Kerberos

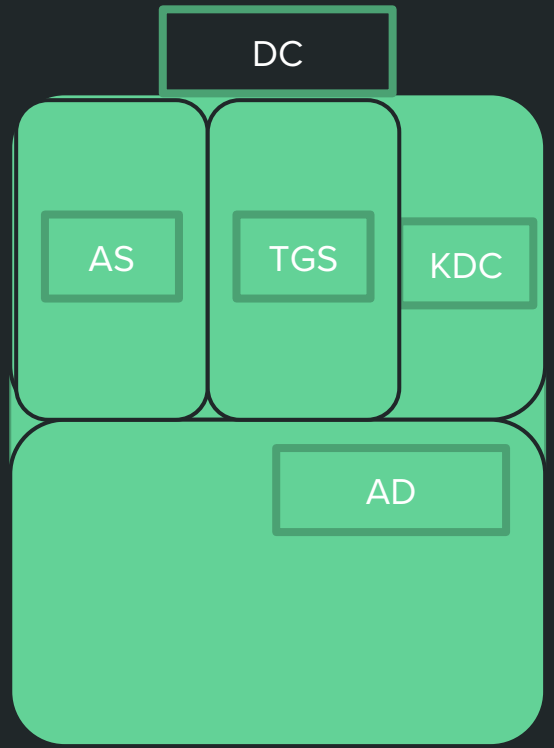
By: 1c3_B3ar

What is Kerberos?

- Primary Authentication method for Active Directory
- Replaced NTLMv1/v2
  - Designed to fix relaying and pass-the-hash
- Relies on trusted 3rd party

Vocab Quiz

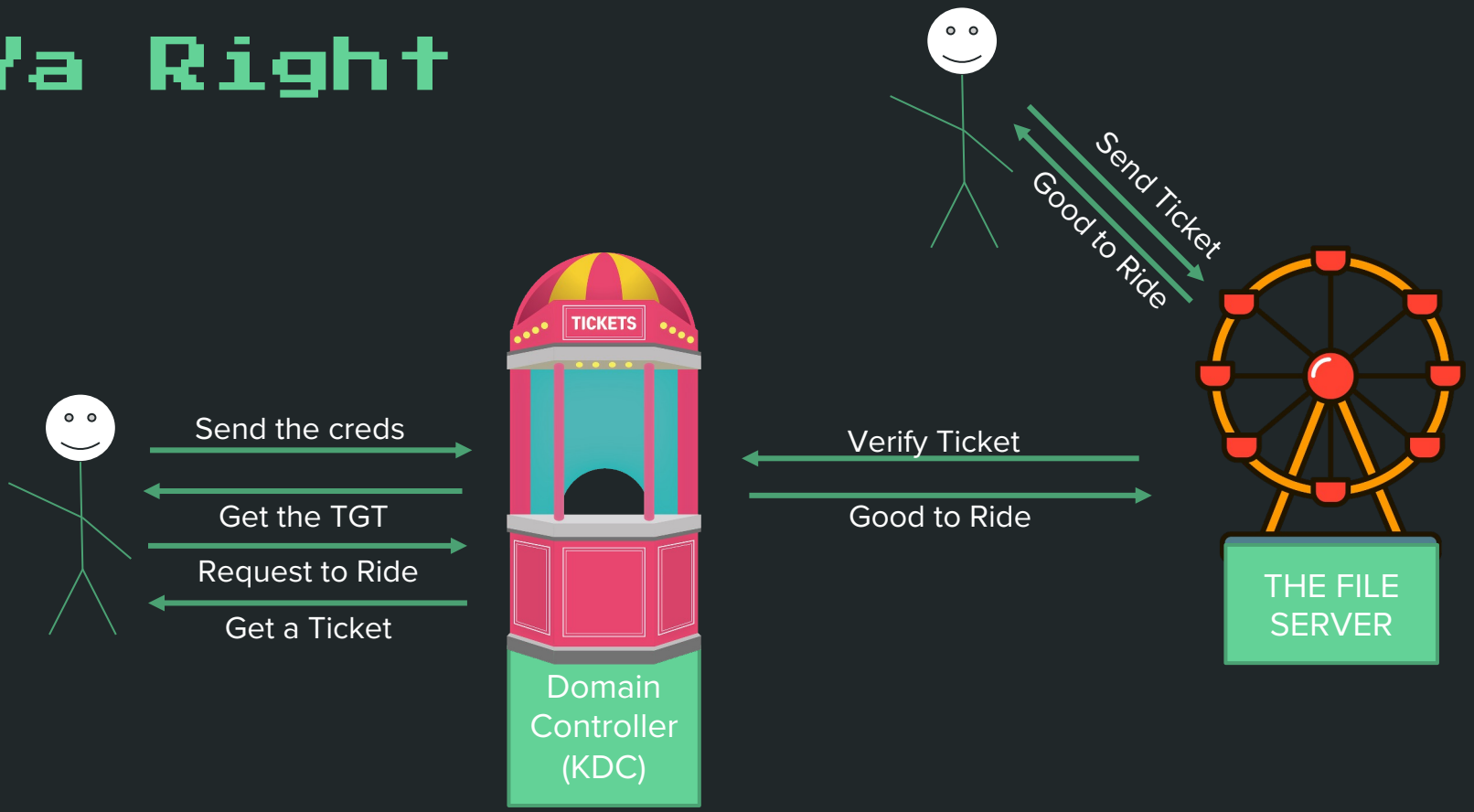
- Domain Controller
  - Main server that generally hosts Active Directory and KDC
- KDC (Key Distribution Center)
  - Two parts, AS and TGS
- AS (Authentication Server)
  - Handles translating credentials into TGTs
- TGS (Ticket-Granting Server)
  - Handles translating TGTs to Tickets
- TGT (Ticket Granting Ticket)
  - Main form of authentication inside of domain
- Ticket/TGS Ticket (Valid Session for Service)
  - Gives access to a service



