Virtual Private Network (VPN) Lab

2018级 信息安全 管箫 18307130012

Task 1: VM Setup

我们将需要三台虚拟机。

Server

ens33（Internet)

ip : 192.168.61.138 mac： 00:0c:29:01:41:ae

ens38（Internel)

ip： 192.168.226.1 mac： 00:0c:29:01:41:b8

Host U

ens33（Internet)

ip： 192.168.61.139 mac： 00:0c:29:a3:8a:e6

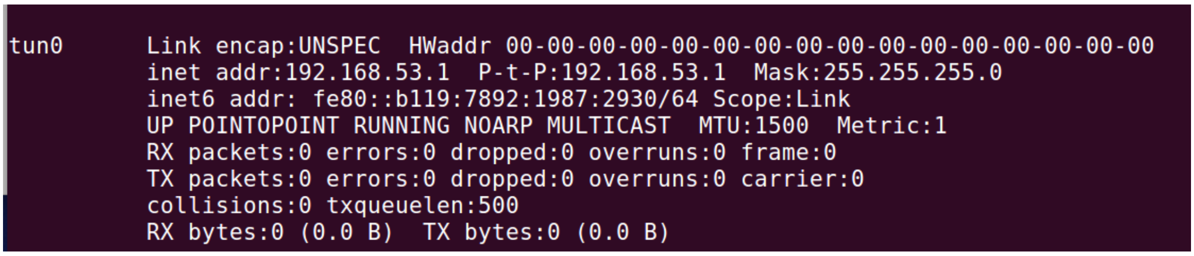
Host V

ens33（Internel)

ip： 192.168.226.101 mac： 00:0c:29:aa:55:ad

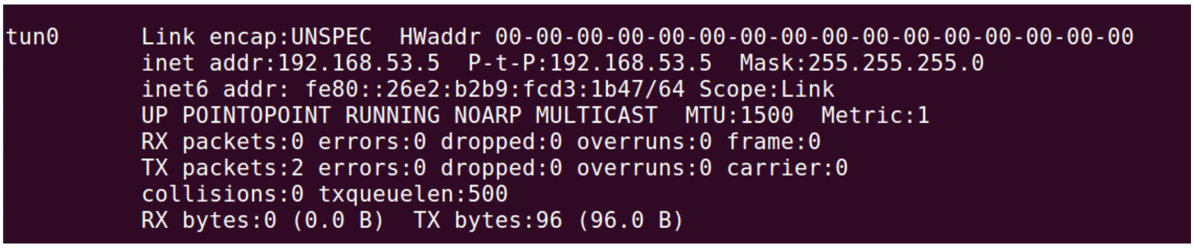
Task 2: Creating a VPN Tunnel using TUN/TAP

Step 1: Run VPN Server.



```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.53.1  P-t-P:192.168.53.1  Mask:255.255.255.0
          inet6 addr: fe80::b119:7892:1987:2930/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

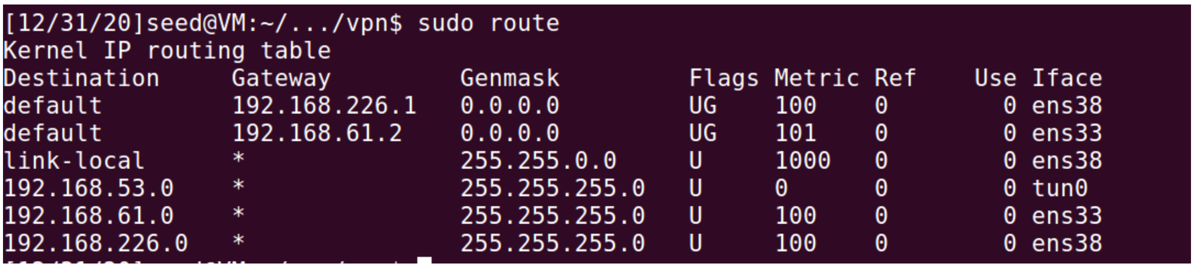
Step 2: Run VPN Client.



