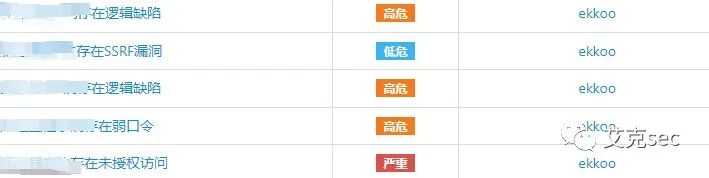
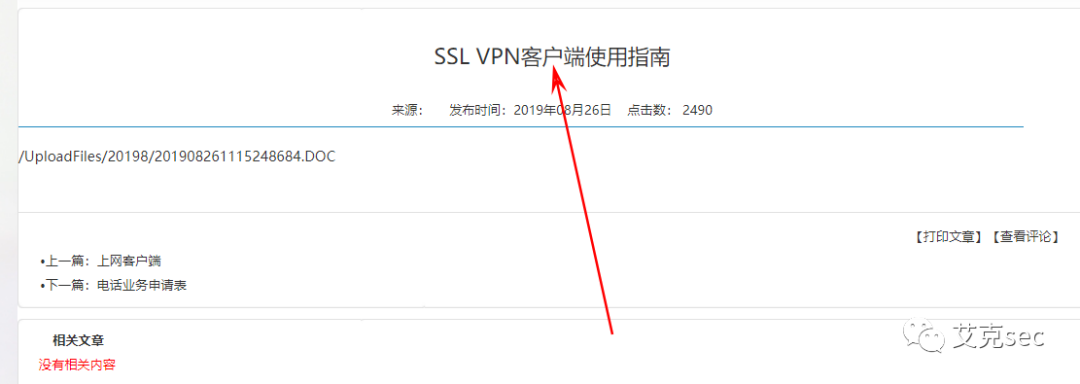
打点了很多天，只是进入了一些系统的后台，挖到了一些逻辑洞，但是找不到shell点。

