Kerberos Authentication Protocol

Introduction :-

Kerberos is a network-based authentication protocol. It was developed around mid-1980s at MIT. It worked on the client/server model and user symmetric key cryptography.

It is a Computer Network authentication Network which works on the basis of the tickets of secure communication. It contains Client – Server model, Symmetric Model, KDC & TGS.

Key Distribution Centre (KDC) :- A trusted third-party that verifies user identities located on a Domain Controller (DC), such as the Active Directory domain.

The KDC includes two servers:

1. **Authentication Server (AS) :** Confirms that the access request the user is making is from a known service and issues Ticket Granting Tickets (TGTs).
2. **Ticket Granting Service (TGS):** Confirms that the access request the user is making is from a known service and issues service tickets.

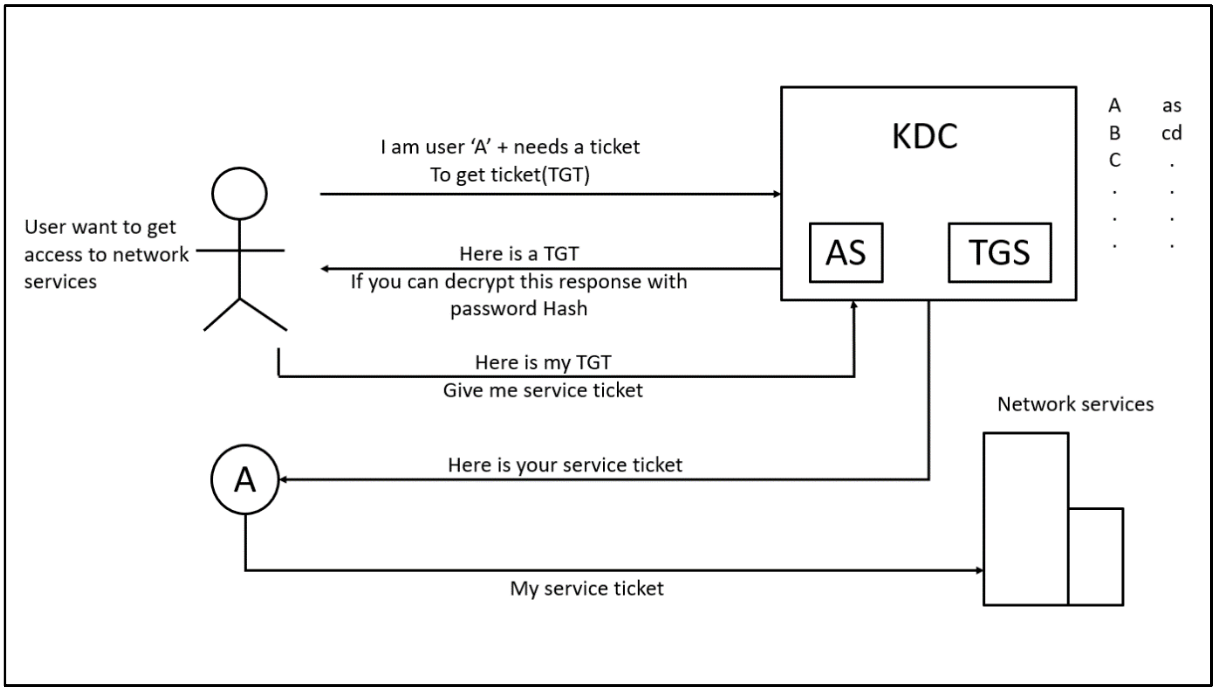
KDC
AS
TGS
A as
B cd
C
User want to get access to network services
I am user 'A' + needs a ticket To get ticket(TGT)
Here is a TGT
If you can decrypt this response with password Hash
Here is my TGT
Give me service ticket
Network services
A
Here is your service ticket
My service ticket

Fig. Kerberos Authentication protocol

Working :-

i) A person ‘A’ want to gain access from network services

ii) So ‘A’ can be send the message to KDC as a “I am user ‘A’ & needs a ticket to get ticket (TGT)”

iii) KDC is divided into two parts one is AS & other is TGS.

iv) AS authenticate the person ‘A’ & send the message “Here is a TGT , You can decrypt this response with password Hash.”

v) Then the person ‘A’ decrypt this message by using password Hash by using MD5 algorithm and send message to authenticate server as a “Here is my TGT. Give me a service ticket.”

vi) TGS will send the service ticket with session keys and send to person ‘A’.

vii) Person ‘A’ can send this session key with network services & gain the access of network.

Applications :-

Kerberos implementations are used on a number of operating systems and networking systems to verify user accounts.

Examples include:

1) Amazon Web Services (AWS)
2) Google Cloud
3) Linux
4) UNIX

Benefits :-

Kerberos offers many benefits to users, such as:

i) Single Sign-On (SSO):

The Kerberos service enables SSO, an authentication method that allows users to access all authorized services via one login.

ii) Cybersecurity:

Kerberos’ use of strong encryption, cryptography, and trusted third-party authorization helps strengthen data security to avoid cyber attacks.

iii) Mutual Authentication:

The Kerberos protocol allows both the User and the Service to authenticate one another, ensuring each party is genuine.

iv) Access Control:

Kerberos facilitates access control by performing authentication to help ensure security policies are met before granting access permissions

Advantages :-

i) In Kerberos, clients and services are mutually authenticated.

ii) Various operating systems support it.

Disadvantages :-

i) It is vulnerable to weak or repeated passwords.

ii) It only provides authentication for services and clients.

Conclusion :-

In this case study, we have seen what Kerberos is, how it works, its applications, benefits, and its advantages and disadvantages.