```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.53.5  P-t-P:192.168.53.5  Mask:255.255.255.0
          inet6 addr: fe80::26e2:b2b9:fcd3:1b47/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:96 (96.0 B)
```

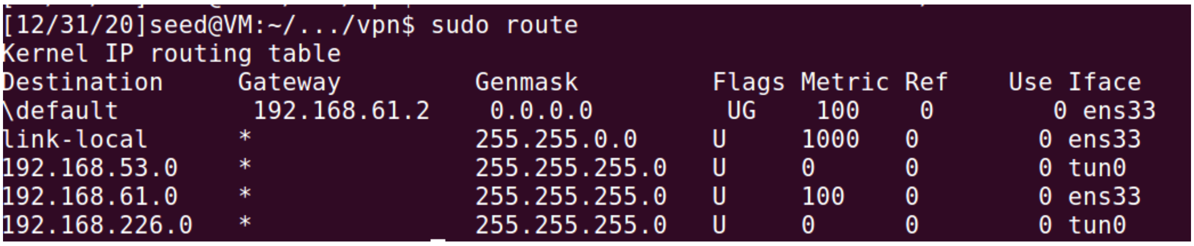
Step 3: Set Up Routing on Client and Server VMs

server



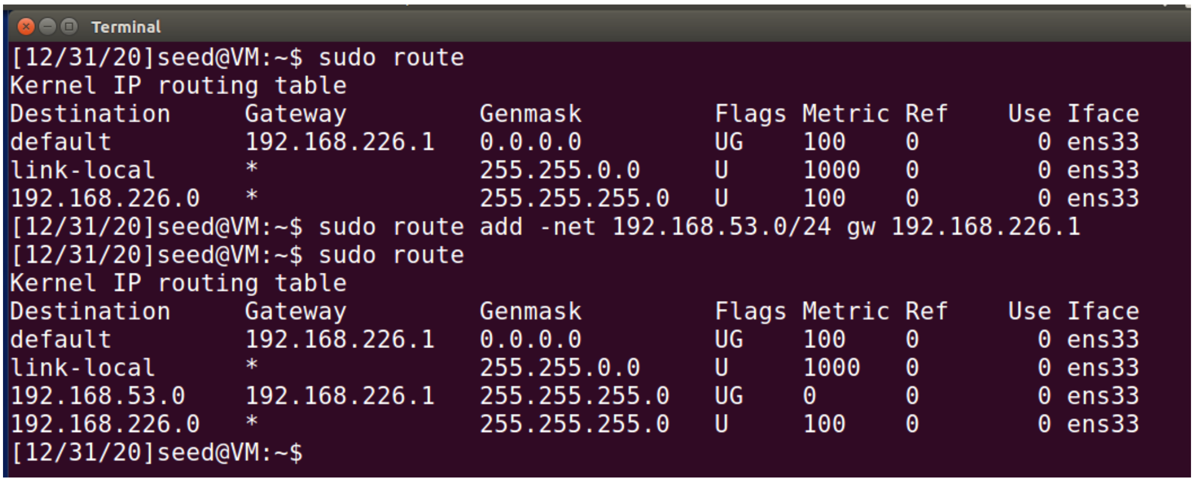
```
[12/31/20]seed@VM:~/.../vpn$ sudo route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.226.1   0.0.0.0         UG    100    0        0 ens38
default         192.168.61.2    0.0.0.0         UG    101    0        0 ens33
link-local      *               255.255.0.0     U     1000   0        0 ens38
192.168.53.0    *               255.255.255.0   U     0      0        0 tun0
192.168.61.0    *               255.255.255.0   U     100    0        0 ens33
192.168.226.0   *               255.255.255.0   U     100    0        0 ens38
```

client



```
[12/31/20]seed@VM:~/.../vpn$ sudo route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
\default         192.168.61.2    0.0.0.0         UG    100    0        0 ens33
link-local      *               255.255.0.0     U     1000   0        0 ens33
192.168.53.0    *               255.255.255.0   U     0      0        0 tun0
192.168.61.0    *               255.255.255.0   U     100    0        0 ens33
192.168.226.0   *               255.255.255.0   U     0      0        0 tun0
```

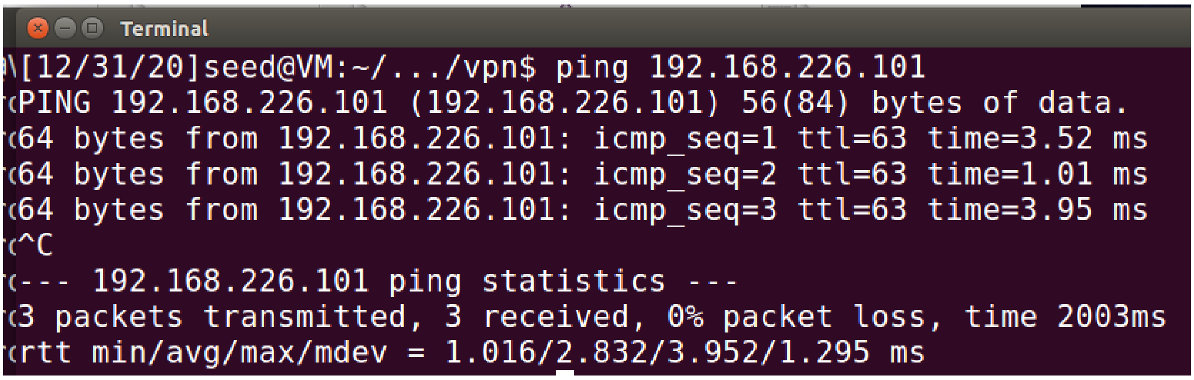
Step 4: Set Up Routing on Host V.



