2021寒假MISC打卡DAY1

原创

煤矿路口西_CTF小学生 于 2021-01-11 20:29:39 发布 136 收藏 1

分类专栏： 打卡日常 文章标签： 信息安全

本文链接：https://blog.csdn.net/LLKJSAF/article/details/112468179

打卡日常 专栏收录该内容

40 篇文章 0 订阅

订阅专栏

CSDN上将按时间顺序更新，每天8道。个人博客上按类别分类。

> [SUCTF2018]single dog
>
> > 得到的 flag 请包上 flag{} 提交。来源：https://github.com/hebtuerror404/CTF_competition_warehouse_2018

一张JPG

右键文件属性无果，查看二进制，文件末尾存在504B0102字样，全文搜索504B0304，得到完整压缩包。

得到1.txt

```
ﾟωﾟ/= / ｀m´) ﾉ ~┻━┻   //*´▽｀*/ ['_']; o=(ﾟｰﾟ)  =_=3; c=(ﾟΘﾟ) =(ﾟｰﾟ)-(ﾟｰﾟ); (ﾟДﾟ) =(ﾟΘﾟ)= (o^_^o)/ (o^_^o);(ﾟДﾟ)={ﾟΘﾟ: '_' ,ﾟωﾟﾉ : ((ﾟωﾟﾉ==3) +'_') [ﾟΘﾟ] ,ﾟｰﾟﾉ :(ﾟωﾟﾉ+ '_')[o^_^o -(ﾟΘﾟ)] ,ﾟДﾟ/:((ﾟｰﾟ==3) +'_')[ﾟｰﾟ] }; (ﾟДﾟ) [ﾟΘﾟ] =(
```

类似上文

AAencode编码(http://ctf.ssleye.com/aaencode.html)

得

```
function a()
{
var a="SUCTF{happy double eleven}";
alert("双十一快乐");
}
a();
```

> [安洵杯 2019]吹着贝斯扫二维码
>
> > 得到的 flag 请包上 flag{} 提交。

555,我讨厌拼图，giao

得到压缩包里很多无后缀的文件。通过010editor，可得这些都为jpg文件。

打开得到碎片化的二维码。拼！

人都傻了，得到

```
BASE Family Bucket ??? 85->64->85->13->16->32
```

根据提示，一步一步来吧。中间还用到了rot13

得ThisIsSecret!233

打开压缩包，得到flag

```
flag{Qr_Is_MeAn1nGfuL}
```

> 从娃娃抓起

> 得到的 flag 请包上 flag{} 提交。

```
0086 1562 2535 5174
bnhn s wwy vffg vffg rrhy fhnv

请将你得到的这句话转为md5提交，md5统一为32位小写。
提交格式：flag{md5}
```

之前做过类似的题，那道题为"计算机要从娃娃抓起"，用到了中国电码。试试看

第一排数字正好对应中国电码中的“人工智能”

第二排两个重复的vffg猜测为“娃娃”

另，若熟悉五笔打字的话，就能知道第二行其实是五笔编码“也要从娃娃抓起”

“人工智能也要从娃娃抓起”的32位小写md5就是

```
3b4b5dccd2c008fe7e2664bd1bc19292
```

4.

> [[DDCTF2018](ノ°□°)ノ ┻━┻](https://buuoj.cn/challenges#DDCTF2018
>
> > 得到的 flag 请包上 flag{} 提交。

```
d4e8e1f4a0f7e1f3a0e6e1f3f4a1a0d4e8e5a0e6ece1e7a0e9f3baa0c4c4c3d4c6fbb9b2b2e1e2b9b9b7b4e1b4b7e3e4b3b2b2e3e6b4b3e2b5b0b6b1b0e6e1e5e1b5fd
```

十六进制丢进010editor中，未果。

进制转换，得

```
212 232 225 244 160 247 225 243 160 230 225 243 244 161 160 212 232 229 160 230 236 225 231 160 2332431861601961961952121982511851781782252261851851831802251801832272281791781782272301801792261811761821771762302252292251812533
```

未见有意义字符串。

对128取余试试，212-》84-》T

成了，依次操作得

```
That was fast! The flag is: DDCTF{922ab9974a47cd322cf43b50610faea5}
```

> 小易的U盘

> 小易的U盘中了一个奇怪的病毒，电脑中莫名其妙会多出来东西。小易重装了系统，把U盘送到了攻防实验室，希望借各位的知识分析出里面有啥。请大家加油噢，不过他特别关照，千万别乱点他U盘中的资料，那是机密。 注意：得到的 flag 请包上 flag{} 提交

额，这道题还挺啊这的。

一开始以为是流量分析啥的，后来发现二进制查看就是个压缩包，还原rar后缀名。

得到一串exe和一堆有的没的（例如不要在上班时间打开的某雷链接

找到autorun.inf,写着

```
[AutoRun]
Open=autoflag - 副本 (32)
```

把autoflag - 副本 (32).exe放进ida，main函数直接得flag

```
flag{29a0vkrlek3eu10ue89yug9y4r0wdu10}
```

1.

> [ACTF新生赛2020]swp
>
> 得到的 flag 请包上 flag{} 提交。

得到wget.pcapng

流量分析！！

导出http流，得到一堆有的没的

观察，发现其中有hint.html

you don't need password

](https://imgchr.com/i/s8UNNV)

很好，不知道他在说什么

继续观察，发现一个名为secret.zip的压缩包，有东西！

存在名为flag的文件，丢进010

找到flag

```
actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5}
```

> [WUSTCTF2020]alison_likes_jojo

> 得到的 flag 请包上 flag{} 提交。
> 感谢 Iven Huang 师傅供题。
> 比赛平台：https://ctfgame.w-ais.cn/

得到两张图片，对第一张图查看二进制，提取出一加密压缩包。ZIP爆破得密码888866

beisi.txt

```
WVRKc2MySkhWbmxqV0Zac1dsYzBQUT09
```

64->64->64

得

```
killerqueen
```

至此咱们拥有了一个密钥及第二张图片

需要密钥的图片隐写，steghide无果，尝试outguess

```
outguess -r jljy.jpg -k killerqueen -t out.txt
```

得到wctf2020{pretty_girl_alison_likes_jojo}

> [安洵杯 2019]Attack

> 得到的 flag 请包上 flag{} 提交。

学到了流量分析新姿势

常规操作：

1）分析，导出HTTP流，得到lsass.dmp

```
lsass是Windows系统的一个进程，用于本地安全和登陆策略
```

2)foremost分离得到加密压缩包

通过大神WP学到新姿势，mimikatz一个名叫猕猴桃的软件(内网渗透工具，可在lsass.exe进程中获取windows的账号明文密码)

以管理员权限打开后：

```
//提升权限
privilege::debug
//载入dmp文件
sekurlsa::minidump lsass.dmp
//读取登陆密码
sekurlsa::logonpasswords full

得到密码
W3lc0meToD0g3
```

解压缩包得D0g3{3466b11de8894198af3636c5bd1efce2}