

## گزارش سوم

### تفاوت بین احراز هویت کربروس و احراز هویت مبتنی بر پسورد

در سیستم های سنتی احراز هویت، تنها با وارد کردن پسورد، کاربر به سیستم دسترسی پیدا می کرد. چالش این نوع احراز هویت، از این نظر بود که اگر هکر به پسورد دسترسی پیدا می کرد، هویت کاربر را بدست آورده و می توانست از آن طریق به اکانت شخص و یا شبکه آن سازمان متصل شود. بنابراین باید سیستمی فراهم می شد که از بدست آوردن پسورد کاربران توسط هکرها در یک شبکه ناامن جلوگیری شود و کاربران بتوانند از طریق این سیستم در هر زمانی و برای هر سرویسی احراز هویت شوند. می توان این کار را با استفاده از کربروس انجام داد.

### سیستم کربروس و دستورات آن در خط فرمان

فرض می کنیم کلاینت می خواهد به یک فایل سرور متصل شود. در کربروس کلاینت باید ابتدا از طریق شخص ثالث مورد اعتماد تصدیق اصالت شود که در این سیستم ای شخص ثالث همان KDC می باشد. KDC خود شامل ، Authentication Server(AS) و Ticket Granting Server(TGS) می شود. در قدم اول کلاینت درخواست تیکت خود را برای AS ارسال می کند و این درخواست را از طریق پسورد خود رمز می کند و پسورد خود را به صورت فاش شده در یک شبکه ناامن ارسال نمی کند و از آن به عنوان کلید رمزنگاری استفاده می کند. وقتی AS درخواست کلاینت را دریافت می کند براساس ID کاربر پسورد او را از دیتابیس استخراج می کند و با استفاده از آن پیام را رمزگشایی می کند و اینگونه کاربر راستی آزمایی می شود. پس از این مرحله AS یک تیکت به نام TGT برای کاربر ارسال می کند که با یک کلید مخفی دیگر رمز شده است. وقتی کلاینت TGT را دریافت می کند آن را به همراه درخواستش برای دسترسی به فایل سرور به TGS ارسال می کند. هنگامی که TGS آن را دریافت می کند از طریق کلید مخفی اشتراکی اش با AS آن را رمزگشایی می کند و سپس برای کلاینت یک توکن ارسال می کند که با کلید مخفی مشترک بین TGS و فایل سرور رمز شده است. سپس کلاینت این توکن را برای فایل سرور می فرستد و فایل سرور با کلید مخفی مشترکش با TGS آن را رمزگشایی کرده و در بازه زمانی مشخصی به کلاینت اجازه استفاده از منابعش را می دهد.

KINIT : این دستور برای کلاینت از KDC با استفاده از پسوردش TGT ارسال می کند و اجازه استفاده از سرویس های فایل سرویس را می دهد.

KDESTROY : همه تیکت های موجود در ماشین را پاک می کند.

KLIST : تیکت های روی ماشین را لیست می کند.

KPASSWD : پسورد را آپدیت می کند.

KADMIN : برای مدیریت (حذف، ایجاد، آپدیت principle) دیتابیزی که اطلاعات principle ها را ذخیره می کند و مدیریت قلمرو استفاده می شود.

KERBEROS/ADMIN : یک principle خاص است که کلاینت از آن برای احراز هویت خودش به KDC استفاده می کند.

KDB5\_UTIL : برای مدیریت دیتابیس به کار می رود.

