

4 口令破解技术



4 口令破解技术

- ◆ 随着网络应用的不断深入，在服务器或存储设备中甚至客户端都可能保存着大量的敏感信息或数据。为了保护这些敏感信息或数据不会丢失或者被恶意用户非法访问，网络用户往往会给这些服务器或存储设备进行口令加密。
- ◆ 口令的作用就是向系统提供唯一标识个体身份的机制，只给个体所需信息的访问权，从而达到保护敏感信息和个人隐私的作用。
- ◆ 在日常生活中，口令又称密码。事实上，两者是有差异的。**口令较为简单，密码则更为复杂、正式。密码是按照特定法则编成的，是在通信时对通信双方的信息进行明、密变换的符号。口令是与用户名对应的，被用来验证是否拥有该用户名对应的权限。例如，对于一台计算机上的账号来说，密码是一个变量，而口令则是一个常量。**

4 口令破解技术

- ◆ 使用口令也面临着很多安全问题。如果口令过于简单，则很容易被猜出。过于复杂的口令又将增加用户的记忆难度，而将其写下以防遗忘也会带来新的安全问题。

4 口令破解技术

- ◆ 主要内容

- 4.1 口令破解方式

- 4.2 口令破解工具

- ◆ Wi-Fi口令破解工具Aircrack-ng

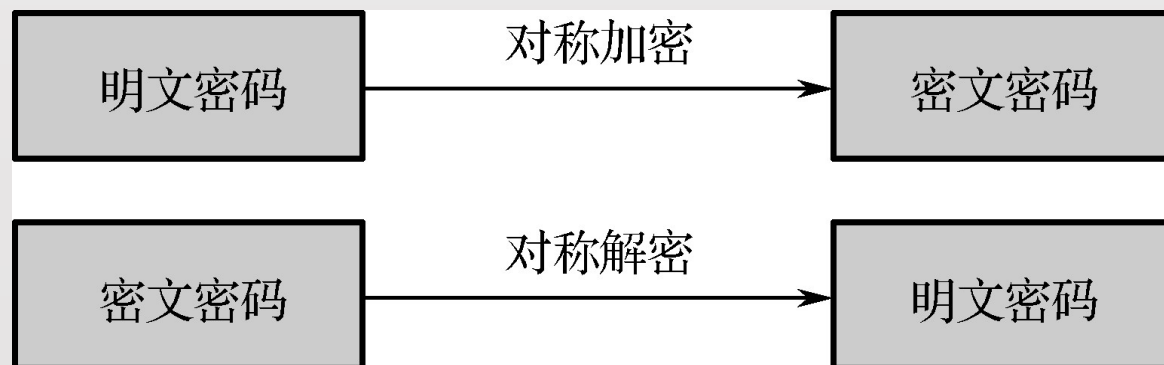
- ◆ Hydra破解Web

4.1 口令破解方式



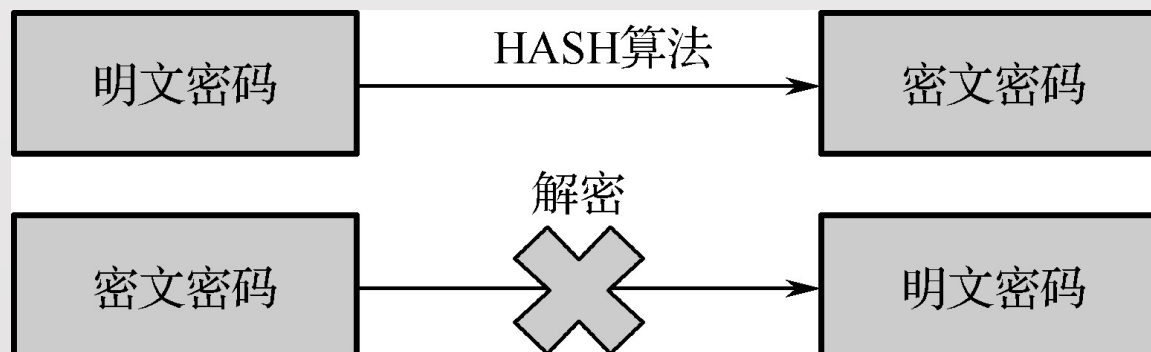
常见口令保存方式

- ◆ 在介绍口令破解的方式之前有必要了解口令的保存方式。
 - 1) 直接明文的保存。
 - 例如，用户设置的口令是“123456”，直接将“123456”保存在数据库中。
 - 2) 使用对称加密算法的保存方式
 - 使用3DES、AES等对称加密算法加密口令。但一旦密钥泄露，就可以通过解密来还原出口令。



