

SAMR Interface Calls and Active Directory

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-03/msg00237.html>

- *From:* sarshah20@xxxxxxxxxx
 - *Date:* 29 Mar 2006 05:16:53 -0800
-

Hi,

This is a repost of the message that i earlier posted on different forums but unfortunately there was no response. May be i made it look too complicated.

To put it simply, the question was related to domain Security Account Manager (SAM). In Windows 2000/2003/XP, domain SAM does not exist (not used) anymore. It is replaced by Active Directory. But, for the aforementioned OS, local SAM still exists.

Everything was fine until when i setup a Windows 2000 domain controller and made a Windows 2000 Client to join it. I used a network packet capture utility to capture the packets that were exchanged during the process of joining the domain controller. The packet capture for this activity showed a number of SAMR calls. Now if the domain SAM does not exist for Windows 2000 (and above) then why there are SAMR calls made when joining a domain. I observed the same behavior for another scenario where accessing user account on the domain controller was involved. Why SAMR interface calls are being used? What is the role of SAMR calls here? Can someone shed some light on this?

Thanks for your help. The original post is as follows:

=====

I have a slight confusion regarding SAM and Active Directory. From the research that i have conducted so far, among other things, i have found out that SAM DB was used up till windows NT 4 and after that it was replaced with Active Directory (Windows 2000/Windows 2003). A local SAM DB is still maintained on these systems.SAMR are the interfaces used to access SAM DB and LDAP is used to access contents of Active Directory (not sure about LDAP). I also know that in order to maintain backward compatibility, SAMR interfaces are still being supported. This implies that if for example, in a domain, Windows NT 4 based client is joined to a server which is running W2k or W2k3 then SAMR interfaces are used. Everything seemed fine untill the point when i took some captures on the wire (using a network protocol analyzer). What i did was i setup a windows 2000 domain controller. Then i made a windows 2000 based client to join that domain. While analyzing the network capture, i found out

SAMR Interface Calls and Active Directory

that several SAMR interface calls are being made. This is quite confusing considering the fact that for W2k and above ActiveDirectory is being used and perhaps LDAP calls were suppose to be made instead of SAMR calls. So the questions that i have are:

- Is SAMR a legacy interface/protocol and only being kept for backward compatibility?
- Active Directory is a successor to SAM DB. Is LDAP a successor to SAMR?
- Why there are SAMR calls even when Windows NT 4 is not being used at all in the scenario as mentioned above? Or in other words if in Windows 2000 and above, Active Directory is being used then why SAMR calls are being used?

=====

sarshah.

.