```
[12/31/20]seed@VM:~$ sudo route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.226.1   0.0.0.0         UG    100    0        0 ens33
link-local      *               255.255.0.0     U     1000   0        0 ens33
192.168.226.0   *               255.255.255.0   U     100    0        0 ens33
[12/31/20]seed@VM:~$ sudo route add -net 192.168.53.0/24 gw 192.168.226.1
[12/31/20]seed@VM:~$ sudo route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.226.1   0.0.0.0         UG    100    0        0 ens33
link-local      *               255.255.0.0     U     1000   0        0 ens33
192.168.53.0    192.168.226.1   255.255.255.0   UG    0      0        0 ens33
192.168.226.0   *               255.255.255.0   U     100    0        0 ens33
[12/31/20]seed@VM:~$
```

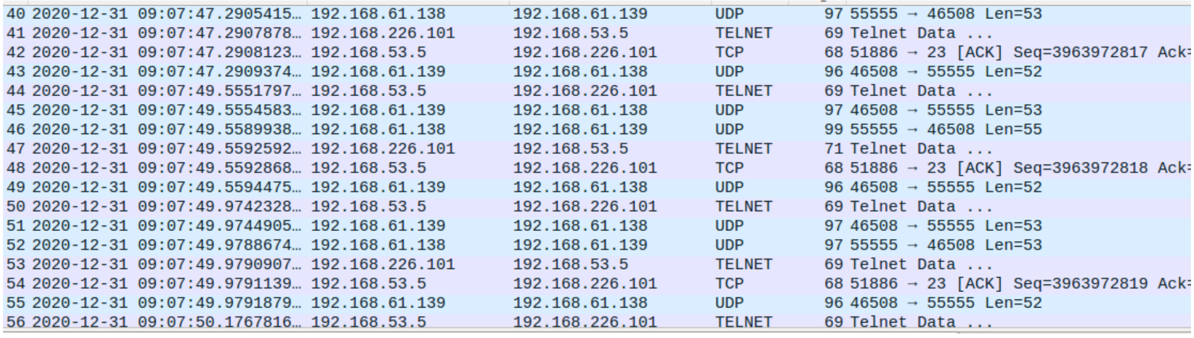
Step 5: Test the VPN Tunnel

ping