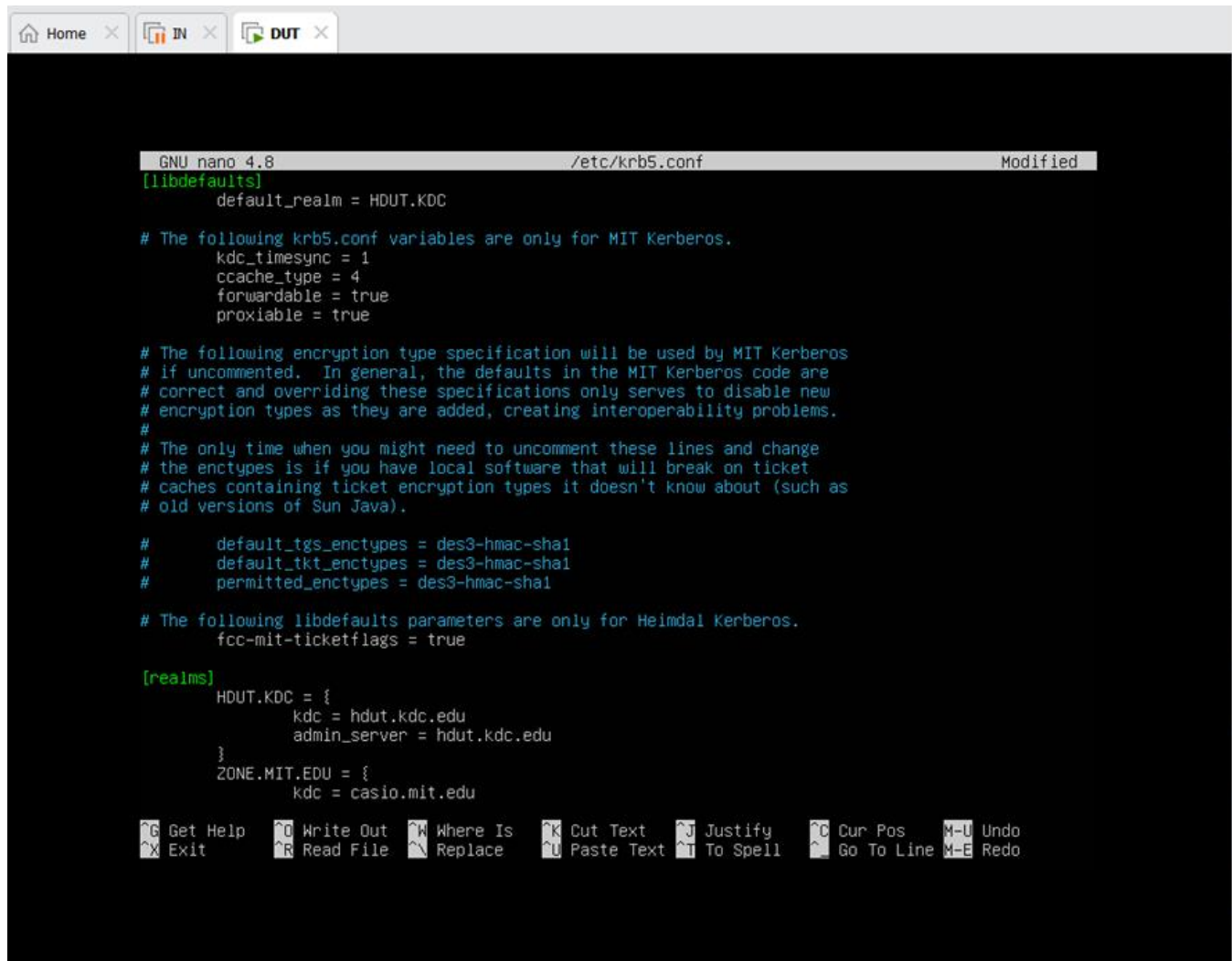
KRB\$CONFIGURE : برای ست آپ و کانفیگ های اولیه برای ایجاد قلمرو در کربروس استفاده می شود.

### ایجاد قلمرو در کربروس

در این سناریو ماشین in سرور در نظر گرفته شده و ماشین out، کلاینت و ماشین dut، نیز KDC می باشد. به منظور کانفیگ dut دستور زیر را وارد کرده.

```
homa@dut:~$ sudo nano /etc/krb5.conf
```

