

BUUCTF-wireshark

原创

Nothing-one 于 2021-06-28 18:03:31 发布 148 收藏

分类专栏: [MISC](#) 文章标签: [安全](#)

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/li2254477890/article/details/118309052>

版权

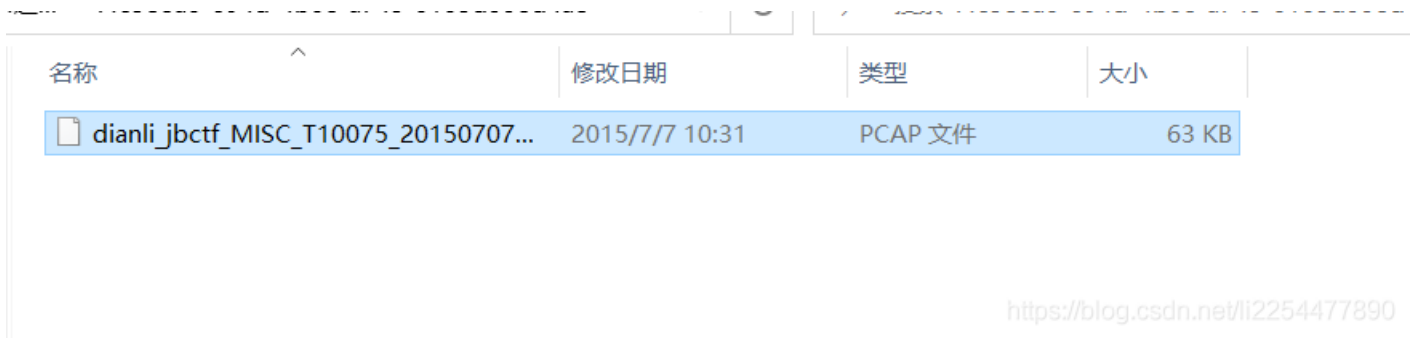


[MISC 专栏收录该内容](#)

15 篇文章 0 订阅

订阅专栏

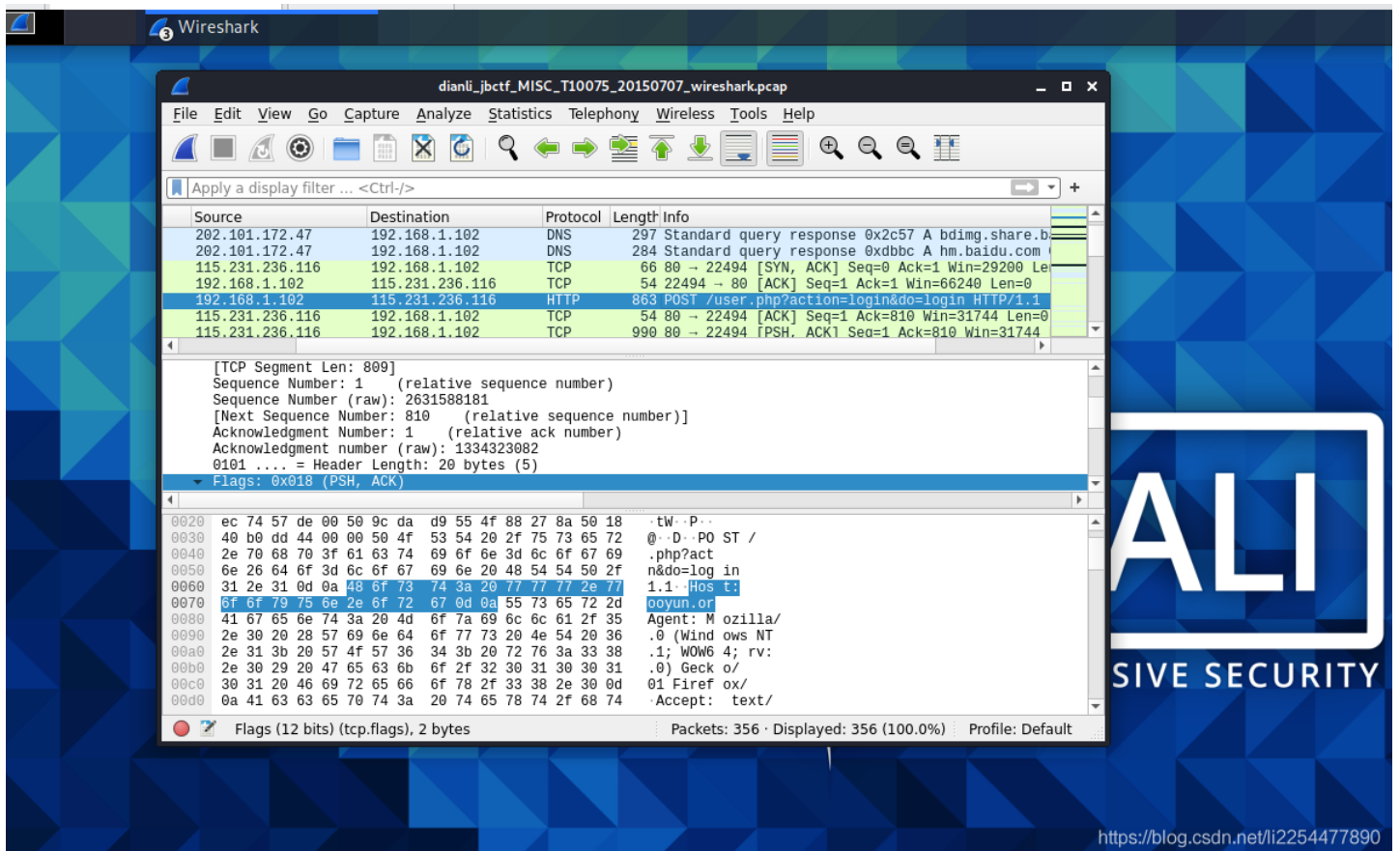
将文件下载之后就可以看到PCAP文件一般就是用流量分析(从题目也可以看到wireshark(这是一个流量分析文件))