```
\[12/31/20]seed@VM:~/.../vpn$ ping 192.168.226.101
(PING 192.168.226.101 (192.168.226.101) 56(84) bytes of data.
(64 bytes from 192.168.226.101: icmp_seq=1 ttl=63 time=3.52 ms
(64 bytes from 192.168.226.101: icmp_seq=2 ttl=63 time=1.01 ms
(64 bytes from 192.168.226.101: icmp_seq=3 ttl=63 time=3.95 ms
(^C
(--- 192.168.226.101 ping statistics ---
(3 packets transmitted, 3 received, 0% packet loss, time 2003ms
(rtt min/avg/max/mdev = 1.016/2.832/3.952/1.295 ms
```

telnet



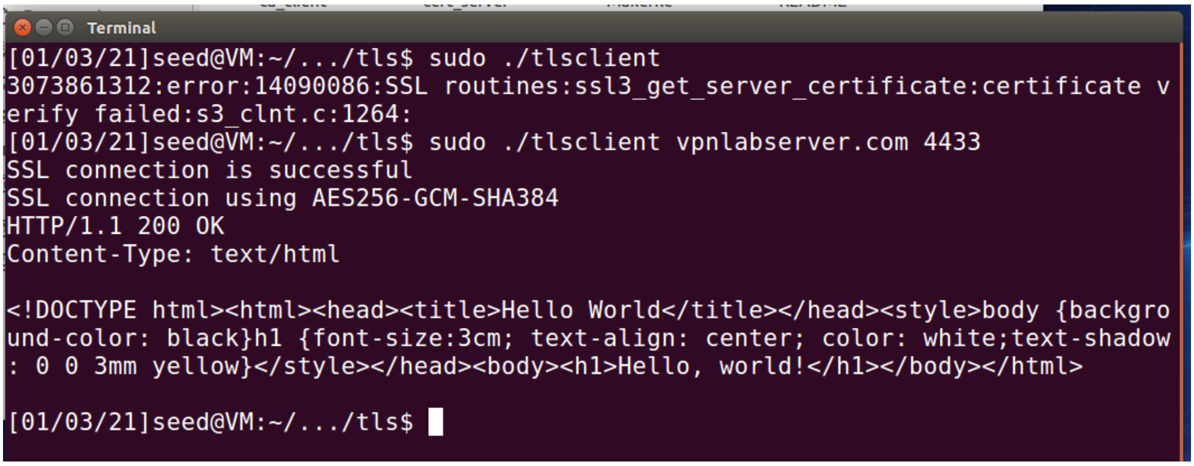
```
40 2020-12-31 09:07:47.2905415… 192.168.61.138    192.168.61.139    UDP       97 55555 → 46508 Len=53
41 2020-12-31 09:07:47.2907878… 192.168.226.101   192.168.53.5      TELNET    69 Telnet Data ...
42 2020-12-31 09:07:47.2908123… 192.168.53.5      192.168.226.101   TCP       68 51886 → 23 [ACK] Seq=3963972817 Ack=
43 2020-12-31 09:07:47.2909374… 192.168.61.139    192.168.61.138    UDP       96 46508 → 55555 Len=52
44 2020-12-31 09:07:49.5551797… 192.168.53.5      192.168.226.101   TELNET    69 Telnet Data ...
45 2020-12-31 09:07:49.5554583… 192.168.61.139    192.168.61.138    UDP       97 46508 → 55555 Len=53
46 2020-12-31 09:07:49.5589938… 192.168.61.138    192.168.61.139    UDP       99 55555 → 46508 Len=55
47 2020-12-31 09:07:49.5592592… 192.168.226.101   192.168.53.5      TELNET    71 Telnet Data ...
48 2020-12-31 09:07:49.5592868… 192.168.53.5      192.168.226.101   TCP       68 51886 → 23 [ACK] Seq=3963972818 Ack=