و نام قلمرو و دامنه را مطابق تصویر زیر تعریف می کنیم و با استفاده از دستور زیر در فایل etc/hosts ، ip ماشین را برای این دامنه تعریف می کنیم.



```
GNU nano 4.8 /etc/krb5.conf Modified
[libdefaults]
    default_realm = HDUT.KDC

# The following krb5.conf variables are only for MIT Kerberos.
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented. In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypees is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

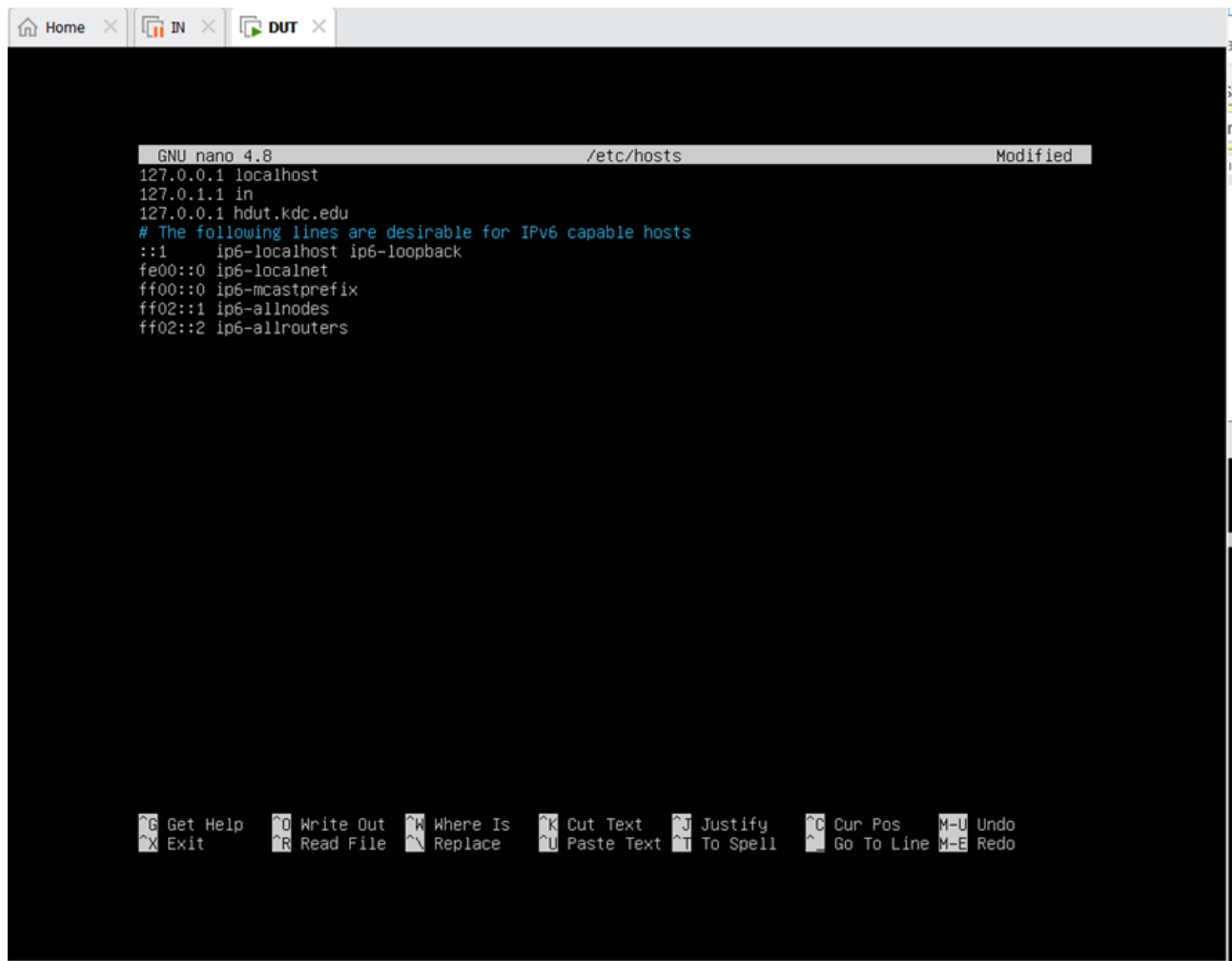
#     default_tgs_enctypes = des3-hmac-sha1
#     default_tkt_enctypes = des3-hmac-sha1
#     permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
    fcc-mit-ticketflags = true

[realms]
    HDUT.KDC = {
        kdc = hdut.kdc.edu
        admin_server = hdut.kdc.edu
    }
    ZONE.MIT.EDU = {
        kdc = casio.mit.edu
    }

^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line  M-E Redo
```

```
homa@dut:~$
homa@dut:~$ sudo nano /etc/hosts
```

