

Re: Inserting Raw SID Into User Group

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-02/msg00090.html>

- *From:* Jan Hugo Prins <jhp@xxxxxxxxxxxx>
 - *Date:* Fri, 17 Feb 2006 17:33:41 +0100
-

On Mon, 13 Feb 2006 20:31:03 -0800, Will wrote:

On a computer that was hacked I have a user who created a raw SID in the Administrator's group that doesn't appear to correspond to any forest on our network. Before I retire the machine and rebuilt it, I would like to add the SID in question to a group that is denied access to any resources on the computer. But I can't add in raw SID's in the User and Computers AD administration application. Does anyone know how to put a raw SID into a group? The hacker knew how to do it, apparently. :)

I think the only reason you see a raw SID is because your system is not able to find what the name is that belongs to this SID. This SID is probably a SID that belongs to the machine or network of the hacker. That is also the reason that he was able to at is to your ACL, he was able to resolve it. He did not at a raw SID but he just added his account.

Jan Hugo

.