49 2020-12-31 09:07:49.5594475… 192.168.61.139    192.168.61.138    UDP       96 46508 → 55555 Len=52
50 2020-12-31 09:07:49.9742328… 192.168.53.5      192.168.226.101   TELNET    69 Telnet Data ...
51 2020-12-31 09:07:49.9744905… 192.168.61.139    192.168.61.138    UDP       97 46508 → 55555 Len=53
52 2020-12-31 09:07:49.9788674… 192.168.61.138    192.168.61.139    UDP       97 55555 → 46508 Len=53
53 2020-12-31 09:07:49.9790907… 192.168.226.101   192.168.53.5      TELNET    69 Telnet Data ...
54 2020-12-31 09:07:49.9791139… 192.168.53.5      192.168.226.101   TCP       68 51886 → 23 [ACK] Seq=3963972819 Ack=
55 2020-12-31 09:07:49.9791879… 192.168.61.139    192.168.61.138    UDP       96 46508 → 55555 Len=52
56 2020-12-31 09:07:50.1767816… 192.168.53.5      192.168.226.101   TELNET    69 Telnet Data ...
```

我们可以看出，蓝色部分的UDP包是tunnel包，紫色部分的则是实际的包内容

Step 6: Tunnel-Breaking Test.

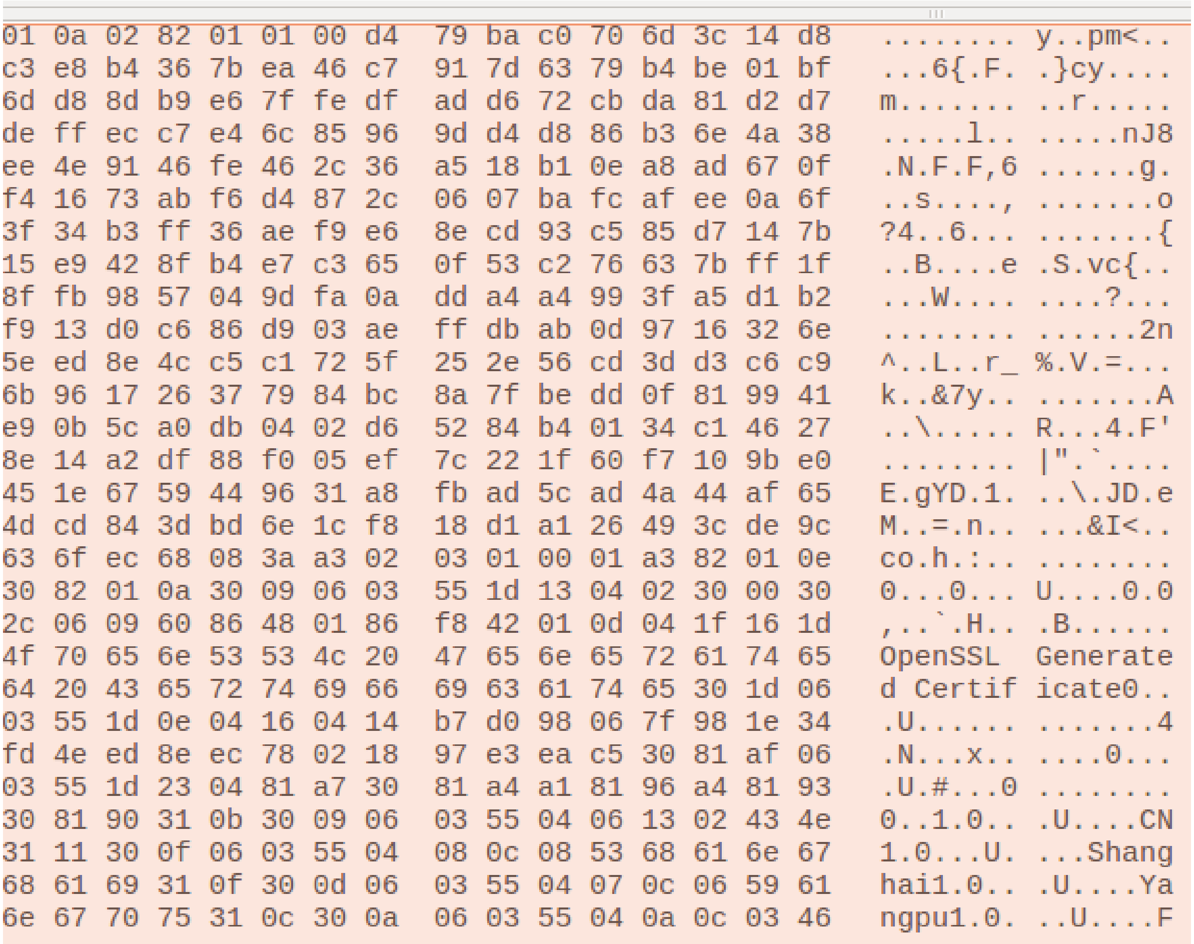
这一部分结果同上个lab，不再赘述。

Task 3: Encrypting the Tunnel



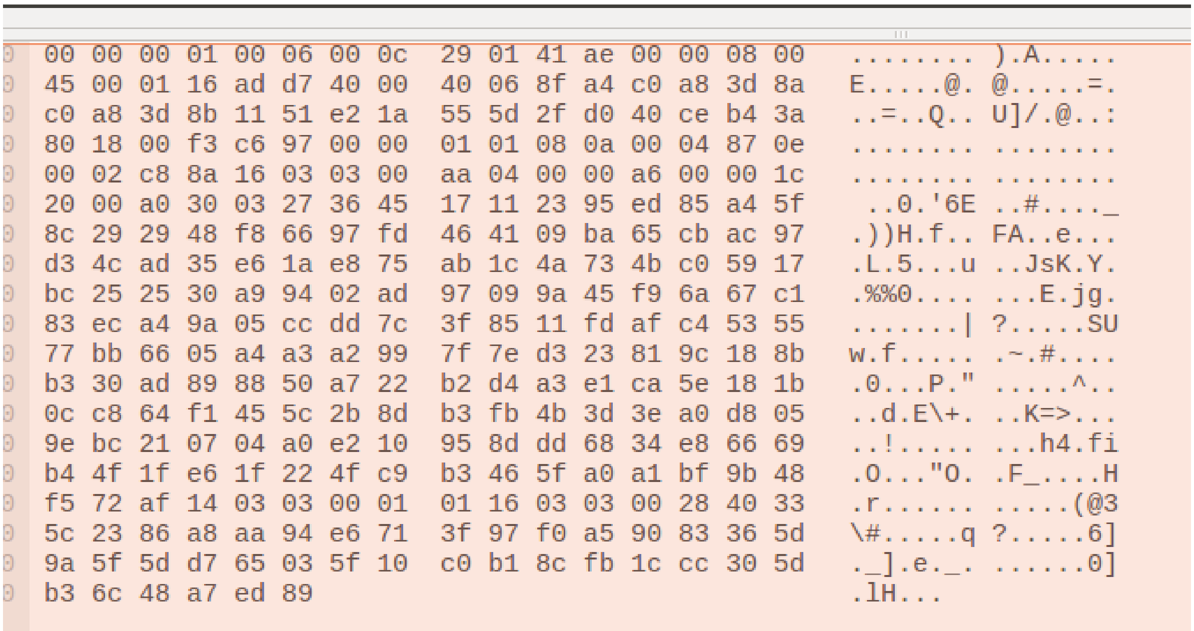
```
[01/03/21]seed@VM:~/.../tls$ sudo ./tlsclient
3073861312:error:14090086:SSL routines:ssl3_get_server_certificate:certificate v
erify failed:s3_clnt.c:1264:
[01/03/21]seed@VM:~/.../tls$ sudo ./tlsclient vpnlabserver.com 4433
SSL connection is successful
SSL connection using AES256-GCM-SHA384
HTTP/1.1 200 OK
Content-Type: text/html

