Steal or Forge Kerberos Tickets: AS-REP Roasting, Sub-technique T1558.004 - Enterprise

Archived: 2026-04-05 15:45:42 UTC

Adversaries may reveal credentials of accounts that have disabled Kerberos preauthentication by Password Cracking Kerberos messages.[1]

Preauthentication offers protection against offline Password Cracking. When enabled, a user requesting access to a resource initiates communication with the Domain Controller (DC) by sending an Authentication Server Request (AS-REQ) message with a timestamp that is encrypted with the hash of their password. If and only if the DC is able to successfully decrypt the timestamp with the hash of the user's password, it will then send an Authentication Server Response (AS-REP) message that contains the Ticket Granting Ticket (TGT) to the user. Part of the AS-REP message is signed with the user's password.[2]

For each account found without preauthentication, an adversary may send an AS-REQ message without the encrypted timestamp and receive an AS-REP message with TGT data which may be encrypted with an insecure algorithm such as RC4. The recovered encrypted data may be vulnerable to offline Password Cracking attacks similarly to Kerberoasting and expose plaintext credentials. [1][3]

An account registered to a domain, with or without special privileges, can be abused to list all domain accounts that have preauthentication disabled by utilizing Windows tools like PowerShell with an LDAP filter. Alternatively, the adversary may send an AS-REQ message for each user. If the DC responds without errors, the account does not require preauthentication and the AS-REP message will already contain the encrypted data. [1][3]

Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to Valid Accounts. [4]

Source: https://attack.mitre.org/techniques/T1558/004