ATTACKS

Active Directory Persistence

What is Domain Persistence?

- Ways to Persist Administrative Access:
  - Dump ntds.dit
  - Creation of domain admin account
  - Creation of golden ticket
  - Creation of Skeleton key
  - Use of DCSync/DCShadow

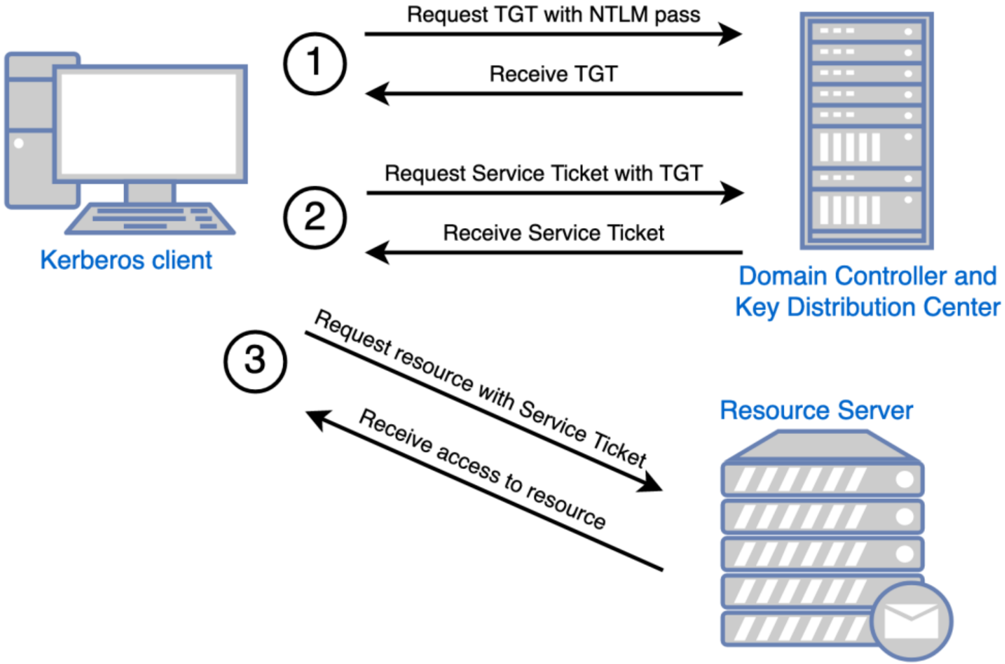
1

PASS THE TICKET: GOLDEN TICKET

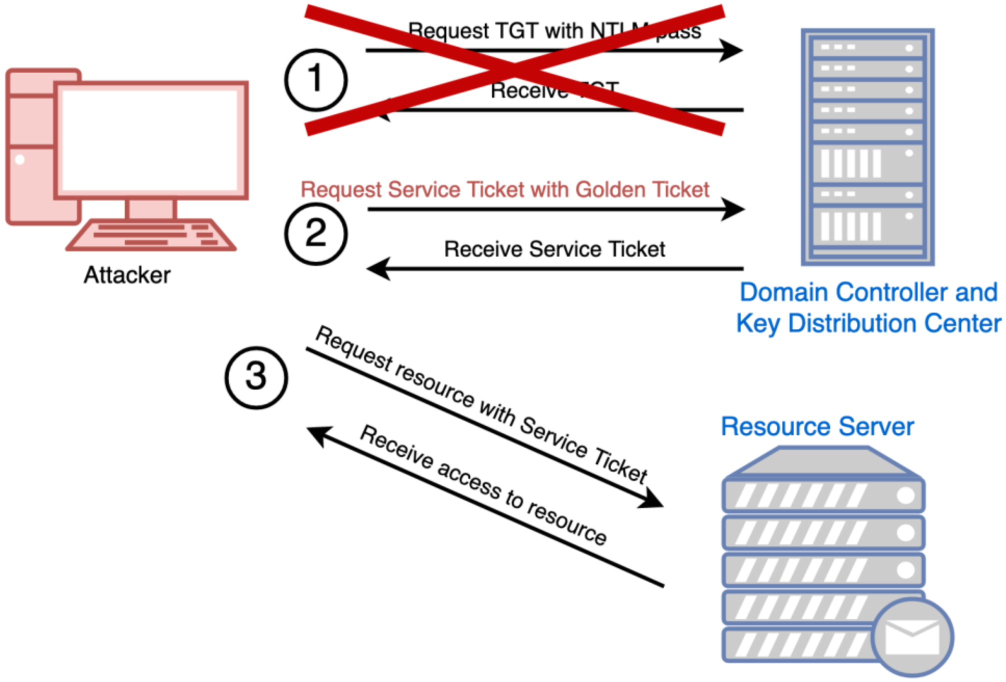
What is Golden Ticket?

- It is a special Ticket Granting Ticket (TGT) providing maximum access for maximum time
- To create a valid TGT (with valid PAC):
  - Target LT Key
  - KDC LT Key
- In case of TGT both are same (krbtgt NT hash)
- All other info is mostly public:
  - Domain name,
  - Name of admin account,
  - SID of admin account Kerberos tickets

What is Golden Ticket?


Request TGT with NTLM pass
1
Receive TGT
Request Service Ticket with TGT
2
Receive Service Ticket
Kerberos client
Domain Controller and
Key Distribution Center
3
Request resource with Service Ticket
Receive access to resource
Resource Server

What is Golden Ticket?



1 ~~Request TGT with NTLM pass~~

~~Receive TGT~~

2 Request Service Ticket with Golden Ticket

Receive Service Ticket

3 Request resource with Service Ticket

Receive access to resource

Attacker

Domain Controller and Key Distribution Center

Resource Server

Properties

- Created without interaction with DC (without AS-REQ/AS-REP). Kerberos is a stateless protocol.
- Requires KDC LT Key (not easy)
- It's a TGT for admin account (RID 500)
- Valid for 10 years by default!

Mitigations

- Change the krbtgt account password TWICE

2

DCSync

DCSync

- For **redundancy** and **backups**, domains **more than 1** domain **controllers**
- For **synchronization**, a DC may **request an update** for an **object** to another, but that request has no verification for the source
- If the SID is valid and privileged, we can attempt a malicious update request from a user of “Domain Admins” group, it will produce a copy of user password hashes
- We don’t need to authenticate to any DC in this attack!