<!DOCTYPE html><html><head><title>Hello World</title></head><style>body {backgro
und-color: black}h1 {font-size:3cm; text-align: center; color: white;text-shadow
: 0 0 3mm yellow}</style></head><body><h1>Hello, world!</h1></body></html>

[01/03/21]seed@VM:~/.../tls$ 
```

可以观察到传输的数据包中的证书



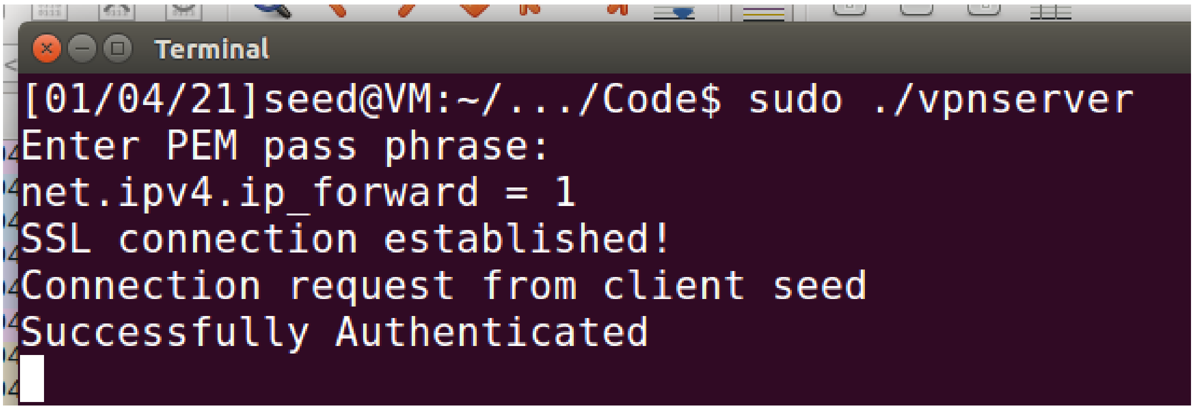
```
01 0a 02 82 01 01 00 d4  79 ba c0 70 6d 3c 14 d8   ........ y..pm<..
c3 e8 b4 36 7b ea 46 c7  91 7d 63 79 b4 be 01 bf   ...6{.F. .}cy....
6d d8 8d b9 e6 7f fe df  ad d6 72 cb da 81 d2 d7   m....... ..r.....
de ff ec c7 e4 6c 85 96  9d d4 d8 86 b3 6e 4a 38   .....l.. .....nJ8
ee 4e 91 46 fe 46 2c 36  a5 18 b1 0e a8 ad 67 0f   .N.F.F,6 ......g.
f4 16 73 ab f6 d4 87 2c  06 07 ba fc af ee 0a 6f   ..s...., .......o
3f 34 b3 ff 36 ae f9 e6  8e cd 93 c5 85 d7 14 7b   ?4..6... .......{
15 e9 42 8f b4 e7 c3 65  0f 53 c2 76 63 7b ff 1f   ..B....e .S.vc{..
8f fb 98 57 04 9d fa 0a  dd a4 a4 99 3f a5 d1 b2   ...W.... ....?...
f9 13 d0 c6 86 d9 03 ae  ff db ab 0d 97 16 32 6e   ........ ......2n
5e ed 8e 4c c5 c1 72 5f  25 2e 56 cd 3d d3 c6 c9   ^..L..r_ %.V.=...
6b 96 17 26 37 79 84 bc  8a 7f be dd 0f 81 99 41   k..&7y.. .......A
e9 0b 5c a0 db 04 02 d6  52 84 b4 01 34 c1 46 27   ..\..... R...4.F'
8e 14 a2 df 88 f0 05 ef  7c 22 1f 60 f7 10 9b e0   ........ |".`....
45 1e 67 59 44 96 31 a8  fb ad 5c ad 4a 44 af 65   E.gYD.1. ..\.JD.e
4d cd 84 3d bd 6e 1c f8  18 d1 a1 26 49 3c de 9c   M..=.n.. ...&I<..
63 6f ec 68 08 3a a3 02  03 01 00 01 a3 82 01 0e   co.h.:.. ........
30 82 01 0a 30 09 06 03  55 1d 13 04 02 30 00 30   0...0... U....0.0
2c 06 09 60 86 48 01 86  f8 42 01 0d 04 1f 16 1d   ,..`.H.. .B......
4f 70 65 6e 53 53 4c 20  47 65 6e 65 72 61 74 65   OpenSSL  Generate
64 20 43 65 72 74 69 66  69 63 61 74 65 30 1d 06   d Certif icate0..
03 55 1d 0e 04 16 04 14  b7 d0 98 06 7f 98 1e 34   .U...... .......4
fd 4e ed 8e ec 78 02 18  97 e3 ea c5 30 81 af 06   .N...x.. ....0...
03 55 1d 23 04 81 a7 30  81 a4 a1 81 96 a4 81 93   .U.#...0 ........
30 81 90 31 0b 30 09 06  03 55 04 06 13 02 43 4e   0..1.0.. .U....CN
31 11 30 0f 06 03 55 04  08 0c 08 53 68 61 6e 67   1.0...U. ...Shang
68 61 69 31 0f 30 0d 06  03 55 04 07 0c 06 59 61   hai1.0.. .U....Ya
6e 67 70 75 31 0c 30 0a  06 03 55 04 0a 0c 03 46   ngpu1.0. ..U....F
```

而实际网页被加密

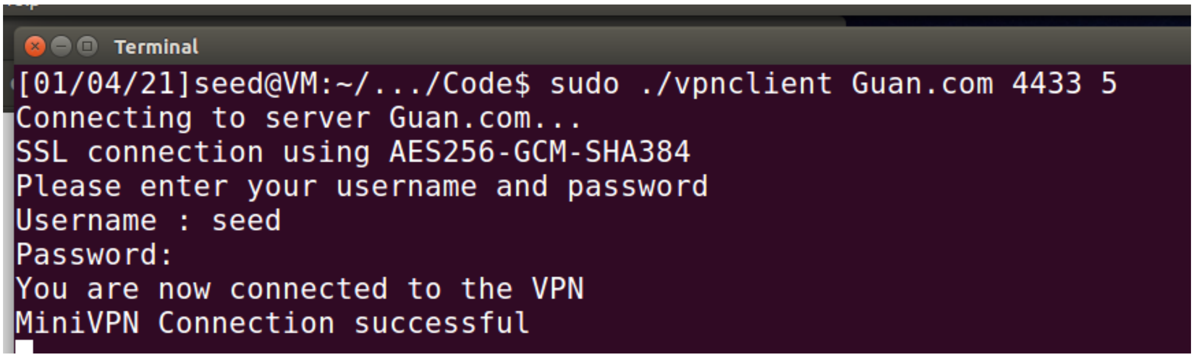


