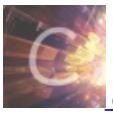
Securinets CTF Quals 2022 Forensics Writeup

原创

是Mumuzi 已于 2022-04-11 22:44:05 修改 2894 收藏 3

分类专栏： ctf 笔记 文章标签： 信息安全

于 2022-04-11 21:57:31 首次发布



文章目录

Forensics

mal

Whale

题目大小：mal:2G Whale:2.2G

google链接：

mal: https://drive.google.com/file/d/16rzauO0LMyRGLg3-wer2fJ8lxq-yMmLt/view

Whale: https://drive.google.com/file/d/1Z89cnqKt0dvLLlstsX5D_Cl8j02YVT_8/view

没魔法或者失效了吗？试试百度网盘链接

mal:链接：https://pan.baidu.com/s/1OWP_pgAYnW_Giuafgc_MiQ

提取码：xia0

Whale:

链接：https://pan.baidu.com/s/14GoXbKX8OXgzScTleXuhfg

提取码：xia0

Forensics

mal

> popped up message destroyed me.
> flag format:Securinets{flag}

内存转储文件，使用volatility进行分析。
使用imageinfo参数判断出版本号为Win7SP1x64。
使用pslist查看一下当前运行的程序。

```
0xfffffa801aa1bb30 firefox.exe           2204   2808     26      321      1      1 2022-04-09 12:26:04 UTC+0000
0xfffffa801a9a7b30 firefox.exe           3128   2808     20      292      1      1 2022-04-09 12:26:07 UTC+0000
0xfffffa801ac24b30 firefox.exe           3232   2808     20      290      1      1 2022-04-09 12:26:09 UTC+0000
0xfffffa801ac90b30 firefox.exe           3320   2808     20      290      1      1 2022-04-09 12:26:11 UTC+0000
0xfffffa801acb8060 StikyNot.exe          3888   1904      9      176      1      0 2022-04-09 12:26:22 UTC+0000
0xfffffa801ad8bb30 firefox.exe           4040   2808     20      290      1      1 2022-04-09 12:26:24 UTC+0000
0xfffffa801ad865b0 notepad.exe           1360   1904      1       60      1      0 2022-04-09 12:26:25 UTC+0000
0xfffffa801adadb30 firefox.exe           2384   2808      9      185      1      1 2022-04-09 12:26:26 UTC+0000
0xfffffa8019467170 firefox.exe           3220   2808     16      270      1      1 2022-04-09 12:26:29 UTC+0000
0xfffffa80193ef260 Solitaire.exe         2152   1904      9      226      1      0 2022-04-09 12:26:29 UTC+0000
0xfffffa801a88da70 svchost.exe           2492    456      5       77      0      0 2022-04-09 12:27:25 UTC+0000
0xfffffa801a970a90 firef0x.exeexe        3492   1904      8      198      1      1 2022-04-09 12:27:38 UTC+0000
0xfffffa801a3edb30 WindowsUpdater        3468   3492      1       74      1      1 2022-04-09 12:27:38 UTC+0000
0xfffffa801ad30560 WerFault.exe          3996   2492      6      133      1      1 2022-04-09 12:27:38 UTC+0000
0xfffffa801ad04060 firefox.exe           1032   2808     19      280      1      1 2022-04-09 12:27:44 UTC+0000
0xfffffa801a9ec6c0 firefox.exe           2860   2808     18      276      1      1 2022-04-09 12:28:17 UTC+0000
0xfffffa801acd5060 DumpIt.exe            3624   1904      2       45      1      1 2022-04-09 12:28:24 UTC+0000
0xfffffa801a95f3e0 conhost.exe           4036    360      2       53      1      0 2022-04-09 12:28:24 UTC+0000
```


其中该名字非常可疑，因此使用filescan指令查找一下该文件并dump下来

```
mumuzi@kali:~/桌面$ volatility -f mal.raw --profile=Win7SP1x64 filescan |grep "firef0x"
Volatility Foundation Volatility Framework 2.6.1
0x000000007de99070      6      0 R--r-d \Device\HarddiskVolume2\Users\CTF\Videos\firef0x.exeexe
0x000000007deac450      2      0 -W-rw- \Device\HarddiskVolume2\Users\CTF\Videos\firef0x.exeexe
```