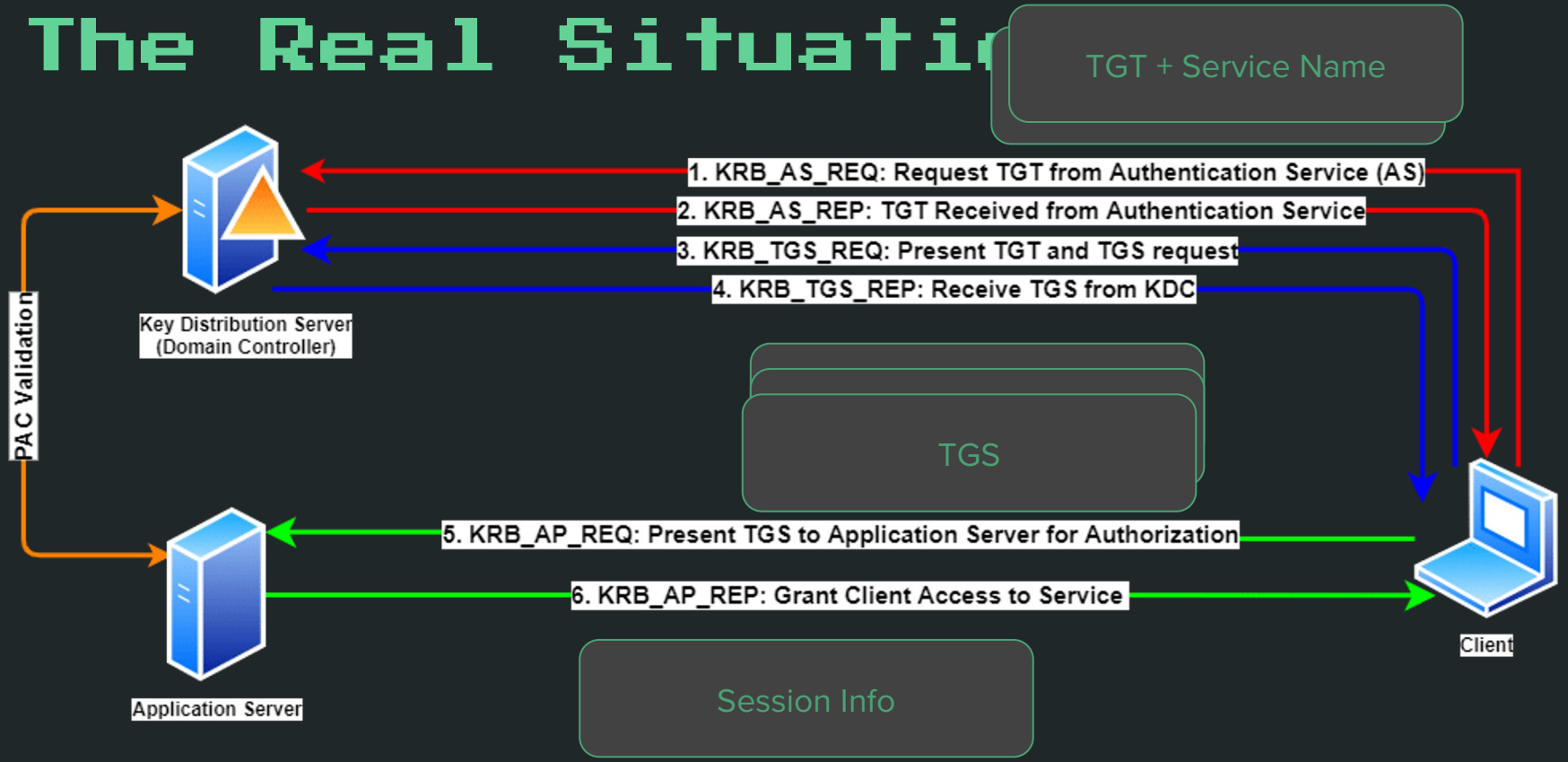
What is it like?

