What is a Silver Ticket?

A Silver Ticket is a forged Kerberos service ticket (TGS) for one specific service, created with that service account's password hash rather than the KRBTGT key. It grants access only to that one service (a file share, database, or host), but it is stealthier than a Golden Ticket because the attacker never asks the Domain Controller for the ticket. It requires the target service account's hash, often obtained from a Kerberoast or an LSASS dump.

HOW IT WORKS

01 How it is forged and payload

The attacker needs the service account's hash, then forges the service ticket:

- Obtain the service-account hash (Kerberoast crack, or LSASS dump of a host running the service).
- Forge the TGS for the target service: `kerberos::golden /user:Administrator /domain:corp.local /sid:<SID> /target:host01.corp.local /service:cifs /rc4:<service-hash> /ptt` (Mimikatz Silver Ticket)
- Access the service (for example the file share) as the impersonated user.

Documented techniques shown for defensive context.

> QUIETER, NARROWER
>
> *Golden = whole domain, signed by KRBTGT, contacts the DC. Silver = one service, signed by that service hash, never contacts the DC. The silence is the danger.*

HOW TO DEFEND

- Use strong, machine-managed service-account passwords (gMSAs) so the service hash cannot be cracked from a Kerberoast.
- Protect host memory (Credential Guard, Protected Users) so service hashes are not dumped from LSASS.
- Enable host-based monitoring, since the DC sees nothing; the service host is where evidence lives.
- Limit service-account privilege so a forged ticket to one service is not also broad access.
- Rotate service-account passwords to invalidate older forged tickets.

SOURCES

[1] Microsoft: Kerberos Authentication Overview

[2] MITRE ATT&CK Enterprise Matrix

[3] NIST SP 800-115 Technical Guide to Security Testing

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-a-silver-ticket

Open online