可以发现此文件在videos文件夹下，根据名字和该文件的路径，判断此文件很有可能为病毒文件（结合题目名字mal）
因此使用dumpfiles将其dump出来

```
volatility -f mal.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000007de99070 -D ./
```

会dump出两个文件，均报毒，因此丢进沙箱，确实报毒。那么打开IDA进行分析。

地址	长度	类型	字符串
.text:0040A471	00000013	C	WindowsUpdater.exe
.rdata:0040C2...	00000007	C	(null)
.rdata:0040C2...	00000011	C	0123456789abcdef
.rdata:0040C2...	00000011	C	0123456789ABCDEF
.rdata:0040C2...	00000011	C	0123456789abcdef
.rdata:0040C2...	00000011	C	0123456789ABCDEF
.rdata:0040C5...	0000000B	C	0123456789
.rdata:0040C6...	00000042	C	@@@@@@@@@@@@@@@@@@@@@@@@@@
.rdata:0040C6...	00000005	C	\a\b\t\n\v
.rdata:0040C6...	00000006	C	@@@@@@
.rdata:0040C6...	000000DA	C	!\"#$%&'()*+,-./0123@@@@@@@@@@@@@@@@
.rdata:0040C9...	00000008	C	fprintf
.rdata:0040C9...	00000007	C	strchr
.rdata:0040C9...	00000008	C	_pctype

```
.rdata:0040C9... 0000000D C __mb_cur_max
.rdata:0040CA... 00000009 C _isctype
```


可以发现字符串的第一行就是WindowsUpdateer，极可能说明该文件与windowsupdater有关。

```
0xfffffa801a970a90 firef0x.exeexe          3492   1904      8      198      1      1 2022-04-09 12:27:38 UTC+0000
0xfffffa801a3edb30 WindowsUpdater          3468   3492      1       74      1      1 2022-04-09 12:27:38 UTC+0000
```

