Advanced Adversary Simulation: A Guide To Kerberoasting

Kerberoasting is one step in the AAS Attack Narrative and is a technique used to retrieve hashes with the ultimate goal of password cracking.
This infographic represents this process using the analogy of visiting the carnival.

To The Carnival

Boot computer and enter credentials to log onto your corporate network.

Main Entrance

Computer requests a ticket granting ticket from the domain controller to enter the realm.

Ticket Booth

To access a file share server with your work files on it, the computer takes a ticket granting ticket to the ticket granting server (domain controller) to receive the encrypted session information and a ticket to access the service you requested.

Rider Access

User or computer takes the service ticket it just received and sends it to the file server.

Enjoy The RIde

If the user has permission, the file server will allow the user access to its appropriate files on its share.

RedTeam Security™
THREAT PREVENTION EXPERTS