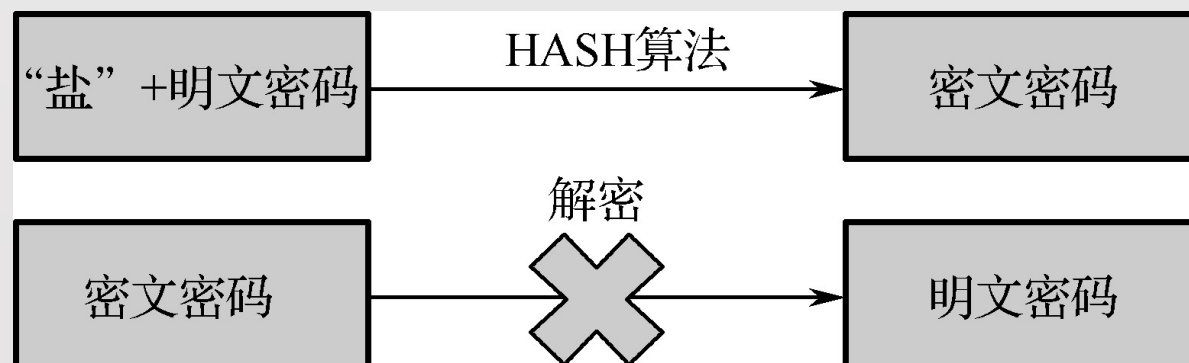
常见口令保存方式

- 3) 使用MD5、SHA1等单向Hash算法的保存方式
- 使用这些算法对口令进行加密后，无法通过计算还原出原始密码，而且其实现比较简单。
- 但随着彩虹表（一个庞大的和针对各种可能的字母组合预先计算好的哈希值的集合）技术的兴起，通过建立彩虹表可以进行口令查表破解，使得这种保存方式也不安全了。



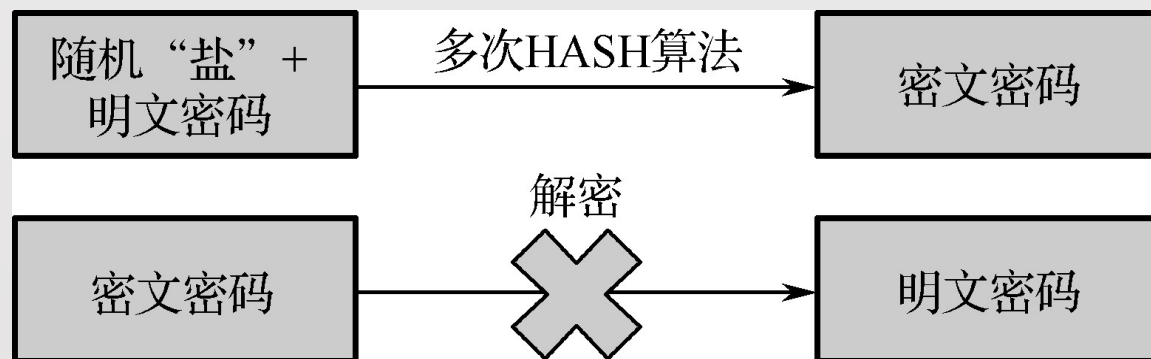
常见口令保存方式

- 4) 使用特殊的单向Hash算法的保存方式
- 在单向Hash算法基础上进行加“盐”（N位随机数）、多次Hash等扩展。这些保存方式可以在一定程度上增加破解口令的难度。对于加了“固定盐”的Hash算法，则和保护“盐”不能被泄露。这就会遇到“保护对称密钥”一样的问题，一旦“盐”被泄露了，可以根据“盐”重新建立彩虹表进行口令破解，对于多次Hash算法，也只是增加了破解的时间，并没有从本质上解决这个问题。



