What is a Kerberos ticket?

A Kerberos ticket is an encrypted proof of identity issued by a Domain Controller so a user can access services without sending their password. There are two kinds: the Ticket Granting Ticket (TGT), issued at logon and used to request other tickets, and the service ticket (TGS), which grants access to one specific service. The TGT is signed with the KRBTGT key and the TGS with the service account's key, and those two facts explain most Active Directory ticket attacks.

HOW IT WORKS

01 Why tickets matter to attackers

Every ticket attack flows from how these are signed:

- Kerberoasting abuses that a TGS is encrypted with the service account hash, so the attacker requests one and cracks it offline (`GetUserSPNs.py -request`).
- AS-REP Roasting abuses accounts that skip pre-authentication to get crackable material before logon.
- Golden Ticket forges a TGT using the KRBTGT hash; Silver Ticket forges a TGS using a service hash.
- Pass-the-Ticket steals a real ticket from memory and reuses it.

Knowing which key signs which ticket tells you which secret each attack is really after.

> TWO KEYS TO REMEMBER
>
> *TGT is signed by KRBTGT. TGS is signed by the service account. Steal the KRBTGT key and you forge any TGT (Golden); steal a service key and you forge that TGS (Silver) or crack it (Kerberoast).*

HOW TO DEFEND

- Use gMSAs and strong service-account passwords so TGS encryption cannot be cracked (stops Kerberoasting and Silver Tickets).
- Protect the KRBTGT hash (Tier 0 discipline, regular rotation) to prevent Golden Tickets.
- Require Kerberos pre-authentication everywhere to stop AS-REP Roasting.
- Prefer AES over RC4 for ticket encryption.
- Protect ticket memory with Credential Guard to limit Pass-the-Ticket.

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-kerberos-ticket

Open online