Université Sultan Moulay Slimane
Ecole National des Sciences Appliquées
KHOURIBGA

Ingénierie des Réseaux Intelligents et de la Cybersécurité {IRIC}

KERBEROS LAB

Prepared by :

Rharif Anass

Supervised by:

Mr.MALEH Yassine

Année universitaire : 2021/202

In this lab, we will show you how to set up Kerberos authentication between two Ubuntu servers. We will install and configure the Kerberos server on the Ubuntu server and then install the Kerberos client on the other. Finally, we will test the authentication of the SSH service with the Kerberos server.

What we will do?

- *Setup FQDN File*
- *Install KDC Kerberos Server*
- *Configure KDC Kerberos Server*
- *Install and Configure Kerberos Client*
- *Testing*

How to install and configure Kerberos Server/Client

Step 0 - Clock synchronization between machines:

How to Set or Change the Time Zone in Linux

- **Checking** the **Current** Time Zone: using one of this commands:
  - **timedatectl**

```
                      Local time: Tue 2019-12-03 16:30:44 UTC
                  Universal time: Tue 2019-12-03 16:30:44 UTC
                        RTC time: Tue 2019-12-03 16:30:44
                       Time zone: Etc/UTC (UTC, +0000)
       System clock synchronized: no
systemd-timesyncd.service active: yes
                 RTC in local TZ: no
```

  - **ls -l /etc/localtime**

```
lrwxrwxrwx 1 root root 27 Dec  3 16:29 /etc/localtime -> /usr/share/zoneinfo/Etc/UTC
```

- **Changing** the Time Zone:

Before changing the time zone, you'll need to find out the long name of the time zone you want to useby typing the command: `timedatectl list-timezones`.
The time zone naming convention usually uses a "Region/City" format:

```
...
America/Montserrat
America/Nassau
America/New_York
America/Nipigon
America/Nome
America/Noronha
...
```

Once you identify which time zone is accurate to your location, run the following command as **root** or **sudo user**:

```
sudo timedatectl set-timezone <your_time_zone>
```

The objective of this is to synchronize the time between the server and the client machine:

Step 1 - Setup FQDN in kerberos server and client.

First of all, we must configure the FQDN(Fully Qualified Domain Name) on the Kerberos server and then edit the '**/etc/hosts**' file of the server.
Change the FQDN of the Kerberos server using the following command.

```
hostnamectl set-hostname krb5.anass.io
```

After that, edit the '/etc/hosts' file using vim editor:

```
vim /etc/hosts
```

Change the IP address and FQDN with your own and paste into it:

```
10.10.10.15     krb5.anass.io   krb5
```

Save and close.
Now test using the 'ping' command below and make sure the FQDN is resolved to the right IP address.

```
ping -c 3 $(hostname -f)
```

Step 2 - Install KDC Kerberos Server:

Now we're going to install the Kerberos server on the '**krb5**' server with IP address '10.10.10.15' and the FQDN is 'krb5.anass.io'.

Install Kerberos server using the following apt command:

```
sudo apt install krb5-kdc krb5-admin-server krb5-config -y
```

During the installation, you will be asked about the Kerberos Realm, the Kerberos server of the Realm, and the Admin server.

By default, the Kerberos will use the Kerberos server domain name as a REALM, '**ANASS.IO**'.
The Kerberos server is '**krb5.anass.io**'.
And the Admin server same as the Kerberos server '**krb5.anass.io**'.

Once the installation is finished, you will be shown the **Kerberos service is failed to run**.
It's fine because we will configure on the next stage.