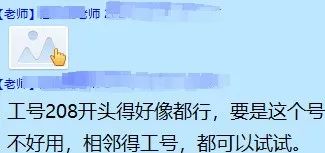


转换思路直接用vpn去连接内网，去官网收集vpn的信息，很顺利 默认账号密码和使用说明都写在了官网上 ^^





信息收集老师的工号（收集不到直接爆破也可以 6位数可能时间较久）



收集到了前三个字母为208，直接上burpsuite爆破 很多账号都是默认密码，成功连vpn进入内网（没想到这一切能这么顺利~）

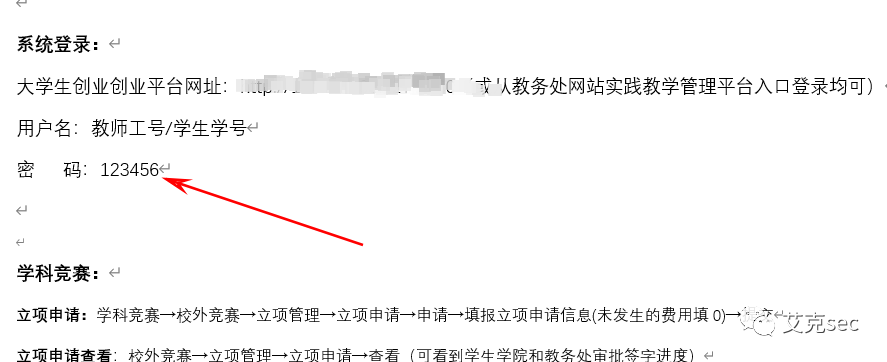


**内网渗透**

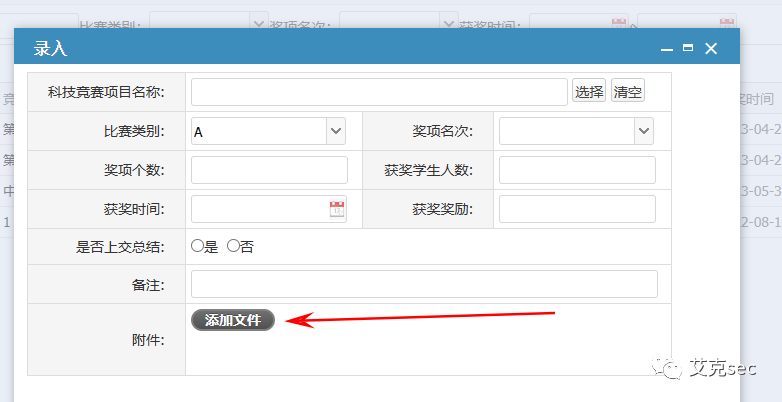
之前收集到一个资产，外网访问不到，连了vpn再试试，果然~



这种系统一看就是那种学生或者老师开发的，安全意识肯定不是很高，且收集到了默认密码

