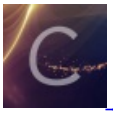
网络安全实验1 敏感信息搜集与密码心理分析

原创

一半西瓜 于 2019-10-30 14:23:09 发布 2056 收藏 11
分类专栏： 网络安全实验 文章标签： 网络安全实验



赞赏码 & 联系方式 & 个人闲话

【实验名称】敏感信息搜集与密码心理分析

【实验目的】

1.理解社会工程学的概念，掌握获取敏感信息的方法

2.提高自我信息保护的意识和方法

3.理解密码心理学的概念、密码特征分析

4.掌握黑客猜解密码的切入方法、如何提高密码强壮性

【实验原理】

社会工程学(Social Engineering)，一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的手法。它并不能等同于一般的欺骗手法，社会工程学尤其复杂，即使自认为最警惕最小心的人，一样可能会被高明的社会工程学手段损害利益。

密码心理学就是从用户的心理入手，分析对方心理，从而更快的破解出密码。掌握好密码心理学可以缩短破解时间，快速获得用户信息。

密码本身的保密性是来源于其随机性，整个密码的被猜中概率(P)是多个密码特征概率的乘积，只有所有密码特征概率（Pi|i=1,2,3,……n）都处在一个较低的水平上时，整个密码才是安全的。可以用公式表达成：

$P(c)=P1\times P2\times P3\times\ldots\ldots\times Pn$

我们可以看出，当特征数量增多时（即n比较大），密码的安全性也较高。

【实验内容】

敏感信息搜集

由于对实验环境的限制，本实验不能进行实验步骤上的设计，故举出一个通过在互联网上使用信息搜集的方法来获取某人敏感信息的过程。

开始进行信息搜集，具体过程如下：

（1）查看并分析目标个人资料，参见下图：

图1-1-1

可以获取有可利用价值的信息包括：

表1-1-1

可能具有利用价值的信息	
性别	男
生日	6月21日
血型	B型
生肖	兔
星座	双子座
省份	山东
城市	泰安

（2）访问其QQ空间，除照片外，并未发现有价值信息，参见下图：

图1-1-2

（3）查看其留言板现实中朋友，参见下图：

图1-1-3

表1-1-2

可能具有利用价值的信息	
真实朋友	王建

（4）访问王建的qq空间，发现王建的头像照片，参见下图：

图1-1-4

（5）使用校内网的搜索，配合推测的“王建”个人信息，搜索此人，见下图：

图1-1-5

（6）在所有搜索结果中，配合4中已确定的王建的相貌，排除其他同名者，最终确定王建校内网账号，参见下图：

图1-1-6

（7）通过校内网中王建的好友信息，配合目标qq空间中的照片，确定其真实姓名及资料，参见下图：

图1-1-7

表1-1-3

可能具有利用价值的信息	
目标姓名	张磊
目标学校	鲁东大学

（8）通过已获得目标的真实姓名和所在学校，通过google搜索查询，可得到如下结果：

图1-1-8

（9）进入网页，分析详细信息，获得目标的中学信息及毕业年份，参见下图：

图1-1-9

（10）我们继续使用google，使用其姓名、大学、中学信息进行信息搜集，甚至发现了此人更多的敏感信息，参见下图：

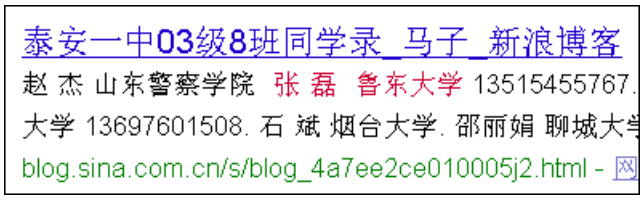
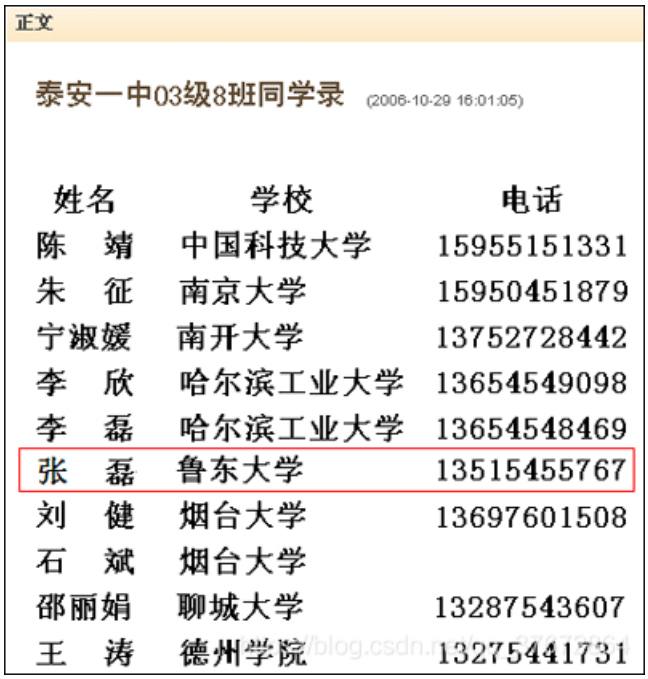


图1-1-10


正文

泰安一中03级8班同学录 (2006-10-29 16:01:05)

姓名	学校	电话
陈　靖	中国科技大学	15955151331
朱　征	南京大学	15950451879
宁淑媛	南开大学	13752728442
李　欣	哈尔滨工业大学	13654549098
李　磊	哈尔滨工业大学	13654548469
张　磊	鲁东大学	13515455767
刘　健	烟台大学	13697601508
石　斌	烟台大学	
邵丽娟	聊城大学	13287543607
王　涛	德州学院	13275441731

