What is Pass-the-Ticket?

Pass-the-Ticket (PtT) is an attack where an attacker steals a Kerberos ticket (a TGT or a service ticket) from a machine's memory and injects it into their own session to authenticate as the ticket's owner, no password or hash needed. It is the Kerberos counterpart of Pass-the-Hash. Tickets are harvested from LSASS with tools like Mimikatz or Rubeus, and a stolen TGT for a privileged user is a direct path to their access.

HOW IT WORKS

01 How it is done and payload

The attacker harvests tickets, then injects the one they want:

- Dump tickets from memory: `sekurlsa::tickets /export` (Mimikatz) or `Rubeus.exe dump`
- Inject a stolen ticket into the current session: `kerberos::ptt ticket.kirbi` (Mimikatz) or `Rubeus.exe ptt /ticket:<base64>`
- Act as the victim, for example requesting access to systems the stolen TGT allows.

Documented techniques shown for defensive context.

> TICKETS EXPIRE, BUT
>
> *A normal stolen TGT is limited by its lifetime, but a privileged TGT captured at the right moment, or a forged Golden Ticket, removes that limit. Treat any privileged ticket in memory as a credential to protect.*

HOW TO DEFEND

- Enable Credential Guard so tickets in LSASS cannot be read by ordinary admin-level tools.
- Add privileged users to Protected Users, which shortens ticket lifetimes and hardens Kerberos for them.
- Keep Domain Admins off ordinary machines so their tickets are never sitting in a workstation's memory.
- Limit ticket lifetimes and monitor for ticket export or injection activity.
- Detect abnormal Kerberos usage from unexpected hosts.

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-pass-the-ticket

Open online