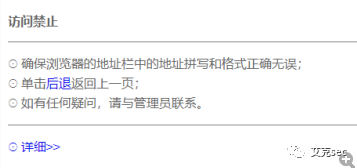


进入后台目的明确，直接寻找上传点

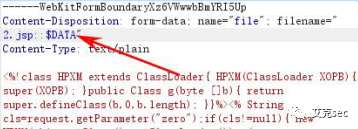


看看是黑白名单，发现为黑名单 且有waf

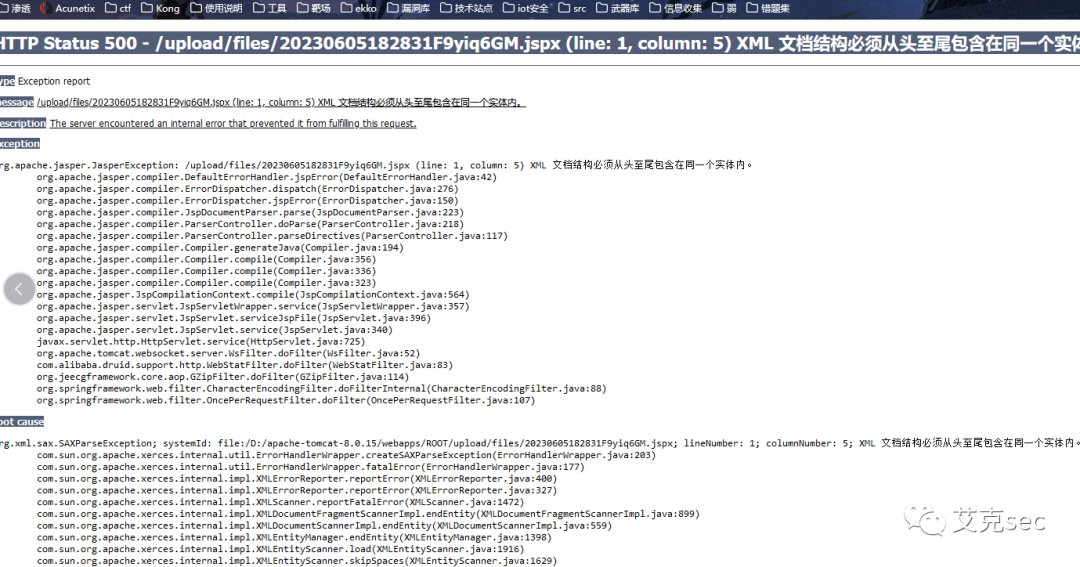
文件名只要是jsp或者jspx直接给你ban掉，用空格等思路都绕过不了，



发现该主机为windows主机，windows主机有个特性就是文件名识别到jsp:$DATA 会自动去掉 成功bypass文件名

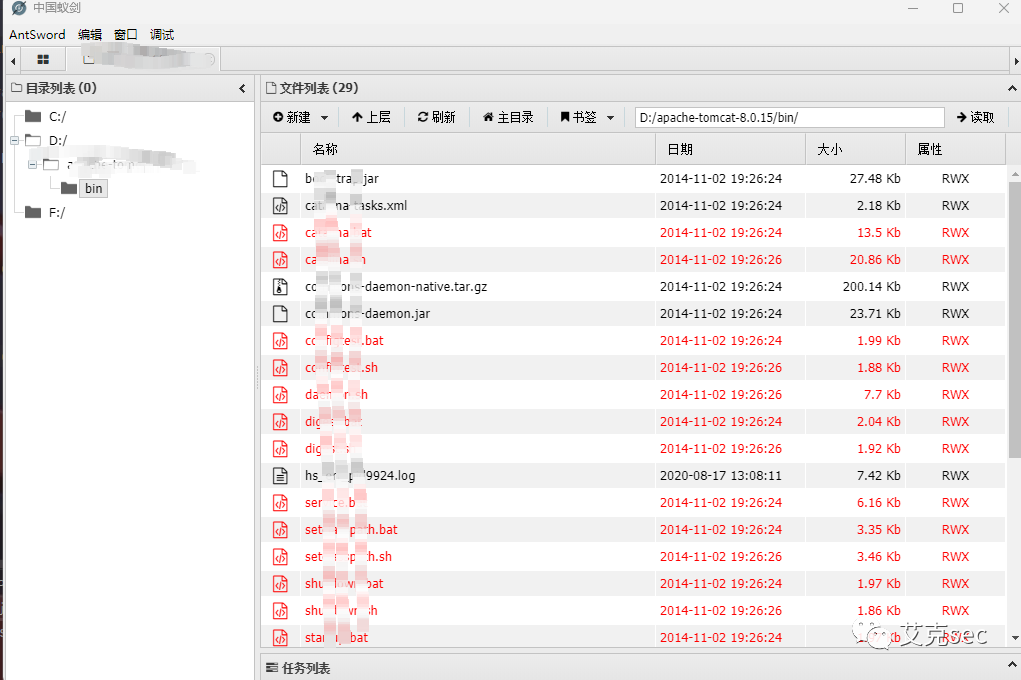


但是马子上传还是拦截，找了一些免杀的方法都不太可行

