GACTF oldmodem writeup

原创

尸者狗 于 2020-09-01 06:32:36 发布 902 收藏

分类专栏： ctf-writeup 文章标签： 安全 信息安全

本文链接：https://blog.csdn.net/Alexhcf/article/details/108333175

版权

ctf-writeup 专栏收录该内容

6 篇文章 1 订阅

订阅专栏

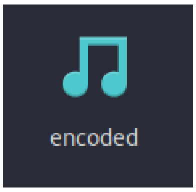
题目描述

old modem (bell 202)
China:
https://pan.baidu.com/s/184Trg9M94uVSekGycaAR_w (密码:5mp2)
Overseas:
https://drive.google.com/drive/folders/1T94OrcveHAZTmTCwaVCojLXYlJc3lL3f?usp=sharing

Writeup

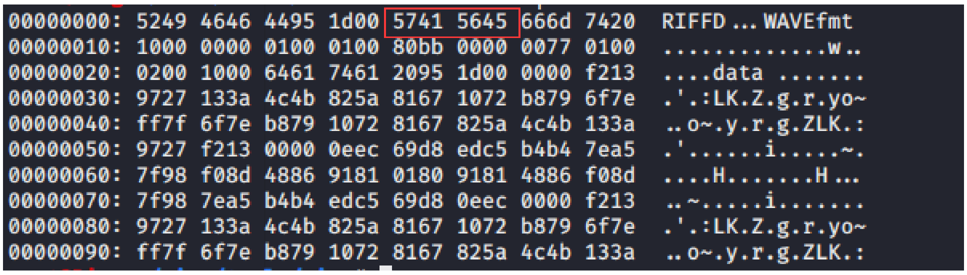
首先，modem是调制解调器（猫）的意思，Google发现bell 202是一种标准，完成这些信息收集后，正式开始
下载文件，文件无后缀，放入Kali
首先`file`命令看下文件类型
得到信息`oldmodem: Zip archive data, at least v2.0 to extract`
所以解压`unzip oldmodem`
解压后得到一个疑似音频类文件

```
Archive:  oldmodem
  inflating: encoded
```



再次`file`命令查看格式得到信息`encoded: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 48000 Hz`
由于是kali里，所以就不再拖入Windows使用winhex查看hex了，直接使用`xxd`命令

```
xxd encoded | head -n 10
```



```
00000000: 5249 4646 4495 1d00 5741 5645 666d 7420  RIFFD...WAVEfmt
00000010: 1000 0000 0100 0100 80bb 0000 0077 0100  .............w..
00000020: 0200 1000 6461 7461 2095 1d00 0000 f213  ....data .......
00000030: 9727 133a 4c4b 825a 8167 1072 b879 6f7e  .'.:LK.Z.g.r.yo~
00000040: ff7f 6f7e b879 1072 8167 825a 4c4b 133a  ..o~.y.r.g.ZLK.:
00000050: 9727 f213 0000 0eec 69d8 edc5 b4b4 7ea5  .'......i.....~.
00000060: 7f98 f08d 4886 9181 0180 9181 4886 f08d  ....H.......H...
00000070: 7f98 7ea5 b4b4 edc5 69d8 0eec 0000 f213  ..~.....i.......
00000080: 9727 133a 4c4b 825a 8167 1072 b879 6f7e  .'.:LK.Z.g.r.yo~
00000090: ff7f 6f7e b879 1072 8167 825a 4c4b 133a  ..o~.y.r.g.ZLK.:
```

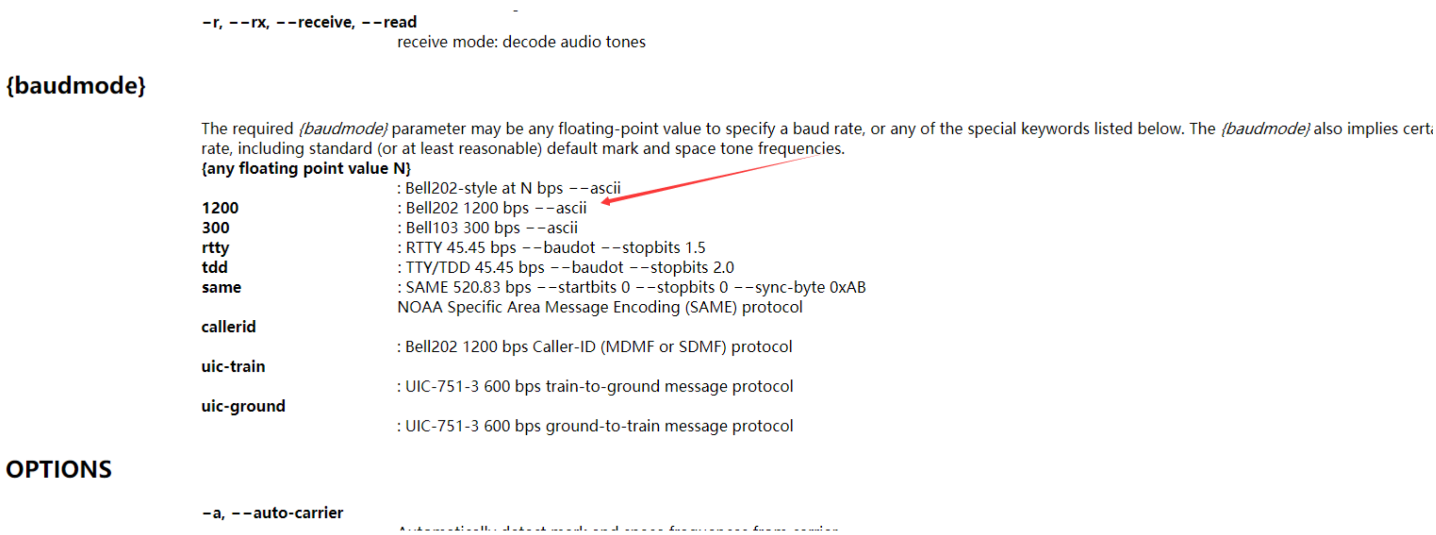
确定encode文件是一个WAV文件，修改后缀，尝试播放，声音很杂，联想开头收集的信息，尝试从帽上入手