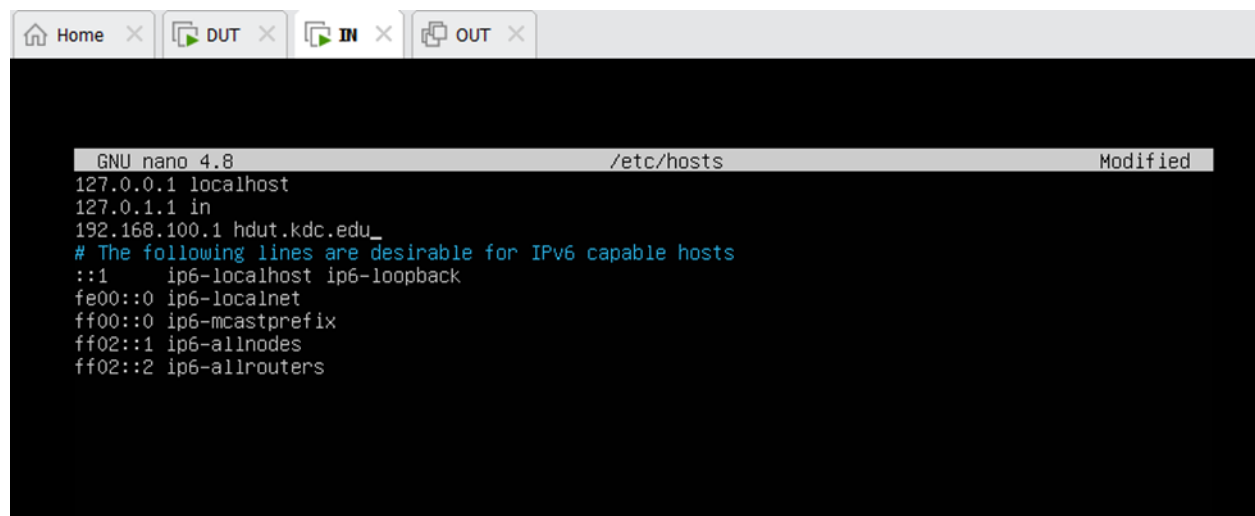


The screenshot shows a terminal window with three tabs: 'Home', 'IN', and 'DUT'. The 'DUT' tab is active, displaying the contents of the `/etc/hosts` file using the GNU nano 4.8 editor. The file contains the following text:

```
GNU nano 4.8 /etc/hosts Modified
127.0.0.1 localhost
127.0.1.1 in
127.0.0.1 hdut.kdc.edu
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

At the bottom of the terminal, a status bar lists various keyboard shortcuts for the nano editor, such as `^G Get Help`, `^O Write Out`, `^W Where Is`, `^K Cut Text`, `^J Justify`, `^C Cur Pos`, `M-U Undo`, `^X Exit`, `^R Read File`, `^_ Replace`, `^U Paste Text`, `^T To Spell`, `^_ Go To Line`, and `M-E Redo`.

مشابه کانفیگ های بالا برای ماشین های in و out نیز انجام می دهیم.



The screenshot shows a terminal window with four tabs: 'Home', 'DUT', 'IN', and 'OUT'. The 'IN' tab is active, displaying the contents of the `/etc/hosts` file using the GNU nano 4.8 editor. The file contains the following text:

```
GNU nano 4.8 /etc/hosts Modified
127.0.0.1 localhost
127.0.1.1 in
192.168.100.1 hdut.kdc.edu_
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

