

Complete Domain Compromise with a Golden Ticket Attack

 blog.netwrix.com/2022/08/31/complete-domain-compromise-with-golden-tickets

Jeff Warren

This [blog post series](#) covers techniques that attackers can use to find and compromise [Active Directory](#) service accounts. First, we detailed how they can discover service accounts with [LDAP reconnaissance](#); then we revealed how they can extract account passwords with [Kerberoasting](#); and then we explained how [elevate an account's](#) rights using Silver Tickets to enable additional access and activities.

Handpicked related content:

[\[Free Guide\] Active Directory Security Best Practices](#)

In this final post, we explore the most powerful service account in any Active Directory environment: the KRBTGT account, which is used to issue the Kerberos tickets required to access IT systems and data. By obtaining the password hash for this account from the Key Distribution Center (KDC), an attacker is able to compromise every account in Active Directory, giving them unlimited and virtually undetectable access to any system connected to the AD network.

What is the KRBTGT account in AD?



Windows Active Directory domain controllers are responsible for handling Kerberos ticket requests, which are used to authenticate users and grant them access to computers and applications. The KRBTGT account's password is used to encrypt and decrypt Kerberos tickets. This password rarely changes and the account name is the same in every domain, so it is a common target for attackers.

Creating Golden Tickets

Using Mimikatz, it is possible to leverage the password of the KRBTGT account to create forged Kerberos Ticket Granting Tickets (TGTs) which can be used to request Ticket Granting Server (TGS) tickets for any service on any computer in the domain.

To create Kerberos Golden Tickets, an adversary needs the following information:

- KRBTGT account password hash
- The name and SID of the domain to which the KRBTGT account belongs

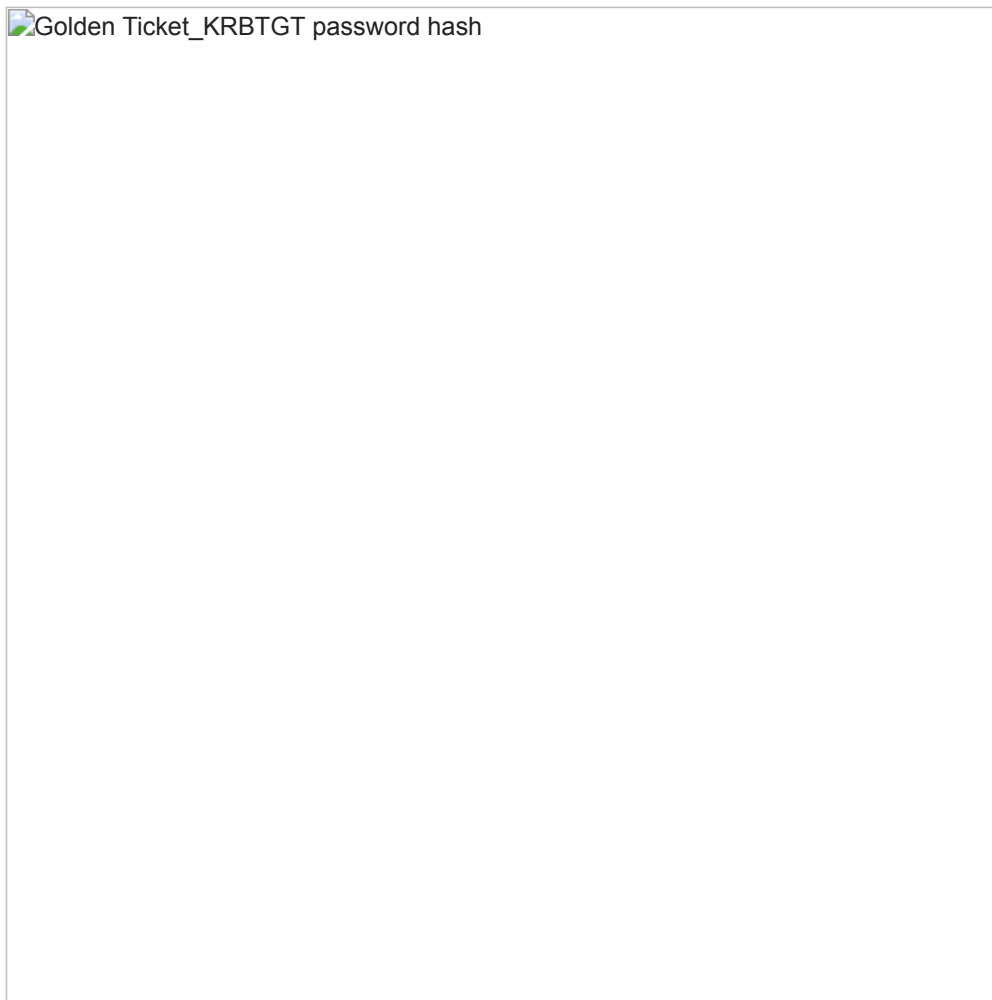
Let's take a look at how to gather this information and create Golden Tickets for Kerberos, step by step.

