NAME

smbpasswd - The Samba encrypted password file

SYNOPSIS

smbpasswd

DESCRIPTION

This tool is part of the **samba**(7) suite.

smbpasswd is the Samba encrypted password file. It contains the username, Unix user id and the SMB hashed passwords of the user, as well as account flag information and the time the password was last changed. This file format has been evolving with Samba and has had several different formats in the past.

FILE FORMAT

The format of the smbpasswd file used by Samba 2.2 is very similar to the familiar Unix passwd(5) file. It is an ASCII file containing one line for each user. Each field within each line is separated from the next by a colon. Any entry beginning with ’#’ is ignored. The smbpasswd file contains the following information for each user:

name
: This is the user name. It must be a name that already exists in the standard UNIX passwd file.

uid
: This is the UNIX uid. It must match the uid field for the same user entry in the standard UNIX passwd file. If this does not match then Samba will refuse to recognize this smbpasswd file entry as being valid for a user.

Lanman Password Hash
: This is the LANMAN hash of the user’s password, encoded as 32 hex digits. The LANMAN hash is created by DES encrypting a well known string with the user’s password as the DES key. This is the same password used by Windows 95/98 machines. Note that this password hash is regarded as weak as it is vulnerable to dictionary attacks and if two users choose the same password this entry will be identical (i.e. the password is not "salted" as the UNIX password is). If the user has a null password this field will contain the characters "NO PASSWORD" as the start of the hex string. If the hex string is equal to 32 ’X’ characters then the user’s account is marked as **disabled** and the user will not be able to log onto the Samba server.

  WARNING !! Note that, due to the challenge-response nature of the SMB/CIFS authentication protocol, anyone with a knowledge of this password hash will be able to impersonate the user on

the network. For this reason these hashes are known as *plain text equivalents* and must *NOT* be made available to anyone but the root user. To protect these passwords the smbpasswd file is placed in a directory with read and traverse access only to the root user and the smbpasswd file itself must be set to be read/write only by root, with no other access.

NT Password Hash

This is the Windows NT hash of the user's password, encoded as 32 hex digits. The Windows NT hash is created by taking the user's password as represented in 16-bit, little-endian UNICODE and then applying the MD4 (internet rfc1321) hashing algorithm to it.

This password hash is considered more secure than the LANMAN Password Hash as it preserves the case of the password and uses a much higher quality hashing algorithm. However, it is still the case that if two users choose the same password this entry will be identical (i.e. the password is not "salted" as the UNIX password is).

WARNING !!. Note that, due to the challenge-response nature of the SMB/CIFS authentication protocol, anyone with a knowledge of this password hash will be able to impersonate the user on the network. For this reason these hashes are known as *plain text equivalents* and must *NOT* be made available to anyone but the root user. To protect these passwords the smbpasswd file is placed in a directory with read and traverse access only to the root user and the smbpasswd file itself must be set to be read/write only by root, with no other access.

Account Flags

This section contains flags that describe the attributes of the users account. This field is bracketed by '[' and ']' characters and is always 13 characters in length (including the '[' and ']' characters). The contents of this field may be any of the following characters:

- This means this is a "User" account, i.e. an ordinary user.

- This means the account has no password (the passwords in the fields LANMAN Password Hash and NT Password Hash are ignored). Note that this will only allow users to log on with no password if the *null passwords* parameter is set in the **smb.conf**(5) config file.

- This means the account is disabled and no SMB/CIFS logins will be allowed for this user.

- This means the password does not expire.

- This means this account is a "Workstation Trust" account. This kind of account is used in the Samba PDC code stream to allow Windows NT Workstations and Servers to join a Domain hosted by a Samba PDC.

Other flags may be added as the code is extended in future. The rest of this field space is filled in with spaces. For further information regarding the flags that are supported please refer to the man page for the pdbedit command.

Last Change Time

This field consists of the time the account was last modified. It consists of the characters ’LCT-’ (standing for "Last Change Time") followed by a numeric encoding of the UNIX time in seconds since the epoch (1970) that the last change was made.

All other colon separated fields are ignored at this time.

VERSION

This man page is part of version 4.16.11 of the Samba suite.

SEE ALSO

smbpasswd(8), **Samba**(7), and the Internet RFC1321 for details on the MD4 algorithm.

AUTHOR

The original Samba software and related utilities were created by Andrew Tridgell. Samba is now developed by the Samba Team as an Open Source project similar to the way the Linux kernel is developed.