观察后发现，windowsupdater的父进程为firef0x.exeexe

`PID(Process Identifier)：进程控制符`

`PPID(Parent Process IDentification):父进程标识`

因此dump出windowsupdater文件，使用命令

`volatility -f mal.raw --profile=Win7SP1x64 procdump -p 3468 -D ./`

并将dump出来的文件修改名字为WindowsUpdater

运行即可得到flag


```
Securinets{easy_malware_detection}
```

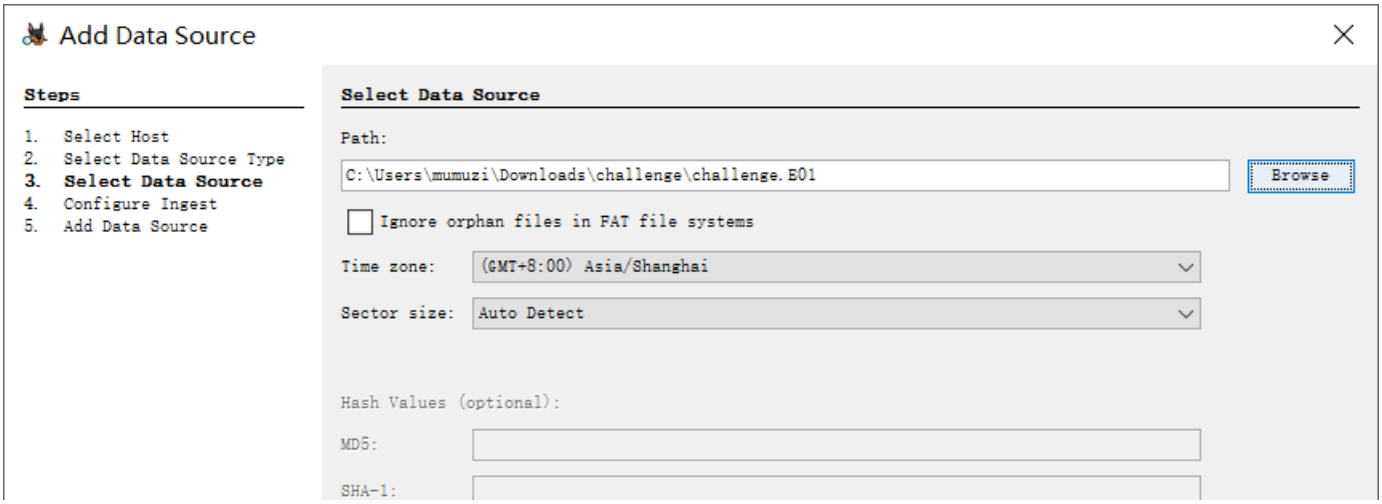
Whale

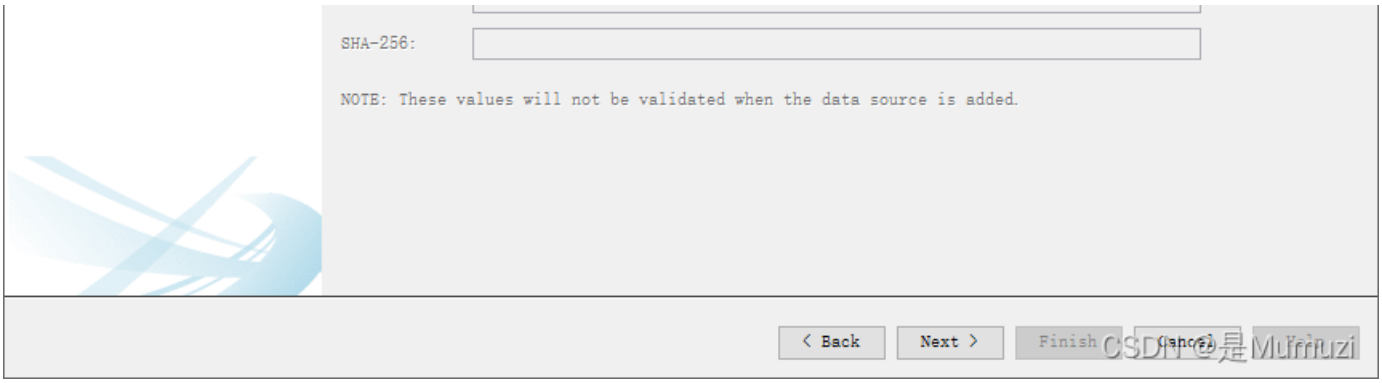
> Who doesn't love whales? I do, You do, they do.

