

一般打内网，有域是肯定要打域控的。没域的话，是工作组环境，就打内网的其他服务。要打域控，首先得找到域控。

这里所谓的找到域控，主要是拿到三要素：

- 1、域控的机器的名字
- 2、域的名字
- 3、域控的机器对应的域内的 ip

有的时候不一定三要素都能俱全，需要通过横向慢慢的来摸。

但是内网中，根据环境不同，找域控的实战环境也不尽相同。

下面以笔者的实战为例：

**eg1: 进入内网，有域，但是不能直接查找域控的机器名字**  
net group "Domain Controllers" /Domain #查找域控机器的名字

```
C:\phpStudy\PHPTutorial\WWW\public> net group "Domain Controllers" /Domain
这项请求将在域 sun.com 的域控制器处理。

发生系统错误 5。

拒绝访问。
```

这里查不了，但是爆出了域的名字

尝试 ping

```
C:\phpStudy\PHPTutorial\WWW\public> ping sun.com
正在 Ping sun.com [192.168.138.138] 具有 32 字节的数据:
来自 192.168.138.138 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.138.138 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.138.138 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.138.138 的回复: 字节=32 时间<1ms TTL=128

192.168.138.138 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

成功定位到域控的 ip

**eg2: 进入内网，也找到了域控的名字，但是 ping 域控的时候发现并不能得到自己想要的域控 ip**

首先通过 ipconfig 得到了 dns 的名字

```
C:\phpStudy\WWW\yxcms> ipconfig /all
Windows IP 配置

. . . . .
主机名 . . . . . : stu1
主 DNS 后缀 . . . . . : god.org
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 . . . . . : god.org
```

通常情况，dns 服务器搭建在域控服务器上

因此这里可以 ping 这个地址尝试获取域控的 ip

```
C:\phpStudy\WWW\yxcms> ping god.org >> god.txt
C:\phpStudy\WWW\yxcms>
```

查看文件

```
编辑: C:/phpStudy/WWW/yxcms/god.txt
C:/phpStudy/WWW/yxcms/god.txt
1
2 正在 Ping god.org [72.14.178.174] 具有 32 字节的数据:
3 请求超时。
4 请求超时。
5 请求超时。
6
```

这个 72 的 ip，很明显是个外网 ip



那么此时 ping 的办法就失效了，需要切换别的办法，这题有以下解法

### 1、尝试找内网的 dns 服务器的 ip，也在 ipconfig /all 里面

```
C:\phpStudy\WWW\yxcms> ipconfig /all
Windows IP 配置

主机名 . . . . . : stu1
主 DNS 后缀 . . . . . : god.org
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 . . . . . : god.org

以太网适配器 本地连接 4:

   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-A7-C1-B2
   DHCP 已启用 . . . . . : 否
   自动配置已启用 . . . . . : 是
   本地链接 IPv6 地址 . . . . . : fe80::fa:367a:e700:4d72%25 (首选)
   IPv4 地址 . . . . . : 192.168.52.143 (首选)
   子网掩码 . . . . . : 255.255.255.0
   默认网关 . . . . . : 192.168.52.2
   DHCPv6 IAID . . . . . : 721423401
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-24-F3-A2-4E-00-0C-29-A7-C1-A8
   DNS 服务器 . . . . . : 192.168.52.138
                               8.8.8.8
   TCP/IP 上的 NetBIOS . . . . . : 已启用
```

可以直接定位域控的 ip

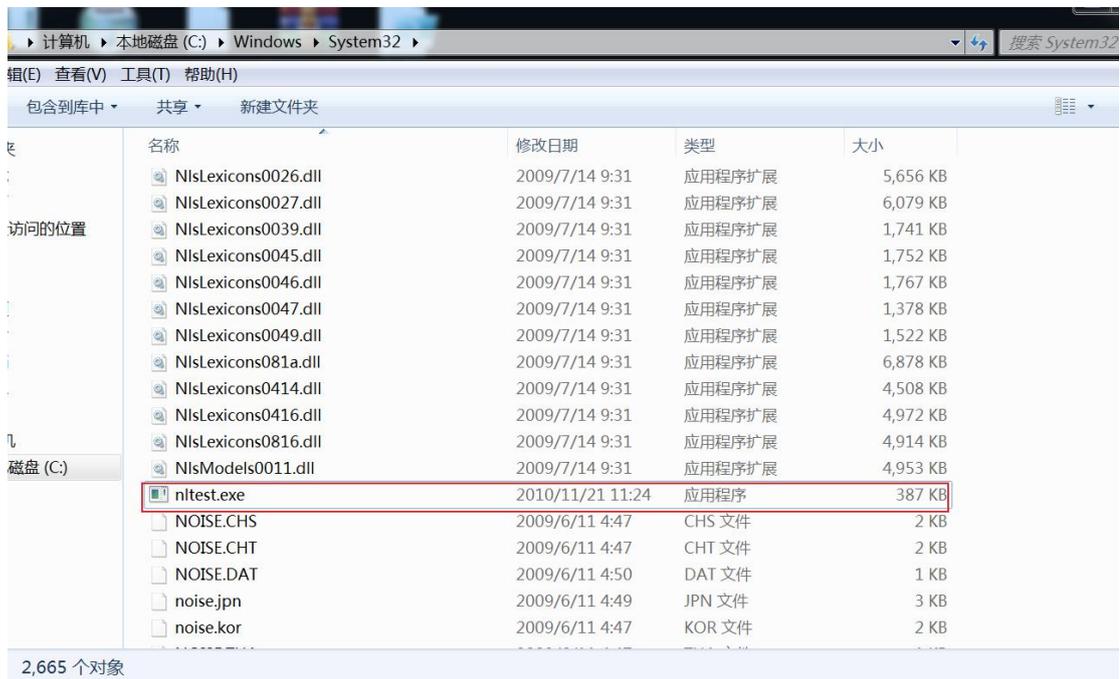
## 2、利用 nltest 命令

nltest /dsgetdc:域名称

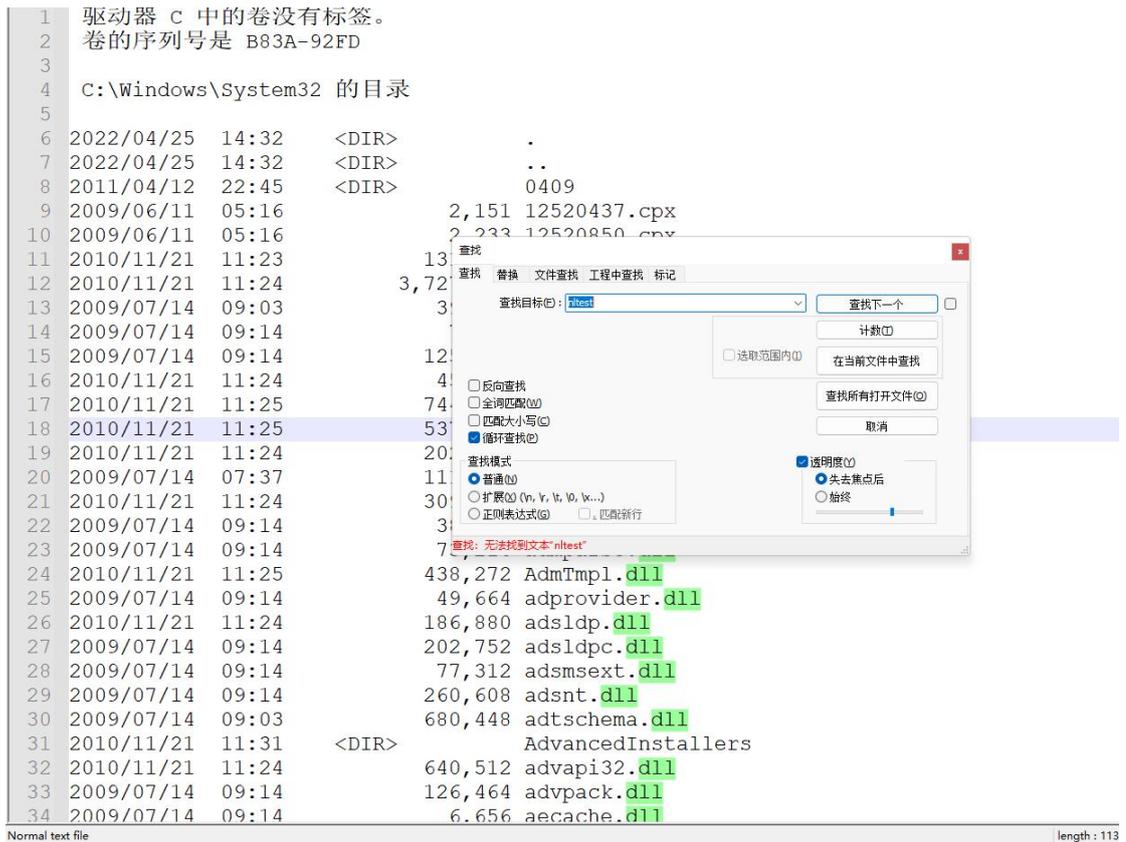
```
C:\Users\Administrator\Desktop>nltest /dsgetdc:god
DC: \\0WA
地址: \\192.168.52.138
Dom Guid: a350098d-b47a-4dc3-b602-68713c90fda4
Dom 名称: GOD
林名称: god.org
DC 站点名称: Default-First-Site-Name
我们的站点名称: Default-First-Site-Name
标志: PDC GC DS LDAP KDC TIMESERU GTIMESERU WRITABLE DNS_FOREST CLOSE_S
TE FULL_SECRET WS
此命令成功完成
```

但是这种方法有时候在拿到 webshell 其实并不能用

在目标机器上，nltest.exe 这个文件是在 Windows/System32 文件夹里面的



但是如果通过 webshell 来寻找



是连个毛都找不到的  
原理未知，但是感觉很神奇。

面对这种情况，也并非没有办法  
直接找到和系统版本相符的 nltest.exe，然后传一个上去试试

| Icon   | Filename   | Modified            | Size     | Permissions |
|--------|------------|---------------------|----------|-------------|
| Folder | upload     | 2019-10-13 09:01:07 | 0 b      | 0777        |
| File   | .htaccess  | 2013-08-20 01:46:49 | 175 b    | 0666        |
| File   | fucku.php  | 2022-04-04 09:48:26 | 6.25 Kb  | 0666        |
| File   | god.txt    | 2022-04-25 06:15:24 | 200 b    | 0666        |
| File   | httpd.ini  | 2013-08-20 01:46:32 | 214 b    | 0666        |
| File   | index.php  | 2013-08-20 01:46:49 | 509 b    | 0666        |
| File   | nltest.exe | 2022-04-25 06:36:15 | 386.5 Kb | 0777        |
| File   | robots.txt | 2013-08-20 01:46:43 | 83 b     | 0666        |
| File   | .....txt   | 2013-12-25 03:13:57 | 920 b    | 0666        |

执行命令