The file is identical to the one in the first screenshot, but with the addition of the line `192.168.100.1 hdut.kdc.edu_`.

```
Home x DUT x IN x
GNU nano 4.8 /etc/krb5.conf Modified
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented. In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctype is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

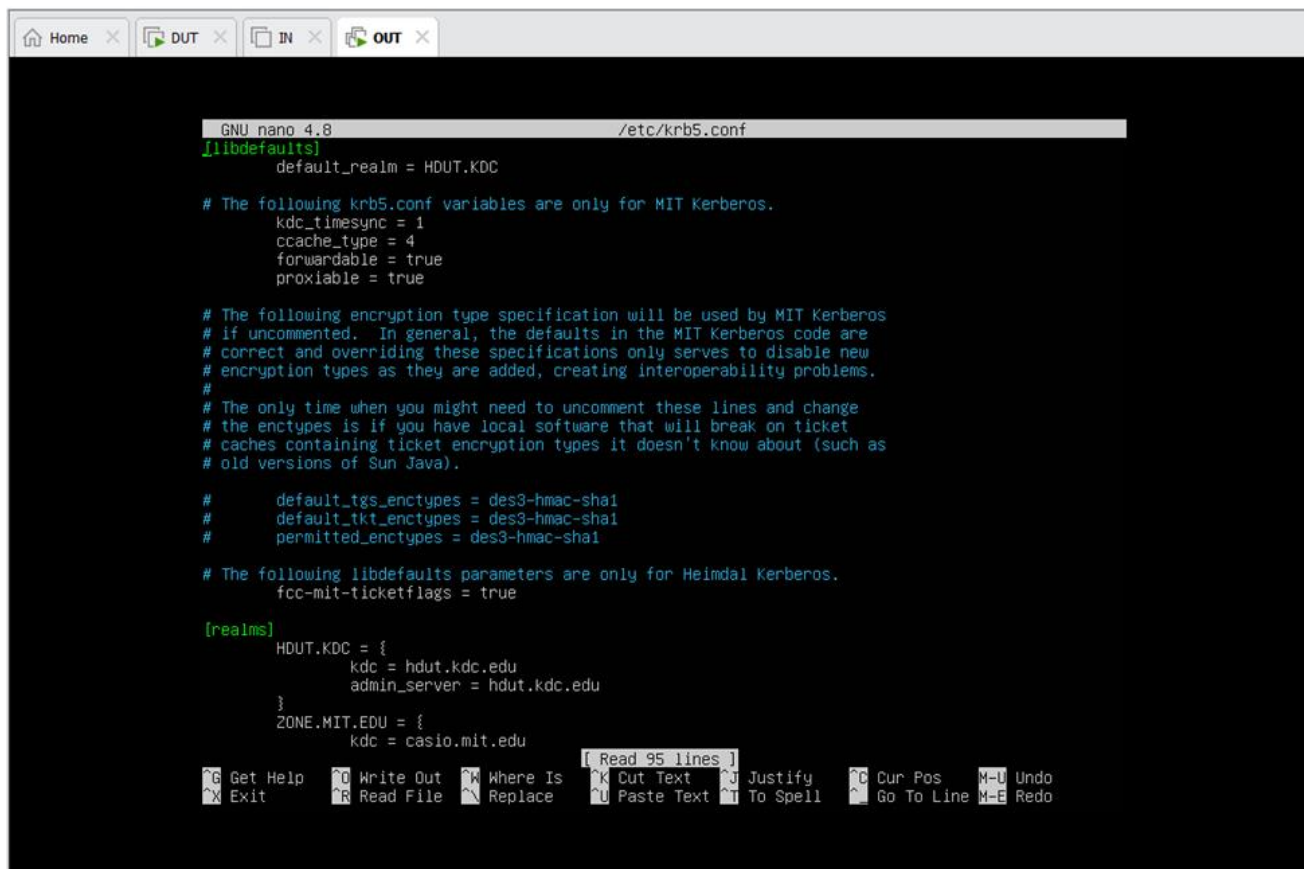
#     default_tgs_enctypes = des3-hmac-sha1
#     default_tkt_enctypes = des3-hmac-sha1
#     permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
    fcc-mit-ticketflags = true

[realms]
    HDUT.KDC = {
        kdc = hdut.kdc.edu
        admin_server = hdut.kdc.edu
    }
    ZONE.MIT.EDU = {
        kdc = casio.mit.edu
        kdc = seiko.mit.edu
        admin_server = casio.mit.edu
    }
    CSAIL.MIT.EDU = {

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo
^X Exit      ^R Read File  ^N Replace   ^U Paste Text ^T To Spell  ^_ Go To Line M-E Redo
```

```
Home x DUT x IN x OUT x
GNU nano 4.8 /etc/hosts
127.0.0.1 localhost
127.0.1.1 in
192.168.100.1 hdut.kdc.edu
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```



