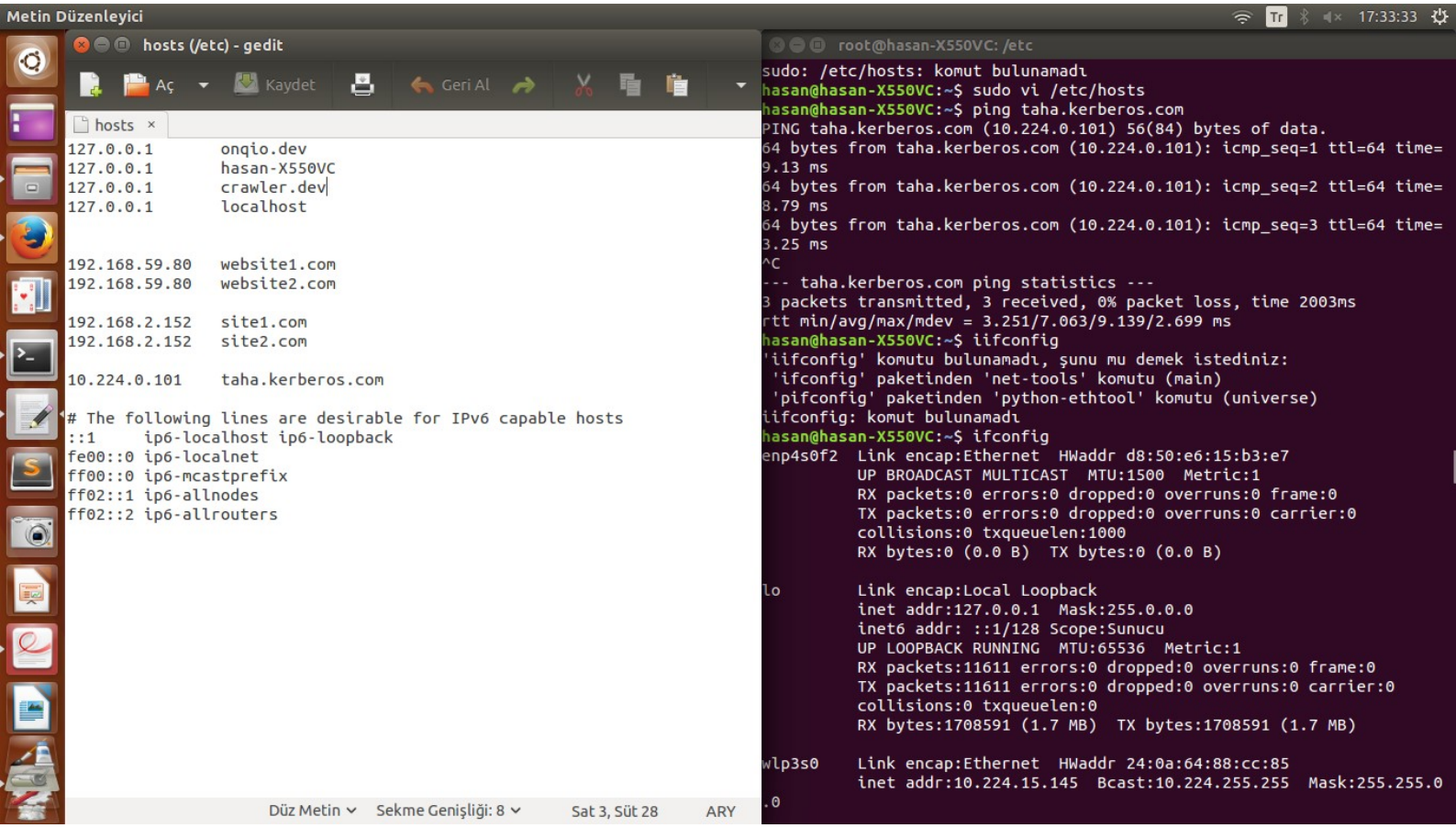


Figure 1

Step 5 : sudo apt-get install krb5-user
##installed packages for client as seen as figure 2.

