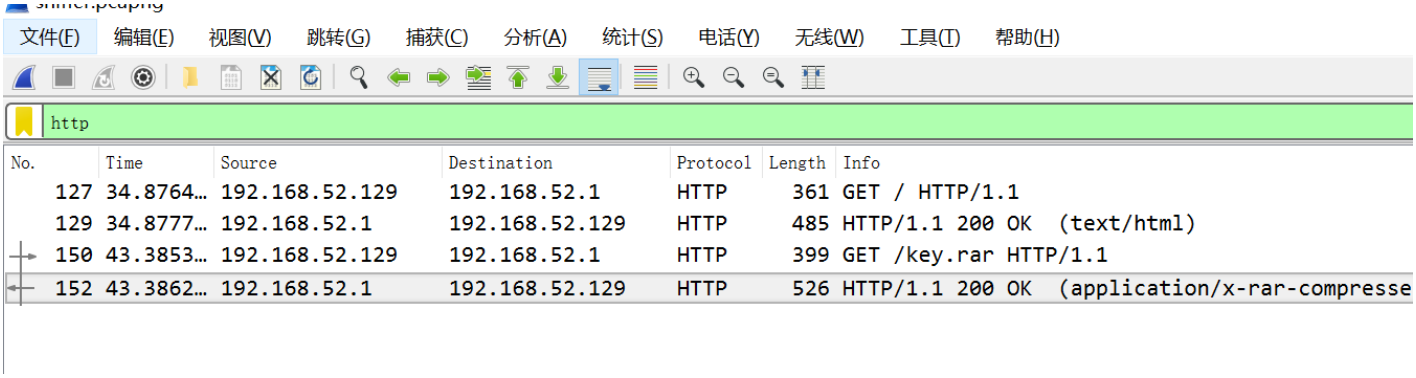
实验吧 NSCTF misc250writeup

原创

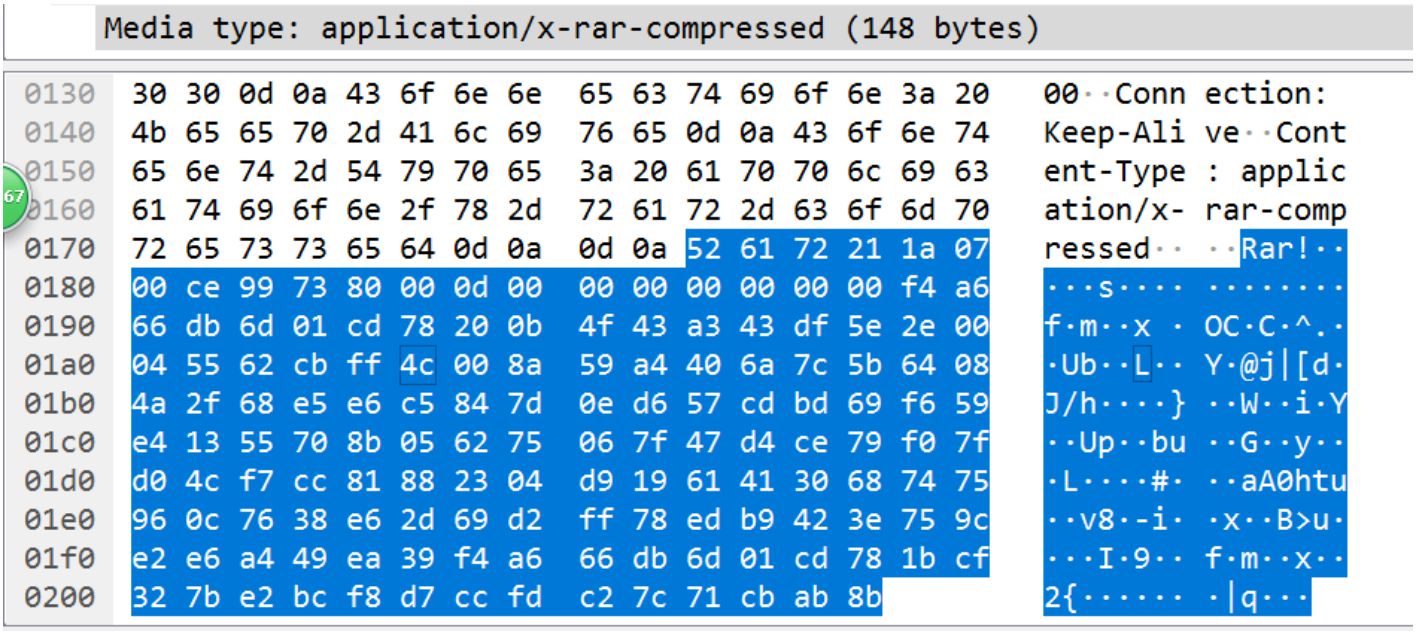
weixin_39296576 于 2018-08-23 01:14:39 发布 831 收藏 1
分类专栏： shiyanbar misc 文章标签： writeup shiyanba

既然是下载了东西，那就看看http吧



发现最后一组有个压缩包

单击最后一个，选中压缩包



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nsfoucus+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 >-<