实验室服务器遭挖矿病毒攻击报告II

在之前经历过挖矿攻击之后，今天（2021.4.15）吴梓凡再次报告GPU跑满，查看占用GPU的进程发现是在同样一个位置运行了挖矿脚本。

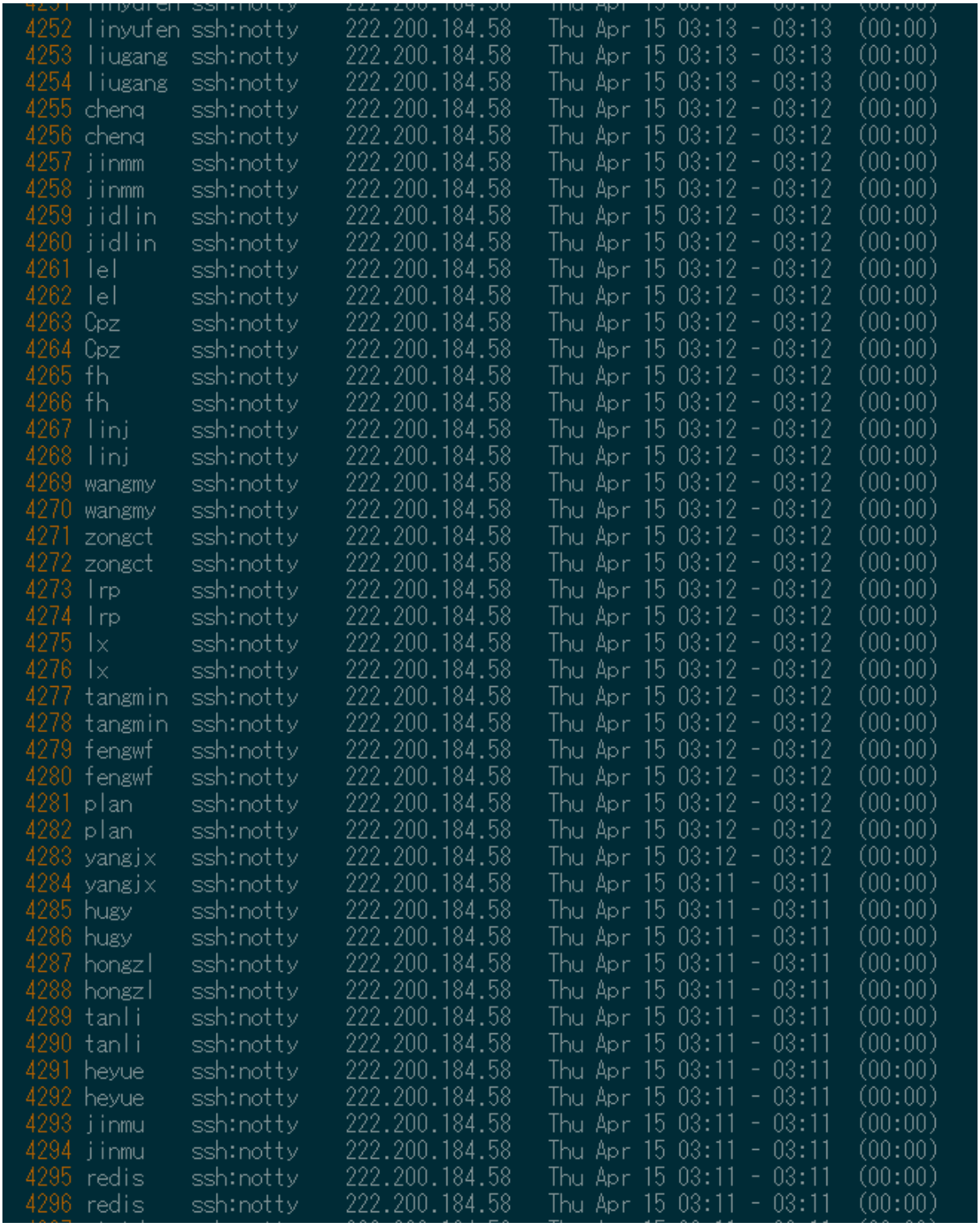
重要结论：

禁用密码登录，采用公钥登录SSH

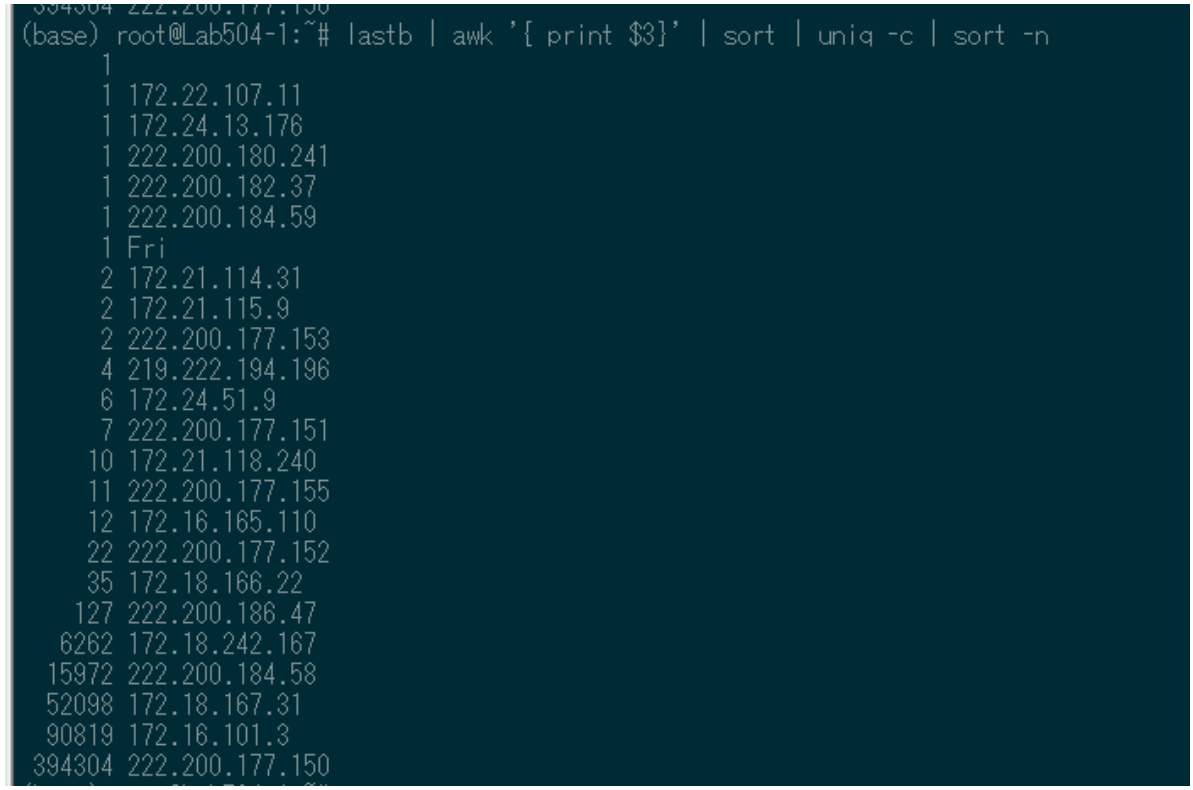
所有用户即刻使用强密码

查证过程：

上轮攻击之后所有用户设置了强密码，并更改了root密码，自此服务器的安全得到了基本保障。但在今天再次报告了GPU挖矿。分析后怀疑对方再次破解密码，遂查询lastb，获得失败的历史连接请求，发现有暴力尝试密码行为：



