TAMPERE UNIVERSITY – DEPARTMENT OF COMPUTING SCIENCES

Security Protocols: Helping Alice and Bob to Share Secrets (COMP.SEC.220)

Tutorial 6: Kerberos

Antonis Michalas antonios.michalas@tuni.fi
Mindaugas Budzys mindaugas.budzys@tuni.fi
Hossein Abdinasibfar hossein.abdinasibfar@tuni.fi

October 4, 2024

SUBMISSION DEADLINE: 21.10.2024 AT 23:00

Tutorial Description

In this lab, students will be introduced to a more technical and practical aspect of Kerberos protocol. The purpose of this lab is to introduce students to the Kerberos key distribution server, in particular, accessing a service (for example, SSH) using a ticket generated by KDC. This will give you a hands-on experience on how Kerberos works in practice by following the steps below:

- Install and configure Kerberos server on a Linux machine
- Create a user and a service principal
- Generate a ticket for the user to access the service
- Access the service using the ticket

For this lab session, you will be using two distinct virtual machines: `KDC` and `client`. Feel free to select the virtualization tool that suits you best. As for the choice of Linux distribution, while you have the flexibility to opt for any, we recommend utilizing the Ubuntu distribution to streamline the process. Note that the commands and instructions in this Lab are for Ubuntu, if you are using a different distribution you have to find the corresponding command by yourself. Let's dive in and get started!

TASK 1 – SETTING UP YOUR VIRTUAL MACHINES

Once you have both virtual machines up and running, first, you should set a hostname for both `KDC` and `cleint` machines. To do so, open a terminal in `KDC` and type the following command:

```
# on KDC machine
$ sudo hostnamectl set-hostname kdc.nisec.test
```

do the same for `client` machine:

```
# on the client machine
$ sudo hostnamectl set-hostname client.nisec.test
```

Next, you should find the VM's IP address. To do so, open a terminal and type the following command in each machine:

```
$ ip a
```

You can find the IP address of your machine under the interface `enXXXX`. In our case the `KDC`'s IP was under the `enp1s0/inet` path, which was 192.168.122.5, same path for `client`, and the IP was 192.168.122.115. You should note down your IP address as you will need it later. Then, it is time to add the IP addresses and the hostnames of your `KDC` and `client` machines to the file `/etc/hosts`. To do so, open a terminal in each machine and type the following command:

```
$ sudo nano /etc/hosts
```

Then add the following lines to the file after localhost addresses and save the changes using `Ctrl` + `O` and exit using `Ctrl` + `X`:

```
... localhost addresses
192.168.122.5 kdc.nisec.test
192.168.122.115 client.nisec.test
```

Do not forget to replace the IP addresses with your own VMs' IP addresses.
You can check the communication between your machines by pinging the `client` machine from `KDC` and vice versa. To do so, open a terminal in each and type the following command:

```
# on KDC machine
$ ping -c 3 client.nisec.test
# on the client machine
$ ping -c 3 kdc.nisec.test
```

If you get a response from the other machine, then you are good to go. If not, you should check your network configuration and make sure that your machines are connected to the same network.
Next step is installing `openssh – server` and `openssh – client` on `KDC`, and `client` machines. To do so, open a terminal in each machine and type the following command:

```
# on the client machine
$ sudo apt install openssh-client -y
# on KDC machine
$ sudo apt install openssh-server -y
$ sudo systemctl enable ssh
$ sudo ufw allow ssh
$ sudo systemctl start ssh
```

Task 2 – Installing and Configuring Kerberos

To install Kerberos on your `KDC` machine, first run the following command:

```
# on KDC machine
$ sudo apt install krb5-kdc -y
```

It will ask you to provide some information about your realm, domain, and server. You can use the following information:

```
# Default Kerberos version 5 realm: NISEC.TEST
# Kerberos servers for your realm: kdc.nisec.test
# Administrative server for your Kerberos realm: kdc.nisec.test
# Create the Kerberos KDC configuration automatically? Yes
```

If you faced an error relating to the DB2 database, you can run the following command to fix it:

```
# on KDC machine
$ sudo kdb5_util create -r NISEC.TEST -s
# then you have to choose a password for the database and restart the service
$ sudo systemctl restart krb5-kdc
```

After, you need to install the Kerberos admin server by running the following command:

```
# on KDC machine
$ sudo apt install krb5-admin-server krb5-config -y
$ sudo systemctl restart krb5-admin-server
# After installing the admin server, you need to create a new realm, but before that, you
    need to destroy the previous database to avoid database conflict using the below command:
$ sudo kdb5_util destroy -r NISEC.TEST
```

To create a new realm, run the following command:

```
# on KDC machine
$ sudo krb5_newrealm
```

Next, you need to add the admin user principal to the access control list (ACL). To do so, open the `kadm5.acl` file and add the following line:

```
$ sudo nano /etc/krb5kdc/kadm5.acl

# uncomment the following line
*/admin *

# save the changes using Ctrl+O and exit using Ctrl+X
$ sudo systemctl restart krb5-admin-server
```