```
GNU nano 4.8 /etc/krb5.conf
[libdefaults]
    default_realm = HDUT.KDC

# The following krb5.conf variables are only for MIT Kerberos.
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented. In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctype is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).
#
    default_tgs_enctypes = des3-hmac-sha1
    default_tkt_enctypes = des3-hmac-sha1
    permitted_enctypes = des3-hmac-sha1

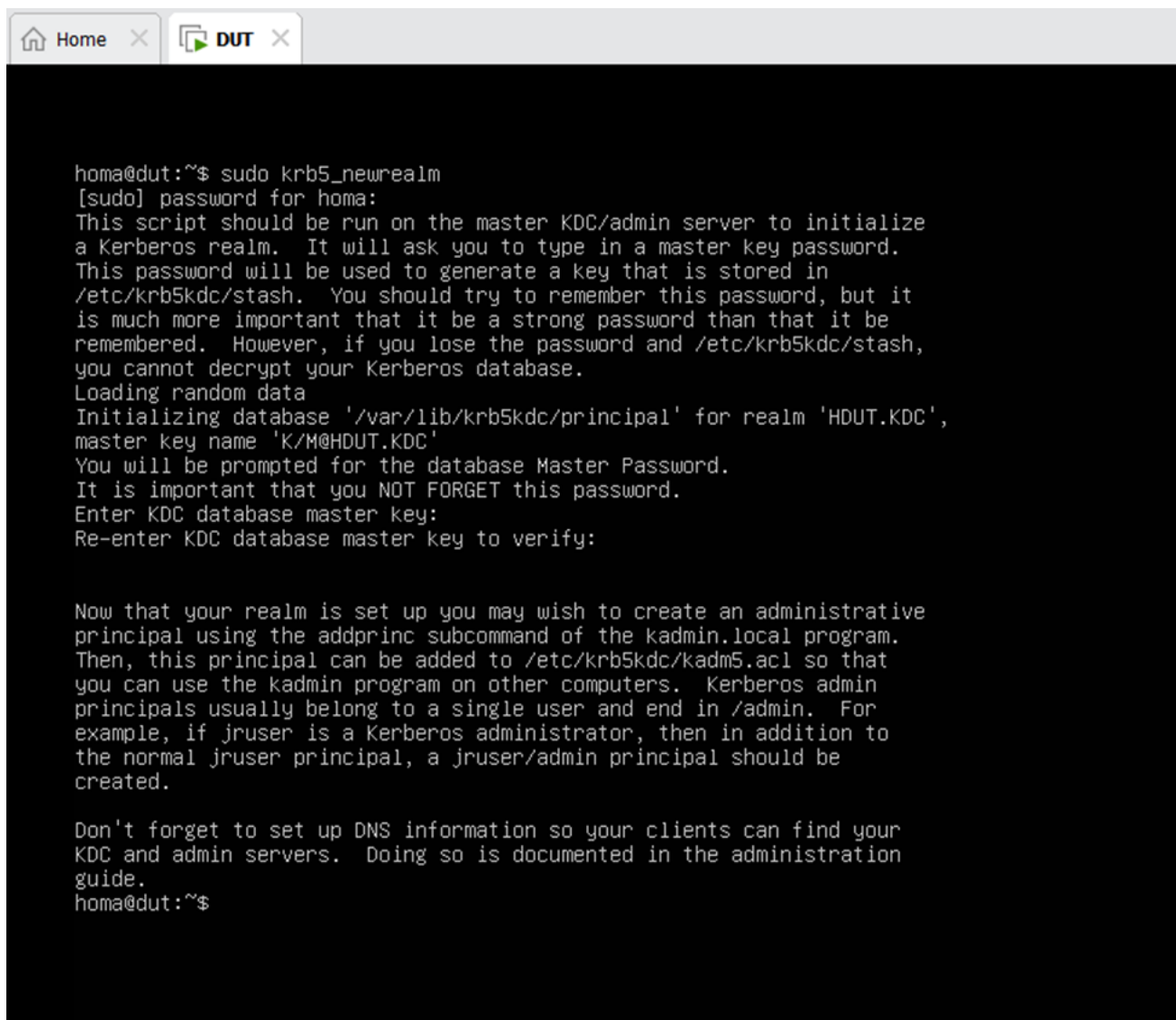
# The following libdefaults parameters are only for Heimdal Kerberos.
    fcc-mit-ticketflags = true

