

BUUCTF Misc 被嗅探的流量

原创

Misc真快乐:) 于 2022-02-26 10:30:12 发布 1624 收藏 1

分类专栏: [BUUCTF Misc](#) 文章标签: [wireshark](#) [网络安全](#) [信息安全](#)

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/Leslie_LIL/article/details/123146089

版权



[BUUCTF Misc 专栏收录该内容](#)

38 篇文章 0 订阅

订阅专栏

题目如下:

题目

解题快手榜

×

被嗅探的流量

1

某黑客潜入到某公司内网通过嗅探抓取了一段文件传输的数据, 该数据也被该公司截获, 你能帮该公司分析他抓取的到底是什么文件的数据吗? 注意: 得到的 flag 请包上 flag{} 提交

efa02e35-ee...

Flag

提交

CSDN @Misc真快乐:)

wireshark打开

No.	Time	Source	Destination	Protocol	Length	Info
54	20.597026	172.16.66.100	172.16.80.120	HTTP	828	POST /upload.php HTTP/1.1
233	25.545072	172.16.66.100	172.16.80.120	HTTP	375	POST /upload.php HTTP/1.1 (JPEG JFIF image)

追踪TCP流, 查找flag, 即可得到flag

```
o..b]-....j.....z6...*.....QM....B.....*.i.....:oe.vd.r.'...n..b.].7..G...T..^...Q,.U.X...@...j.j.m.e...E
9..M..t....e\k_b/.:Y'..'w>.B.....L.l...&,a.....C].C5P%.....).t.k.....8.!@-.J%I.|b.'.+
[a.?.#....=_..!.f....._..0.....s...+.F0....Uv.\*$..}].f.M..e..
...Y\....x.Y+...Q..5gi.Y.0..@w.[ .{...>q'j....s...N.....Zwi.?.
..M.....S.....A.D?\..s..}...
.,..i7$.I.M..Z..... x.o.c..y....s8.b.gwb.6...?.....V....KZ.
.....f.[...J...o.V.v...m...As.mP.....+.#.....#.....kx^....|.s.%YQ.{.=.....#.....N..*.....1.....!
*.q....g.Z....V?.O.".....m$......?.....?.....Y.>.....EZ...7..S..?.....d\..x..A..P...M...'.(.lou.#
C.*.j..E.....?.....z...(.o.....?Y_00...EW..
Q..9...R3...M.....V.....X.S..X.Z=...XI.....H/.a....j<9Zu0..T.#OKG..E[.
a.....?.....J.....f1-
-----WebKitFormBoundaryIeRPZp2QAo2zkI2U--
HTTP/1.0 500 Internal Server Error
Date: Tue, 18 Aug 2015 10:40:44 GMT
Server: Apache
```

CSDN @Misc真快乐 :)