常见口令保存方式

- 5) 使用PBKDF2算法的保存方式
- 在Hash算法基础上增加随机“盐”，并进行多次Hash算法运算。PBKDF2算法中的Hash算法一般选用SHA-1或SHA-256，随机“盐”的长度一般不能少于8字节，Hash运算次数至少也要1000次。一次密码验证过程进行1000次Hash运算，对服务器来说可能只要1ms，但对于破解者来说计算成本增加了1000倍，而至少8字节随机“盐”，更是把建表难度提升了N个数量级，使得破解几乎不可行。



破解口令的常用方法

◆ 1) 简单口令破解方法

- (1) 猜解简单口令：自己或家人的生日、电话号码、房间号码、简单数字或身份证号码中的几位作为口令；也有的人使用自己、孩子、配偶或宠物的名字作为口令；还有的系统管理员使用“password”作为口令。通过猜测便可获得口令。
- (2) 字典攻击：基于现有知识形成口令字典，利用程序尝试字典中每种可能的字符。所谓的字典实际上是一个单词列表文件，是根据人们设置自己账号口令习惯总结出来的常用口令列表文件。
- (3) 暴力穷举：暴力破解，又称密码穷举。如果用户的口令设置得十分简单，黑客使用暴力破解工具很快就可以破解出口令来。事实上没有攻不破的口令，尝试字母、数字、特殊字符的所有组合，最终都能够破解所有的口令。

破解口令的常用方法

◆ 2) 强度较高的口令或多重口令认证的破解方法

- (1) 遍历攻击：对于以上所有步骤都无法破解的口令，可采取遍历得方式破解口令。使用单个CPU可能会非常慢，但如果使用僵尸网络、ASIC、高速GPU阵列等方式可以将破解口令的速度提升。采用遍历的方式也要运用策略，例如，某网站要求口令长度必须大于8位，应尽量只使用8字符进行口令破解以节省时间；或者网站要求口令必须以大写字母开头，就可以在规则中强制指定字符集。
- (2) 击键记录：黑客通过给用户安装木马，设计“击键记录”程序，记录 and 监听用户的击键操作，再通过分析用户击键信息即可破解出用户口令。

破解口令的常用方法

- (3) 屏幕记录：对于使用鼠标和图片录入口令的方式，黑客可以通过木马程序将用户屏幕截屏下来，然后记录鼠标单击的位置，并与截屏的图片对比，从而破解用户口令。
- (4) 网络嗅探器：大量的账号（包括用户名和口令）信息以明文的形式在网络上传输时，黑客便可以使用网络监听的方式窃取网上传送的数据包。黑客将网络接口设置为监听模式，便可以将网上传输的源源不断的信息截获。任何直接通过HTTP、FTP、POP、SMTP、TELNET协议传输的数据包都会被网络程序监听。

破解口令的常用方法

- (5) 网络钓鱼：利用欺骗性的电子邮件和伪造的网站登录站点来进行诈骗活动，而受骗者往往会泄露自己的敏感信息（如用户名、口令、账号、PIN码或信用卡详细信息）。网络钓鱼主要通过发送电子邮件引诱用户登录假冒的网上银行、网上证券网站，骗取用户账号口令以实施盗窃。

4.2 口令破解工具



Wi-Fi口令破解工具Aircrack-ng

- ◆ Aircrack-ng是一个与802.11标准的无线网络分析有关的安全软件，可以工作在任何支持监听模式的无线网卡上，并嗅探802.11a、802.11b、802.11g的数据。其主要功能是进行网络侦测、数据包嗅探、WEP和WPA/WPA2-PSK口令破解。原理如下：
 - 在目标AP（无线访问接入点）已有合法客户端连接的情况下，可以侦听数据包，然后用“aireplay-ng”的“deauth”强制合法客户端掉线。掉线后客户端会尝试重新连接AP，此时会产生握手包。如果成功抓取到该握手包，则可以用字典进行本地离线口令破解。
 - 在客户端开启无线网络连接，但是没有与目标AP连接的情况下，可以通过“airbase-ng”伪造目标AP来欺骗客户端与其连接，这时也会产生握手包。通过这个握手包，同样可以实现破解目标AP无线口令及入侵该客户端。

