2021年中国工业互联网安全大赛核能行业赛道writeup之日志分析

原创

苦行僧(csdn) 于 2021-11-09 00:22:34 发布 341 收藏 1
分类专栏： 信息安全 文章标签： wireshark rar john 命令注入

本文链接：https://blog.csdn.net/qpeity/article/details/121219279

附件题：日志分析

题目描述：

> 核电站新来的运维小王粗心把一个办公网地址映射到外网，遭到大量攻击，你能从日志当中找到有效信息吗。

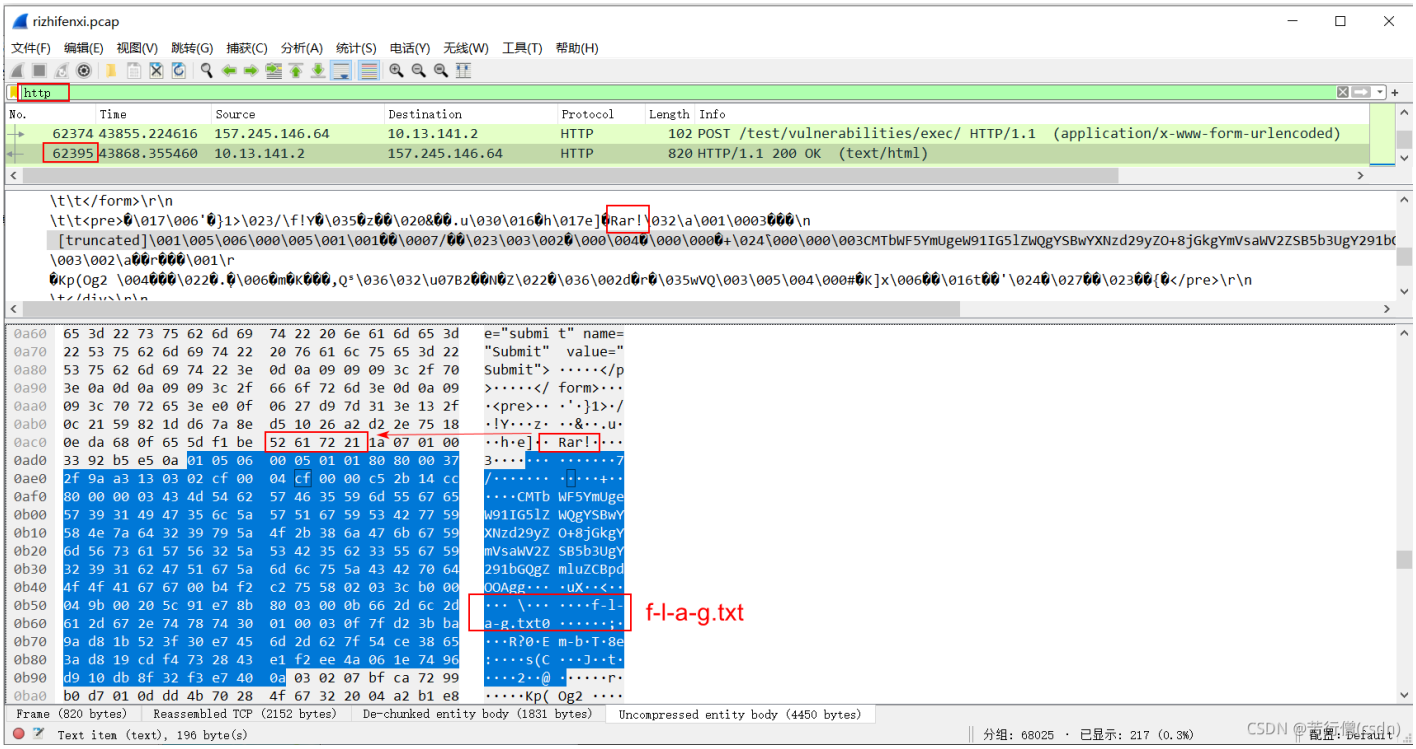
附件下载：

2021-10-12T15_37_51.610646+00_00rizhifenxi.rar-网络攻防文档类资源-CSDN下载

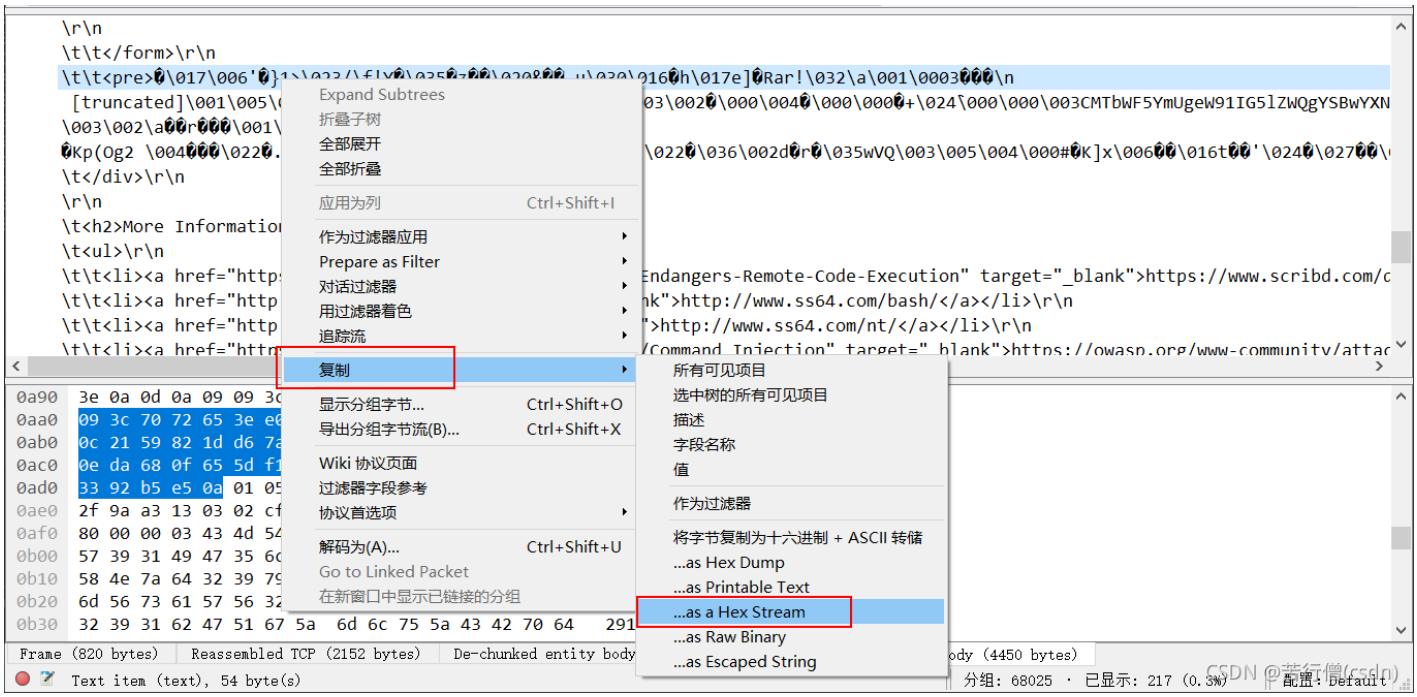
筛选http协议，发现No.62395包前后有几个POST的http请求，执行了命令注入。先执行了uname，后执行了ls，再后cat hsdhe.bin（这个有用），再后cat index.php等等……