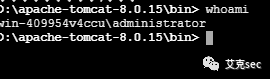


最后 最近刚拿捏面试进大国企的某佬分享了一个免杀马，大哥nb~  直接bypass





经典whoami  高权限用户

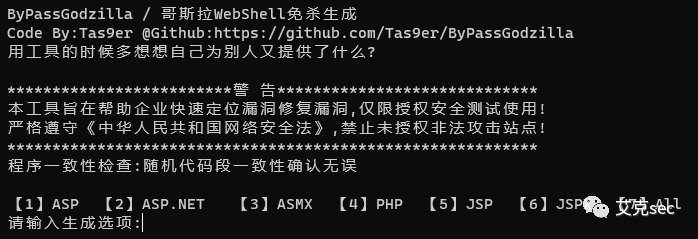


此时感觉要芜湖起飞了 准备传哥斯拉马抓密码， 3389端口是开的 直接上号~

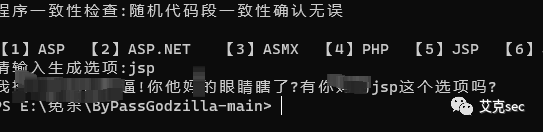
可是现实很骨感  哥斯拉马一上就杀，cs也一样

看了进程是装了360企业版

再次寻找到大佬们写的哥斯拉免杀工具 脚本小子的我 就是白嫖就是用



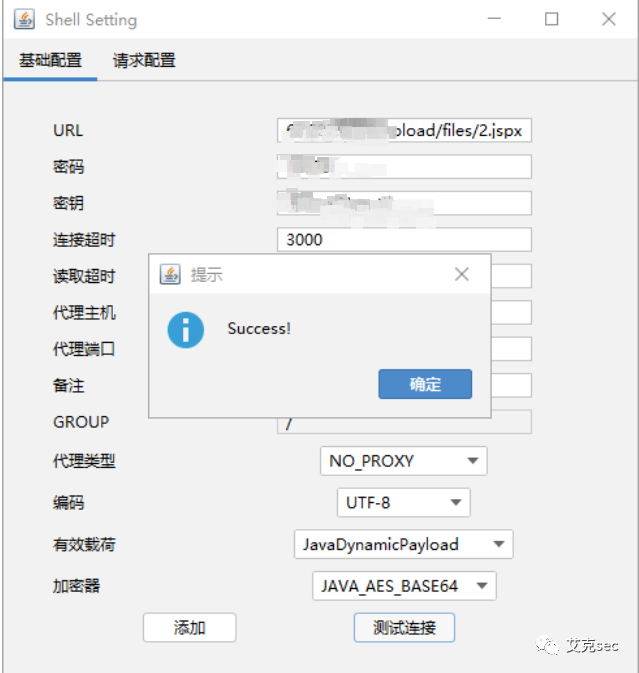
我输入了jsp 然后....... 我人麻了哈哈哈