Wi-Fi破解实例

◆ 实验环境：

- Kali物理机（攻击者）；
- 手机A；
- 手机B。

◆ （1）准备工作。

- ① 用手机A创建一个名为Hack_Wi-Fi_Without_AP的热点。
- ② 用手机B连接A的热点，然后关闭手机A的热点，不关闭手机B的无线网络连接。

◆ （2）关闭会影响抓包的进程，网卡开启侦听模式。

◆ （3）启用Airodump-ng扫描周围的无线信号。

Wi-Fi破解实例

- 扫描的结果如图所示，“74:AD:B7:A7:CB:A2”是手机B的网卡MAC地址，处于“not associated”状态，所以手机B此时正在扫描周围是否有曾经连接过的AP，如有则尝试连接。可以看到，此时正在搜索曾经连过的BSSID名为“ChinaNet-qQRH”和“Hack_Wi-Fi_Without_AP”这两个AP。

```
BSSID          STATION          PWR   Rate   Lost   Frames  Probe
C8:3A:35:0D:13:B8  90:21:81:1A:9D:61  -1    2e- 0    0     30
(not associated)  74:AD:B7:A7:CB:A2 -30    0 - 1    0      8  ChinaNet-qQRH,Hack_WiFi_Without_AP
```

Wi-Fi破解实例

- ◆ (4) 用“airbase-ng”构造一个同名的虚假AP。当手机B发现这个ESSID和加密方式都相同的虚假AP时，则发送握手包。
- ◆ (5) 指定“Hack_Wi-Fi_Without_AP”进行抓包，得到握手包。
- ◆ (6) 用字典离线破解密码。Wi-Fi口令存在于步骤(5)获得的握手包中。攻击者获得Wi-Fi口令为88888888。

```
Aircrack-ng 1.2 rc4
[00:00:00] 128/3437 keys tested (955.22 k/s)
Time left: 3 seconds 3.72%
KEY FOUND! [ 88888888 ]

Master Key      : B7 08 80 B1 4D 93 7E 12 CD 0D 2F 35 6A 91 0D 90
                  32 D6 EE D7 ED 6F F9 56 DB 8D 15 70 BD 23 46 59

Transient Key   : 4D D3 58 49 63 D5 93 0F 2F 00 D6 0E 85 13 EC ED
                  86 59 09 CF 49 43 9B 17 D1 DA E6 2D 2B 18 88 CD
                  29 B7 58 F0 E9 02 37 18 EE DC 09 35 DC 95 36 27
                  FF C3 79 F6 40 0D 7E F2 E3 B6 57 0A 50 EE 59 9D

EAPOL HMAC     : 7A 50 0F CD AC 7A 98 59 E7 C8 53 B4 79 B0 56 C6
```

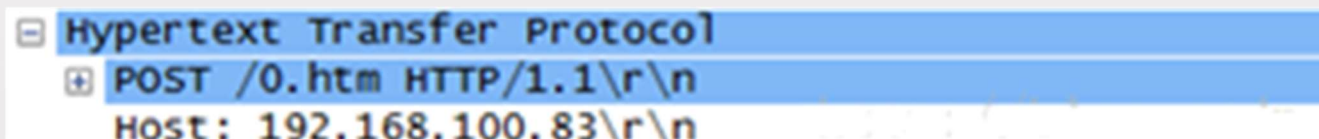
Hydra破解Web

- ◆ Hydra是一款暴力破解工具，支持多种协议的登录口令。Hydra可以用来破解很多种服务，包括IMAP、HTTP、SMB、VNC、MS-SQL、MySQL、SMTP等。
- ◆ 对于基于表单提交的Web登录界面，在破解之前必须知道要Web表达的相关信息。对于每个Web都会有不同的URL、参数、失败和成功的返回信息。破解Web需要的信息如下：
 - 要破解的主机名，或者IP和URL；
 - 区分是HTTPS和HTTP；
 - 表单支持的提交方法（POST or GET）；
 - 请求的参数名；
 - 登录成功和失败时返回信息的区别。