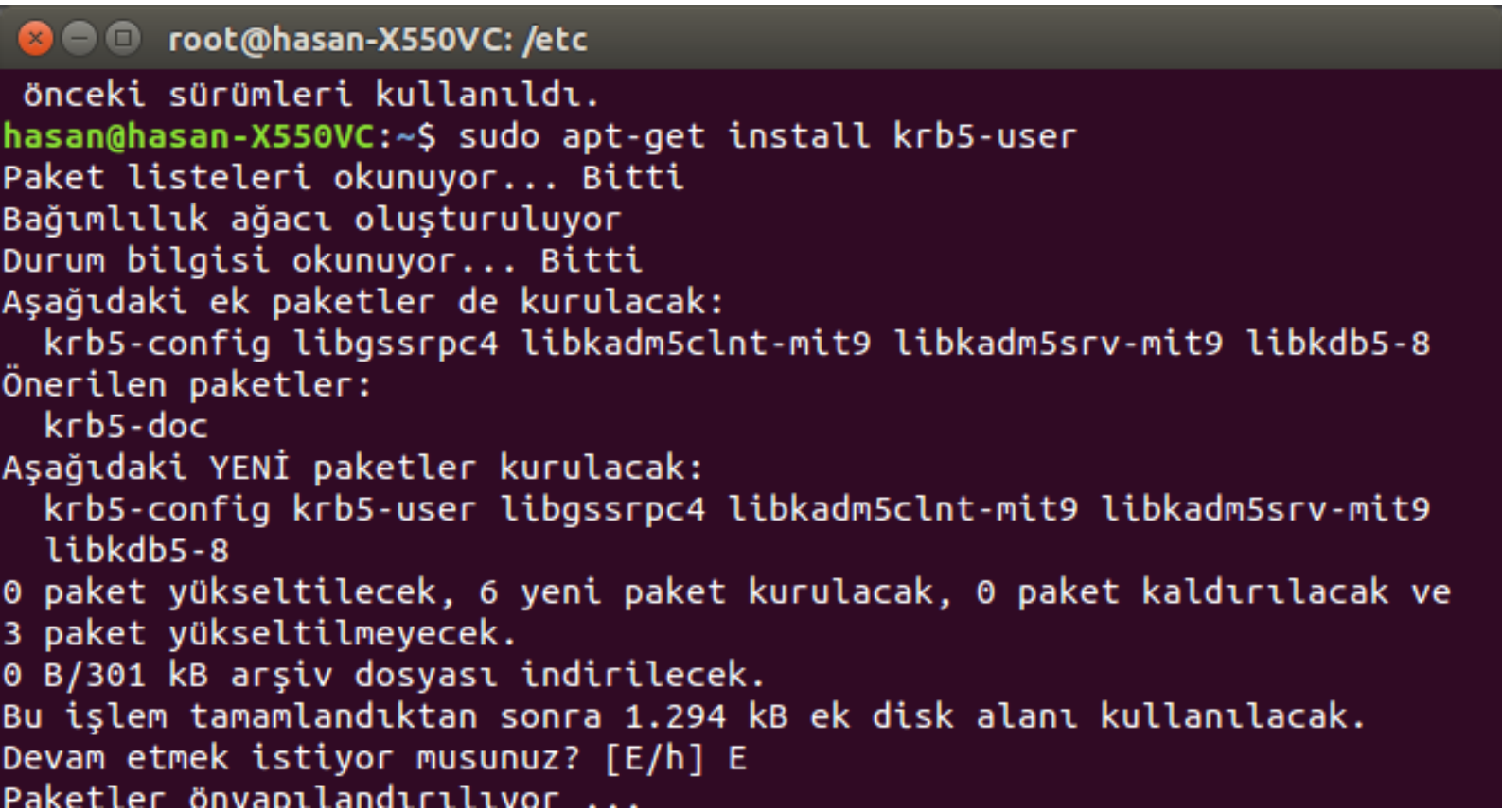


Figure 2

Step 6 : Copied krb5.conf file that taken from server to under "/etc/" folder.

