实验 3 密码破解实验

实验目的

- 1.了解密码学中有关加密、解密、数字签名、消息验证的工作原理。
- 2.掌握两种以上破解密码的工具，例如：hashcat等。

实验前提

在kali 2019虚拟机中运行下列命令，查看使用条件是否满足：

```
root@kali:~# hashcat -I
hashcat (v5.1.0) starting...
No devices found/left.
```

如果你的环境下也出现上述问题，则说明暂不满足使用条件。这是因为hashcat运行时需要（GPU Driver requirements）:

- AMD GPUs on Linux require "RadeonOpenCompute (ROCm)" Software Platform (1.6.180 or later)
- AMD GPUs on Windows require "AMD Radeon Software Crimson Edition" (15.12 or later)
- Intel CPUs require "OpenCL Runtime for Intel Core and Intel Xeon Processors" (16.1.1 or later)
- Intel GPUs on Linux require "OpenCL 2.0 GPU Driver Package for Linux" (2.0 or later)
- Intel GPUs on Windows require "OpenCL Driver for Intel Iris and Intel HD Graphics"
- NVIDIA GPUs require "NVIDIA Driver" (367.x or later)

所以，大多数用户需要下载：Intel CPUs require "OpenCL Runtime for Intel Core and Intel Xeon Processors" (16.1.1 or later)

下面介绍安装方法：

1.在kali的terminal中，运行命令： `service ssh start` 。启动ssh服务器。

2.使用ssh访问终端，例如xshell等，访问kali2019.

3.然后用xftp工具将老师下发的安装包，或从https://software.intel.com/en-us/articles/opencl-drivers 下载的OpenCL Runtime for Intel Core driver 发送到kali root用户的Downloads目录下。

4.使用kali中的terminal，运行下列命令，完成解压。

```
root@kali:~# cd ~/Downloads/

root@kali:~/Downloads# tar -xvf l_opencl_p_18.1.0.015.tgz
```

5.执行安装命令，并根据提示完成安装过程。

```
root@kali:~/Downloads# cd l_opencl_p_18.1.0.015/

root@kali:~/Downloads/l_opencl_p_18.1.0.015# ./install.sh
```

6.安装完成后使用下列命令测试是否有效。

```
root@kali:~# hashcat -I
hashcat (v5.1.0) starting...
```

若不在出现 `No devices found/left.` 即表示安装正确。

实验内容

1.Hashcat 字典破解模式hash 破解密钥实验

2.Hashcat 基于掩码（规则） 破解密钥实验

3.使用John the ripper 破解密钥实验

实验步骤

一.Hashcat 字段破解模式hash密码破解实验

初步使用

1.使用ssh工具访问kali 2019虚拟机

2.执行下列命令建立一个简单的password文件。

```
root@kali:~# cd Documents/
root@kali:~/Documents# nano password.txt

#进入nano编辑器后，键入如下内容：
123456
admin
hashcat
```

3.之后，按ctrl+O，再按回车保存，再按 ctrl+x退出nano编辑器。

4.使用nano，在Documents目录下建立一个空文件，名为 hashcat_output.txt

```
root@kali:~/Documents# nano hashcat_output.txt

#内容为空
```

之后，按ctrl+O，再按回车保存，再按 ctrl+x退出nano编辑器。

5.执行下列命令：

```
hashcat  -m 0 8743b52063cd84097a65d1633f5c74f5 ~/Documents/password.txt -o output.txt
```

6.请回答hash密文8743b52063cd84097a65d1633f5c74f5的明文为什么？

使用**kali**自带的字典的**hash**破解实例

在ssh终端中键入如下命令，尝试破解相关hash密文。

```
root@kali:~/Documents# hashcat -a 0 ede900ac1424436b55dc3c9f20cb97a8 /usr/share/wordlists/sqlmap.txt  -o output.t
```

执行上述命令后的结果是什么？

使用**kali**自带的字典组合破解实例

在ssh终端中键入如下命令，尝试破解相关hash密文。

```
hashcat -a 1 25f9e794323b453885f5181f1b624d0b  /usr/share/wordlists/sqlmap.txt /usr/share/wordlists/nmap.lst
```

