AS-REP Roasting.

AS-REP Roasting is an Active Directory attack against accounts that have Kerberos pre-authentication disabled. Normally the Domain Controller proves you know the password before issuing a ticket. With pre-auth off, the DC returns a response (the AS-REP) encrypted with the account's password hash to anyone who asks, so the attacker cracks it offline. Unlike Kerberoasting, it can be done without any valid credentials if the attacker can guess or list usernames, which makes the "do not require pre-authentication" flag a setting worth hunting down and removing.

HOW IT WORKS

01 How the attack works

The mechanics are short:

1. The attacker asks the Domain Controller for a ticket for a target user, skipping pre-authentication. 2. Because pre-auth is not required for that account, the DC replies with an AS-REP that contains data encrypted with the user's password hash. 3. The attacker takes that offline and cracks it, just like Kerberoasting.

Impacket's GetNPUsers and Rubeus can both find vulnerable accounts and pull the hashes. If the attacker has no credentials yet, they can still try a list of likely usernames, since the request itself needs no login.

02 How it differs from Kerberoasting

The two are cousins, and people mix them up:

- Kerberoasting targets accounts with an SPN (service accounts) and needs one valid domain account to request the tickets.
- AS-REP Roasting targets accounts with pre-auth disabled (often regular users) and can be attempted with no credentials at all if usernames are known or guessable.

Both end the same way: an offline crack of a password hash. Both are defeated by strong passwords, but the misconfiguration that enables AS-REP Roasting is unique to it.

HOW TO DEFEND

- Audit for the flag. Find every account with "Do not require Kerberos pre-authentication" set and remove it unless a documented legacy system truly needs it.
- Strong passwords on any account that must keep the flag, so an offline crack fails.
- Tier your accounts so that even a cracked legacy account is not also a privileged one.
- Monitor for AS-REP requests for accounts that do not require pre-auth, which are abnormal in a healthy domain.

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/as-rep-roasting

Open online