Hacettepe University
Department of Computer Engineering
BBM465 Information Security Laboratory
Experiment 4

Subject: Kerberos Authentication System
Due Date: 24/12/2019 - 23:59

1 Introduction

Kerberos is a network authentication protocol which employs the symmetric key cryptography along with needing authorization from a trusted third party in order to authenticate client-server applications. It has been developed by the Massachusetts Institute of Technology (MIT) to secure the network services. It is also noteworthy that many vendors such as Microsoft and Oracle use Kerberos architecture for Single Sign-on (SSO) techniques.

In this homework, you will show how to set up Kerberos authentication between 2 Ubuntu based devices. To do so, you will need to install and configure the *Kerberos server* on the Ubuntu and then install the *Kerberos client* on the client side (preferably Ubuntu). Finally, you will test the authentication of the SSH service with the Kerberos server and demonstrate the components of this setup along with a live SSH based connection

2 Glossary

There are a few terms that are good to understand before setting up a Kerberos server. Some of them are listed below:

1. **Principal**: any users, computers, and services provided by servers need to be defined as Kerberos Principals.
2. **Instances**: are used for service principals and special administrative principals.

3. **Realms**: the unique realm of control provided by the Kerberos installation. Think of it as the domain or group your hosts and users belong to. Convention dictates the realm should be in uppercase. By default, Ubuntu will use the DNS domain converted to uppercase (EXAMPLE.COM) as the realm.

4. **Key Distribution Center**: (KDC) consist of three parts, a database of all principals, the authentication server, and the ticket granting server. For each realm there must be at least one KDC.

5. **Ticket Granting Ticket**: issued by the Authentication Server (AS), the Ticket Granting Ticket (TGT) is encrypted in the user's password which is known only to the user and the KDC.

6. **Ticket Granting Server**: (TGS) issues service tickets to clients upon request.

7. **Tickets**: confirm the identity of the two principals. One principal being a user and the other a service requested by the user. Tickets establish an encryption key used for secure communication during the authenticated session.

8. **Keytab Files**: are files extracted from the KDC principal database and contain the encryption key for a service or host.

As a summary, shown in Figure 1, a Realm has at least one KDC, preferably more for redundancy, which contains a database of Principals. When a user principal logs into a workstation that is configured for Kerberos authentication, the KDC issues a Ticket Granting Ticket (TGT). If the user supplied credentials match, the user is authenticated and can then request tickets for Kerberized services from the Ticket Granting Server (TGS). The service tickets allow the user to authenticate to the service without entering another username and password.

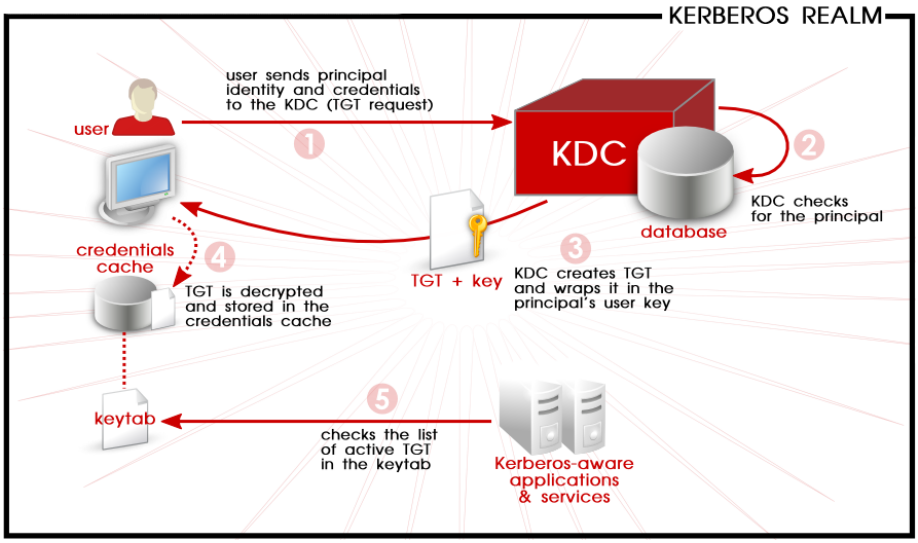

Figure 1: General workflow of a Kerberos authentication mechanism

3 Experiment

In this experiment; the Kerberos authorization protocol, which controls whether users are authorized to access any network service, will be installed and configured for the ssh connection.

The instructions for the homework is listed below:

1. You must use two different Ubuntu instances in which one of them will be working as Kerberos server whereas the other will function as the Kerberos client. Keep in mind that, the same Ubuntu installation cannot be used for both server and client purposes. Therefore, prepare two different OS instances in order to complete this experiment. One alternative way could be use of virtual machines.

2. Since timestamp is an important parameter in Kerberos, the clocks of two computers must be synchronized.

3. Pick a unique realm in order to make both the client and the server computers compatible for the Kerberos name on the network.

4. Do the necessary adjustments so that the two computers can communicate with each other. Meanwhile, apart from the use of virtual machines, you can use cross cable or wi-fi connections as the physical connections between the client and server.

5. The necessary settings for Kerberos and SSH will be made on the server computer. (The server computer will be used as both KDC and ssh server for Kerberos.)

6. Do the necessary settings in order to log into the server computer with Kerberos.

7. Do the necessary settings for the Kerberos for the client computer.

8. When the "kinit username" statement is executed on the client side, a TGT should be obtained by interacting with KDC. The password must be requested from the user in this step. If the "ssh username @ sshserverIP" statement is executed, the password must be entered without asking for the password.

9. In order to get evaluated, you will demonstrate the system you have configured.

4 Notes

1. You need to submit a detailed lab report (i.e report.pdf) to describe what you have done and throughout the homework.

2. You can ask questions about the experiment via Piazza group (`piazza.com/hacettepe.edu.tr/fall2019/bbm465`).

3. Late submission will not be accepted!

4. You are going to submit your experiment to online submission system: `www.submit.cs.hacettepe.edu.tr`

   The submission format is given below:
   <bxxxx id>.zip
   −conf/
   krb5kdc/
   –exp files
   krb5.conf
   krb5.keytab
   etc/hosts
   −report/
   report.pdf

5 Policy

All work on assignments must be done with your own group unless stated otherwise. You are encouraged to discuss with your classmates about the given

assignments, but these discussions should be carried out in an abstract way. That is, discussions related to a particular solution to a specific problem (either in actual code or in the pseudocode) will not be tolerated. In short, turning in someone else's work(from internet), in whole or in part, as your own will be considered as a violation of academic integrity. Please note that the former condition also holds for the material found on the web as everything on the web has been written by someone else.

The content of this assignment can be partially changed by the instructor. However, all modifications will be reported into the Piazza system. Therefore, do not forget to keep an eye on Piazza for potential changes.