字典+掩码破解

在ssh终端中键入如下命令，尝试破解相关hash密文。

```
hashcat -a 6 9dc9d5ed5031367d42543763423c24ee /usr/share/wordlists/nmap.lst ?l?l?l?l?l
```

破解非MD5标准hash的密文实例

1.通过ssh终端访问kali2019

2.运行下列命令检查 hash密文：b89eaac7e61417341b710b727768294d0e6a277b

```
hash-identifier

# 然后输入b89eaac7e61417341b710b727768294d0e6a277b
```

3.根据判断结果，查找hashcat中相应的-m 参数，尝试破解此hash密文。可参考：

```
hashcat -m 此处填写适当参数 b89eaac7e61417341b710b727768294d0e6a277b password.txt
```

二.Hashcat 基于掩码（规则）的hash破解实验

破解 7位数字组成的 hash值

在ssh终端中键入如下命令，尝试破解相关hash密文。

```
hashcat -a 3 -m 0 --force 25c3e88f81b4853f2a8faacad4c871b6 ?d?d?d?d?d?d?d
```

破解 7位小写字母 hash值

在ssh终端中键入如下命令，尝试破解相关hash密文。

```
hashcat -a 3 -m 0 --force 7a47c6db227df60a6d67245d7d8063f3 ?l?l?l?l?l?l?l
```

破解 1-8位数字 hash值

在ssh终端中键入如下命令，尝试破解相关hash密文。

```
hashcat -a 3 -m 0 --force 4488cec2aea535179e085367d8a17d75 --increment --increment-min 1 --increment-max 8 ?d?d?d
```

破解 1-8位小写字母+数字 hash值

在ssh终端中键入如下命令，尝试破解相关hash密文。

```
hashcat -a 3 -m 0 --force ab65d749cba1656ca11dfa1cc2383102 --increment --increment-min 1 --increment-max 8 ?h?h?h
```

破解 特定字符集：123456abcdf!@+- hash值

在ssh终端中键入如下命令，尝试破解相关hash密文。

```
hashcat -a 3 -1 123456abcdf!@+- 8b78ba5089b11326290bc15cf0b9a07d ?1?1?1?1?1
# 注意一下：这里的-1和?1是数字1，不是字母l
```

破解 1-8为位符集:123456abcdf!@+- hash值

在ssh终端中键入如下命令，尝试破解相关hash密文。

```
hashcat -a 3 -1 123456abcdf!@+- 9054fa315ce16f7f0955b4af06d1aa1b --increment --increment-min 1 --increment-max 8
```

1-8位数字+大小写字母+可见特殊符号

在ssh终端中键入如下命令，尝试破解相关hash密文。

```
hashcat -a 3 -1 ?d?u?l?s d37fc9ee39dd45a7717e3e3e9415f65d --increment --increment-min 1 --increment-max 8 ?1?1?1?
# 或者：
hashcat -a 3 d37fc9ee39dd45a7717e3e3e9415f65d --increment --increment-min 1 --increment-max 8 ?a?a?a?a?a?a?a?a
```

破解mysql生成的hash码

Mysql4.1/5的PASSWORD函数可以生成某个字符串的hash码，有的项目使用hash码作为密文。

```
hashcat -a 3 -m 300 --force 6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 ?d?d?d?d?d?d
```

sha512crypt $6, SHA512 (Unix)破解

可以cat /etc/shadow获取.

```
hashcat -a 3 -m 1800 --force $6$mxuA5cdy$XZRk0CvnPFqOgVopqiPEFAFK72SogKVwwwp7gWaUOb7b6tVwfCpcSUsCEk64ktLLYmzyew/
```

不用整理用户名，使用--username

```
hashcat -a 3 -m 1800 --force qiyou:$6$QDq75ki3$jsKm7qTDHz/xBob0kF1Lp170Cgg0i5Tslf3JW/sm9k9Q916mBTyilU3PoOsbRdxV8
```

Windows NT-hash，LM-hash破解

可以用saminside获取NT-hash,LM-hash的值

```
# NT-hash:
hashcat -a 3 -m 1000 209C6174DA490CAEB422F3FA5A7AE634 ?l?l?l?l?l?l

# LM-hash:
hashcat -a 3 -m 3000 F0D412BD764FFE81AAD3B435B51404EE ?l?l?l?l?l?l
```

