CTF mysql

原创

艺博东 于 2020-10-05 07:51:52 发布 9120 收藏 9

分类专栏： 网络攻防 文章标签： CTF

本文链接：https://blog.csdn.net/HYD696/article/details/108897020

网络攻防 专栏收录该内容

24 篇文章 17 订阅

订阅专栏

难度系数： ★★★★★

题目来源： XCTF

题目描述： 我们在Mysql数据库中存放了flag，但是黑客已经把它删除了。你能找回来flag吗？

题目场景： 暂无

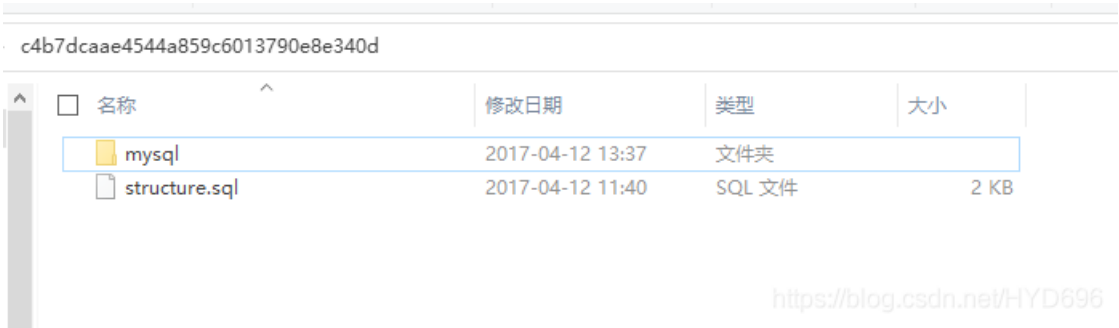
题目附件： 附件1

1、附件1

链接：https://pan.baidu.com/s/12RPRNl7PPgNBLpLatl68Fw

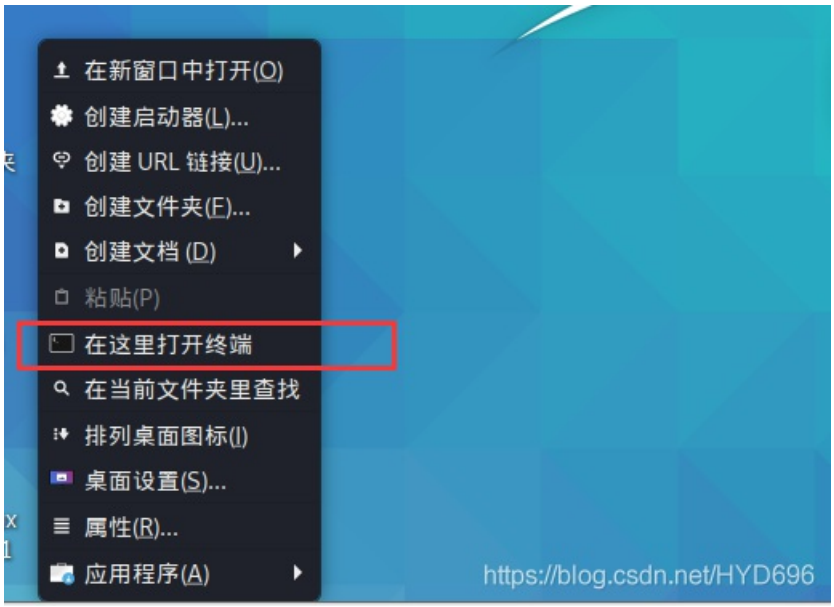
提取码：q57k

2、文件



3、把文件拷贝到 kail Linux 环境

4、点击空白处，鼠标右键—>在这里打开终端



5、strings：在对象文件或二进制文件中查找可打印的字符串。

用法：strings [选项] [文件]
打印 [文件] (默认为标准输入) 中可打印的字符串
选项为：
-a - --all----------扫描整个文件，而不仅仅是数据部分[默认]
-d --data----------只扫描文件中的数据部分
-f --print-file-name-------在每个字符串之前打印文件的名称
-n --bytes=[number]-----找到并打印任何以null结尾的at序列

-t --radix={o,d,x}----------打印以8、10或16为基数的字符串位置
-w --include-all-whitespace----包括所有的空白作为有效的字符串字符
-o An alias for --radix=o
-T --target=----------指定二进制文件格式
-e --encoding={s,S,b,l,B,L}-----选择字符大小和字节：
s = 7-bit, S = 8-bit, {b,l} = 16-bit, {B,L} = 32-bit
-s --output-separator= ----------用于在输出中分隔字符串的字符串。
@----------读取中选项
-h --help----------显示这个信息
-v -V --version----------打印程序的版本号

```
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d$ strings -help
用法：strings [选项] [文件]
 打印 [文件]（默认为标准输入）中可打印的字符串
 选项为：
  -a - --all                Scan the entire file, not just the data sectio
n [default]
  -d --data                 Only scan the data sections in the file
  -f --print-file-name      Print the name of the file before each string
  -n --bytes=[number]       Locate & print any NUL-terminated sequence of
at
  -<number>                   least [number] characters (default 4).
  -t --radix={o,d,x}        Print the location of the string in base 8, 10
 or 16
  -w --include-all-whitespace Include all whitespace as valid string chara
cters
  -o                        An alias for --radix=o
  -T --target=<BFDNAME>     Specify the binary file format
  -e --encoding={s,S,b,l,B,L} Select character size and endianness:
                            s = 7-bit, S = 8-bit, {b,l} = 16-bit, {B,L} =
32-bit
  -s --output-separator=<string> String used to separate strings in output
.
  @<file>                   Read options from <file>
  -h --help                 Display this information
  -v -V --version           Print the program's version number
strings：支持的目标： elf64-x86-64 elf32-i386 elf32-iamcu elf32-x86-64 pei
-i386 pei-x86-64 elf64-l1om elf64-k1om elf64-little elf64-big elf32-little
 elf32-big pe-x86-64 pe-bigobj-x86-64 pe-i386 srec symbolsrec verilog tekh
ex binary ihex plugin
将 bug 报告到 <http://www.sourceware.org/bugzilla/>
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d$
```


6、ls

```
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d$ ls
mysql  structure.sql
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d$
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d$
```

7、cd mysql

```
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d$
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d$
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d$ cd mysql
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d/mysql$ ls
debian-5.5.flag  ib_logfile0  mysql                performance_schema
ibdata1          ib_logfile1  mysql_upgrade_info
```

8、strings XXXX | grep 'flag'

```
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d/mysql$
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d/mysql$
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d/mysql$ strings mysql_upgrade_info | grep 'flag
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d/mysql$ strings ib_logfile1 | grep 'flag'
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d/mysql$ strings ib_logfile0 | grep 'flag'
.flag71e55075163d5c6410c0d9eae499c977
yibodong@locahost:~/桌面/c4b7dcaae4544a859c6013790e8e340d/mysql$
```

9、OK

71e55075163d5c6410c0d9eae499c977