Step 7 : kinit hasan #request a Ticket-Granting Ticket (TGT) as seen as figure 3.
klist #listed the TGT as seen as figure 3.

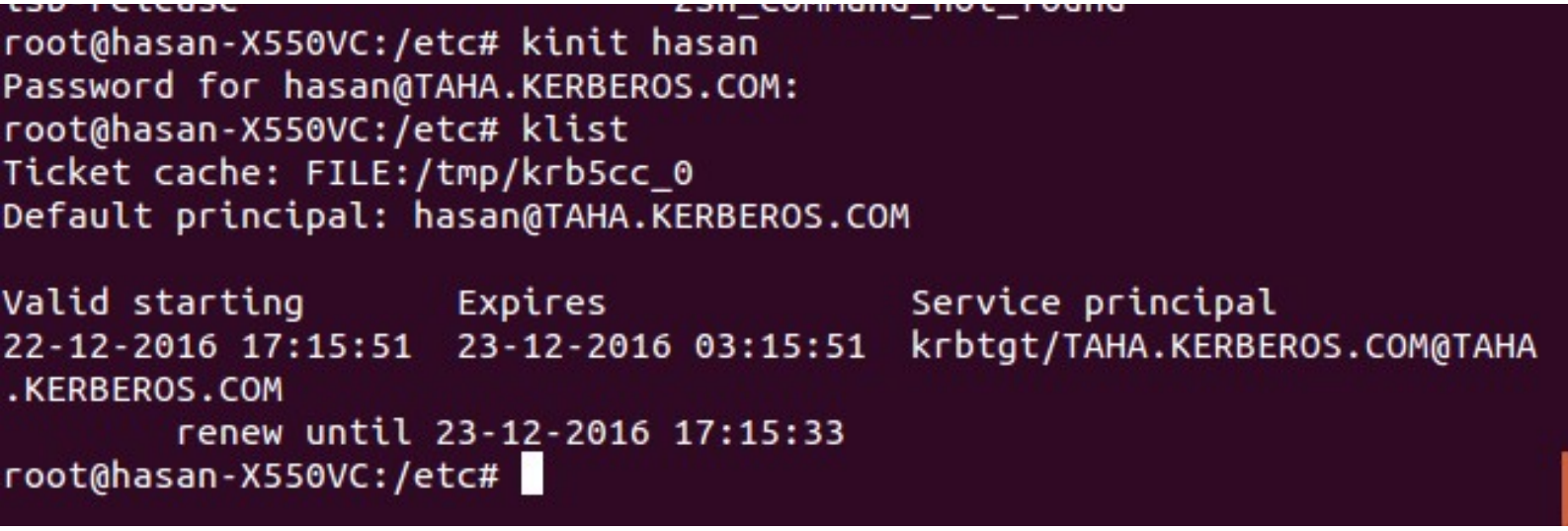


Figure 3

Note : We get an error when trying to connect with ssh.We could do this homework so far.

REFERENCES

[1] **https://tr.wikipedia.org/wiki/Kerberos_(ileti%C5%9Fim_kural%C4%B1**)
http://www.mshowto.org/kerberos-protokolu-nedir-temel-isleyisi-nasildir.html
https://tr.wikipedia.org/wiki/Kerberos_(iletişim_kuralı)
http://www.belgeler.org/howto/kerberos-howto-overview.html
http://www.cozumpark.com/blogs/gvenlik/archive/2010/08/16/bilgi-g-venli-i-ve-genel-g-venlik-kavramlar-b-l-m-1.aspx
http://blog.manula.org/2012/04/setting-up-kerberos-server-with-debian.html
http://www.alittletooquiet.net/text/kerberos-on-ubuntu.html
https://help.ubuntu.com/community/Kerberos
http://www.kerberos.org/software/adminkerberos.pdf