

## Real-World Scenario 12-3: Defending Against Password Cracking

It's been said over and over again that weak passwords can easily be cracked. Plenty of free tools available on the Internet can crack a weak password in a matter of seconds.

**Scenario:** You are in charge of a small peer-to-peer Windows network where people configure their own passwords on computers that have no other configured security than the out-of-the-box security that comes with the operating system. Your task is to test the users' passwords and set up a way to enforce the use of complex passwords. You are not allowed to know the current user passwords (unless of course you can crack them!).

Use freely downloadable tools to test accounts (and their passwords). Then define what a complex password is. Finally, explain how you can enforce whether people use complex passwords.

## Real-World Scenario 12-3 Solution

*Remember to perform these types of tests on a closed network that you are allowed to have access to.*

Passwords can be very unsecure out-of-the-box. An account is generally configured with no password by default. In addition, different operating systems have different ways of hashing the password. In fact, in Windows there are multiple ways of hashing, depending on the Windows version and several other factors. (Hashing is discussed later in the book.) Aside from the lack of default security, users often select very simple passwords such as *love*, *secret*, or the best one, *password*. Those passwords are just about as good as using no password at all. For example, a four-character password can be cracked by today's password-cracking programs in a matter of seconds.

You can download plenty of tools for free and use them to check the quality of users' passwords; for example, ophcrack, Cain & Abel, and RainbowCrack. Try some of these programs on a closed network (and a clean machine) and see how they function. You will see that they are designed to use various password-cracking methods (brute force, for example) that are very good at breaking LM and NTLM password hashes in Windows.

In many networks, chances are you will find a lot of non-complex passwords—ones that can be cracked very easily. How do you fix this? Do the following:

- Give the administrator account a complex password. (Also consider making a secondary administrator account—with a complex password—and disabling the original admin account.)
- Disable generic accounts and give them complex passwords.
- Set up a policy that governs the type of password that users can choose.

Now, that last bullet will vary depending on the type of network. In a small peer-to-peer network that has, say, five or six Windows computers, the policy would have to be configured on one machine, then exported, and imported to the rest of the computers. In this scenario you would go to Run and type **secpol.msc**. That displays the local security policy, and from there you would access Account Policies > Password Policy, where you would enforce complexity and a minimum password length. In a larger network, such as a Windows domain, you would configure the policy based on the OU in question, and/or use the gpedit.msc utility.

**Video Solution:** Watch the video solution “12-3: Defending Against Password Cracking.”