攻防世界 Misc高手进阶区 5分题 latlong

原创

思源湖的鱼 于 2020-12-18 11:24:58 发布 500 收藏 1
分类专栏： ctf 文章标签： ctf 攻防世界 misc multimon-ng 无线电

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111355222

前言

继续ctf的旅程
攻防世界Misc高手进阶区的5分题
本篇是latlong的writeup

发现攻防世界的题目分数是动态的
就仅以做题时的分数为准了

解题过程

得到一个无后缀文件

file命令查看

```
latlong: RIFF (little-endian) data, WAVE audio, mono 48000 Hz
```

是个wav文件

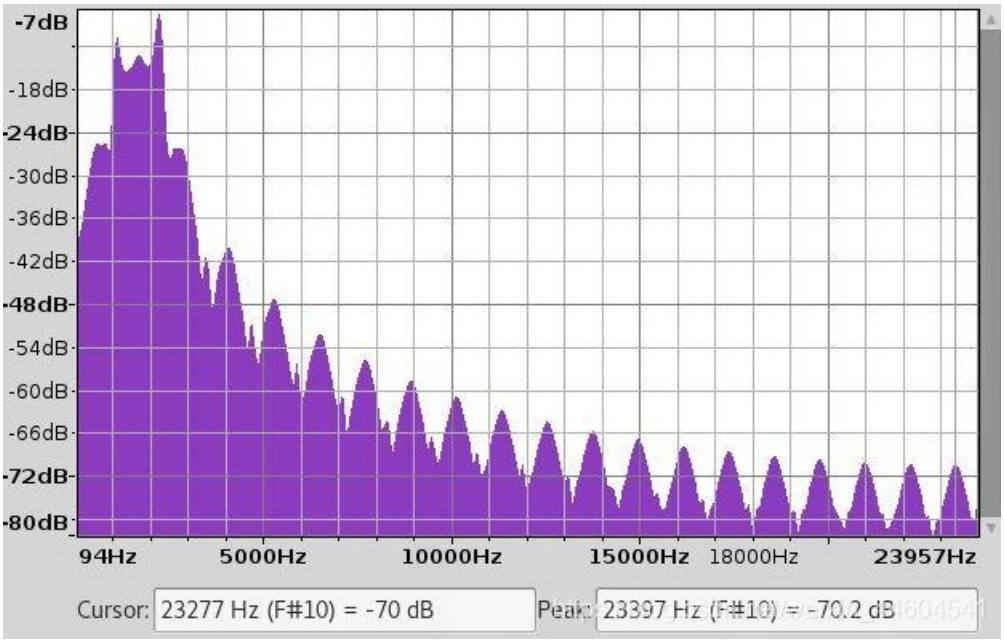
扔进audacity
无果

查了查
原题有提示

> Hint - "Ax25 will lead you in the direction"

AX.25（Amateur X.25）是数据链路层协议套件，旨在供业余无线电运营商使用
AX.25协议在物理层使用BFSK调制

用audacity看频谱



在1100 Hz和2200 Hz处有两个峰值
这是AX.25的BFSK中使用的两个音调

一个新工具’multimon-ng’

黑客工具名称：multimon-ng

开发者名称：EliasOenal

multimon-ng的开发者，包含在Kali Linux中

您能告诉我们您开发的工具的名称以及您为什么要创建它们的想法？

我在2012年第一次进入SDR时开始使用multimon-ng。（软件定义无线电）扫描频谱中的信号我注意到寻呼机通信，并且很遗憾地发现在Linux上没有简单的方法来解码这些数据。我尝试了与Debian捆绑在一起的multimon，但该项目多年来一直没有维护，64位版本完全没有功能。反过来，最初的工作重点是修复错误并将其移植到不同的操作系统，如Windows和MacOS X.一旦我再次使用基础知识，其他人加入了开发并帮助我大大扩展了功能。

您使用什么语言开发工具，为什么选择该语言？

最初的multimon是用C语言编写的，所以从来没有真正是我自己的选择。尽管如此，我可能会选择C，因为我的日常工作涉及很多嵌入式开发，我很欣赏这种语言的优点。一旦很多人开始在像树莓派这样的嵌入式平台上部署multimon-ng，我很高兴这个项目很少使用资源。

哪个是你最喜欢的黑客工具？它是一个框架吗？

我不确定我是否喜欢它，但是使用大量硬件我非常喜欢开源信号分析软件sigrok。

在使用multimon-ng前
需要先用sox把wav转为raw

```
sox -t wav latlong -esigned-integer -b16 -r 22050 -t raw latlong.raw
```

然后使用multimon-ng

```
cy@kalifisher:~/ctf$ multimon-ng -t raw -a AFSK1200 latlong.raw
multimon-ng 1.1.9
  (C) 1996/1997 by Tom Sailer HB9JNX/AE4WA
  (C) 2012-2020 by Elias Oenal
Available demodulators: POCSAG512 POCSAG1200 POCSAG2400 FLEX EAS UFSK1200 CLIPFSK FMSFSK AFSK1200 AFSK2400 AFSK2400_2 AFSK2400_3 HA
PN4800 FSK9600 DTMF ZVEI1 ZVEI2 ZVEI3 DZVEI PZVEI EEA EIA CCIR MORSE_CW DUMPCSV X10 SCOPE
Enabled demodulators: AFSK1200
AFSK1200: fm WDPX01-0 to APRS-0 UI  pid=F0
!/;E'q/Sz'O   /A=000000flag{f4ils4f3c0mms}
```

得到flag

结语

学到新的无线电知识了

知识点

- AX.25（Amateur X.25）协议
- multimon-ng工具