<https://blog.csdn.net/li2254477890>

将

这个文件传到linux虚拟机中然后用虚拟机中的wireshark(这个可能是kali中的自带的。好久了忘了)



<https://blog.csdn.net/li2254477890>

将这个文件用wireshark打开，然后就可以在这里面找到登录的网站从题目中可以得到

题目

解题快手榜

X

wireshark

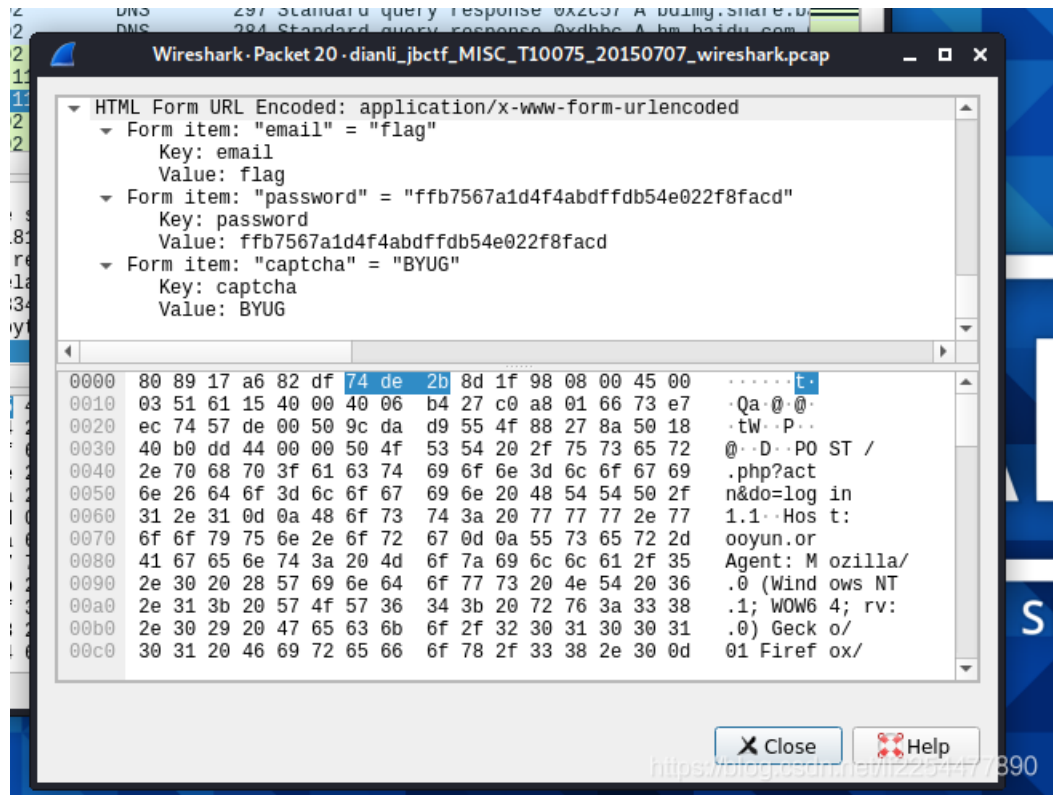
1

黑客通过wireshark抓到管理员登录网站的一段流量包（管理员的密码即是答案）注意：得到的flag 请包上 flag{} 提交

7fc3e8a0-69...

<https://blog.csdn.net/li2254477890>

flag就是密码。点开之后最下面我们可以看到这个网站的用



用户名和密码（也就是flag）

flag{ffb7567a1d4f4abdfdb54e022f8facd}



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)