Laptop User Not Authenticating in an NT Domain After Changing Password

Thursday, September 28th, 2006

I just spent a ton of time figuring this one out, so maybe it will help someone else out there doing a Google search (which is kind of the point of everything on this blog). We had a user with an XP pro laptop who changed his password one morning (it was going to expire soon). Later he noticed that none of his drives were mapped, and that his Outlook client not connecting properly. Normally the problem in this scenario is **cached logon credentials**. When you change your domain password, the laptop doesn't cache your credentials until the next time you log in. So, to ensure that they get cached properly, you need to log out and log back in again using your new password while still connected to the domain network (i.e., do this before disconnecting the laptop and bringing it home). Now, we reset the password several times and it still didn't work. A capture of all network packets during the login (using Ethereal on the server) showed that the Kerberos authentication was failing but of course didn't say why. Articles and mailing lists found while googling for an answer suggested the following:

- **Edit the Registry to disable caching of credentials** (info found here[1], scroll down towards the middle): this didn't work for me, I think because it doesn't actually remove the cached credentials.
- **Manually map a drive using NET USE to authenticate**: This idea was found on this page[2] (first item on the list) which seems to contain a lot of good info but it really turned out not to be helpful. In this case I was able to map drives manually using this method but this didn't trigger a re-caching of the credentials, thus in the end the windows login still was not authenticating the session into the domain. Bzzt!
- Some loser somewhere even claimed the problem for him had been a bad network cable, even though (like me) he was still able to get an IP address and browse the web. Umm, yeah.

Solution: I finally found out where the cached credentials arew actually stored: Go to Control Panel → User Accounts → Advanced tab → Manage Passwords. In this case I found

1. http://www.irongeek.com/i.php?page=security/cachecrack
2. http://www.chicagotech.net/domainfaqs.htm

that there was a saved username/password combo stored for the domain controller. I deleted it, logged out, and logged back in again, and it worked.