Introduction to kerberos

What is Kerberos and how it works ?

- Kerberos is a computer network security protocol that authenticates service requests between two or more trusted hosts across an untrusted network, like the internet. It uses secret-key cryptography and a trusted third party for authenticating client-server applications and verifying users' identities.
- Initially developed by the Massachusetts Institute of Technology (MIT) for Project Athena in the late '80s, Kerberos is now the default authorization technology used by Microsoft Windows. Kerberos implementations also exist for other operating systems such as Apple OS, FreeBSD, UNIX, and Linux.
- Microsoft rolled out its version of Kerberos in Windows 2000, and it's become the go-to protocol for websites and single sign-on implementations over different platforms. The Kerberos Consortium maintains the Kerberos as an open-source project.
- The protocol derives its name from the legendary three-headed dog Kerberos (also known as Cerberus) from Greek myths, the canine guardian to the entrance to the underworld. Kerberos had a snake tail and a particularly bad temper and, despite one notable exception, was a very useful guardian.
- But in the protocol's case, the three heads of Kerberos represent the client, the server, and the Key Distribution Center (KDC). The latter functions as the trusted third-party authentication service.

- Users, machines, and services that use Kerberos depend on the KDC alone, which works as a single process that provides two functions: authentication and ticket-granting. KDC "tickets" offer authentication to all parties, allowing nodes to verify their identity securely. The Kerberos authentication process employs a conventional shared secret cryptography that prevents packets traveling across the network from being read or altered, as well as protecting messages from eavesdropping and replay (or playback) attacks

The main uses of Kerberos include:

- Single Sign-On (SSO)
  - Kerberos enables users to authenticate once and obtain a ticket, known as a Kerberos ticket-granting ticket (TGT). This TGT can be used to request service tickets for various resources without repeatedly providing credentials. This SSO capability improves user convenience and reduces the need for managing multiple passwords.
- Network Authentication
  - Kerberos provides a secure mechanism for verifying the identity of network services, such as servers and applications. Clients can request a service ticket from the Key Distribution Center (KDC) using their TGT, and the service ticket is used to authenticate and establish a secure session with the requested service.
- Mutual Authentication
  - Kerberos ensures mutual authentication, meaning both the client and the server authenticate each other during the initial authentication process. This prevents impersonation and man-in-the-middle attacks by verifying the authenticity of both parties involved in the communication.
- Authorization
  - Kerberos can also be used to enforce access control policies. Once a client is authenticated, the Kerberos ticket includes information about the client's identity and access permissions. Servers can use this information to enforce authorization rules and grant or deny access to specific resources based on the client's privileges.

What Does Kerberos Authentication Protocol Do?

MIT developed this protocol for a project named Athena. It gets its name from the three-headed dog of Hades, who guarded hell in Greek Mythology. They chose this name because the Kerberos protocol represents the following three things:

- Client
- Network Resource (Application server)
- Key Distribution Center (KDC)

With these three components, Kerberos enables trusted host authentication over untrusted networks. Kerberos ensures that only authorized users can access the network resources. Additionally, it provides AAA security: Authentication, Authorization, and Accounting.

In Kerberos, KDC grants tickets. These allow different hosts to prove their identity. In addition, the developers intended for Kerberos' authentication that supports authorizations. That means a client authenticated by Kerberos also has access.

How Do Kerberos Authentication Protocols Work?

- Authentication Server Request: The client requests authentication from KDC. This authentication request would be in plain text.
- Authentication Server Response: KDC sends a TGT and a session key if the client exists in the database. If the client is not in the database, the authentication fails.
- Service Ticket Request: The client asks for the service ticket along with the TGT sent earlier by the KDC.
- Service Ticket Response: KDC sends the ticket encrypted with the session key. The client can use the session key sent earlier by KDC to decrypt the service ticket.
- Application Server Request: The client requests the application server for access using the service ticket. T
- Application Server Response: The application server authenticates the client. It sends a ticket that will grant access to that particular service.
- The service ticket has a specific expiry time. You can use the same session ticket to access services until it expires.

There are two versions of kerberos

Kerberos Version 4 :

- Kerberos version 4 is an update of the Kerberos software that is a computer-network authentication system. Kerberos version 4 is a web-based authentication software which is used for authentication of users information while logging into the system by DES technique for encryption. It was launched in late 1980s.

