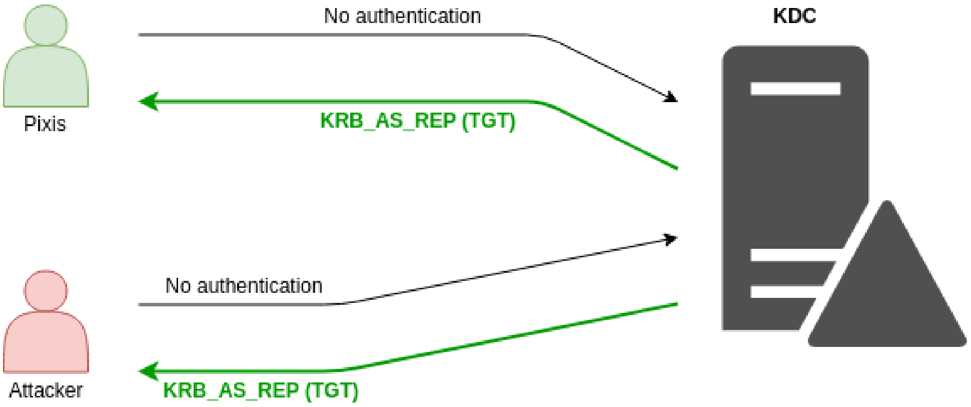
AS_REP Roasting - hackndo

en.hackndo.com/kerberos-asrep-roasting

Pixis

March 19, 2020



AS_REP Roasting

19 Mar 2020 · 4 min

In this post

Author : **Pixis**

When asking for a TGT, by default, a user has to authenticate himself to the domain controller in order to get a response. Sometimes, no authentication is asked before returning a TGT for specific account, allowing an attacker to abuse this configuration.

Preamble

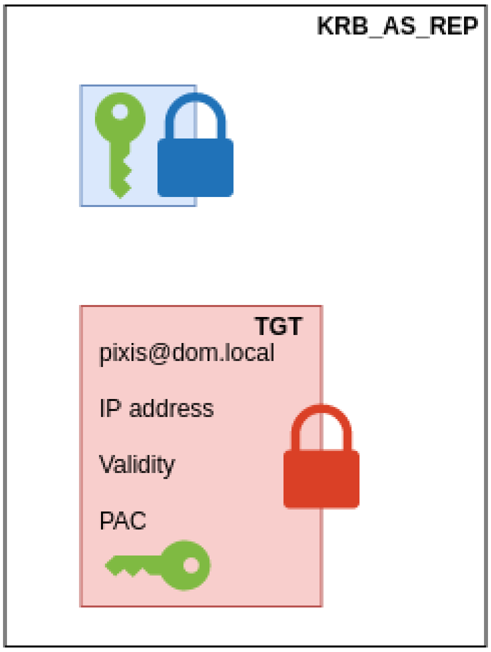
When we talk about TGT it’s often a language abuse, because we are talking about the KRB_AS_REP which contains the TGT (encrypted by the domain controller’s secret) and the session key (encrypted with the user account secret).