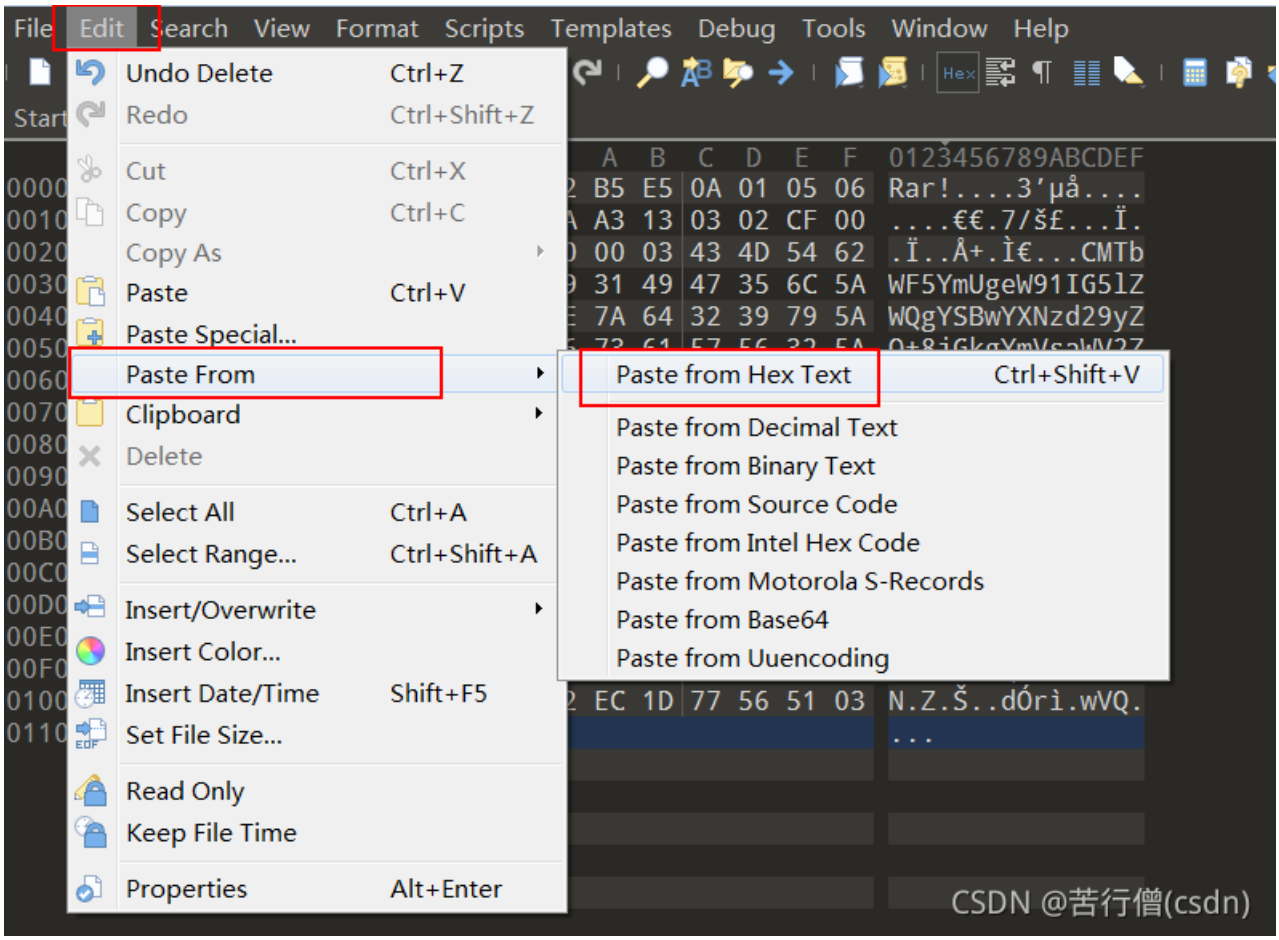
No.62395包，在 Line-based text data: text/html (111 lines) 右键-导出分组字节流-保存为.html，选择all files，浏览器打开这个html文件，就看到 f-l-a-g.txt 字样，前面还有Rar！，看来是个.rar压缩包里藏了flag。

关于rar文件格式，参考 RAR5 文件格式解析 - 乾坤盘的个人技术博客 。或者参考 RAR 5.0 archive format。注意，RAR5文件头(0x526172211A070100)，RAR5文件结尾(0x1D77565103050400) 这些显著的特征！

