Re300

出题背景：

Re300原本的出题人跑路了，我临时帮他出题。随手找了个DDoS木马。本着不互相伤害的原则。没有用MIPS版本，没有去掉符号表。所以就很easy了。

首先，题目提供一个ELF可执行文件（re300）和抓的包（dump.pcap）。提示信息flag(ip:port)，那自然是找被打的ip和端口号了。

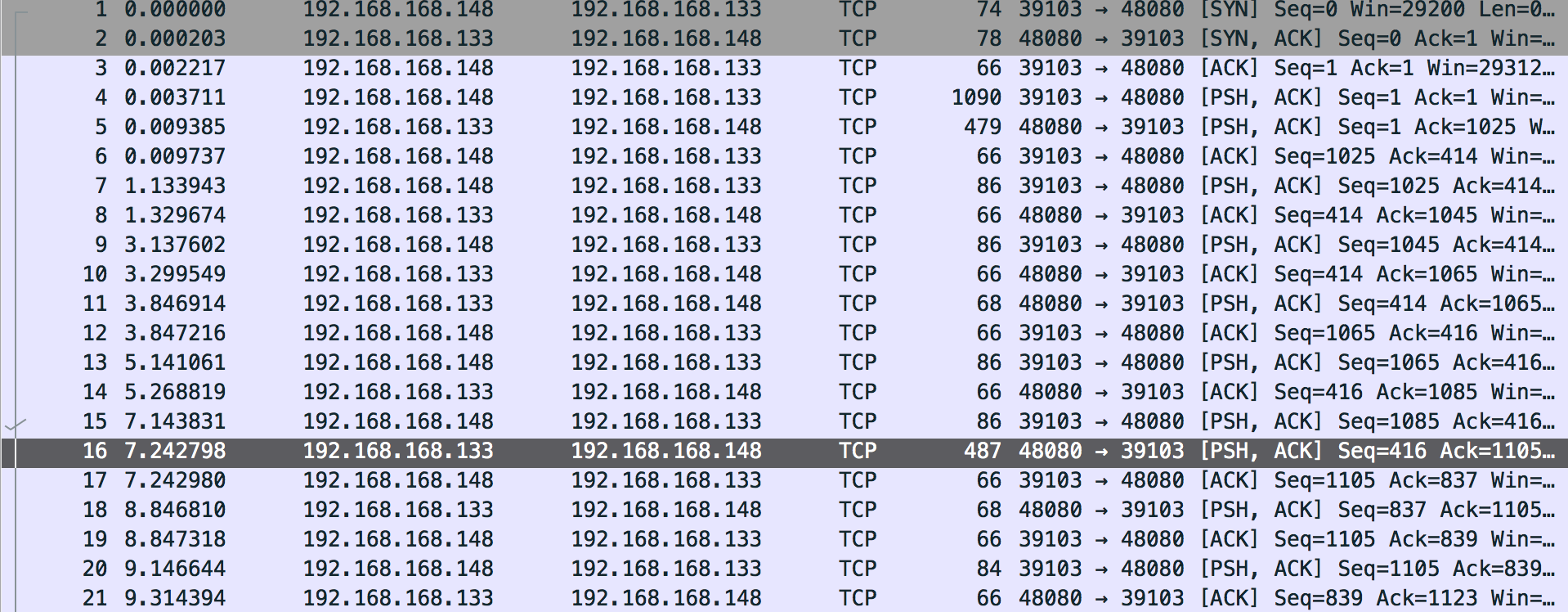
关于此马的详细分析可参考

<https://www.sans.org/reading-room/whitepapers/malicious/analyzing-backdoor-bot-mips-platform-35902R_y_RQ>

因为使用AES加密数据包，遂家族命名为AES.DDoS。本样本产自China的变种台风ddos，支持多平台MIPS，Windows，Linux等。

解题思路：

首先观察数据包，就那么几条。显然C&C IP为192.168.168.133，上线端口48080，而Victim IP 为192.168.168.148（由第4个数据包可以确定）。那么可以确定第16个数据包，为中控IP像肉鸡发送的指令包。



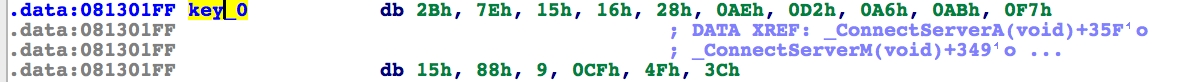
懂得人自然懂。数据包的格式一般为【指令号+数据内容】

在**\_ConnectServerA**函数里

106行接收buffer，前4个字节表示指令号，当其为6时（118行），执行DealwithDDoS



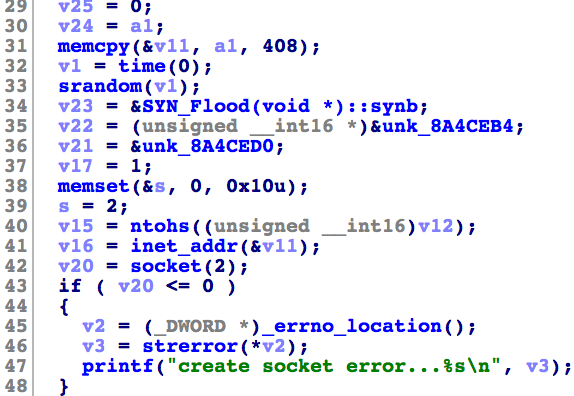
ok，接下来我们可以发现程序使用AES算法开始解密，同时注意到数据包中存在重复的数据“7df76b0c1ab899b33e42f047b91b546f”，很容易联想到分组加密的ECB（电码本）模式，并且分组长度是16，这点从**key0**也可以辅证。



由此我们可以解密出数据包。接下来就是找到数据包中表示ip和port的字段。这个看一下DealwithDDoS（128行）这个函数。数据包的偏移位置0x184表示attackMode(SYN,TCP,UDP...)，那0x188处就是轮数了吧。



随便挑一个mode跟进，**SYN\_Flood**函数。40行和41行分别取出port，ip。至此，题目想要的数据已经分析出来了。



最后就是写个脚本的事情了。

from Crypto.Cipher import AES

from struct import unpack

from hashlib import md5

with open('./re300') as fp:

fp.seek(0xe81ff)

key = fp.read(16)

with open('./dump.pcap') as fp:

data = fp.read()

idex = data.find('\x06\x00\x00\x00')

data = data[idex+4:idex+0x1a4]

aes = AES.new(key , AES.MODE\_ECB)

text = aes.decrypt(data)

ip = text[:text.find('\x00')]

port = unpack('<H',text[0x1d4-0x54:][:2])[0]

flag = md5(ip+':'+str(port)).hexdigest()

print 'flag is: {0}'.format(flag)