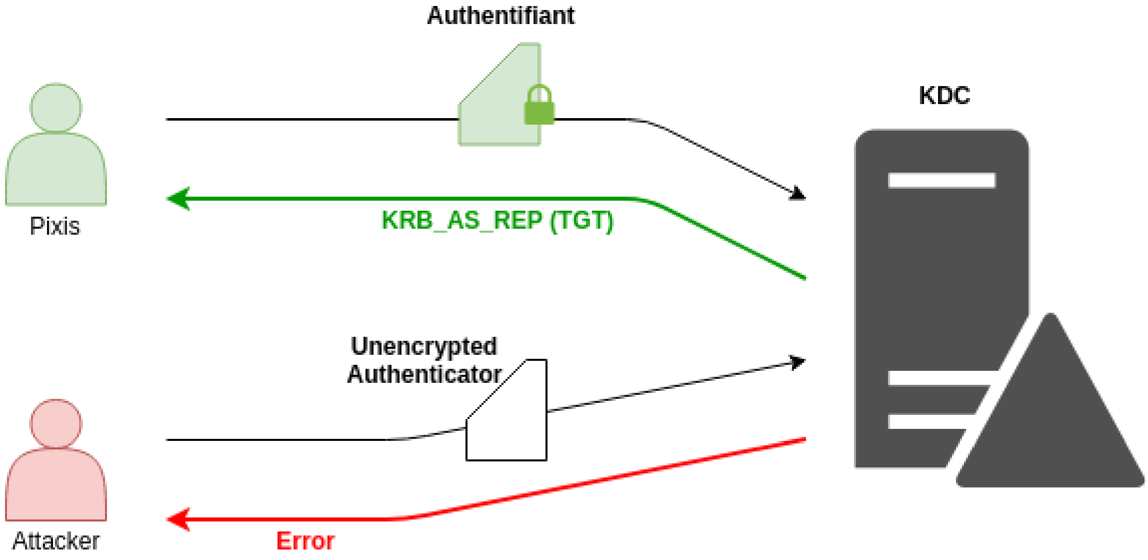
In this article, the TGT notion will refer to the TGT contained in the KRB_AS_REP response.

Pre-authentication

When we talked about how Kerberos works, it was highlighted that during the first exchange (KRB_AS_REQ - KRB_AS_REP), the client must first authenticate himself to the domain controller, before obtaining a TGT. A part of the response of the domain controller being encrypted with the client’s account secret (the session key), it is important that this information is not accessible without authentication. Otherwise, anyone could ask for a TGT for a given account, and try to decrypt the encrypted part of the response KRB_AS_REP in a brute-force way in order to recover the password of the targeted user.

That's why the user, in his KRB_AS_REQ request, must send an authenticator encrypted with his own secret in order for the domain controller to decrypt it and send back the KRB_AS_REP if it is successful. If an attacker asks for a TGT with an account he does not have control over, he won't be able to encrypt the authenticator correctly, therefore the domain controller will not return the desired information.