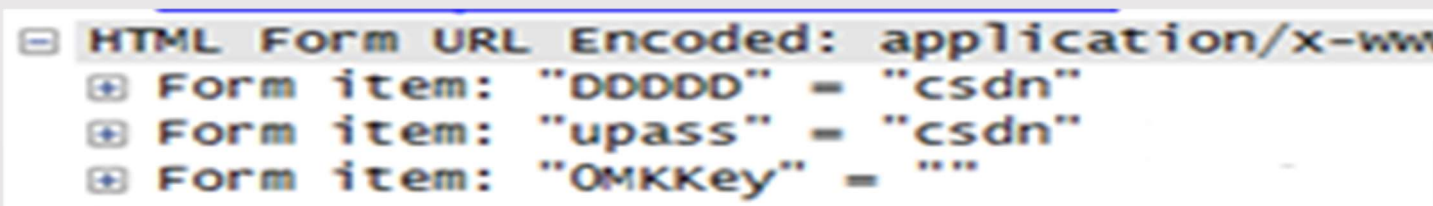
Web破解实例

- ◆ (1) 输入任意账户名和口令，并用Wireshark抓取使用错误的账户名和口令登录时的数据包。

可得主机IP、请求的URL、表单的提交方式：



以及提交的表单选项与参数：



Web破解实例

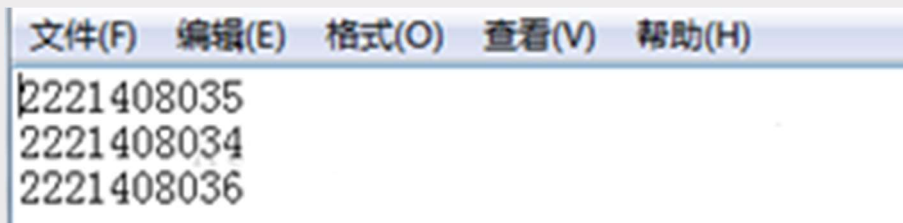
- ◆ (2) 查看网页返回的信息。网页显示错误提示，“账号或口令不对，请重新输入”。查看网页源码寻找具有代表性的登录错误提示，如图所示，可以看到Msg字符串。Msg字符串可以作为登录错误页面的返回判断条件，因为登录成功的页面是不含有Msg字符串的。

```
<html>
▼<head>
  <meta http-equiv="Content-Type" content="text/html; charset=gb2312">
  <meta id="viewport" name="viewport" content="width=800; initial-scale=0.4; maximum-scale=1.0; user-scalable=0;">
  <title>信息返回窗</title>
  ▼<script language="javascript">
    <!--
    Msg=01;time='1234567890';flow='1234567890';fsele=0;fee'1234567890';xsele=0;xip='000.000.000.000.';mac='00-00-00-00-
```

Web破解实例

- ◆ (3) 使用Hydra暴力破解。获取以上信息之后，构造用户字典。并使用Hydra对Web进行破解。

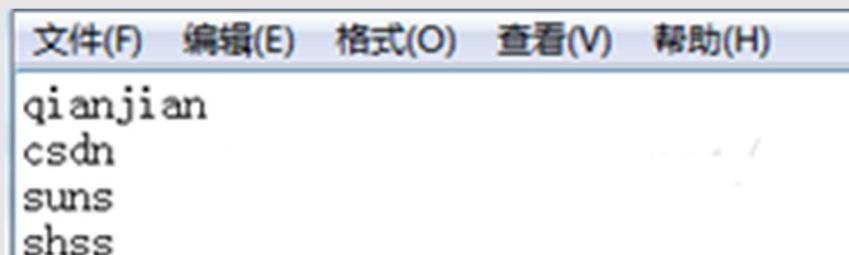
用户账号字典：



A screenshot of a text file with a menu bar at the top containing '文件(F)', '编辑(E)', '格式(O)', '查看(V)', and '帮助(H)'. The file content consists of three lines of text: '2221408035', '2221408034', and '2221408036'.

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
2221408035
2221408034
2221408036
```

用户口令字典：



A screenshot of a text file with a menu bar at the top containing '文件(F)', '编辑(E)', '格式(O)', '查看(V)', and '帮助(H)'. The file content consists of four lines of text: 'qianjian', 'csdn', 'suns', and 'shss'.

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
qianjian
csdn
suns
shss
```

Web破解实例

- ◆ (4) 查看破解结果。如果登录页面需要验证码，Hydra则没有办法对其进行破译。

```
[STATUS] attack finished for 192.168.100.83 <waiting for children to complete tests>
[STATUS] 12.00 tries/min, 12 tries in 00:01h, 0 todo in 00:01h, 1 active[80][www-form] host: 192.168.100.83 login: 22214 password: qian,`
1 of 1 target successfully completed, 1 valid password found
Hydra <http://www.thc.org/thc-hydra> finished at 2015-07-18 11:42:52
```