Features of Kerberos V4:

- Authentication: Kerberos V4 provides authentication and encryption services to network clients and servers.
- Encryption: Kerberos V4 uses a simple encryption algorithm that is less secure than the encryption used in Kerberos V5.
- Ticket-granting service (TGS): Kerberos V4 uses a single TGS for all network services, which means that the TGS has to handle a large number of requests.
- No support for timestamps: Kerberos V4 does not support timestamps, which makes it vulnerable to replay attacks

Shortcomings of Kerberos version 4

- Encryption system dependence: version 4 requires the use od DES export restrictions on DES as well as doubts about the strength of DES were thus of concern. In version 5, ciphertext is tagged with an encryption type identifier so that any encryption technique may be used.
- Internet protocol dependence: version 4 requires the use of internet protocol addresses. Other address types such as the ISO address network are not accommodated. Version 5 network address are tagged with type and length, allowing any network address type to be used.
- Message byte ordering: In version 4 the sender of a message employes a byte ordering of its own choosing and tags the message to indicate least significant byte in lowest address or most significant byte in lowest address. This technique works but does not follow established conventions. In version 5 all message structures are defined using Abstract syntax notation 1 (ASN 1) and basic encoding rules, which provide an unambiguous byte ordering.

- Ticket lifetime: lifetime values in version 4 are encoded in an 8-bit quantity in units of five minutes. Thus the maximum lifetime that can be expressed is 2^8 * 5 = 1280 mins. This may be inadequate for some application . In version 5, tickets include an explicit start time and end time allowing tickets with arbitrary lifetimes.
- Authentication forwarding: version 4 does not allow credentials issued t one client to be forwarded to some other host and used by some other client. This capability will enable a client to access a server and have that server access another server on behalf of the client.
- Interrealm authentication: In version 4 interoperability among N realms requires on the order of n^2 Kerberos to Kerberos relationships as described earlier. Version 5 supports a method that requires fewer relationships.

Kerberos Version 5 :

- Kerberos version 5 is a later version of the Kerberos software came after Kerberos version 4, developed for enhancing security in the authentication. Kerberos version 5 provides a single authentication service in a network which is distributed over an enterprise. It was launched in the year 1993.
- **Features of Kerberos V5:**
  - Authentication: Kerberos V5 provides authentication, encryption, and authorization services to network clients and servers.
  - Encryption: Kerberos V5 uses a more secure encryption algorithm than Kerberos V4, which makes it less vulnerable to attacks.
  - Ticket-granting service (TGS): Kerberos V5 uses multiple TGS servers to handle requests for different network services. This improves scalability and reduces the load on individual TGS servers.
  - Support for timestamps: Kerberos V5 supports timestamps, which makes it less vulnerable to replay attacks.
  - Support for renewable tickets: Kerberos V5 supports renewable tickets, which allows users to extend their authentication without having to re-enter their passwords.

Similarities between the two versions of Kerberos:

- Authentication process: Both Kerberos V4 and V5 use a similar authentication process that involves a client, a server, and a trusted third-party authentication server (TAS) that issues tickets to the client.
- Encryption: Both Kerberos V4 and V5 use encryption to protect sensitive data and prevent eavesdropping.
- Password-based authentication: Both Kerberos V4 and V5 use password-based authentication, which requires users to enter their passwords to access network resources.
- Ticket-based authentication: Both Kerberos V4 and V5 use ticket-based authentication, which enables users to authenticate to multiple network resources without having to enter their passwords multiple times.
- Key distribution: Both Kerberos V4 and V5 use a key distribution center (KDC) to distribute secret keys to network clients and servers.
- Network interoperability: Both Kerberos V4 and V5 are designed to be compatible with a wide range of network operating systems and protocols, which makes them suitable for use in heterogeneous network environments.

Difference between Kerberos Version 4 and Kerberos Version 5 :

S. no.	Kerberos Version 4	Kerberos Version 5
1.	Kerberos version 4 was launched in late 1980s.	Kerberos version 5 was launched in 1993.
2.	It provides ticket support.	It provides ticket support with extra facilities for forwarding, renewing and postdating tickets.
3.	Kerberos version 4 works on the Receiver-makes-Right encoding system.	Kerberos version 5 works on the ASN.1 encoding system.
4.	It does not support transitive cross-realm authentication.	It supports transitive cross-realm authentication.
5.	It uses Data Encryption Standard technique for encryption.	It uses any encryption techniques as the cipher text is tagged with an encryption identifier.
6.	In Kerberos version 4, the ticket lifetime has to be specified in units for a lifetime of 5 minutes.	In Kerberos version 5, the ticket lifetime is specified with the freedom of arbitrary time.