Step 1. Obtain the KRBTGT password hash and domain name and SID.

Obtaining the KRBGT password hash is the hardest part of the attack because it requires gaining privileged access to a domain controller. Once an adversary is able to log on interactively or remotely to a DC, they can use Mimikatz to extract the required information using the following commands:

```
privilege::debug  
lsadump::lsa /inject /name:krbtgt
```

This will output the password hash, as well as the domain name and SID:




Step 2. Create Golden Tickets.

Now the hacker can create Golden Tickets at will. Useful Mimikatz parameters for creating Golden Tickets include:

- **User**— The name of the user account the ticket will be created. Note that this can be a valid account name, but it doesn't have to be.
- **ID**— The RID of the account the attacker will be impersonating. This could be a real account ID, such as the default administrator ID of 500, or a fake ID.
- **Groups**— A list of groups to which the account in the ticket will belong. Domain Admins is included by default so the ticket will be created with maximum privileges.
- **SIDs**— This will insert a SID into the SIDHistory attribute of the account in the ticket. This is useful to authenticate across domains.

The following example creates a ticket for a fake user but provides the default administrator ID. We will see in a moment how when these values come into play when this ticket is used. The **/ptt** (Pass the Ticket) trigger injects the Golden Ticket being created into the current session.

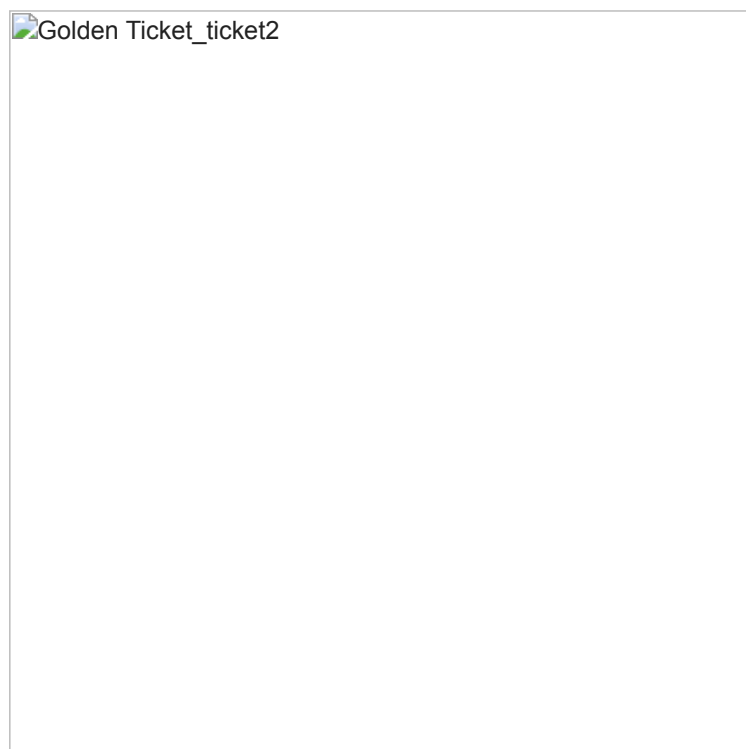
 Golden Ticket_ticket

Step 3. Pass the ticket.

Now it is time to use the Golden Ticket that was loaded into the current session. Let's launch a command prompt under the context of that ticket using the **misc::cmd** command.



You can see in the command prompt that the attacker operates as a regular domain user with no domain group membership, which means they should have no rights to any other domain computers.



However, because the Kerberos ticket is in memory, it's possible to connect to a domain controller and gain access to all of the files stored there.



Using PSEXec, the attacker can open a session on the target domain controller; according to that session, they are now logged in as Administrator.



The system believes the attacker is the Administrator because of the RID of 500 they used to generate the Golden Ticket. The event logs on the domain controller also show that system believes the attacker is the Administrator, but the credentials are the one that were spoofed during the Golden Ticket attack. This can be particularly useful for attackers looking to evade detection or create deceptive security logs.

Protecting against Golden Ticket attacks

Active Directory Golden Ticket attacks are very difficult to detect because Golden Tickets look like perfectly valid TGTs. However, in most cases, they are created with lifespans of 10 years or more, which far exceeds the default values in Active Directory for ticket duration. Although TGT timestamps are not recorded in the Kerberos authentication logs, proper [Active Directory security solutions](#) are capable of monitoring them. If you do see that Golden Tickets are in use within your organization, you must reset the KRBTGT account twice; doing so can have far-reaching consequences, so proceed with caution.

The most important protection against Golden Tickets is to restrict domain controller logon rights. There should be the absolute minimum number of Domain Admins, as well as members of other groups that provide logon rights to DCs, such as Print and Server Operators. In addition, a tiered logon protocol should be used to prevent Domain Admins from logging on to servers and workstations where their password hashes can be dumped from memory and used to access a DC to extract the KRBTGT account hash.