Kerberos

av

Pål Karlsen

IKT 207

Cybersikkerhet

Veiledet av

Sigurd Kristian Brinch

Fakultet for teknologi og realfag

Universitetet i Agder

Grimstad, September 2020

Kerberos is a creation of MIT and got its nickname from the three-headed dog Cerberus in Greek mythology. Kerberos's three heads represent the client, server, and the Key Distribution Center(KDC)[5]. It is a network authentication protocol that creates strong authentication for clients- and server applications. This is achieved by using secret-key cryptography. Why should one use Kerberos, and what makes it effective?

The internet is an insecure place. Transferring data such as passwords between a host on the internet are quickly picked up by "sniff" tools, and those tools are common for hackers. Therefore one will need a secure transfer of such valuable data. This is where Kerberos comes to play. Kerberos gives a reliable authentication between known hosts over an insecure network, such as the internet[3].

Users and services that use Kerberos rely on the KDC, which provides two functions: authentication and ticket-granting. KDC provides authentication for all parties, allowing nodes to verify their identity. Kerberos utilizes a shared secret that prevents packets that travels across the internet from being read or altered. This will also protect the message from eavesdropping and replay/playback attacks[5].

The main difference between a firewall and Kerberos is that a firewall assumes the attack will come from the outside. In contrast, Kerberos will assume that the network connection is the weakest link, rather than servers and work station.

There are several components that Kerberos relies on.

1. Key Distribution Center contains the authentication service, the Ticket-Granting service, and the master database for Kerberos
2. Authentication Service takes care of user authentication
3. Ticket-Granting Service will give a user a Ticket Granting Ticket(TGT) and a ticket session, which gives the user the right to use that ticket.
4. The Kerberos Database contains all the user information, such as their password.
5. Kerberos Utility Programs, which grants three different versions of the Kerberos user interface[4]
6. Kerberos Registry is where your parameter are stored[2]

When a client uses a service with Kerberos, an authentication request is sent to the KDC. Then a TGT is return as a result of the authentication. The client application will then start, and the TGT is used to request an application ticket. The application ticket is then sent to the application server, verifying the application ticket with the KDC. The service ticket for the required service is sent to the server. The server then sends the request data to the client[4].

Kerberos is primarily used between two trusted hosts over an untrusted network. It will encrypt all the information, so even if someone intercepts this information, it will be almost impossible to decrypt it without the proper key. Since it is so hard to decrypt, it is an extremely reliable protocol used by many such as Microsoft, Apple OSx, and Linux. But because such big companies, hackers have developed several ways to hack and infiltrate Kerberos[1]. Despite this, it is one of the best protocol available today. With its flexibility and use of good password practice, one should be fine.

References

[1] Kerberos Authentication Explained. *JEFF PETTERS*. 3/29/2020. URL: `https://www.varonis.com/blog/kerberos-authentication-explained/`.

[2] *Kerberos protocol registry entries and KDC configuration keys in Windows*. 9/08/2020. URL: `https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kerberos-protocol-registry-kdc-configuration-keys`.

[3] MIT. *Kerberos: The Network Authentication Protocol*. 22/05/2020 16:25:17. URL: `https://web.mit.edu/kerberos/#what_is`.

[4] OMAL PERERA. *kerberos Simplified*. FEBRUARY 1ST, 2018. URL: `https://omalperera.github.io/security/2018/02/01/kerberos-simplified.html`.

[5] Simplilearn. *What Is Kerberos, How Does It Work, and What Is It Used For?* Sep 21, 2020. URL: `https://www.simplilearn.com/what-is-kerberos-article`.