AN AMUSEMENT PARK

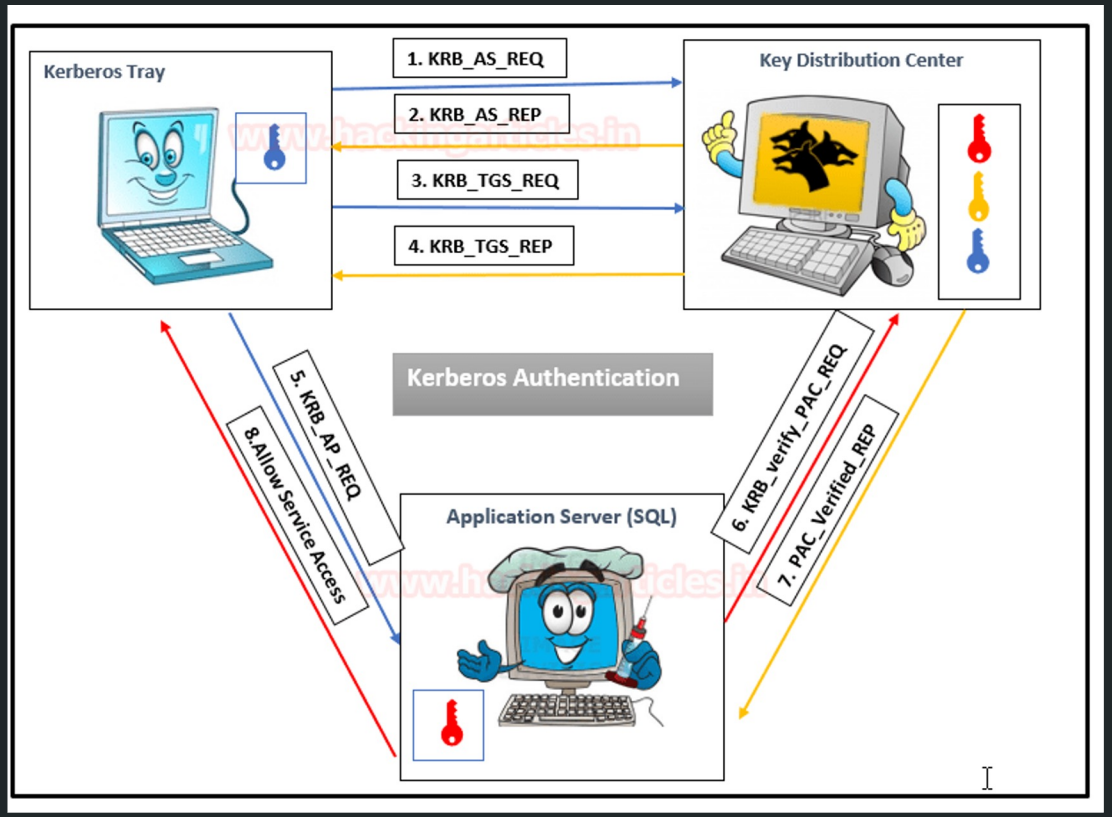
Ya Right


Send Ticket
Good to Ride
TICKETS
Send the creds
Get the TGT
Request to Ride
Get a Ticket
Verify Ticket
Good to Ride
Domain Controller (KDC)
THE FILE SERVER

The Real Situati



Another Diagram



Attacking Words

- Golden Ticket
  - A Forged TGT
  - Need password hash of KRBTGT account
    - Hidden Kerberos account for signing tickets
  - Allows you to create any tickets we want
- Silver Ticket
  - A Forged TGS Ticket
  - Need password hash of service account
  - Allows you to create a valid session to that specific service

Common Attacks

- Kerberoasting
  - Ask to ride all the rides!
  - Get all the Ticket!
  - ~Mimicatz~
- AS-REP-Roasting
  - Account with disabled pre-auth
    - Normally kdc will have you encrypt a timestamp with your password hash before giving a tgt
  - Ask for TGT for any user account
  - Take offline and crack
  - Can’t send requests for TGS yet since we don’t have the password hash