三.使用John the ripper 破解密钥实验

使用John the ripper 破解密钥实验

Usage: john [OPTIONS] [PASSWORD-FILES]

1.在kali 2019虚拟机中运行下列命令： `service ssh start` 。之后，使用xshell等ssh工具访问kali 2019虚拟机。这一步的目的是容易复制粘贴文本内容。

2.在连接了kali 2019虚拟机的xshell终端中，运行下列命令：

```
root@kali:~# cd Documents/
root@kali:~/Documents# mkdir examples
root@kali:~/Documents# cd examples
root@kali:~/Documents/examples# nano passwd_example.txt
```

向文本编辑器中粘贴下列内容，之后保存并退出。

```
Administrator:500:cb5f77772e5178b77b9fbd79429286db:b78fe104983b5c754a27c1784544fda7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:810185b1c0dd86dd756d138f54162df8:7b8f23708aec7107bfdf0925dbb2fed7:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:8be4bbf2ad7bd7cec4e1cdddcd4b052e:::
rAWjAW:1003:aad3b435b51404eeaad3b435b51404ee:117a2f6059824c686e7a16a137768a20:::
rAWjAW2:1004:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
```

3.运行下列命令进行密钥破解：

```
john passwd_example.txt
# 或

john --wordlist=/usr/share/wordlists/nmap.lst  passwd_example.txt
```

4.使用下列命令显示结果：

```
john --show passwd_example.txt
```

以下为选读内容，不必交作业

wordpress密码hash破解

具体加密脚本在./wp-includes/class-phpass.php的HashPassword函数.

```
hashcat -a 3 -m 400 --force $P$BYEYcHEj3vDhV1lwGBv6rpxurKOEWY/ ?d?d?d?d?d?d
```

discuz用户密码hash破解

其密码加密方式md5(md5($pass$).salt)

```
hashcat -a 3 -m 2611 --force 14e1b600b1fd579f47433b88e8d85291: ?d?d?d?d?d?d
```

破解RAR压缩密码

```
# 获取rar文件的hash值：rar2john.exe 1.rar
# 结果：
# 1.rar:$rar5$16$639e9ce8344c680da12e8bdd4346a6a3$15$a2b056a21a9836d8d48c2844d171b73d$8$04a52d2224ad082e

hashcat -a 3 -m 13000 --force $rar5$16$639e9ce8344c680da12e8bdd4346a6a3$15$a2b056a21a9836d8d48c2844d171b73d$8$04a
```

hashcat 支持 RAR3-hp 和 RAR5，官方示例如下：

-m 参数	类型	示例 **hash**
12500	RAR3-hp	`$RAR3$*0*45109af8ab5f297a*adbf6c5385d7a40373e8f77d7b89d317`
13000	RAR5	`$rar5$16$74575567518807622265582327032280$15$f8b4064de34ac02ecabfe`

zip密码破解

```
# 用zip2john获取文件的hash值：zip2john.exe 1.zip
# 结果：
# 1.zip:$zip2$*0*3*0*554bb43ff71cb0cac76326f292119dfd*ff23*5*24b28885ee*d4fe362bb1e91319ab53*$/zip2$:::::1.zip-1.

hashcat -a 3 -m 13600 $zip2$*0*3*0*554bb43ff71cb0cac76326f292119dfd*ff23*5*24b28885ee*d4fe362bb1e91319ab53*$/zip2
```

破解office密码

```
# 获取office的hash值：python office2john.py 11.docx
# 结果：# 11.docx:$office$*2013*100000*256*16*e4a3eb62e8d3576f861f9eded75e0525*9eeb35f0849a7800d48113440b4bbb9c*5

hashcat -a 3 -m 9600 $office$*2013*100000*256*16*e4a3eb62e8d3576f861f9eded75e0525*9eeb35f0849a7800d48113440b4bbb9
```

破解WIFI密码

首先把握手包转化为hccapx格式，现在最新版的hashcat只支持hccapx格式.

官方在线转化https://hashcat.net/cap2hccapx/

```
hashcat -a 3 -m 2500 1.hccapx 1391040?d?d?d?d
```