[realms]
    HDUT.KDC = {
        kdc = hdut.kdc.edu
        admin_server = hdut.kdc.edu
    }
    ZONE.MIT.EDU = {
        kdc = casio.mit.edu
    }
```

## راه اندازی پایگاه داده برای قلمرو

با استفاده از دستور `krb5_newrealm` در ماشین `dut` برای قلمرو ایجاد شده یک دیتابیس می سازیم.

(بررسی درستی KDC با استفاده از KINIT با ایجاد تیکت نیز انجام می شود)



The image shows a terminal window with a title bar containing 'Home' and 'DUT' tabs. The terminal output shows the execution of the `sudo krb5_newrealm` command. It prompts for a password, then displays instructions for setting up a Kerberos realm. The script generates a master key and prompts for a master password, which is then verified. Finally, it provides instructions on how to create an administrative principal and set up DNS information.

```
homa@dut:~$ sudo krb5_newrealm
[sudo] password for homa:
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 'HDUT.KDC',
master key name 'K/M@HDUT.KDC'
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
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.
homa@dut:~$
```

با استفاده از دستورات زیر درستی عملکرد KDC و Admin Server را بررسی می کنیم.

```
homa@dut:~$ systemctl status krb5-kdc
• krb5-kdc.service - Kerberos 5 Key Distribution Center
   Loaded: loaded (/lib/systemd/system/krb5-kdc.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2024-04-21 20:41:35 UTC; 3min 35s ago
     Process: 4192 ExecStart=/usr/sbin/krb5kdc -P /var/run/krb5-kdc.pid $DAEMON_ARGS (code=exited, status=0/SUCCESS)
    Main PID: 4207 (krb5kdc)
      Tasks: 1 (limit: 4557)
     Memory: 1.7M
    CGroup: /system.slice/krb5-kdc.service
            └─4207 /usr/sbin/krb5kdc -P /var/run/krb5-kdc.pid

Apr 21 20:41:35 dut krb5kdc[4192]: Setting pktinfo on socket 0.0.0.0.88
Apr 21 20:41:35 dut krb5kdc[4192]: Setting up UDP socket for address ::.88
Apr 21 20:41:35 dut krb5kdc[4192]: setsockopt(12,IPV6_V6ONLY,1) worked
Apr 21 20:41:35 dut krb5kdc[4192]: Setting pktinfo on socket ::.88
Apr 21 20:41:35 dut krb5kdc[4192]: Setting up TCP socket for address 0.0.0.0.88
Apr 21 20:41:35 dut krb5kdc[4192]: Setting up TCP socket for address ::.88
Apr 21 20:41:35 dut krb5kdc[4192]: setsockopt(14,IPV6_V6ONLY,1) worked
Apr 21 20:41:35 dut krb5kdc[4192]: set up 6 sockets
Apr 21 20:41:35 dut krb5kdc[4207]: commencing operation
Apr 21 20:41:35 dut systemd[1]: Started Kerberos 5 Key Distribution Center.
lines 1-20/20 (END)
```

```
homa@dut:~$ systemctl status krb5-admin-server
• krb5-admin-server.service - Kerberos 5 Admin Server
   Loaded: loaded (/lib/systemd/system/krb5-admin-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2024-04-21 20:41:36 UTC; 2min 28s ago
     Main PID: 4218 (kadmind)
      Tasks: 1 (limit: 4557)
     Memory: 1.0M
    CGroup: /system.slice/krb5-admin-server.service
            └─4218 /usr/sbin/kadmind -nofork

