

实验吧 NSCTF misc250writeup

原创

weixin_39296576 于 2018-08-23 01:14:39 发布 831 收藏 1

分类专栏: [shiyambar misc](#) 文章标签: [writeup shiyambar](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_39296576/article/details/81953615

版权



[shiyambar](#) 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏



[misc](#)

1 篇文章 0 订阅

订阅专栏

既然是下载了东西, 那就看看http吧

No.	Time	Source	Destination	Protocol	Length	Info
127	34.8764...	192.168.52.129	192.168.52.1	HTTP	361	GET / HTTP/1.1
129	34.8777...	192.168.52.1	192.168.52.129	HTTP	485	HTTP/1.1 200 OK (text/html)
150	43.3853...	192.168.52.129	192.168.52.1	HTTP	399	GET /key.rar HTTP/1.1
152	43.3862...	192.168.52.1	192.168.52.129	HTTP	526	HTTP/1.1 200 OK (application/x-rar-compressed)

发现最后一组有个压缩包

单击最后一个, 选中压缩包

Media type: application/x-rar-compressed (148 bytes)		
0130	30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20	00 · Conn ection:
0140	4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6e 74	Keep-Ali ve · Cont
0150	65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63	ent-Type : applic
0160	61 74 69 6f 6e 2f 78 2d 72 61 72 2d 63 6f 6d 70	ation/x- rar-comp
0170	72 65 73 73 65 64 0d 0a 0d 0a 52 61 72 21 1a 07	ressed · · · Rar! · ·
0180	00 ce 99 73 80 00 0d 00 00 00 00 00 00 00 f4 a6	· · · s · · · · · · · · · ·
0190	66 db 6d 01 cd 78 20 0b 4f 43 a3 43 df 5e 2e 00	f · m · x · OC · C · ^ · ·
01a0	04 55 62 cb ff 4c 00 8a 59 a4 40 6a 7c 5b 64 08	· Ub · L · Y · @j [d ·
01b0	4a 2f 68 e5 e6 c5 84 7d 0e d6 57 cd bd 69 f6 59	J/h · · · } · · W · i · Y
01c0	e4 13 55 70 8b 05 62 75 06 7f 47 d4 ce 79 f0 7f	· Up · bu · · G · y · ·
01d0	d0 4c f7 cc 81 88 23 04 d9 19 61 41 30 68 74 75	· L · · · # · · aA0htu
01e0	96 0c 76 38 e6 2d 69 d2 ff 78 ed b9 42 3e 75 9c	· v8 · -i · x · B>u ·
01f0	e2 e6 a4 49 ea 39 f4 a6 66 db 6d 01 cd 78 1b cf	· · · I · 9 · · f · m · x · ·
0200	32 7b e2 bc f8 d7 cc fd c2 7c 71 cb ab 8b	2{ · · · · · · · q · ·

然后ctrl+shift+x导出字节流, 就其实是 文件 >> 导出分组字节流

记得另存为xxx.rar!!!!!!

然后以为这样子就好了吗，解压的时候发现要密码 我：???

倒回去看了那个下载的网页，就第二个分组

```
152 43.3862... 192.168.52.1      192.168.52.129    HTTP      526 HTTP/1.1 200
```

```
<
```

```
▼ Line-based text data: text/html (7 lines)
  <html>\r\n
  <head><tittle>KEY</tittle></head>\r\n
  <body>\r\n
  <p>\303\334\302\353\312\307nsfocus+5\316\273\312\375\327\326</p>\r\n
  <a href="./key.rar">key</a>\r\n
  </body>\r\n
  </html>
```

在line-based text data 那里右键导出分组字节流，保存为xxx.html, 用记事本或者Notepad++打开都行
发现说密码是nsfococus+5位数字密码

然后用crunch工具去生成了字典，下载的话我在<https://sourceforge.net/projects/crunch-wordlist/>下载
用法参考<https://www.jianshu.com/p/884af86daeb0>

在解压下来的文件夹李敏啊打开终端 `crunch 12 12 -t nsfocus%%%%%%%% >> xxx.txt`

然后就在当前目录下生成一个字典啦

然后用archpr的字典爆破，洗个澡回来就好啦

然后解压，得到txt文档，打开即得flag >-<



[创作打卡挑战赛](#) >
[赢取流量/现金/CSDN周边激励大奖](#)