Kerberoasting explained simply.

Kerberoasting is an Active Directory attack where a normal authenticated user requests a Kerberos service ticket (TGS) for any account that has a Service Principal Name (SPN). Part of that ticket is encrypted with the service account's password hash, so the attacker takes it offline and brute-forces the password with tools like Hashcat. It needs no elevated rights and triggers no failed-logon alarms, which is why service accounts with weak, non-expiring passwords are one of the most reliable footholds toward Domain Admin.

HOW IT WORKS

01 Why it is so effective

Three things make Kerberoasting a favourite:

- No privileges required. Any single domain account can request the tickets. One phished user is enough.
- It is quiet. The ticket request is normal Kerberos traffic and the cracking happens offline, so there are no failed logons or lockouts to alert on.
- Service accounts are weak. They often have passwords set years ago by a human, never rotated, and the account is frequently a member of a privileged group so it can do its job.
  A cracked service-account password can hand over high privileges directly.

02 What attackers look for

Not every SPN is worth cracking. Attackers prioritise:

- Accounts that are members of privileged groups (a kerberoastable Domain Admin is the jackpot).
- Accounts with old passwords (the `pwdLastSet` date gives it away).
- Accounts that still accept RC4 encryption, which cracks far faster than AES.

BloodHound flags kerberoastable accounts and shows which ones have a path to high privilege, so the attacker spends cracking time only where it pays.

HOW TO DEFEND

- Use Group Managed Service Accounts (gMSAs), where Windows manages a long, random, auto-rotating password no human can guess.
- For any remaining service account, set a long passphrase (25+ characters) so offline cracking is infeasible.
- Do not put service accounts in Domain Admins. Grant the minimum rights the service needs.
- Disable RC4 for Kerberos where you can, forcing the stronger AES encryption.
- Monitor for a single account requesting many service tickets in a short window.

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/kerberoasting

Open online