

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.

The main components of Kerberos are:

Authentication Server (AS):

The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

Database:

The Authentication Server verifies the access rights of users in the database.

Ticket Granting Server (TGS):

The Ticket Granting Server issues the ticket for the Server

Step-1:

User login and request services on the host. Thus user requests for ticket-granting service.

Step-2:

Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.

Step-3:

The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network addresses.

Step-4:

Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting services from the Server.

Step-5:

The user sends the Ticket and Authenticator to the Server.

Step-6:

The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.

Kerberos Limitations

Each network service must be modified individually for use with Kerberos

It doesn't work well in a timeshare environment

Secured Kerberos Server

Requires an always-on Kerberos server

Stores all passwords are encrypted with a single key

Assumes workstations are secure

May result in cascading loss of trust.

Scalability

Is Kerberos Infallible?

No security measure is 100% impregnable, and Kerberos is no exception. Because it's been around for so long, hackers have had the ability over the years to find ways around it, typically through forging tickets, repeated attempts at password guessing (brute force/credential stuffing), and the use of malware, to downgrade the encryption.