```
00 00 00 01 00 06 00 0c  29 01 41 ae 00 00 08 00   ........ ).A.....
45 00 01 16 ad d7 40 00  40 06 8f a4 c0 a8 3d 8a   E.....@. @.....=.
c0 a8 3d 8b 11 51 e2 1a  55 5d 2f d0 40 ce b4 3a   ..=..Q.. U]/.@..:
80 18 00 f3 c6 97 00 00  01 01 08 0a 00 04 87 0e   ........ ........
00 02 c8 8a 16 03 03 00  aa 04 00 00 a6 00 00 1c   ........ ........
20 00 a0 30 03 27 36 45  17 11 23 95 ed 85 a4 5f    ..0.'6E ..#...._
8c 29 29 48 f8 66 97 fd  46 41 09 ba 65 cb ac 97   .))H.f.. FA..e...
d3 4c ad 35 e6 1a e8 75  ab 1c 4a 73 4b c0 59 17   .L.5...u ..JsK.Y.
bc 25 25 30 a9 94 02 ad  97 09 9a 45 f9 6a 67 c1   .%%0.... ...E.jg.
83 ec a4 9a 05 cc dd 7c  3f 85 11 fd af c4 53 55   .......| ?.....SU
77 bb 66 05 a4 a3 a2 99  7f 7e d3 23 81 9c 18 8b   w.f..... .~.#....
b3 30 ad 89 88 50 a7 22  b2 d4 a3 e1 ca 5e 18 1b   .0...P." .....^..
0c c8 64 f1 45 5c 2b 8d  b3 fb 4b 3d 3e a0 d8 05   ..d.E\+. ..K=>...
9e bc 21 07 04 a0 e2 10  95 8d dd 68 34 e8 66 69   ..!..... ...h4.fi
b4 4f 1f e6 1f 22 4f c9  b3 46 5f a0 a1 bf 9b 48   .O..."O. .F_....H
f5 72 af 14 03 03 00 01  01 16 03 03 00 28 40 33   .r...... .....(@3
5c 23 86 a8 aa 94 e6 71  3f 97 f0 a5 90 83 36 5d   \#.....q ?.....6]
9a 5f 5d d7 65 03 5f 10  c0 b1 8c fb 1c cc 30 5d   ._].e._. ......0]
b3 6c 48 a7 ed 89                                  .lH...
```

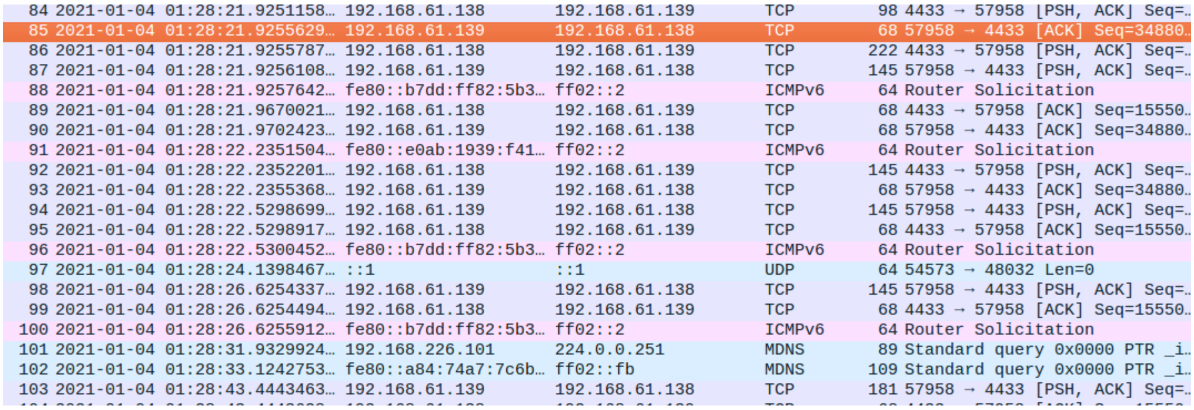
MiniVPN