E01系统镜像，Hum取证大师过期了。

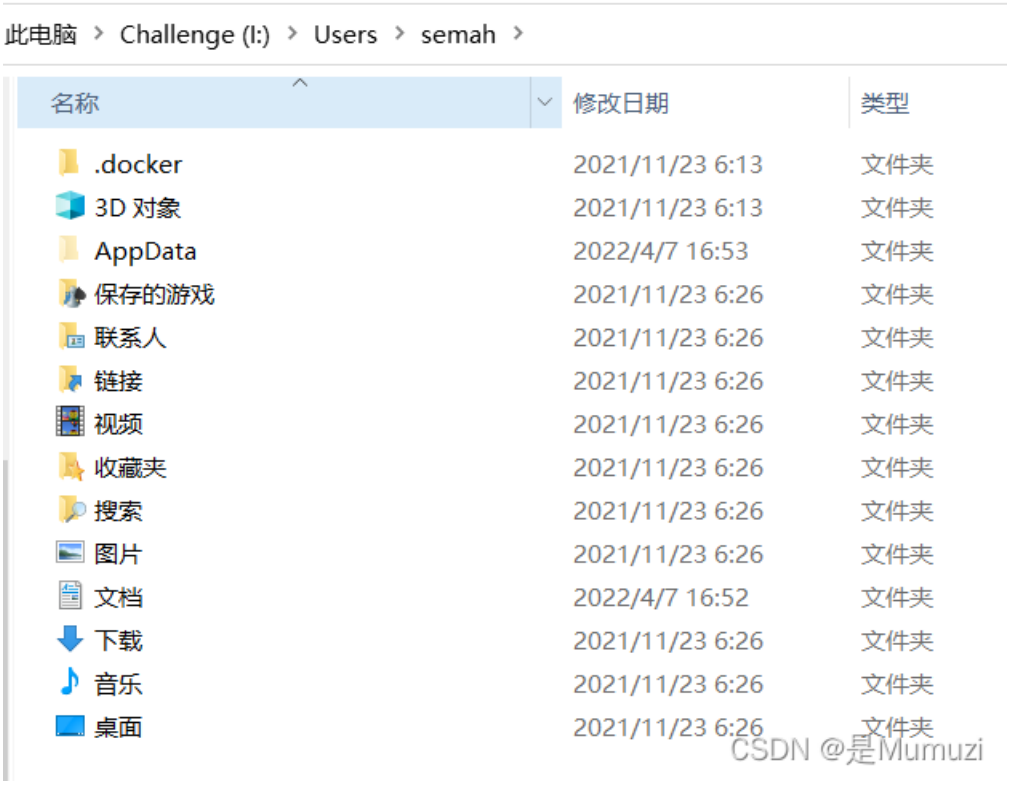
那就试试autospy，还没怎么用autospy取过，只取过注册表项文件

添加添加





在取的时候顺便用FTK挂载进去看一下

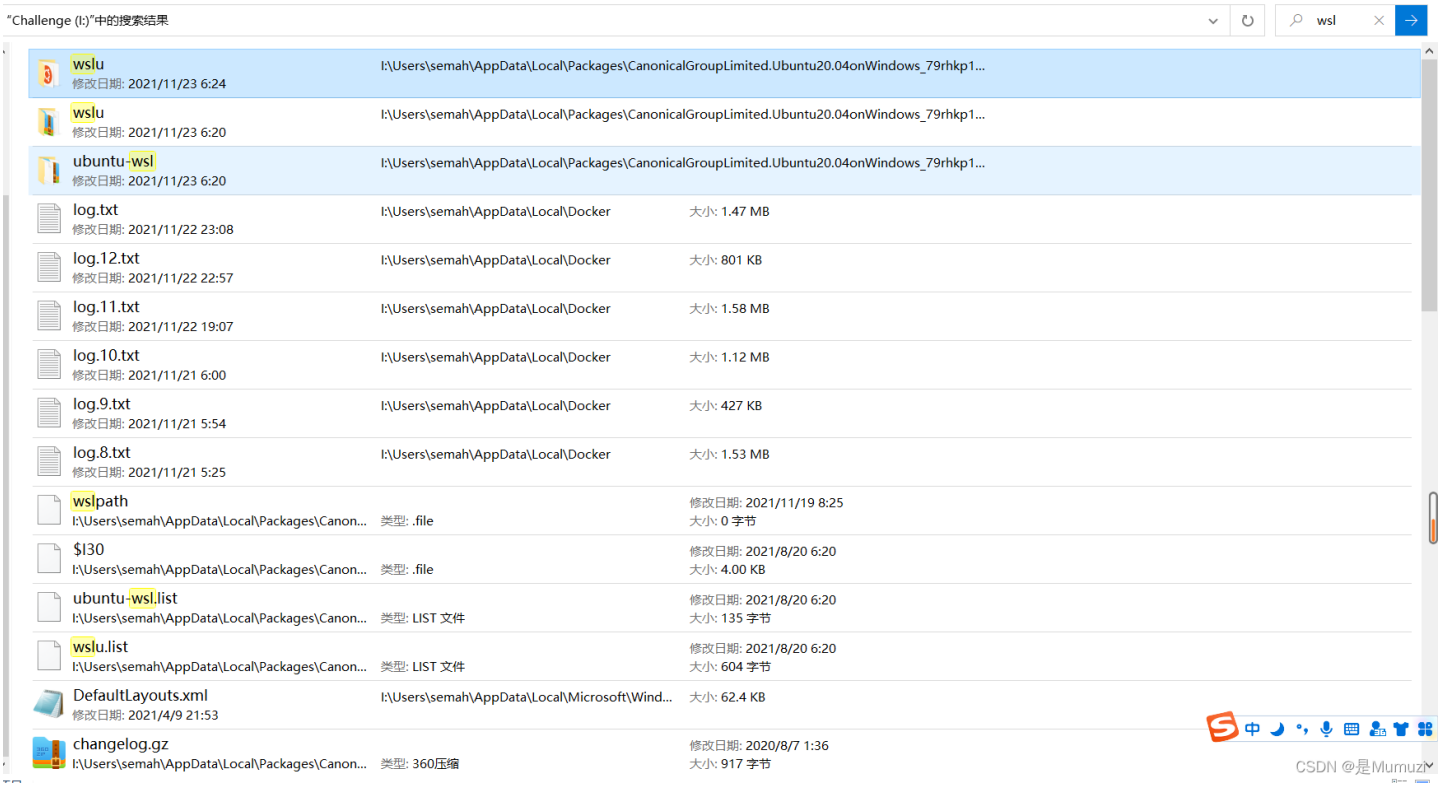


诶，进入之后发现一个在取证中很不常见的，那就是.docker文件
里面只有一个`{ "path": "C:\\Program Files\\Docker\\Docker\\resources\\snyk.exe" }`
然后去program文件夹中没有找到有关文件，在桌面找到的有关信息也就只有`Docker Desktop`
而安装过`Docker Desktop`的都知道，要使用必须在windows上同时安装wsl。怀疑需要对wsl进行取证。

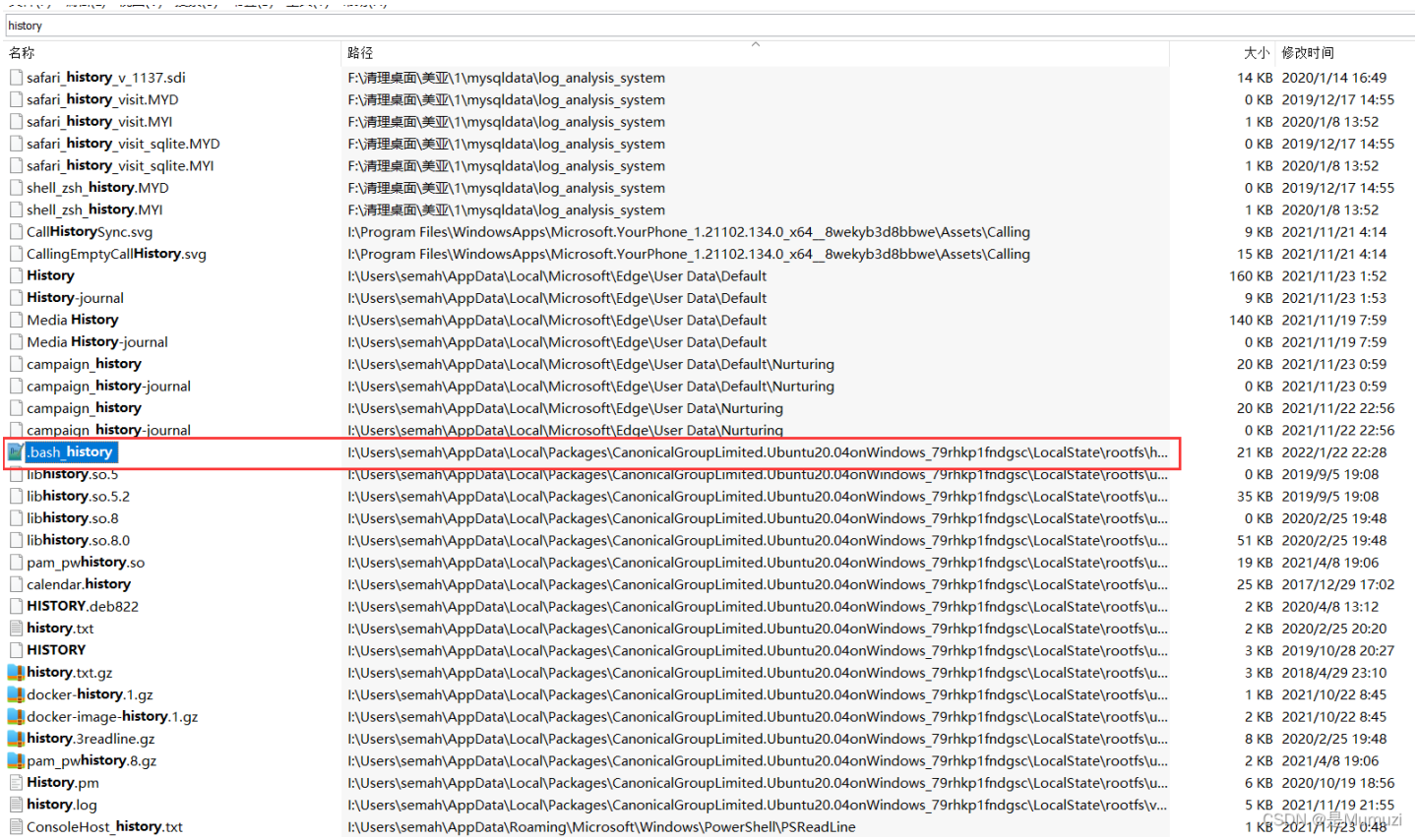
UsrClass.dat	My Computer\C:\ProgramData\Microsoft\Windows
UsrClass.dat	My Computer\C:\ProgramData\Microsoft\Windows\Start Menu
UsrClass.dat	My Computer\C:\ProgramData\Microsoft\Windows\Start Menu\Programs
UsrClass.dat	My Computer\C:\ProgramData\Microsoft\Windows\Start Menu\Programs\WinRAR
UsrClass.dat	My Computer\D:\
UsrClass.dat	My Computer\CLSID_Desktop
UsrClass.dat	My Computer\E:\
UsrClass.dat	My Network Places
UsrClass.dat	My Network Places\wsl$
UsrClass.dat	My Network Places\wsl$\\\wsl$\Ubuntu-20.04
UsrClass.dat	My Network Places\wsl$\\\wsl$\Ubuntu-20.04\home
UsrClass.dat	My Network Places\wsl$\\\wsl$\Ubuntu-20.04\home\semahba
UsrClass.dat	My Network Places\wsl$\\\wsl$\Ubuntu-20.04\home\semahba\.landscape
UsrClass.dat	Explorer
UsrClass.dat	AA
UsrClass.dat	Explorer