Step 3 - Configure KDC Kerberos Server:

Now generate a new strong master password for the Kerberos REALM using the following command:

```
sudo krb5_newrealm
```

Type your strong password and the REALM password will be generated at the '**/etc/krb5kdc/stash**' file.
After that, we need to **create the admin user** (admin principal) for the KDC Kerberos server, add the Kerberos server hostname to the database, and then create the keytab for the Kerberos server.
Run the '**kadmin.local**' command-line interface for Kerberos administration command below:

```
sudo kadmin.local
```

Create a new admin user principal called 'root'

```
addprinc root/admin
```

Type the strong password for the 'root' admin principal.
Add the KDC Kerberos server to the database and create the keytab file for the KDC host.

```
addprinc -randkey host/krb5.anass.io
ktadd host/krb5.anass.io
```

Then close the 'kadmin.local' utility

```
quit
```

Next, we need to add the 'root' admin principle to the **access control list** by editing the '**/etc/krb5kdc/kadm5.acl**' file.

```
vim /etc/krb5kdc/kadm5.acl
```

Add the following configuration:

```
root/admin *
```

Save and close the configuration, then restart the Kerberos service.

```
sudo systemctl restart krb5-admin-server.service
```

And the configuration of KDC Kerberos server has been completed.

Step 4 - Install and Configure Kerberos Client:

In this step, we're going to install the Kerberos client on Ubuntu server with IP address '10.10.10.16' and the hostname 'client1'.

- Configure FQDN:

Configure the FQDN on the client machine using the following command:

```
hostnamectl set-hostname client1.anass.io
```

After that, edit the '**/etc/hosts**' file using vim editor.

```
vim /etc/hosts
```

Paste both KDC Kerberos server and the client as below.

```
10.10.10.15     krb5.anass.io   krb5
10.10.10.16     client1.anass.io    client1
```

Save and close.

- Install Kerberos Client:

Install Kerberos client packages by running the following apt command.

```
sudo apt install -y krb5-user libpam-krb5 libpam-ccreds auth-client-c
onfig
```

During the installation, you will be asked about the Kerberos Realm, the Kerberos server of the Realm, and the Admin server.

By default, Kerberos will use the Kerberos server domain name as a REALM, '**ANASS.IO**'.
The Kerberos server is '**krb5.anass.io**'.
And the Admin server same as the Kerberos server '**krb5.anass.io**'.
And the installation for Kerberos client is finished.

- Configure Kerberos Client:

From the client machine, connect to the KDC Kerberos server using the 'kadmin' command.

```
kadmin
```

And you will be asked for the password of 'root/admin' principle. Type the password and you will be logged in to the KDC Kerberos administration system.
Now add the client FQDN 'client1.anass.io' to the Kerberos database and add the keytab file for the client:

```
addprinc -randkey host/client1.anass.io
ktadd host/client1.anass.io
```

Then close the kadmin Kerberos Administration interface.

```
quit
```

And the configuration of Kerberos client is completed.

Step 5 – Testing:

For this testing purpose, we're going to configure the SSH authentication using the Kerberos. The client machine 'client1.anass.io' will connect to the server 'krb5.anass.io' through SSH with the Kerberos authentication.

- Setup 'krb5.anass.io' Server

Create a new system user called 'rania'.

```
useradd -m -s /bin/bash rania
```

Login to the KDC Kerberos administration and add a new principal user called 'rania'.

```
kadmin.local
addprinc rania
```

Close the Kerberos Administration interface and edit the ssh configuration '**/etc/ssh/sshd_config**'.

```
vim /etc/ssh/sshd_config
```

Uncomment the 'GSSAPIAuthentication' and enable it by changing the value to ''.

```
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
```

Save and close the configuration, **then restart the ssh service**.

```
systemctl restart sshd
```

- Setup 'client1.anass.io' Machine

Add new system user 'rania' on the client machine and login into it.

```
useradd -m -s /bin/bash rania
su - rania
```

After that, initialize the Kerberos user principal 'rania'.

```
kinit rania
```

Type the password of the user and after that check the available Ticket using the following command.

```
klist
```

Now you can connect the 'krb5.anass.io' server using the SSH Kerberos authentication.

```
ssh krb5.anass.io
```

And you will be connected to the 'krb5.anass.io' server through SSH with Kerberos authentication.

Below is the SSH Log after logged to the sever

Finally, the installation and configuration of Kerberos server and client has been completed successfully.