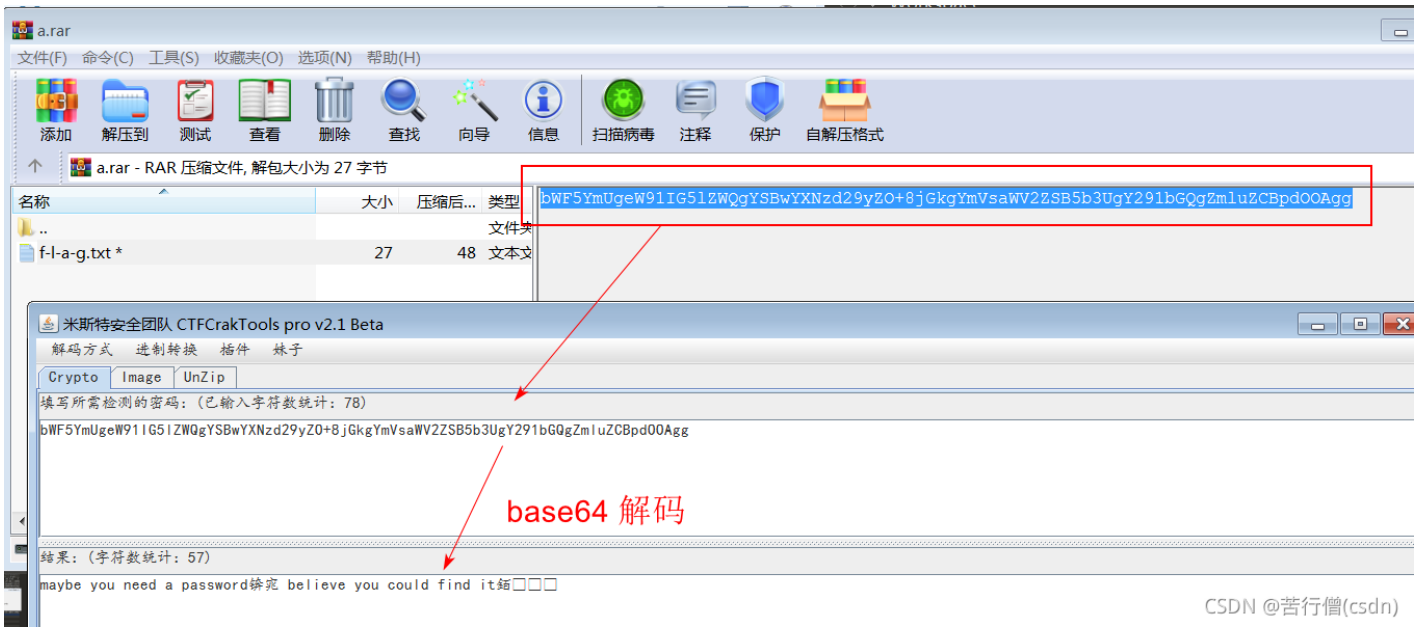


将可疑部分复制为Hex流，在010Editor里面选择Paste from hex，另存为a.rar提取到这个rar文件。





这个rar文件解压缩需要密码，同时也用base64编码提示了你需要一个密码，并且相信你可以找到密码。



那就不找密码了，直接 rar2john a.rar >> a.txt，然后 john a.txt 暴力破解，得到密码为goodluck。解压缩a.rar得到f-l-a-g.txt文件，里面就有flag —— flag{hdbw-dnsjpn-jndaj-AHH}

```
┌──(kali㉿kali)-[~/Desktop]
└─$ rar2john a.rar >> a.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ john a.txt
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 128/128 AVX 4x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 11 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 15 candidates buffered for the current salt, minimum 16 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
goodluck         (a.rar)
1g 0:00:00:27 DONE 2/3 (2021-11-08 11:02) 0.03602g/s 368.6p/s 368.6c/s 368.6C/s joshua..knight
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```