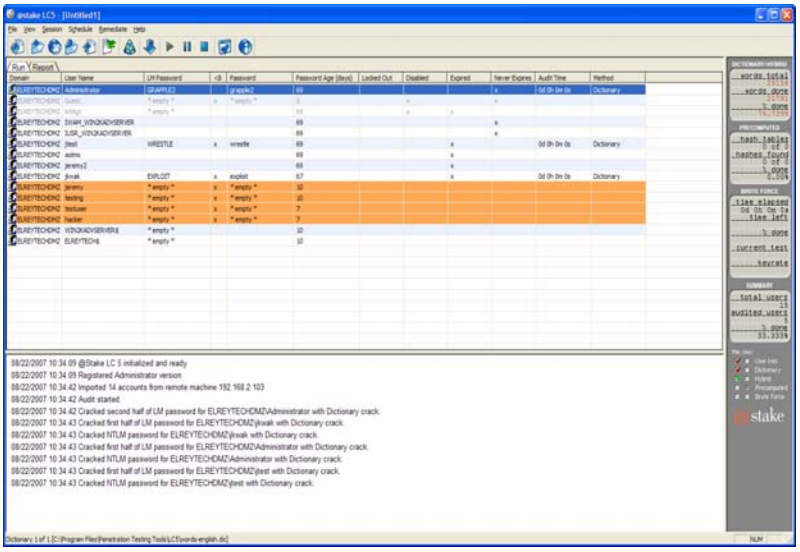
SNODGRASS
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Password Security

As IT examiners, Snodgrass always recommends using the strongest available password security settings as a means of deterring attacks on your network. Recently, Microsoft strenghtened its suggested password requirements to a minimum password length of 8 characters. Snodgrass has determined, however, that this new recommendation may be flawed, as discussed in this article.

Two Types of Windows Hashing Algorithms Used



Microsoft Server Operating Systems (beginning with Microsoft Server 2000) store two different types of password hashes for each password that is created on the network. These two algorithms are the LM (Lan Manager) hash and the NTLM (NT Lan Manager) hash. The NTLM hash is a "pure" hashing algorithm, meaning that the original password is not modified prior to the hash (generally making it harder to calculate when attempting to "crack" the password). The LM hash first truncates all passwords to 14 characters, converts each letter used to an uppercase letter, and then performs the hashing algorithm on the first 7 characters separately from the second 7 characters. This algorithm allows for two weak processes that could allow for an easier password compromise during a "cracking" attempt.

Implications of Storing LM Hashes

From a password "guessing" standpoint, 8-character passwords are always harder to guess than passwords with fewer characters. From a password "cracking" standpoint, however, if an LM hash is stored on the network, the password can be significantly easier to crack once you reach a password length over 7 characters. During training conducted by InfoSec Institute, it was pointed out that good password-cracking tools will always try first to "crack" that last digit (because, as noted above, it will put the first 7 digits into the first hash and the last digit of an 8-character password into the second hash). Once it has cracked that last digit, it is usually significantly faster at cracking the first 7 characters. In addition, the fact that the LM hash always converts letters to uppercase before hashing the password limits the number of combinations that need to be attempted before finding the correct one. For that reason, an 8-character password is potentially less secure than a 7-character password from a password-cracking standpoint. The screen-shot above shows a very common password cracking tool at work finding LM hash passwords.

Why the Need for Two Stored Hashes

The storing of the weaker LM hash was intentionally left within the Windows 2000 and Windows 2003 server environments as a means of reverse compatibility with older operating systems that did not support the NTLM hash. Windows 95, Windows 98, and Windows NT require these LM hashes to be stored locally on the server in order for a client machine using these older operating systems to be allowed authentication to the network. Snodgrass does not recommend the use of these older unsupported operating systems on your network. If your network does not utilize these older unsupported operating systems, there should be no need for the storing of the LM hash.

How to Disable the Storing of LM Hashes

There are two ways to disable your network from storing LM hashes. These methods must be completed on EACH active directory server in order to accomplish the full disabling of these hashes.

Method #1

Upon setting up a Windows 2003 server, you are asked whether the server should be in native mode or mixed mode. Choosing MIXED mode allows the server to store LM hashes on the network to allow for older operating systems. Choosing NATIVE mode will disable the storing of LM hashes on the network and will prevent older clients from authenticating.

Method #2

The second option is to navigate to the following location in the registry:

Start->Run->”regedit”->enter

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\NOLMHASH

Once at this registry setting, you should change the default value of a zero to a one. A setting of one disables the future storing of LM hashes. Note that this disables the FUTURE storing of LM hashes. The LM hash for the current passwords will remain on the server. At first glance, this may appear to be another security concern, but once your password expiration threshold has been achieved and all users have changed their passwords, the storing of older LM hashes can throw off an attacker. As some password-cracking tools would have no way of knowing that an LM hash was current or older, a poor password-cracking tool may successfully find these old LM hashes and crack them, but, because they are not current passwords, it has just wasted the attacker’s time.

Password security should be one control among many logical access controls to protect your network and its data. As password-cracking tools become more and more complex, additional controls to protect your customer data should be established.

If your organization would like to learn more about password controls, please contact our Technology Services Practice (Andrew Olmo, Principal, or Jeremy Burris, Senior IT Audit Consultant) at 724-934-0344.