使用的工具：minimodem

kali可通过apt 命令直接安装`apt-get install minimodem`

查看软件手册

正好就有所谓的bell 202



−r, −−rx, −−receive, −−read
receive mode: decode audio tones

{baudmode}

The required *{baudmode}* parameter may be any floating-point value to specify a baud rate, or any of the special keywords listed below. The *{baudmode}* also implies certa
rate, including standard (or at least reasonable) default mark and space tone frequencies.

{any floating point value N}
: Bell202-style at N bps −−ascii
1200 : Bell202 1200 bps −−ascii
300 : Bell103 300 bps −−ascii
rtty : RTTY 45.45 bps −−baudot −−stopbits 1.5
tdd : TTY/TDD 45.45 bps −−baudot −−stopbits 2.0
same : SAME 520.83 bps −−startbits 0 −−stopbits 0 −−sync-byte 0xAB
NOAA Specific Area Message Encoding (SAME) protocol
callerid
: Bell202 1200 bps Caller-ID (MDMF or SDMF) protocol
uic-train
: UIC-751-3 600 bps train-to-ground message protocol
uic-ground
: UIC-751-3 600 bps ground-to-train message protocol

OPTIONS

−a, −−auto-carrier
Automatically detect mark and space frequencies from carrier

-r 指定读取模式

-f 选择读取的文件

1200 指定Bell202 1200 bps

输入如下

```
minimodem -r -f encoded 1200
### CARRIER 1200 @ 1200.0 Hz ###
The Bell 202 modem was an early (1976) modem standard developed by the Bell System. It specifies audio frequency-shift keying (AFSK) to encode and transfer data at a rate of 1200 bits per second, half-duplex (i.e. transmission only in one direction at a time). These signalling protocols, also used in third-party modems, are referred to generically as Bell 202 modulation, and any device employing it as Bell-202-compatible.

Bell 202 AFSK uses a 1200 Hz tone for mark (typically a binary 1) and 2200 Hz for space (typically a binary 0). In North America, Bell 202 AFSK modulation is used to transmit Caller ID information over POTS lines in the public telephone network. It is also employed in some commercial settings.

In addition, Bell 202 is the basis for the most commonly used physical layer for the HART Communication Protocol - a communication protocol widely used in the process industries.

Surplus Bell 202 modems were used by amateur radio operators to construct the first packet radio stations, despite its low signalling speed. A modified Bell 202 AFSK modulation, a common physical layer for AX.25, remains the standard for amateur VHF operation in most areas. Notably, Automatic Packet Reporting System (APRS) transmissions are encoded this way on VHF. On HF, APRS uses Bell 103 modulation.

The Bell 202 standard was adopted around 1980 as the communications standard for subsea oil and gas production control systems, pioneered by the then FSSL (Ferranti Subsea Systems Ltd.) Controls, a spin-out company from the former TRW - Ferranti joint venture in the UK. This modulation standard was retained until around 2000, when it was superseded by faster FSK and PSK modulation methods, although it is still utilised for extension of existing control systems that are already configured for this technique.

The 202 standard permitted useful techniques such as multi-dropping of slave modems to allow multiple nodes to be connected to the host via a single modem channel. Other techniques have included superposition of signal on power conductors, and distances in excess of 80 km were achieved in subsea applications using these techniques. This has been enhanced through the use of Manchester encoding over the FSK link, to provide simple Modulo-2 RZ (return to Zero) bit error detection and suppression improvement over these long distances.

Here is the flag: GACTF{9621827f-a41b-4f27-8d72-9e0b77415a4f}
### NOCARRIER ndata=2423 confidence=4.397 ampl=0.997 bps=1200.00 (rate perfect) ###
```