

FOCUS on Microsoft: Securing NT - Choosing Strong Passwords

Eric Schultz 2000-12-28

Why 7 is better than 8

Discussions of password length may seem rather passe these days. Internal and external auditors have long suggested the use of lengthy passwords to help fortify the primary authentication mechanism in today's Operating System. Crypto details aside, it would make sense that longer may be better, and the auditors agreed. Their older recommendations of six character passwords have been updated to reflect new times - eight is now the standard recommendation. In some cases, you may hear cause for an even longer password, as long as users won't be tempted to write it down. Unfortunately, the 6/8+ recommendation was pushed forth prior to the rise in popularity of LanMan, OS/2 and Windows NT.

Where longer may be better in the Unix world, longer passwords in NT may actually decrease the 'strength' of one's password. Passwords in NT environments are stored in two separate fashions. NT hashes (used mainly for NT to NT authentication) are created using an MD4 algorithm, while the LanMan hashes (used for Win9x and other non-NT client authentication) are created using a known constant in its hashing algorithm. (For a technical discussion of NT passwords, check out [LOpht's paper](#) on the crypto behind NT passwords.) It is this LanMan hash that creates the need for special length passwords.

A LanMan hash is made by taking the user's password and converting it to all uppercase, padding it (or truncating it) to 14 characters, splitting it into two seven character halves, hashing each half with a known constant, and concatenating the results to form 16 bytes of the one way function (OWF) hash. What does this mean? In short, a seven character password is a seven character password, but a 12 character password is a seven character password plus a five character password. When run through a 'brute force password guesser' such as [LOphtcrack](#), each half can be cracked independantly. While the seven character first half may take weeks or months to crack, the five character second half of the password may crack within hours (depending upon the chosen character set).

You may ask "Isn't a seven character password plus a five character password (12 characters total) stronger than just a seven character password?". In some cases, yes, in most, no. Considering the latter, the 8-12th characters can usually give the malicious password cracker enough information to 'guess' the first half of the password. Consider the following 13 character password: LukeSkywalk3r The upper case letters do not pose a problem as all the characters

are made uppercase during the LanMan hashing routine. The last 6 characters 'walk3r' will 'crack' in a few hours via L0phtcrack using the alpha-numeric character set. Having cracked this half, it may be possible to make educated guesses as to the first seven characters of the password.

In a similar scenario, let's examine an organization who's implemented the passfilt.dll (to enforce complex passwords) and an audit-recommended eight character password length minimum. The passfilt routine demands the password contain three of the following four character sets: lower case alpha, upper case alpha, numbers, and special characters. Of the 100 users, 80 of them will probably put the special character at the end of the password. ie. Pirates1 or Rockets* When these passwords are run through a cracker (with a full character set), anything after the seventh character will be cracked almost instantly - in this case, the 1 and * will be visible. Of the 80 passwords with the special character at the end, 75 of them will probably contain alpha-only characters in within the first seven characters. Resetting L0phtcrack to run with alpha or alpha numeric sets only will hash and compare all variations of the character set within 24 to 48 hours. Once the first half and second half password 'guesses' are combined, the probable 75 passwords are 'decrypted'.

Had the organization enforced only seven character password lengths, we might assume that 75-80 users would select passwords exactly seven characters long. This would immediately rule out guessing the first half based on the context of the second half (as described earlier) for these users. Those who selected non alpha-numeric characters within the first seven characters of their password would prevent a tool such as L0phtcrack from cracking the password quickly.

Suggestions for Stronger Passwords

- Make your password exactly seven or 14 characters long
- Do not use known words or usernames in your password
- Include special characters (!@#\$\$%*) and numbers in each seven character half
- To really increase password strength, use a non-printable ascii character within the first seven characters. ie. within the password 'secret' embed an alt character secret where you hold down the ALT key while pressing the 1,2, and 9 keys on the numeric keypad. NOTE: for laptop users, you'll have to activate numlock and use the j,k,l,u,i,o keys that correspond to the numeric keypad
- SPECIAL BONUS HINT: If you have an account called 'test' and it's an administrator level account, don't give it a password of 'test'. (*Don't laugh, this happens more than you'd*

like to know)

Relevant Links

[Security Watch Article on NT Password Lengths](#)

Stuart McClure and Joel Scambray

[A L0phtCrack Technical Rant](#)

Mudge

[Privacy Statement](#)

Copyright 2006, SecurityFocus