图1-1-11


http://xx.3dxiaonei.com/getinfo.asp?uid=634

姓名：张磊
学校：鲁东大学
院系：交通学院
年级：2006 级 机械本0603 班
手机：1555342**** 1
QQ：44206745
Email：leileiaideni@126.com
注册时间：2009-5-7 17:51:43
已登录：23

图1-1-12

（11）请将搜集到目标的个人信息填入下表：

表1-1-4

可能具有利用价值的信息	
姓名	张磊
性别	男
手机号码	13515455767
邮箱	leileiaideni@126.com
生日	6月21日
血型	B型

生肖	兔
星座	双子座
省份	山东
城市	泰安
大学名称	鲁东大学
大学入学年份	2006年
大学院系	交通学院
大学班级	机械本0603班
中学名称	山东省泰安一中
中学班级	03级8班
中学毕业年份	2006年

思考题：举出保护个人敏感信息的方法（最少三点）。

1、对敏感数据做单向变换后再保存。系统不直接保存敏感数据，只作匹配用。

2、利于新型加密技术处理数据，比如同态加密技术。

3、对个人数据进行分类，确定个人信息数据等级，比如：一般信息，重要信息，关键信息。

4、用户应该有控制自身个人信息被访问和被利用的最高权限。

5、用户应该保存私钥，且此私钥能被更换，如果更换私钥，与用户相关的敏感数据会一并改变。

密码心理学攻击

本实验设置了host1、host2、host3、host4、host5、host6六个主机用户，此六个用户的用户密码是根据实验1|练习一所搜集到的用户敏感信息设置的，具体内容可参见表3-1-1。

表3-1-1 敏感信息

可能具有利用价值的信息	
姓名	张磊
性别	男
手机号码	13515455767
邮箱	leileiaideni@126.com
生日	6月21
血型	B

生肖	兔
星座	双子座
省份	山东
城市	泰安
大学名称	鲁东大学
大学入学年份	2006
大学院系	机械学院
大学班级	0603班
中学名称	山东泰安第一中学
中学班级	03级8班
中学毕业年份	2006年

3-1-1中给出的相应信息，对新建的六个账户密码进行猜解。

解密：

根据题目给出的一些被攻击者的个人信息，我们有理由猜想其密码或密码中的一部分同其人名、邮箱、手机号、生日、入学年月等个人私密信息高度相关。所以我猜想可能会有以下的一些组合，并将其写入superdic.txt文件，作为密码字典。这里当然是一个不断尝试、猜解的过程。

利用LC5软件，结合我们自己猜测出的密码字典和其本身带有的常见数字、字母组合，可以破解出这6个账户的密码。运行结果如下：

Domain	User Name	LM Password	<8	Password	Password Age (d...
HOST3B	Administrator	???????MIN			2422
HOST3B	ASPNET				2419
HOST3B	Guest	* empty *	x	* empty *	0
HOST3B	host1	ZHANGLEI		zhanglei	0
HOST3B	host2	19870621		19870621	0
HOST3B	host3	13515455767		13515455767	0
HOST3B	host4	ZHANGLEI123		zhanglei123	0
HOST3B	host5	ZL0621	x	zl0621	0
HOST3B	host6	LEILEIAIDENI		leileiaideni	0
HOST3B	IUSR_HOST1A				2419
HOST3B	IWAM_HOST1A				2419
HOST3B	SQLDebugger	* empty *			2420
HOST3B	student	123456	x	123456	2411
HOST3B	SUPPORT_388945a0	* empty *			2427
HOST3B	test	1234	x	1234	2400
HOST3B	VUSR_47VFIOC3Z8SZON2				2421

最终的密码表如下：

表3-1-2

账户	密码
host1	ZHANGLEI
host2	19870621
host3	13515455767
host4	ZHANGLEI123
host5	ZL0621
host6	LEILEIAIDENI

思考题：如何提高你的密码强壮性，以避免黑客利用密码心理学猜解你的密码？

1、确保由数字，字母（大写和小写）字符以及特殊符号和类似字符组成的复杂密码

2、定期更改密码

3、使用先前未使用的新密码

【小结或讨论】

首先说敏感信息搜集实验。其实这不能算是一个真正的专业实验吧，更多的是想让我们意识到个人信息泄漏的情况，并结合实验二来告诉我们个人隐私泄露带来的严重后果。实验的时候我尝试这搜索自己的名字。本来觉得不会有什么有价值的信息的，搜索一番的结果却让我很是意外。我搜索到了自己的性别、生日、星座；在一个比赛介绍的网页上还看到了自己当时的合照；在初中的一份奖励名单上还能知道我的初中；在文库里的一份学生会信息表上，我甚至还看到了自己的手机号、QQ号等隐私信息。这些都让我大为诧异，自以为平时信息没有随便泄露，可是一搜索还能搜出来很多。原来不知不觉中我们就陷入了信息泄露的漩涡。

密码心理分析实验简单来说就是利用目标的一些已知的个人信息来猜解其各个账户的密码。这个其实利用了大部分人的一个常见心理，就是利用自己的姓名、生日、电话、邮箱这种有明显的个人色彩的常用信息来作为密码，这也就给了不法分子可乘之机。在知道目标的一些隐私信息后，我们居然能很快破译出他的6个不同账户的密码，这给我们自己敲响了警钟。