

HGAME 2021 Week1 Writeup--6vv+

Pwn

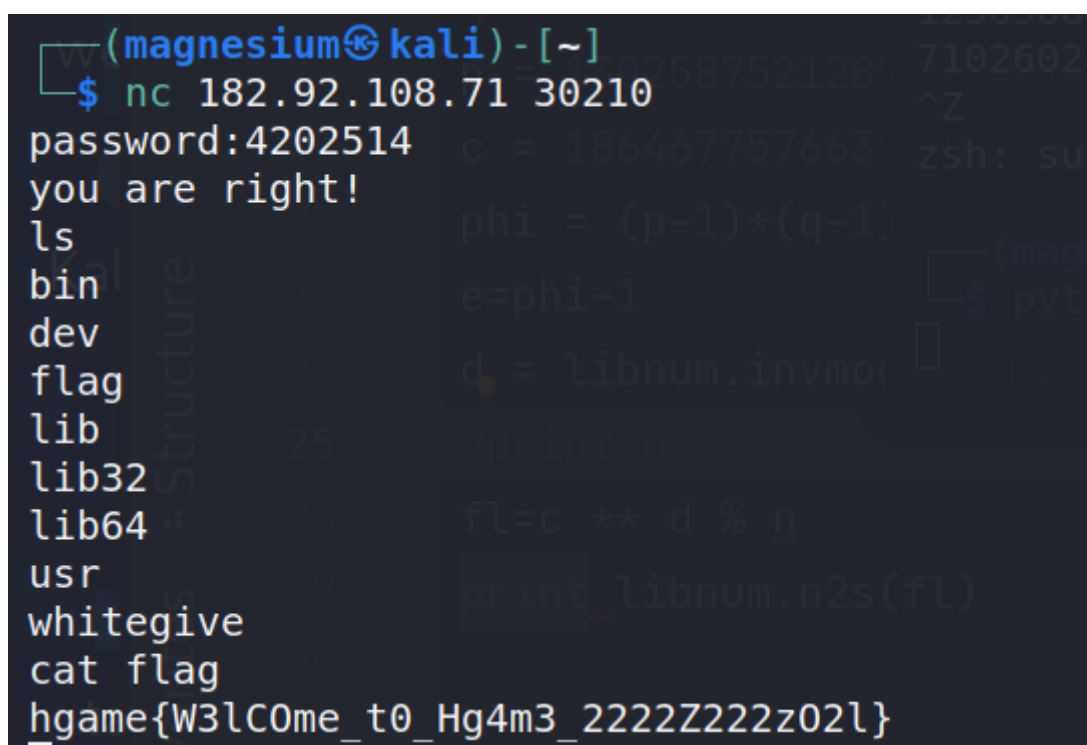
whitegive

c语言中字符串字面量的值是该字符串的首地址，因此用ida打开二进制文件找到“paSsw0rd”字符串的首地址为0x402012

```
0000000040200E aLd          db '%ld',0          ; DATA XREF: main+39fo
00000000402012 aPassw0rd    db 'paSsw0rd',0        ; DATA XREF: main+51fo
0000000040201B ; const char s[]
```

```
nc 182.92.108.71 30009
```

输入0x402012的十进制即可getshell



```
(magnesium@kali) - [~]
$ nc 182.92.108.71 30210
password:4202514
you are right!
ls
bin
dev
flag
lib
lib32
lib64
usr
whitegive
cat flag
hgame{W3lC0me_t0_Hg4m3_2222Z222z02l}
```

```
hgame{w3lC0me_t0_Hg4m3_2222Z222z02l}
```

MISC

Base全家福

Base16编码使用16个ASCII可打印字符（数字0-9和字母A-F）对任意字节数据进行编码。

Base32编码是使用32个可打印字符（字母A-Z和数字2-7）

Base64编码是使用64个可打印ASCII字符（A-Z、a-z、0-9、+、/）将任意字节序列数据编码成ASCII字符串，另有“=”符号用作后缀用途。

```
R1k0RE10WldHRTNFSU5SVkc1QkRLTlpxR1VaVENOUlRHTVlETVJCV0dVMlVNTlpVR01ZREtSUlVIQTJET01
aVuDSQ0RHTVpwsVlAVEVNWlFHTVpER01KWElRPT09PT09
```

使用base64

```
GY4DMNZWGE3EINRVG5BDKNZWGUZTCNRTGMYDMRBWGU2UMNZUGMYDKRRUHA2DOMZUGRCGDMZVIYZTEMZQGMZ  
DGMJXIQ=====
```

使用base32

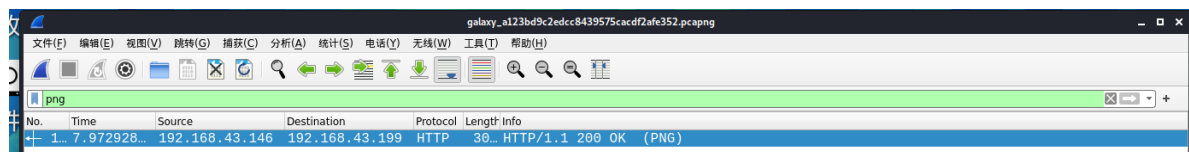
```
6867616D657B57653163306D655F74305F4847344D335F323032317D
```