输入5 生成哥斯拉jsp免杀马 试了一下还是杀，我又生成了一个jspx的上传上去 发现成功bypass了~



激动人心的时刻到了 ！！



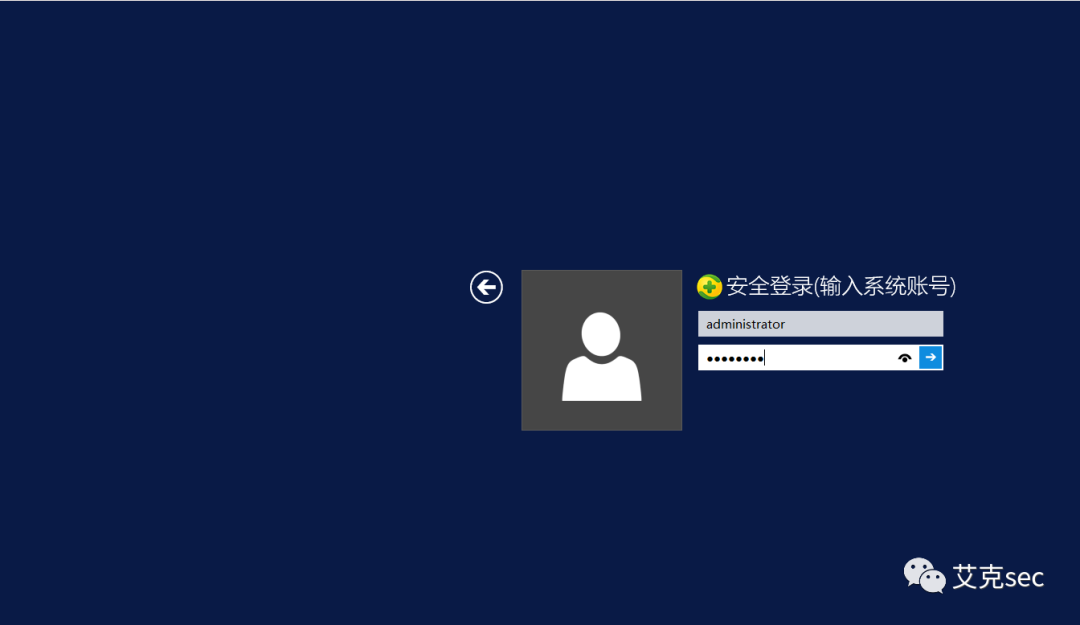
芜湖，用mimikatz抓取windows主机的密码



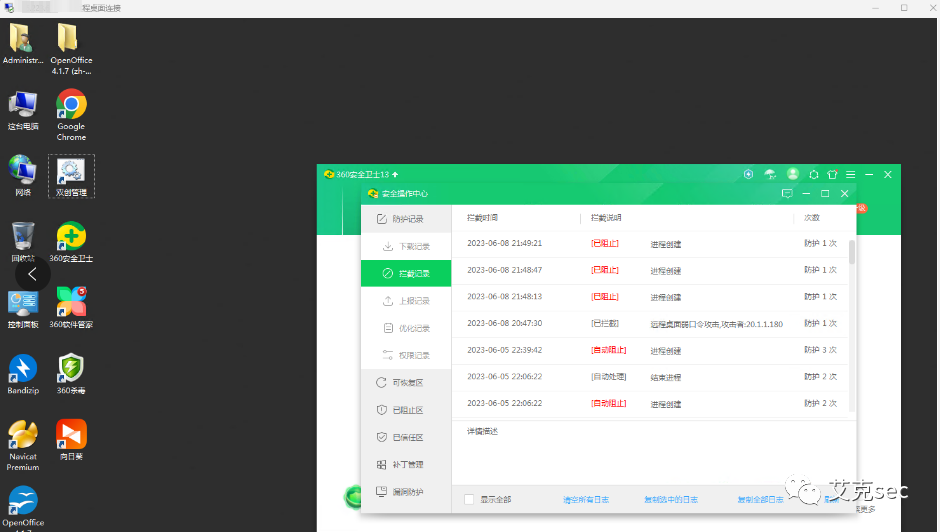
没抓到明文密码 幸运的是是一个弱口令 cmd5直接解密出来了



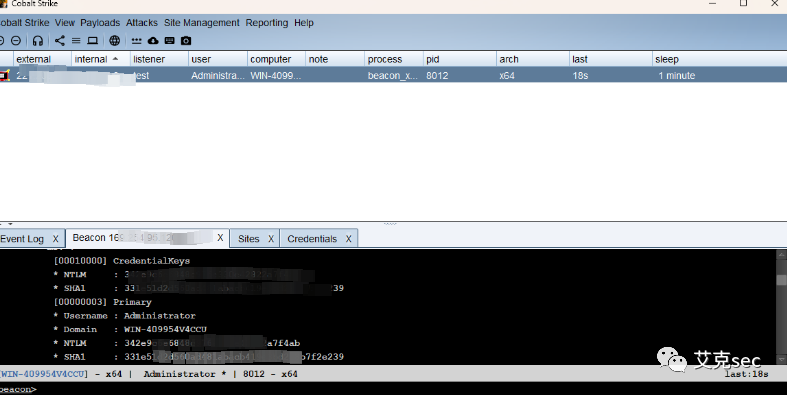
还等什么，直接3389登陆喽



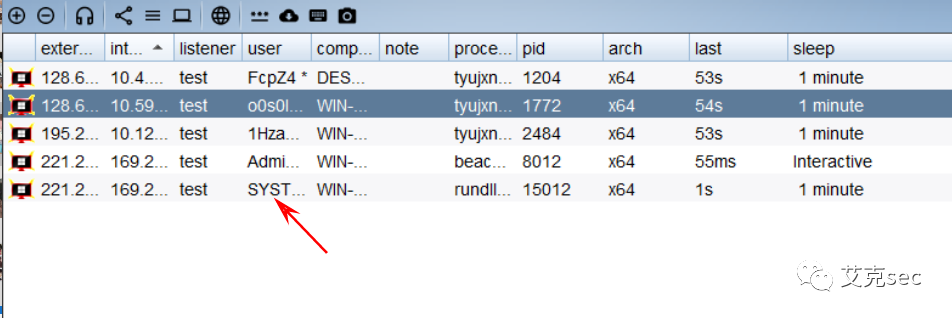
找到了罪恶的360 拦截我的记录 ………… 直接给他关掉，或者加个信任区文件夹 传入心心爱爱的CS马



