👉🎟️Pass The Ticket

Intro

Another Interesting lateral movement technique on Windows Environment that, Although it shares certain similarities with the fundamentals of techniques such as **PTH** and **OPTH**, It has certain peculiarities that made it more effective in some cases of use. This technique is called 👉🎟️**Pass The Ticket.**

One thing that we already know is that we can use techniques to dump ***credentials hashed on memory*** and then use those credentials to overwrite on a new login and ***behave as if we were another user*** at the moment to access different services on a network.

Another thing that is generated when we authenticate on a Windows Machine is a **TGT,** if we are using **Kerberos,** and prolly some **TGS.** If we make the command **klist** in a Powershell, we can see all **Kerberos** tickets associated with that user.

Following the same principles that have been raised in previous sections, we can think: “Just like we can dump the credentials of users that are in some part of the memory, ***those tickets must be somewhere in the memory***. So, we can dump the TGT of other users, for example the DC Administrator user, if that user had logged in on that machine at some point, and ***use that TGT on behalf of this user*** to make requests and consume services on the DC”.

That could sounds good, but, if we remember, when we pick a **TGT** and we want to request to the **TGS** for a **Service Ticket** we have to accompany the **TGT** with an **"Authenticator"** that will be cypher with ***a Session Key*** that we had getting on the request process of the **TGT** to the Authentication Service.

So we don't have the ***Session Key*** we can not encrypt the **Authenticator,** therefore, even having the **TGT** we can not request for the **Services Ticket.** Even so, just having the **TGT,** we can do interesting things, because the ***Sessions Key is in the same part of memory where it is the TGT***. And with the **same technique** that we used to dump the **TGT** ***we can also dump the Sessions Key*** associated with that **TGT.** To dump this information we just need to be the Local Administrators.

👉🎟️Pass The Ticket