UsrClass.dat		Explorer
UsrClass.dat		Explorer\semah

在autospy中也能确认使用过wsl，应该是wsl无误了。在里面找一下wsl



太杂乱啦。用everything查一下history看看吧



从0开始做有点棘手啊，继续看看吧。

既然获取了history的路径，那么也就可以看wsl其他的目录了
暂时翻了一下常见目录，没有东西，那么回到wsl看docker相关的

```
587  sudo docker pull semahba/securinetscongress
```

上仓库看一下

Command

```
/bin/sh -c echo -n $(curl -s https://pastebin.com/raw/mtRhi3tv) | openssl enc -aes-256-cbc -iter 10
-pass pass:$(cat /var/securinetsCongress/5f4dcc3b5aa765d61d8327deb882cf99.txt) -out
/var/securinetsCongress/secret.enc
```

IMAGE LAYERS

1	ADD file ... in /	2.69 MB
2	CMD ["/bin/sh"]	0 B
3	/bin/sh -c apk upgrade	3.72 MB
4	/bin/sh -c apk update	2.19 MB
5	/bin/sh -c apk add openssl	271.21 KB
6	/bin/sh -c apk add curl	1022.04 KB
7	WORKDIR /var/securinetsCongress	165 B
8	COPY file:2b7c831b1588013268b7b33b9008b8c8c94befb756fcc8…	246 B
9	COPY file:562e19cb002ba903fef8b1a9f4c5aa1fc8801bb80acd5c…	291 B
10	/bin/sh -c echo -n $(curl	316 B
11	**/bin/sh -c rm /var/securinetsCongress/5f4dcc3b5aa765d61d…**	**192 B**