上线！用自带的提权脚本提权~



administrator提到system

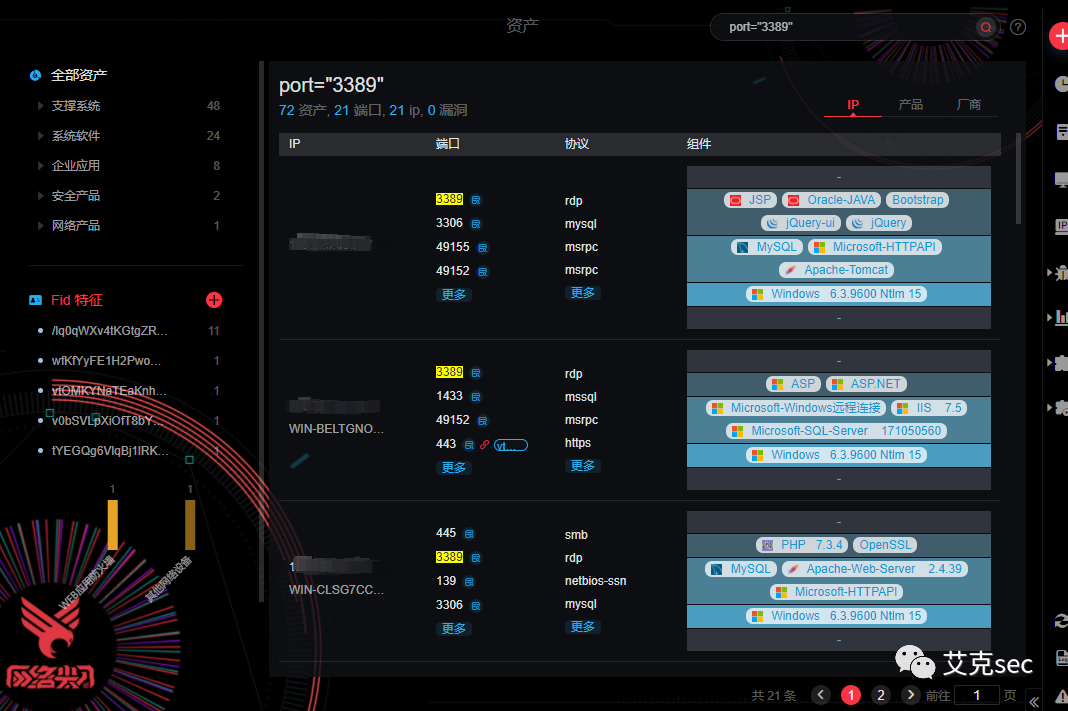


进行信息收集 查看网络信息，路由表，是否在域内 等等



发现有两个网段，不在域内

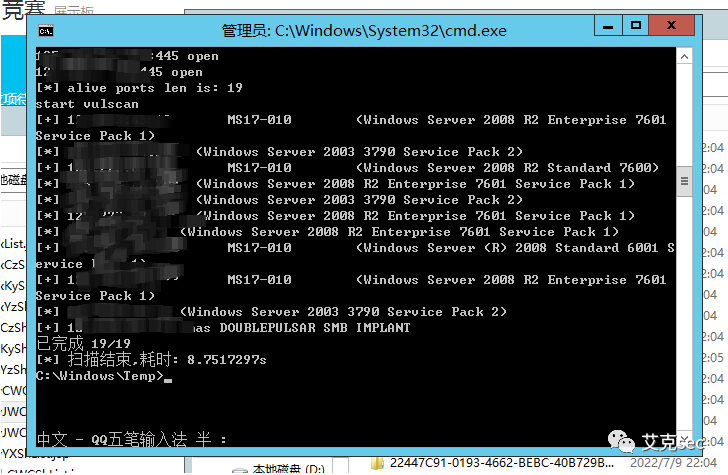
准备拿下更多主机，先用goby整理一下资产 发现开启3389端口的主机还真不少，用这台已知的主机账号密码去碰撞 看看能不能成功登陆



