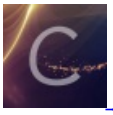
bugku-writeup-MISC-又一张图片，还单纯吗

原创

dark2019 于 2021-09-13 15:58:27 发布 54 收藏
分类专栏： 信息安全 CTF wp 文章标签： bugku 杂项

本文链接：https://blog.csdn.net/qq_22597955/article/details/120268378


信息安全 同时被 3 个专栏收录
53 篇文章 1 订阅
订阅专栏


CTF
5 篇文章 0 订阅
订阅专栏


wp
31 篇文章 0 订阅
订阅专栏

题目：又一张图片，还单纯吗

工具：foremost

01—foremost安装及使用

ctf工具-杂项-foremost_dark的博客-CSDN博客

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for kali:
Get:1 http://mirrors.neusoft.edu.cn/kali kali-rolling InRelease [30.5 kB]
Get:2 http://mirrors.neusoft.edu.cn/kali kali-rolling/main amd64 Packages [18.0 MB]
Get:3 http://mirrors.neusoft.edu.cn/kali kali-rolling/contrib amd64 Packages [107 kB]
Get:4 http://mirrors.neusoft.edu.cn/kali kali-rolling/non-free amd64 Packages [203 kB]
Fetched 18.3 MB in 1min 32s (200 kB/s)
Reading package lists... Done

┌──(kali㉿kali)-[~]
└─$ sudo apt-get install foremost
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  foremost
0 upgraded, 1 newly installed, 0 to remove and 1477 not upgraded.
Need to get 43.0 kB of archives.
After this operation, 103 kB of additional disk space will be used.
Get:1 http://mirrors.neusoft.edu.cn/kali kali-rolling/main amd64 foremost amd64 1.5.7-10+b1 [43.0 kB]
Fetched 43.0 kB in 12s (3,515 B/s)
Selecting previously unselected package foremost.
(Reading database ... 261826 files and directories currently installed.)
Preparing to unpack .../foremost_1.5.7-10+b1_amd64.deb ...
Unpacking foremost (1.5.7-10+b1) ...
Setting up foremost (1.5.7-10+b1) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2020.4.0) ...

┌──(kali㉿kali)-[~]
└─$
```

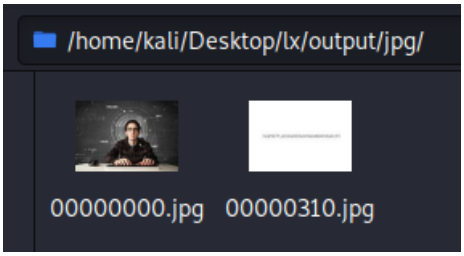

02—foremost分离

安装好之后分离图片，进入到图片目录下，一开始使用binwalk分离图片，无法分离，换用foremost分离。

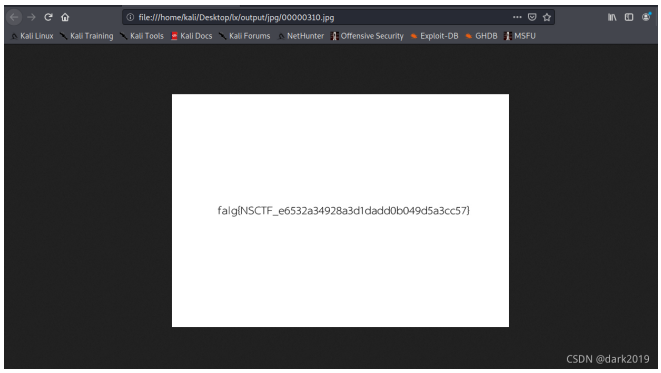
```
┌──(kali㉿kali)-[~/Desktop/lx/whereistheflag]
└─$ cd ..

┌──(kali㉿kali)-[~/Desktop/lx]
└─$ binwalk pic2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, big-endian, offset of first image directory: 8
158792        0x26C48         JPEG image data, JFIF standard 1.02
158822        0x26C66         TIFF image data, big-endian, offset of first image directory: 8
159124        0x26D94         JPEG image data, JFIF standard 1.02
162196        0x27994         JPEG image data, JFIF standard 1.02
168370        0x291B2         Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"

┌──(kali㉿kali)-[~/Desktop/lx]
└─$ binwalk -e pic2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, big-endian, offset of first image directory: 8
158792        0x26C48         JPEG image data, JFIF standard 1.02
158822        0x26C66         TIFF image data, big-endian, offset of first image directory: 8
159124        0x26D94         JPEG image data, JFIF standard 1.02
162196        0x27994         JPEG image data, JFIF standard 1.02
168370        0x291B2         Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"


┌──(kali㉿kali)-[~/Desktop/lx]
└─$ foremost pic2.jpg
zsh: command not found: foremost

┌──(kali㉿kali)-[~/Desktop/lx]
└─$ foremost pic2.jpg
Processing: pic2.jpg
|*|

┌──(kali㉿kali)-[~/Desktop/lx]
└─$
```


03—输出结果

分离输出output文件夹



其中一张图片中为flag


file:///home/kali/Desktop/lx/output/jpg/00000310.jpg
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
flag{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}
CSDN @dark2019