How to Generate Encrypted Password Hashes with mkpasswd Command

Install mkpasswd in Linux

The 'mkpasswd' command is used to generate SHA-512 encrypted password hashes or password-based encryption keys to enhance the security of your Linux distribution.

To install mkpasswd on a Linux system, you can use the package manager specific to your distribution as shown.

```
$ sudo apt install whois          [On Debian, Ubuntu and Mint]
$ sudo yum install expect         [On RHEL/CentOS/Fedora and Rocky/AlmaLinux]
$ sudo emerge -a whois            [On Gentoo Linux]
$ sudo apk add mkpasswd          [On Alpine Linux]
$ sudo pacman -S whois           [On Arch Linux]
$ sudo zypper install whois      [On OpenSUSE]
```

Now that you've installed the "mkpasswd" command, let's dive into the syntax of this incredible utility.

```
$ mkpasswd [OPTIONS]... [PASSWORD [SALT]]
```

Let's break it down to get a better understanding:

- ListenpunktOptions (also known as "flags") – They are used to change the conduct/behavior of the command.
- ListenpunktPassword – This indicates the password for which an encrypted hash is to be generated.
- ListenpunktSalt – This is an optional value utilized in the process of encryption to enhance the security of the password hash.

To create a password hash, we require the "Type", "Password", and "Salt" parameters. In case any of these parameters are missing:

- ListenpunktType – Omitting the "type" parameter would lead to an error message. By using the **"mkpasswd —help"** command, you can list the password hash types.
- ListenpunktPassword – If the "password" parameter is missing, the command will prompt the user to enter the password.
- ListenpunktSalt – If the "salt" parameter is omitted, a random one will be selected based on the Linux distribution you are using.

To see the brief introduction along with the options and usage, you can type.

```
$ mkpasswd --help
```

How to Generate MD5 Password Hash With a Salt

The MD5 algorithm (which stands for Message Digest Algorithm 5) is a cryptographic hash function utilized to produce a hash value of 128 bits (16 bytes).

To create a specified password hash with a designated salt, you can employ the **'-m'** flag for the hash and the **'-S'** flag to provide the salt.

Let's execute the stated command to create the MD5 password hash with "UMsalt12" salt, for the password "UbuntuMintPassword".

```
$ mkpasswd -m md5 -S UMsalt12 UbuntuMintPassword

$1$UMsalt12$LYoVwI/Dt88Rsprd8cLuz0
```

From:
https://www.cooltux.net/ - **TuxNet DokuWiki**

Permanent link:
https://www.cooltux.net/doku.php?id=it-wiki:linux:create_linux_password_with_mkpasswd

Last update: **2024/02/05 12:12**