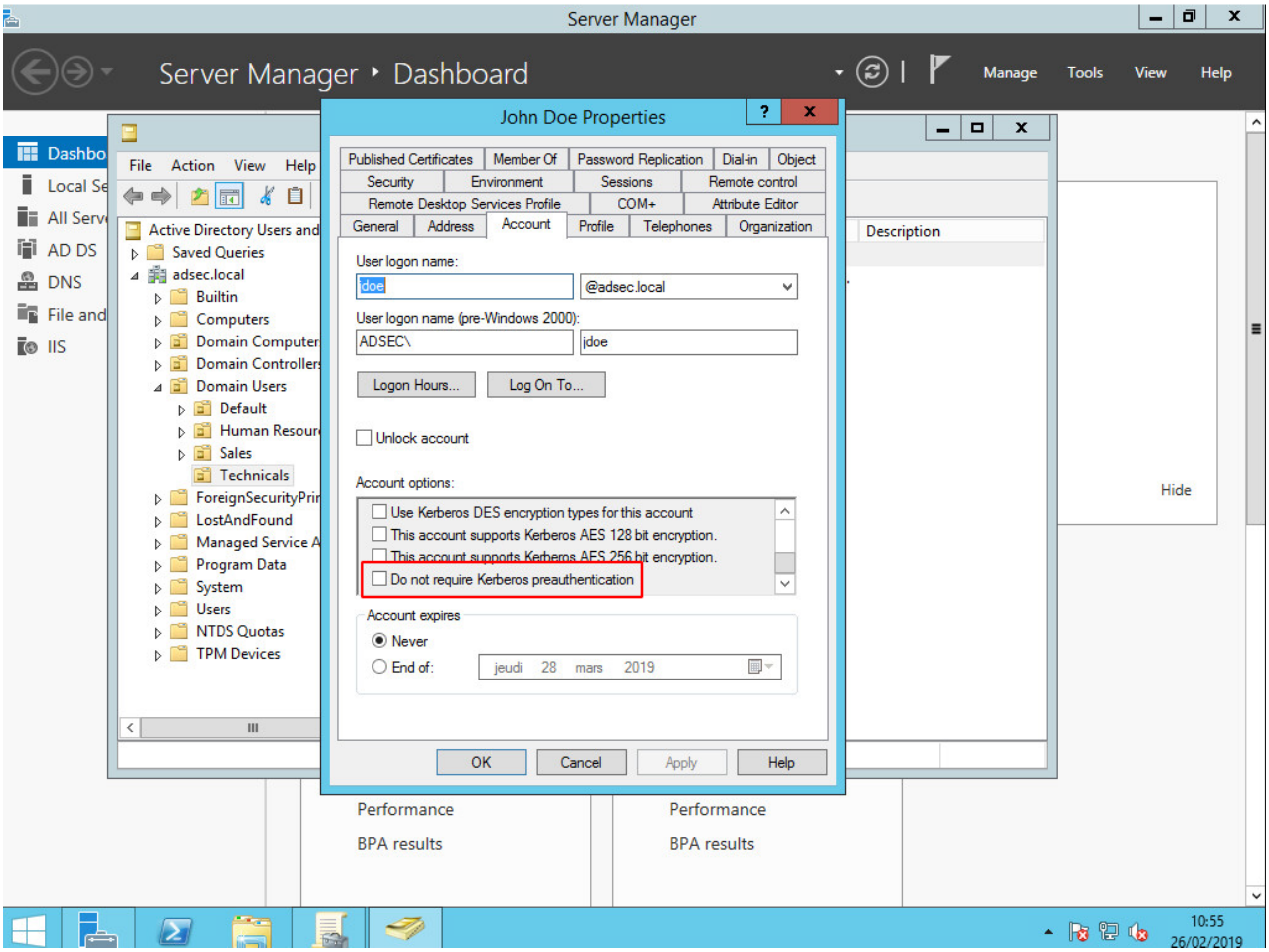




This is the default behavior, it protects the accounts against this offline attack.

KRB_AS_REP Roasting

However, for some strange reason (dark one though), it is possible to disable the pre-authentication prerequisite for one or more account(s).



User logon name: doe @adsec.local

User logon name (pre-Windows 2000): ADSEC\ jdoe

☐ Unlock account

Account options:

☐ Use Kerberos DES encryption types for this account
☐ This account supports Kerberos AES 128 bit encryption.
☐ This account supports Kerberos AES 256 bit encryption.
☐ Do not require Kerberos preauthentication