Apr 21 20:41:36 dut kadmind[4218]: Setting up TCP socket for address 0.0.0.0.464
Apr 21 20:41:36 dut kadmind[4218]: Setting up TCP socket for address ::.464
Apr 21 20:41:36 dut kadmind[4218]: setsockopt(12,IPV6_V6ONLY,1) worked
Apr 21 20:41:36 dut kadmind[4218]: Setting up RPC socket for address 0.0.0.0.749
Apr 21 20:41:36 dut kadmind[4218]: Setting up RPC socket for address ::.749
Apr 21 20:41:36 dut kadmind[4218]: setsockopt(14,IPV6_V6ONLY,1) worked
Apr 21 20:41:36 dut kadmind[4218]: set up 6 sockets
Apr 21 20:41:36 dut kadmind[4218]: Seeding random number generator
Apr 21 20:41:36 dut kadmind[4218]: kadmind: starting...
Apr 21 20:41:36 dut kadmind[4218]: starting
```



## ایجاد principle در کربروس

توسط دستورات زیر ماشین های in و out در ماشین dut، principle عنوان می شوند.

```
homa@dut:~$ sudo kadmin.local
Authenticating as principal root/admin@HDUT.KDC with password.
kadmin.local: addprinc in@HDUT.KDC
WARNING: no policy specified for in@HDUT.KDC; defaulting to no policy
Enter password for principal "in@HDUT.KDC":
Re-enter password for principal "in@HDUT.KDC":
add_principal: Principal or policy already exists while creating "in@HDUT.KDC".
kadmin.local: addprinc out@HDUT.KDC
WARNING: no policy specified for out@HDUT.KDC; defaulting to no policy
Enter password for principal "out@HDUT.KDC":
Re-enter password for principal "out@HDUT.KDC":
add_principal: Principal or policy already exists while creating "out@HDUT.KDC".
kadmin.local:
```

سپس در ماشین dut برای اینکه admin principal قابلیت مدیریت دیتابیس را داشته باشد از دستور زیر استفاده می کنیم و فایل را ویرایش می کنیم.

```
homa@dut:~$ sudo nano /etc/krb5kdc/kadm5.acl_
```

```
GNU nano 4.8 /etc/krb5kdc/kadm5.acl Modified
# This file is the access control list for krb5 administration.
# When this file is edited run service krb5-admin-server restart to activate
# One common way to set up Kerberos administration is to allow any principal
# ending in /admin is given full administrative rights.
# To enable this, uncomment the following line:
*/admin *

[ Read 6 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos   M-U Undo
^X Exit      ^R Read File ^_ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line M-E Redo
```

با استفاده از دستورات زیر سرویس کربروس را ری استارت می کنیم.

```
homa@dut:~$ sudo systemctl restart krb5-kdc krb5-admin-server
homa@dut:~$ sudo systemctl enable krb5-kdc krb5-admin-server
Synchronizing state of krb5-kdc.service with SysV service script with /lib/systemd/systemd-sysv-inst
all.
Executing: /lib/systemd/systemd-sysv-install enable krb5-kdc
[ 6921.884606] blk_update_request: I/O error, dev fd0, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 p
rio class 0
[ 6923.064858] blk_update_request: I/O error, dev fd0, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 p
rio class 0
Synchronizing state of krb5-admin-server.service with SysV service script with /lib/systemd/systemd-
sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable krb5-admin-server
[ 6923.600776] blk_update_request: I/O error, dev fd0, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 p
rio class 0
[ 6924.072691] blk_update_request: I/O error, dev fd0, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 p
rio class 0
[ 6924.516689] blk_update_request: I/O error, dev fd0, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 p
rio class 0
homa@dut:~$
```

## ایجاد تیکت

با استفاده از دستورات زیر تیکت را ایجاد کرده و آن را مشاه هده می کنیم.

```
homa@out:~$ kinit out
Password for out@HDUT.KDC:
homa@out:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: out@HDUT.KDC

Valid starting      Expires            Service principal
04/22/2024 14:51:38  04/23/2024 14:51:38  krbtgt/HDUT.KDC@HDUT.KDC
homa@out:~$
```