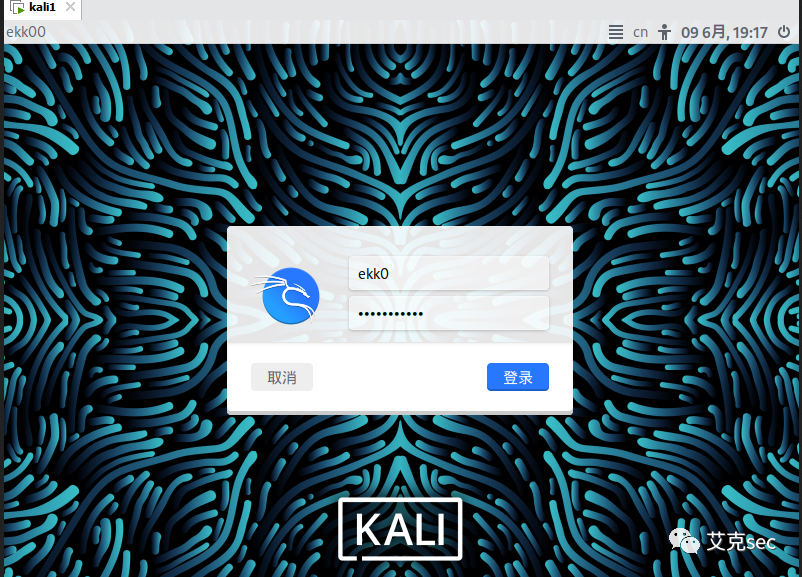
很遗憾只有这一台主机 其他的密码都不相同

转换思路

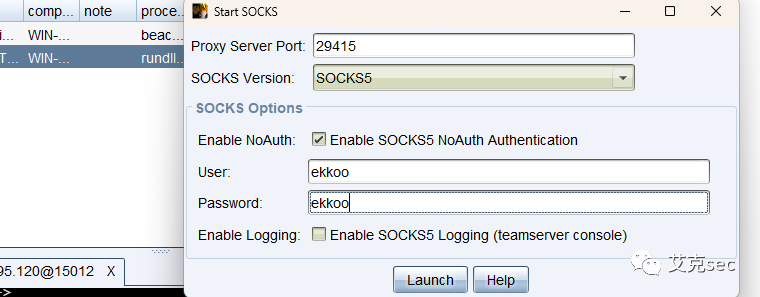
在攻陷的机器上用fscan扫了一下ms17010，有四台主机存在该漏洞



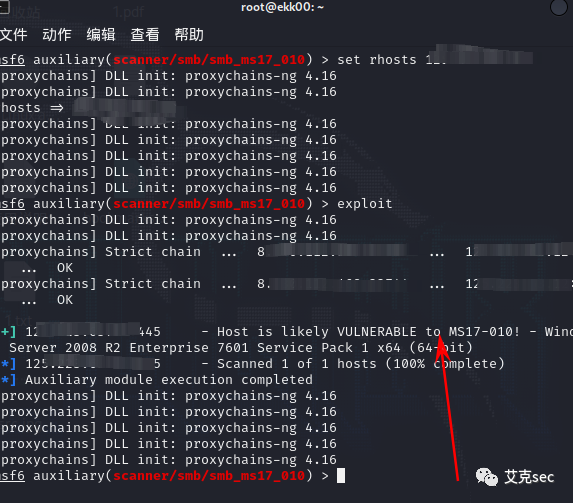
登入kali 打开msf 开搞



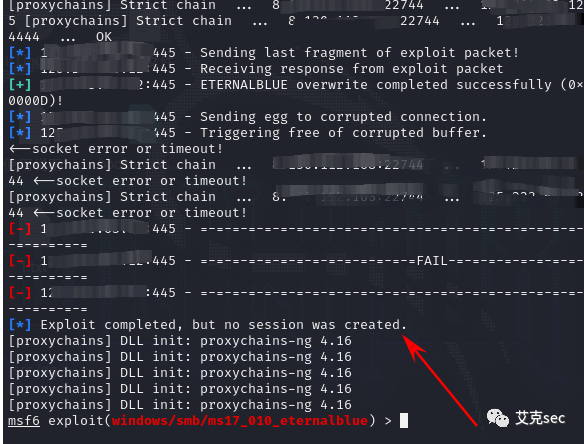
因为存在漏洞主机445端口只对这台机器开放，是不对我们网络开放的，需用cs自带的功能搭建隧道



kali配置socks5隧道代理 并用代理打开msf 进行扫描该漏洞 再次证明该漏洞存在



进行攻击

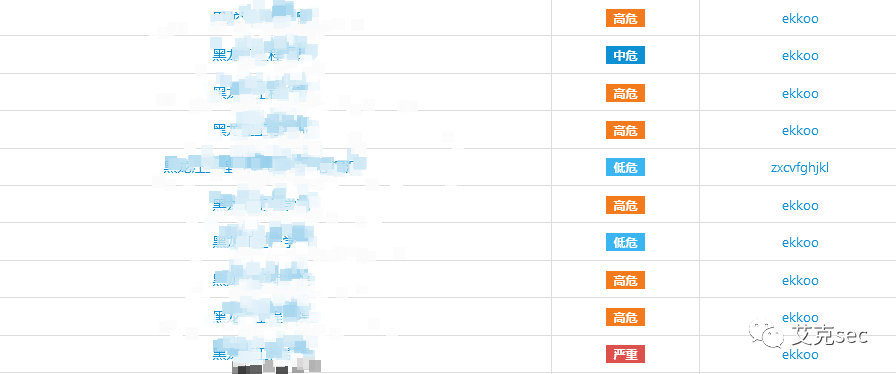


攻击成功但是建立会话失败，刚开始以为是正反向shell的问题

最后发现应该还是360搞的鬼，payload被拦截了

后面又去了其他web站点打了打，找到了一些信息泄露，任意文件读取，弱口令等等但是均未shell，也就不能进行进一步的内网渗透。

一个入门安全圈半年的萌新仔的第一次内网渗透就此结束了...    只拿到了一台主机权限，，，（太菜了）



发现以后要学习的东西还有很多，免杀，代审，工具二开等等