```
[01/04/21]seed@VM:~/.../Code$ sudo ./vpnserver
Enter PEM pass phrase:
net.ipv4.ip_forward = 1
SSL connection established!
Connection request from client seed
Successfully Authenticated
```



```
[01/04/21]seed@VM:~/.../Code$ sudo ./vpnclient Guan.com 4433 5
Connecting to server Guan.com...
SSL connection using AES256-GCM-SHA384
Please enter your username and password
Username : seed
Password:
You are now connected to the VPN
MiniVPN Connection successful
```



```
 84 2021-01-04 01:28:21.9251158… 192.168.61.138       192.168.61.139       TCP        98 4433 → 57958 [PSH, ACK] Seq=…
 85 2021-01-04 01:28:21.9255629… 192.168.61.139       192.168.61.138       TCP        68 57958 → 4433 [ACK] Seq=34880…
 86 2021-01-04 01:28:21.9255787… 192.168.61.138       192.168.61.139       TCP       222 4433 → 57958 [PSH, ACK] Seq=…
 87 2021-01-04 01:28:21.9256108… 192.168.61.139       192.168.61.138       TCP       145 57958 → 4433 [PSH, ACK] Seq=…
 88 2021-01-04 01:28:21.9257642… fe80::b7dd:ff82:5b3… ff02::2              ICMPv6     64 Router Solicitation
 89 2021-01-04 01:28:21.9670021… 192.168.61.138       192.168.61.139       TCP        68 4433 → 57958 [ACK] Seq=15550…
 90 2021-01-04 01:28:21.9702423… 192.168.61.139       192.168.61.138       TCP        68 57958 → 4433 [ACK] Seq=34880…
 91 2021-01-04 01:28:22.2351504… fe80::e0ab:1939:f41… ff02::2              ICMPv6     64 Router Solicitation
 92 2021-01-04 01:28:22.2352201… 192.168.61.138       192.168.61.139       TCP       145 4433 → 57958 [PSH, ACK] Seq=…
 93 2021-01-04 01:28:22.2355368… 192.168.61.139       192.168.61.138       TCP        68 57958 → 4433 [ACK] Seq=34880…
 94 2021-01-04 01:28:22.5298699… 192.168.61.139       192.168.61.138       TCP       145 57958 → 4433 [PSH, ACK] Seq=…
 95 2021-01-04 01:28:22.5298917… 192.168.61.138       192.168.61.139       TCP        68 4433 → 57958 [ACK] Seq=15550…
 96 2021-01-04 01:28:22.5300452… fe80::b7dd:ff82:5b3… ff02::2              ICMPv6     64 Router Solicitation
 97 2021-01-04 01:28:24.1398467… ::1                  ::1                  UDP        64 54573 → 48032 Len=0
 98 2021-01-04 01:28:26.6254337… 192.168.61.139       192.168.61.138       TCP       145 57958 → 4433 [PSH, ACK] Seq=…
 99 2021-01-04 01:28:26.6254494… 192.168.61.138       192.168.61.139       TCP        68 4433 → 57958 [ACK] Seq=15550…
100 2021-01-04 01:28:26.6255912… fe80::b7dd:ff82:5b3… ff02::2              ICMPv6     64 Router Solicitation
101 2021-01-04 01:28:31.9329924… 192.168.226.101      224.0.0.251          MDNS       89 Standard query 0x0000 PTR _i…
102 2021-01-04 01:28:33.1242753… fe80::a84:74a7:7c6b… ff02::fb             MDNS      109 Standard query 0x0000 PTR _i…
103 2021-01-04 01:28:43.4443463… 192.168.61.139       192.168.61.138       TCP       181 57958 → 4433 [PSH, ACK] Seq=…
```