Next, you need to create a principal for `client` to access the `kadmin` using root privilege. To do so, use the following command:

```
# on KDC machine
$ sudo kadmin.local
# You will see a prompt like this: Authenticating as principal root/admin@NISEC.TEST with the
    password.
# first you need to add root/admin principal to the Access Control List (ACL)
$ kadmin.local: addprinc root/admin
# it will ask you to choose a password for the user, choose any password you want, then it
    prompts you: Principal "root/admin@NISEC.TEST" created.
$ kadmin.local: quit
$ sudo systemctl restart krb5-admin-server
# you can check the status of the service by running the following command:
$ sudo systemctl status krb5-admin-server
```

Next, you need to install and configure the `client` machine to use the KDC machine as its Kerberos server. To do so, first open a terminal and type the following command:

```
# on the client machine
$ sudo apt install krb5-user libpam-krb5 libpam-ccreds -y
```

During the installation, you will be asked to provide some information about your realm and domain. You can use the following information:

```
# Default Kerberos version 5 realm: NISEC.TEST
# Kerberos servers for your realm: kdc.nisec.test
# Administrative server for your Kerberos realm: kdc.nisec.test
```

Do not forget that you have to use the KDC server information for this step!

Next, you need to create a **key table file** for the `client` machine. To do so, use the following command:

```
# on the client machine
# enter to the root mode
$ sudo su
# access kadmin
(root)$ kadmin
# It will ask you to enter the password of the root/admin user. Enter the password you have
    chosen before
# Add a host principal for the client machine
(root)$ kadmin: addprinc -randkey host/client.nisec.test
# Add the host key to the keytab file
(root)$ kadmin: ktadd host/client.nisec.test
# you can find the keytab file in /etc/krb5.keytab
(root)$ kadmin: quit
# Then you need to create a dummy user for the client machine
(root)$ useradd -m -s /bin/bash user1
# Try to switch to the dummy user
(root)$ su - user1
(user1)$ exit
# exit from the root mode (NOTE: the whole mentioned process should be done in the root mode)
(root)$ exit
```

Then, you need to create a dummy user and create a principal for it on the KDC machine. To do so, use the following command:

```
# on KDC machine
# enter to the root mode
$ sudo su
# create the user1 bash profile
(root)$ useradd -m -s /bin/bash user1
# access kadmin
(root)$ kadmin
(root)$ kadmin: addprinc user1
(root)$ kadmin: quit
# exit from the root mode (NOTE: the whole mentioned process should be done in the root mode)
(root)$ exit
$ sudo systemctl restart krb5-admin-server
```

Task goal: You should retrieve the keytab file from the client machine and submit it with your report.

TASK 3 – CONFIGURING THE SSH SERVICE

For this task, first, you have to configure the `openssh – server` on your KDC machine. To do so, open a terminal and run the following command:

```
# on KDC machine
$ sudo nano /etc/ssh/sshd_config
# then try to find the following lines and uncomment and change them
KerberosAuthentication yes
...
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
# save the changes using Ctrl+O and exit using Ctrl+X
# restart the ssh service
$ sudo systemctl restart sshd
```

TASK 4 – GENERATING THE TICKET FOR `client`

In this step, you need to initialize the Kerberos client and get the **ticket** for `user1` from `kdc` by running the following command:

```
# on the client machine
# Switch to user1 to check if it is okay
$ sudo su
(root)$ su - user1
(user1)$ exit
(root)$ exit
```

(1) Make sure that you are not in (root) mode. (2) Do not use superuser privileges for this step. No sudo!

```
$ kinit user1
# It will ask you for the password. Use the password you have chosen for the user1, which you
    created during the principal creation step
```

To see the **ticket** information, you can run the following command:

```
$ klist
# you sould see the ticket cache file path as FILE:/tmp/krb5cc_1000
```

Task goal: You should retrieve the ticket file from the cache and submit it with your report.

TASK 5 – ACCESSING THE KDC MACHINE FROM `client` MACHINE USING `ssh`

In this step, you need to access the `KDC` machine from `client` machine using `ssh` and create a file on the `KDC` machine. The goal is to write your name and student number in the file.

```
# on the client machine, switch to user1
$ sudo su
(root)$ su - user1
# For starting an SSH session, you can use the following command
(user1)$ ssh kdc.nisec.test
# It will ask you to provide the user1 password. Use the password you have chosen for user1,
    which you created during the principal creation step
$ hostname -f
# it will show you the hostname of the machine you are connected to "KDC", it should be
    kdc.nisec.test
$ nano IamHere.txt
# write your name and student number in the file, save it using Ctrl+O, and exit using Ctrl+X
```

Try to access the user1 home directory on the `KDC` machine and check if the file is created or not. If the file is created, then you have successfully completed the task. To do so, you can run the following command:

```
# on KDC machine
$ cd /home/user1
$ ls
# you should see the IamHere.txt file
$ cat IamHere.txt
# it should show you the content of the file
```

Task goal: You should take a screenshot of both terminals in the client and KDC while the client is connected using ssh to KDC and the file content is visible. Submit it with your report.

FINAL REPORT

Your final report should contain the following information:

- The `keytab` file from `client` machine
- The `ticket` file for `user1` from `client` machine
- The screenshot of both terminals in client and KDC, while the `client` is connected using ssh to `KDC`, and the file content is visible.
- A very brief description of your personal observations and comments on the tasks.