

用户

第三讲 51:38

认证的过程

指纹 虹膜 字符串表示的密码

密码是让系统验证用户的

Linux 的密码信息放在哪？

放在文本文件中 SQL数据库 还是？放哪都行 但是 明文的密文可能存在泄露的安全

----- 所以加密之后再进行存储 来保证密码的安全性

如何保证密码的安全性？

(1). 密码 --- 叫密码 就不能明文存放

(2). 即使看到密文的结果 也不容易彻底破解

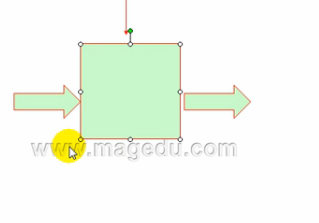
加密算法：常见的有三种

(1). 对称加密

使用密钥保证

盒子表示加密算法

左边是明文 右边是密文



其中 算法可以公开 所以 算法不能保证加密的数据的安全性----- 依靠密钥来保证加密的安全性

也就是加一个密钥进来 ---- 用算法 结合密码 把加密的数据打散成一堆乱码

所以 想还原到原来的样子 用**解密算法**

还是输入一个密码 再把密文还原成明文 ----- 这就是解密

这就是加密解密的过程

加密和解密都需要输入密码

\*加密和解密如果需要相同的密码 就叫做**对称加密**

\*如果加密和解密使用一对密钥中的一个 ---- 有些加密算法很特殊 一对密钥 一个是公钥(public key) 另一个是私钥(secret key)

----- 使用公钥解密的 只能使用与之对应的私钥解密

----- 反之 使用私钥加密的 只能使用对应的公钥解密

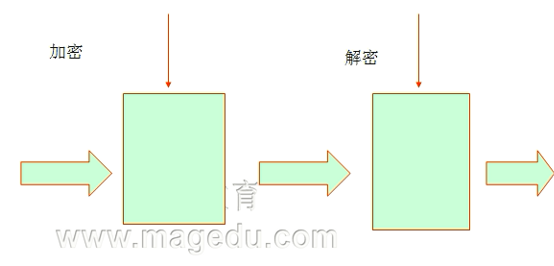
公钥 ---- 公开的 任何人都可以知道

私钥 ---- 不允许别人知道

----- 如果使用私钥加密 那么就用公钥就能解密 --- 公钥人人都可以知道 ----- 所以 人人都能解密 不安全

----- 如果使用公钥加密 那么只能使用使用自己的私钥进行解密

**----- 所以 我们使用公钥加密**

 ----- 非对称加密 也叫公钥加密技术

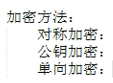
比如下一个ISO镜像 如何保证别人没有打开并且植入木马呢？会给出md5

在网站上提供光盘 下载下来 计算md5 和这个md5进行对比就可以了

但是 拿着md5是不能把光盘还原的

---- 比如拿到这个人的指纹 是无法还原这个人的 可以用来定位这个人

---- 这种加密技术不可逆 就叫做**单向加密技术**



单向加密的用处：对比两次加密是否一样 就知道是否被篡改（单向加密的用处）

所以 单向加密的特性：

(1). 输入一样 输出就一定一样

----- 比如光盘md5比对是否被篡改

----- 反过来 比如100G的数据 只要是有1bit不同 结果就有巨大的不同 ------ 这就叫**雪崩效应** 或者 **蝴蝶效应 ----- 这样避免了逆推**

(2). **定长输出**的效果

(3). **不可逆**



对称加密比较有名的：DES 数据加密标准 早起IBM研发 2000年就不行了 已经被破解

DES加密一轮再来一轮 3DES

AES 高级加密标准 AES有好多种变化 256 192 384等等 现在 256很常用





DSA只能用来认证 不能用来加密 RSA强大一点



MD5 --- message digest version 5 ----- 128位定长输出 ---通常是128/8 =16个字符 信息摘要 单向加密都定长 看到MD5是128/8 =16 还要转成ASCII 然后转换成二进制输出

SHA1 ---- secure hash algorithm 1 安全的哈希算法 --- 160位定长输出

这样md5更快 但是sha1更安全 因为sha1长度更长 出现相同的可能性更小 由于md5

\*\*\* 不算加密 算校验CRC32 ---- 循环冗余校验码 非常容易出现冲突（数据原来不一样 结果一样）

SHA256和SHA512 更加安全

SHA512就是无论你的输入啥样 输出一定是512定长

因此Centos5中 用户的密码加密是md5 但是在Centos6中 是 SHA512

---------

建立用户的时候 需要输入密码 这个密码信息库放在/etc/shadow下面 这个也成为影子口令



为什么不和用户名放在一块？ ---- 用户只能修改密码 不能查看

用户的密码尽可能安全 使用的是单向加密存放的

用户下次登录 如何验证？

加密之后 是不可逆的 ---- 就是把用户的输入再次加密 看看二者是否一样就可以了

但是 两个用户密码是一样的 ----- 这样加密的结果是一样的 这样其中任何一个用户查看到这个文件 发现自己的密码的密文和另一个用户的一样 就存在了风险 – 该怎么办？

只需要在用户输入密码的时候 输入点佐料 ---- 比如

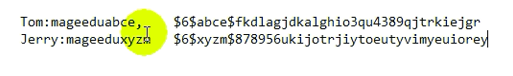
Tom输入密码 magedu 加入了abcd字符

Jerry输入的密码 也是magedu 但是随即加了 xyzm 这样 结果是不一样的

并记录的创建的时候 把这个佐料记住

下次登录的时候 虽然可能看到佐料 但是 看不到全部 因为是单项加密 所以无法逆推 因此安全

假设加密之后结果



密码本来是一模一样的 也可以看到佐料 但是 密文+佐料 不可以逆推 因为是单项加密 具有不可逆的特性

 --- 第一个$6是SHA512的标示 $1是md5的标示

佐料通常是8位的

因为单项加密 所以 定长输出

现在看一下

/etc/shadow只有管理员才有权限访问

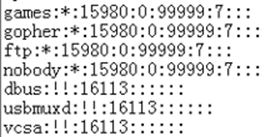


$6表示加密算法是SHA512 $CGsqab6d 这个8位是盐 也就是佐料 选中的部分就是512位的SHA512加密结果

如果是Centos5的话 就会短很多 因为使用的是md5

同一个系统 使用哪种算法都没关系 因为有前面的$6或者$1进行标示

同时发现很多用户是没有密码的 密码为空的用户不能登录系统 并且默认拒绝空密码用户登录



现在简单验证一下

md5sum和sha1sum这两个命令



复制了protocol 修改了一个井号



 ---- 输出的是十六进制的数字

 ---- 没有一位是一样的

所以 内容的微小变化 但是 输出的巨大变化 --- --- 雪崩效应 或者蝴蝶效应

这就是md5sum

下面验证一下sha1sum





这个也是十六进制的输出 不是ascII码

1:25:35