Kerberos Pre-Authentication: Why It Should Not Be Disabled

By Archiveddocs

Archived: 2026-04-06 02:50:58 UTC

The Key Distribution Center (KDC) is available as part of the domain controller and performs two key functions which are: Authentication Service (AS) and Ticket-Granting Service (TGS)

By default the KDC requires all accounts to use pre-authentication. This is a security feature which offers protection against password-guessing attacks. The AS request identifies the client to the KDC in plain text. If pre-authentication is enabled, a time stamp will be encrypted using the user's password hash as an encryption key. If the KDC reads a valid time when using the user's password hash, which is available in the Active Directory, to decrypt the time stamp, the KDC knows that request isn't a replay of a previous request.

When you do not enforce pre-authentication, a malicious attacker can directly send a dummy request for authentication. The KDC will return an encrypted TGT and the attacker can brute force it offline. Upon checking the KDC logs, nothing will be seen except a single request for a TGT. When Kerberos timestamp pre-authentication is enforced, the attacker cannot directly ask the KDCs for the encrypted material to brute force offline. The attacker has to encrypt a timestamp with a password and offer it to the KDC. The attacker can repeat this over and over. However, the KDC log will record the entry every time the pre-authentication fails.

Thus, Kerberos pre-authentication can prevent the active attacker. However, it does not prevent a passive attacker from sniffing the client's encrypted timestamp message to the KDC. If the attacker can sniff that full packet, he can brute force it offline. To mitigate this problem, it is recommended that the users use lengthy passwords. Additionally, a good password rotation policy should also be implemented in the domain to make the offline brute-forcing infeasible or increasingly difficult.

I am sure that like me you too have seen many organizations (if not all) where this security feature of Kerberos pre-authentication is disabled for some (read many) users in order to support some applications that do not support the security feature offered by Kerberos pre-auth.

Should you continue using those applications in your domain? Let’s debate this some other time.

One of the challenges is that while one can find out if Kerberos pre-authentication security feature is disabled for user accounts in the domain, it is almost impossible to list exactly all those user-accounts without constructing one LDAP filter and using the same in a script or tool.

This encouraged me to write this wiki post to inform you all that I have written a script that can be used to find out and enlist all user accounts in the domain for which Kerberos pre-authentication has been disabled.

Please refer to the link below from where the script can be downloaded.

http://gallery.technet.microsoft.com/scriptcenter/List-All-User-Accounts-For-36823486

Wishing you a happy experience while you are using the script. Have a nice day. Cheers!!

Additional Reference About Kerberos Pre-Authentication

** **

Extensible Pre-Authentication in Kerberos

http://www.acsac.org/2007/papers/30.pdf

How the Kerberos Version 5 Authentication Protocol Works

http://technet.microsoft.com/en-us/library/cc772815(v=ws.10).aspx

Kerberos Protocol Tutorial

http://www.kerberos.org/software/tutorial.html

Kerberos Explained

http://technet.microsoft.com/en-us/library/bb742516.aspx

Changes in default encryption type for Kerberos pre-authentication on Vista and Windows 7 clients cause security audit events 675 and 680 on Windows Server 2003 DC's

http://blogs.technet.com/b/instan/archive/2009/10/12/changes-in-default-encryption-type-for-kerberos-pre-authentication-on-vista-and-windows-7-clients-cause-security-audit-events-675-and-680-on-windows-server-2003-dc-s.aspx

RC4 pre-authentication failure for the Network Service account in Windows Server 2008 R2 or in Windows 7

http://support.microsoft.com/kb/2566059