```

C:\phpStudy\WWW\yxcms> cd C:/phpStudy/WWW/yxcms/

C:\phpStudy\WWW\yxcms> nltest.exe
Error loading resource: 0x00003b01

C:\phpStudy\WWW\yxcms> nltest.exe -h
Error loading resource: 0x00003b01

C:\phpStudy\WWW\yxcms>

```

什么鬼，还是不行  
但是如果我换一套环境，又可以了

```
C:/Oracle/Middleware/user_projects/domains/base_domain/ >nlttest /dsgetdc:delay
DC: \\DC
地址: \\10.10.10.10
Dom Guid: 53b5fede-5137-4186-bc46-f3fdda3fd5a1
Dom 名称: DE1AY
林名称: delay.com
DC 站点名称: Default-First-Site-Name
我们的站点名称: Default-First-Site-Name
标志: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_FOREST CLOSE_SITE FULL_SECRET WS 0xC000
此命令成功完成
```

感觉有点玄学，后期再来研究这个小问题  
总之给了两套解决方案，哪套行就用哪套

最后附上几条比较关键的域内命令，也不是很多，但是经常用。

我是建议背下来，一方面是面试官喜欢问，另一方面做项目的时候，有时候甲方在我旁边看着我做，我直接键盘一敲，给他夸夸一顿整，甲方目瞪口呆，项目的预算顿时又增加了，嘻嘻。

ipconfig /all //可以查看域控名字 然后找到 dns 服务器 然后找到域控

net view /domain:demo //可以查看域内机器

net group "domain users" /domain //域内用户列表

net user /domain //短版域内用户列表，但是需要 rpc 开启

net group "domain admins" /domain //域内管理员用户列表

done