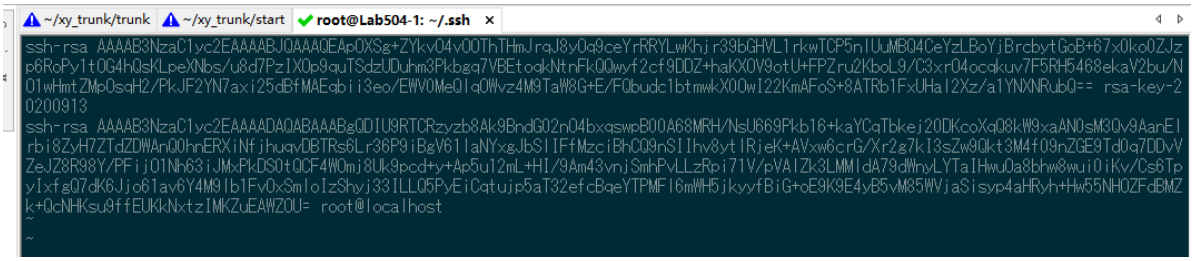
分析连接发起者，得到几个非实验室主机的高失败链接ip：



值得注意的是本机ip也进行了多次失败连接，怀疑是获得了用户密码后尝试获得root密码。

对连接进行分析，发现实验室成员的姓名全拼和缩写均出现在记录中，每个用户名尝试十余次，怀疑攻击者爬取中山大学学生及教师名单，并用预设简单密码暴力破解。

分析发现，至今有外部链接尝试我服务器密码，分析后认为服务器密码更改后未泄露，怀疑攻击者在本机放置公钥后密钥登陆。遂在root目录下发现两条无人认领公钥， 该authorized_keys文件更新日期为4月6日，与服务器遭受攻击日期相符。



处理：

删除无人认领公钥；

再次更换密码；

未来计划全面禁用密码ssh登录。