Command

```
/bin/sh -c rm /var/securinetsCongress/5f4dcc3b5aa765d61d8327deb882cf99.txt
```


最后两条看起来有小秘密哦，然后的话，直接搜镜像是搜不到的，试过了，因此需要本地也pull。

```
sudo docker pull semahba/securinetscongress
sudo docker run -it semahba/securinetscongress
```

通过本地搜索，能够找到5f4dcc3b5aa765d61d8327deb882cf99.txt
在/var/lib/docker/overlay2/c33b509c6669343ae5f9daed47d7e5f7f1e88b3113c2208498e2b8a7d776101d/diff/var/securinetsCongress/5f4dcc3b5aa765d61d8327deb882cf99.txt
cat之后得到内容为`Lgt6G6T2wZlM3A2o1QkgkE\IvN}]QJ!N9\dxLO/Q`
写一个到本地然后用openssl解密当前文件夹下的secret

```
ubuntu@VM-0-8-ubuntu:~$ sudo docker run -it semahba/securinetscongress
/var/securinetsCongress # ls
README.md   secret.enc
/var/securinetsCongress # cat README.md
# Securinets Team

Hello,

We contacted the Fword Team for this image, and this is our secure app.
It will have our sensitive data. use it well!

** SemahBA **/var/securinetsCongress # openssl enc -aes-256-cbc -d -iter 10 -in secret.enc -kfile "Lgt6G6T2wZlM3A2o1QkgkE\IvN}]QJ!N9\dxLO/Q"
Can't open Lgt6G6T2wZlM3A2o1QkgkE\IvN}]QJ!N9\dxLO/Q for reading, No such file or directory
140171455904584:error:02001002:system library:fopen:No such file or directory:crypto/bio/bss_file.c:69:fopen('Lgt6G6T2wZlM3A2o1QkgkE\IvN}]QJ!N9\dxLO/Q','r')
140171455904584:error:2006D080:BIO routines:BIO_new_file:no such file:crypto/bio/bss_file.c:76:
enc: Use -help for summary.
/var/securinetsCongress # echo "Lgt6G6T2wZlM3A2o1QkgkE\IvN}]QJ!N9\dxLO/Q" > key.txt
/var/securinetsCongress # openssl enc -aes-256-cbc -d -iter 10 -in secret.enc -kfile key.txt
Only Employees have access to our sensitive work data. Don't share it! pwd: cvvsBZhRBgjqXefLkMwW/var/securinetsCongress #
```


`Only Employees have access to our sensitive work data. Don't share it! pwd: cvvsBZhRBgjqXefLkMwW`

wait,你说你没听懂什么是本地搜索而进入了容器吗？
就是pull容器之后直接搜，毕竟已经下载下来了，docker的位置在/var/lib中

就是在/var/lib/docker里搜`find ./ -name "5f4dcc3b5aa765d61d8327deb882cf99.txt"`

好，现在获取了一个密码，这个密码需要解密在E01镜像中的某样东西

震惊，文档下竟然有神奇文件
有一个`work.kdbx`文件在文档中
百度发现其是通过KeePass密码安全创建的数据文件称为KDBX文件,它们通常所说的KeePass的密码数据库。
于是去下载一个keepass

然后解密,使用docker里面解密出的pwd，成功解密出一个网址和一句话还有一个password

`password: Vb0CkhUnRsnObwFA2vBvMjfGEg9ZtSYgB/3RGgQCRGuL5h4RJQcOdTzb/hs/fUP0`

`https://defuse.ca/b/efCaJpFIl2NPUFnpoQyxlh`

`Our sensitive data`

使用这个password去解密那个网站即可


```
Securinets{docker_layers_are_fun_right?}
```

前面做的比较麻烦啦(其实是思路有点乱)，到最后几步才发现空白神发了wp到discord，真好，我还说今天只能盲复现了(指复现不完咕咕咕(指得到了密码但是不知道要解密啥玩意。

然后比赛的取证题，质量很高，很喜欢