在 Linux 中产生、加密或解密随机密码

谢权 2015年5月24日 Awesome, Blog No Comments

安全是数字时代中的一个主要话题。在电脑，email，云端，手机，文档和其他的场合中，我们都会使用到密码。众所周知，选择密码的基本原则是“易记，难猜”。考虑过使用基于机器自动生成的密码吗？相信我，Linux 非常擅长这方面的工作。

1. 使用命令 **pwgen** 来生成一个长度为 **10** 个字符的独特的随机密码。假如你还没有安装 **pwgen**，请使用 **Apt** 或 **YUM** 等包管理器来安装它。

```
$ pwgen 10 1
```

生成一个独特的随机密码

一口气生成若干组长度为 50 个字符的唯一的随机密码!

```
$ pwgen 50
```

生成多组随机密码

2. 你还可以使用 **makepasswd** 来每次生成一个给定长度的独特的随机密码。在你把玩 **makepasswd** 命令之前，请确保你已经安装了它。如若没有安装它，试试使用 **Apt** 或 **YUM** 包管理器来安装 **makepasswd**这个软件包。

生成一个长度为 10 个字符的随机密码。该命令产生的密码的长度默认为 10。

```
$ makepasswd
```

使用 *makepasswd* 生成独特的密码

生成一个长度为 50 个字符的随机密码。

```
$ makepasswd  --char 50
```

生成长度为 *50* 的密码

生成 7 个长度为 20 个字符的随机密码。

```
$ makepasswd --char 20 --count 7
```

3. 使用带“盐”的 **Crypt**(注：这里应该指的是一个函数，可以参考这里) 来加密一个密码。提供手动或自动添加 “盐”。

对于那些不清楚 盐 的意义的人，这里的 “盐” 指的是一个随机数

据，它作为密码生成函数的一个额外的输入， 目的是保护密码免受词典攻击。

在执行下面的操作前，请确保你已经安装了 mkpasswd。

下面的命令将带 “盐” 加密一个密码。“盐” 的值是随机自动生成的。所以每次你运行下面的命令时，都将产生不同的输出，因为它每次接受了随机取值的 “盐”。

```
$ mkpasswd tecmint
```

使用 *Crypt* 来加密密码

现在让我们来手动定义 “盐” 的值。每次它将产生相同的结果。请注意你可以输入任何你想输入的值来作为 “盐” 的值。

```
$ mkpasswd tecmint -s tt
```

带 “盐” 加密密码

另外， mkpasswd 还是交互式的，假如你在命令中没有提供密码，它将主动询问你来输入密码。

4. 使用 **aes-256-cbc** 加密算法并使用带**“盐”**的密码**(**如 **“tecmint”)** 加密一个字符串**(**如 **“Tecmint-is-a-Linux-Community”)**。

```
# echo Tecmint-is-a-Linux-Community | openssl enc -aes-25
```

在 *Linux* 中加密一个字符串

在上面例子中， echo 命令的输出通过管道传递给了 openssl 命令，使得该输出通过加密编码方式(enc：Encoding with Cipher) 所加密，这个过程中使用了 aes-256-cbc 加密算法，并附带了密码 (tecmint) 和 “盐” 。

5. 使用 **openssl** 命令的 **-aes-256-cbc** 解密选项来解密上面的字符串。

```
# echo U2FsdGVkX18Zgoc+dfAdpIK58JbcEYFdJBPMINU91DKPeVVrUZ
```

via: http://www.tecmint.com/generate-encrypt-decrypt-random-passwords-in-linux/

Tagged on: linux password