Jarvis OJ平台WEB部分port51 writeup

原创

昔曰 于 2020-08-19 13:02:18 发布 261 收藏 2

分类专栏： CTF

本文链接：https://blog.csdn.net/dkz6174510/article/details/108098035

题目链接：http://web.jarvisoj.com:32770/

看到提示说要用51端口访问该网页，注意！这里的51端口指的是源端口，不是目的端口，目的端口是服务器搭建该服务的端口，只有服务器可以变动，你能改变的是你使用的源端口，这里可以用curl的local-port选项来实现。

```
C:\Users\Administrator>curl --local-port 51 http://web.jarvisoj.com:32770/
<!DOCTYPE html>
<html>
<head>
<title>Web 100</title>
<style type="text/css">
        body {
                background:gray;
                text-align:center;
        }
</style>
</head>

<body>
        <h3>Please use port 51 to visit this site.</h3>
</body>
</html>
```


相信很多小伙伴都遇到上图的问题，我不是指定源端口为51端口了吗？它怎么还继续叫我用51端口访问呢？

这里需要注意一下，在公网上跑的数据包都是用的公网地址，如果你的源地址用的是私网地址的话，能跑出去但是回不来，所以这里就需要经过地址转换（理解地址转换的可以忽略，比如说你叫小明，你想送个数据包给百度，麻烦网络设备转交：请帮我转交给百度，大家都知道百度，所以顺利送达，可是百度回信的时候：请帮我转交回给小明，这时网络路由设备就蒙了，可是如果你进行了地址转换就不一样了，比如说转换成了广东省xx市电信，这时百度回信的时候就可以说请帮我转交给广东省xx市电信，这时网络路由设备就能顺利回信了，当然进行了地址转换的话，百度也只知道信是广东xx市电信送给他的，不知道有小明这号人，所以不管你小明在那喊我要用哪个端口送出去都是没用的）现在因为ipv4地址不够用的问题，现在很多运营商给家用宽带分配的都是运营商的保留地址，并不是公网地址，最后再由运营商的NAT设备将你的地址进行转换，因为大家都需要上网，所以运营商不可能给你按照你的源端口进行转换，而是随机选一个空闲的端口转换，所以很有可能源端口就不是51了，你直接用网况且如此，更别说虚拟机了，虚拟机联网从虚拟机出到物理机就已经经过一次地址转换，不过不管经过多少次地址转换，你需要访问的服务器看到你的源端口都是你使用的公网地址的端口。

所以说，其实需要你拥有公网地址，你访问公网服务器的源端口才真正掌握在你的手上，这里我用我租的阿里云的vps来进行

```
[root@izn56k051ui0v8z ~]# curl --local-port 51 http://web.jarvisoj.com:32770/
<!DOCTYPE html>
<html>
<head>
<title>Web 100</title>
<style type="text/css">
        body {
                background:gray;
                text-align:center;
        }
</style>
</head>

<body>
        <h3>Yeah!! Here's your flag:PCTF{M45t3r_oF_CuRl}</h3>
</body>
</html>
```


成功拿到flag！！！