Account expires

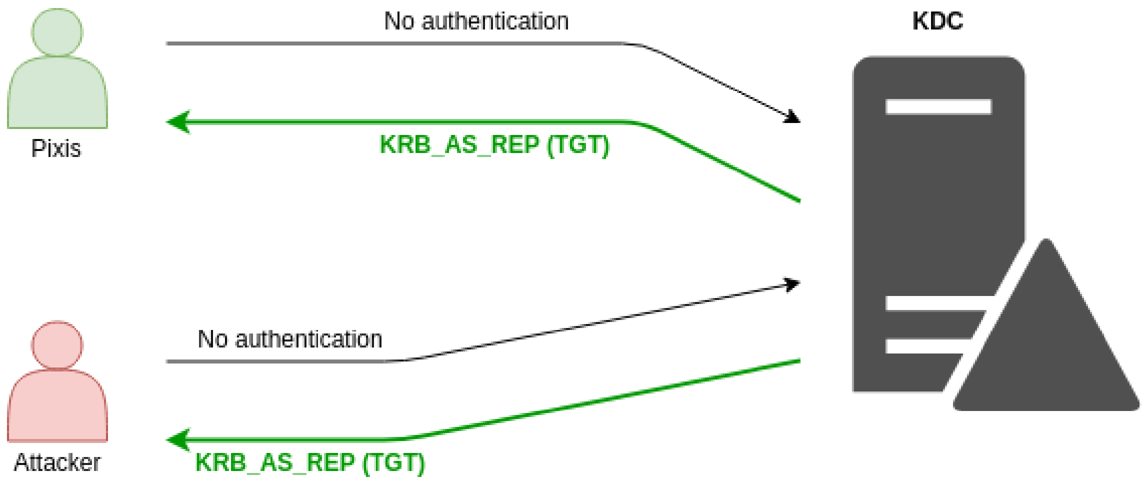
● Never
○ End of: jeudi 28 mars 2019

For example in this article, the author states that in order to benefit from SSO on a database hosted on a Unix server, he has to disable the pre-authentication for the user. It remains a very rare case, and even cptjesus and Harmj0y don't really have an answer.

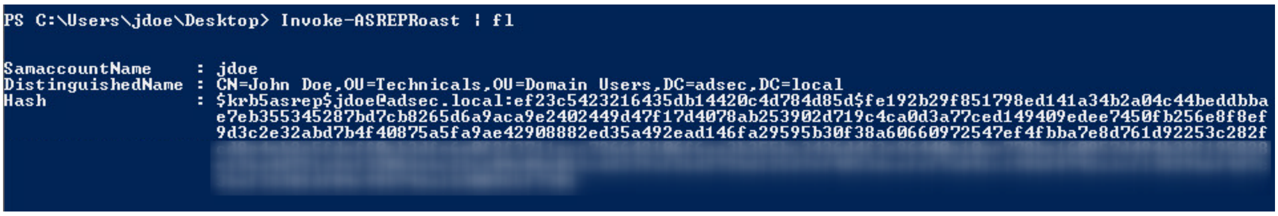
> cptjesus > As far as why its disabled, I couldn't tell you

> Harmj0y > I honestly don't really know why it would be disabled, just have heard from a people about the linux/"old" angle.

Anyway, if this option is disabled, anyone could ask for a TGT in the name of one of these accounts, without sending any authenticator, and the domain controller will send back a KRB_AS_REP.



This can be done with the ASREPRoast tool of @Harmj0y or more recently with Rubeus using `asreproast` functionnality.



```
PS C:\Users\jdoe\Desktop> Invoke-ASREPRoast | fl

SamaccountName    : jdoe
DistinguishedName : CN=John Doe,OU=Technicals,OU=Domain Users,DC=adsec,DC=local
Hash              : $krb5asrep$jdoe@adsec.local:ef23c5423216435db14420c4d784d85d$fe192b29f851798ed141a34b2a04c44beddbba
                    e7eb355345287bd7cb8265d6a9aca9e2402449d47f17d4078ab253902d719c4ca0d3a77ced149409edee7450fb256e8f8ef
                    9d3c2e32abd7b4f40875a5fa9ae42908882ed35a492ead146fa29595b30f38a60660972547ef4fbba7e8d761d92253c282f
                    [redacted]
```

There is also impacket GetNPUsers.py tool that can perform this operation.

Once in possession of the domain controller response KRB_AS_REP, the attacker can try to find out the victim's clear text password offline, by using John The Ripper with the `krb5asrep` mode, or with hashcat for example.

Conclusion

This technique, also described in an article wrote by Harmj0y, is a way to retrieve a clear text password within an Active Directory environment **when you don't have any foothold**. But if you don't have any account yet, it can be difficult to find out this information as you are not able to talk with the domain controller. An OSINT phase can be useful to enumerate as many valid account as possible, and try this attack on every account you found.

If any account is set up so that it does not need a pre-authentication, an attacker could simply ask for a TGT for this account and try to recover its password. With powerful machine, the cracking speed can be really huge. However, you should be aware that accounts without the necessary pre-authentication required are pretty rare. They can exist for historical reason, but kerberoasting is still more widespread.