AYI NEDJIMI Consultants

Golden Ticket : Attaque Kerberos Domain Admin Persiste

10 mai 2026 • Mis à jour le 17 mai 2026 • 22 min de lecture •

4503 mots • 62 vues •

Golden Ticket est une attaque de persistance Active Directory (MITRE T1558.001) qui consiste a forger un Ticket Granting Ticket Kerberos arbitraire en signant celui-ci avec le hash NTLM ou les cles AES du compte krbtgt du domaine. Revelee en 2014 par Benjamin Delpy via le module kerberos::golden de Mimikatz, elle exploite le fait que le KDC ne valide que la signature cryptographique du TGT, pas l'existence des comptes encodes. Le ticket forge confere une persistance Domain Admin pouvant atteindre 10 ans, survivant aux changements de mots de passe et aux desactivations. Ce guide entity-first detaille le fonctionnement Kerberos, la fabrication avec Mimikatz, Rubeus et Impacket ticketer.py, la difference avec Silver Ticket, la detection (Event 4769, Defender for Identity) et les mitigations (double rotation krbtgt, AES-only, T

Golden Ticket est une attaque de persistance Active Directory qui consiste à **forger un Ticket Granting Ticket (TGT) Kerberos arbitraire** en signant celui-ci avec le hash NTLM ou les clés AES du compte de service `krbtgt` du domaine. Référencée sous l'identifiant **T1558.001** dans le framework MITRE ATT&CK (catégorie *Steal or Forge Kerberos Tickets*, tactique *Credential Access*), cette technique a été révélée publiquement en 2014 par **Benjamin Delpy** via le module `kerberos::golden` de Mimikatz. Le Golden Ticket exploite une caractéristique fondamentale du protocole Kerberos d'Active Directory : le Key Distribution Center (KDC) ne valide pas l'existence ni le statut des comptes encodés dans un TGT — il vérifie uniquement la signature cryptographique réalisée avec la clé du compte `krbtgt`. Posséder ce hash permet donc à l'attaquant de fabriquer un ticket impersonnant n'importe quel utilisateur, avec n'importe quels groupes (Domain Admins, Enterprise Admins, Schema Admins), pour une durée arbitraire pouvant atteindre **dix ans**. Conséquence : un Golden Ticket forgé survit aux réinitialisations de mots de passe et aux désactivations de comptes, offrant une *persistance Domain Admin durable* tant que le hash krbtgt n'est pas régénéré deux fois consécutivement. Cette page entity-first détaille le fonctionnement Kerberos, les pré-requis (compromission krbtgt via DCSync), la fabrication avec Mimikatz, Rubeus et Impacket ticketer.py, la différence avec le Silver Ticket, la détection (Event 4769, anomalies, Defender for Identity) et les mitigations (rotation krbtgt double, AES-only).

Réponse sous 24h

Devis gratuit →