使用base16

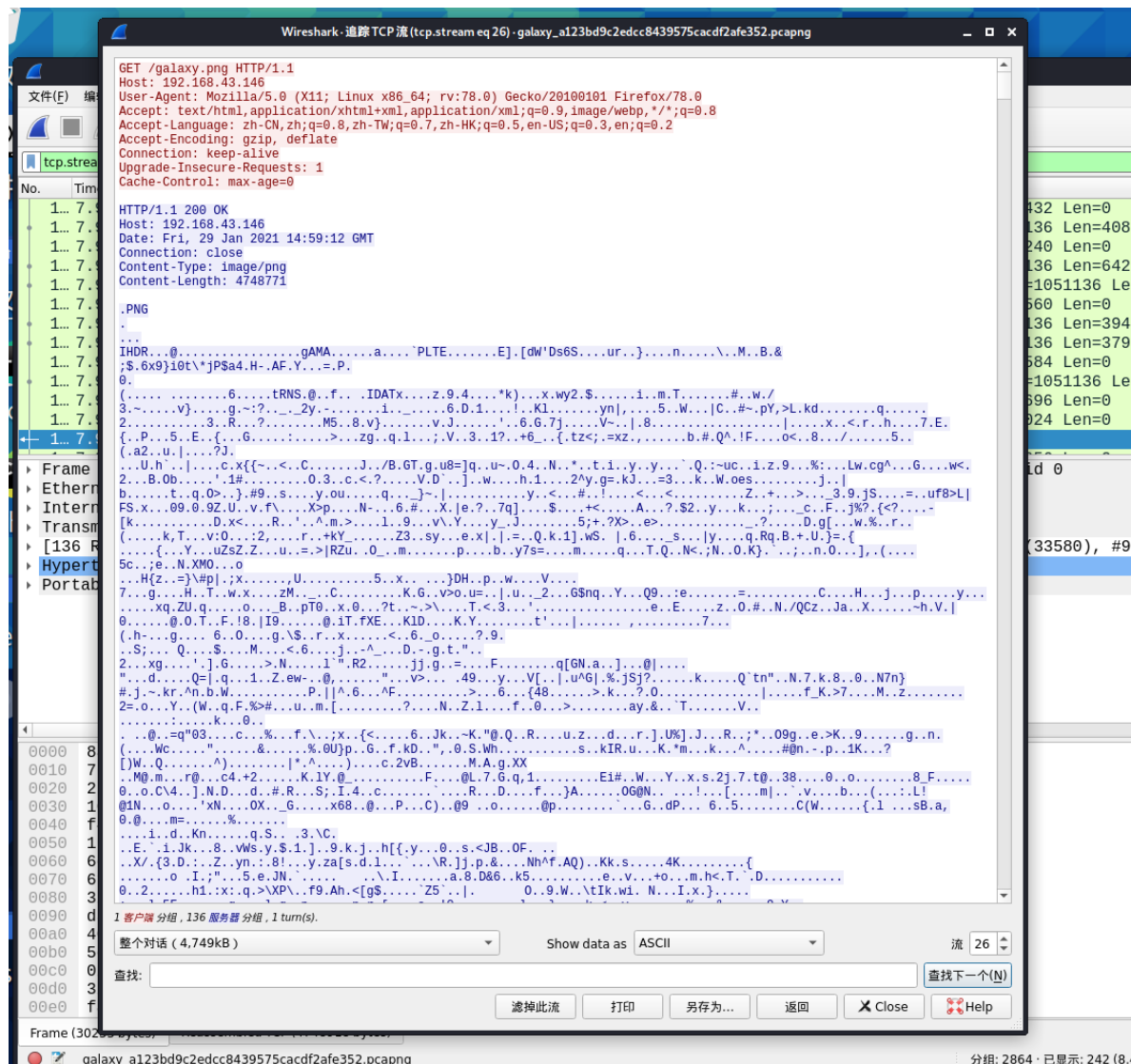
```
hgame{we1c0me_t0_HG4M3_2021}
```

Galaxy

拿到一个pcapng文件，放进wireshark里流量分析，因为找的是图片，尝试搜索一下png，找到一个包



追踪TCP流



发现png格式图片信息，把它导出得到图片，ghex修改一下图片的尺寸后发现flag在图片下方

PNG文件结构分析<https://my.oschina.net/ososchina/blog/801358>

