Packets analyze report

B075040041 鄭煥榮

本次使用的分析軟體為 ubuntu 內的 tcpdump

第一個觀察到的是使用瀏覽器開啟網路大學

(由於版面關係，右側資訊做裁切)

```
root@Ryzen3600:/home/heisenberg# tcpdump host 192.168.50.11 and cu.nsysu.edu.tw
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
23:15:28.987895 IP Ryzen3600.52440 > cu.nsysu.edu.tw.https: Flags [S], seq 795128567, win 64240, opt
23:15:28.993067 IP cu.nsysu.edu.tw.https > Ryzen3600.52440: Flags [S.], seq 88429612, ack 795128568,
23:15:28.993094 IP Ryzen3600.52440 > cu.nsysu.edu.tw.https: Flags [.], ack 1, win 502, options [nop,
```

我使用的指令為 tcpdump host 192.168.50.11 and cu.nsysu.edu.tw

(電腦本地 ip) (中山大學)

輸出所有本地對中山大學的連線。

從結果圖可以看到 TCP 在開始連線前的 3-way hand shake, 分別為 SYN, SYN+ACK, ACK。

之後我再從網站下載一份 ppt

```
23:16:15.465674 IP cu.nsysu.edu.tw.https > Ryzen3600.52492: Flags [.], seq 25013:26453, ack 1513,
23:16:15.465797 IP cu.nsysu.edu.tw.https > Ryzen3600.52492: Flags [.], seq 26453:27893, ack 1513,
23:16:15.465803 IP Ryzen3600.52492 > cu.nsysu.edu.tw.https: Flags [.], ack 27893, win 501, option
23:16:15.465914 IP cu.nsysu.edu.tw.https > Ryzen3600.52492: Flags [.], seq 27893:29333, ack 1513,
23:16:15.466073 IP cu.nsysu.edu.tw.https > Ryzen3600.52492: Flags [.], seq 29333:30773, ack 1513,
23:16:15.466080 IP Ryzen3600.52492 > cu.nsysu.edu.tw.https: Flags [.], ack 30773, win 501, option
23:16:15.466192 IP cu.nsysu.edu.tw.https > Ryzen3600.52492: Flags [.], seq 30773:32213, ack 1513,
23:16:15.466319 IP cu.nsysu.edu.tw.https > Ryzen3600.52492: Flags [.], seq 32213:33653, ack 1513,
23:16:15.466325 IP Ryzen3600.52492 > cu.nsysu.edu.tw.https: Flags [.], ack 33653, win 501, option
```

可以觀察到 TCP 傳輸資料的方式，由 server 傳送兩段資料(25013:26453 , 26453:27893)，本機收到後會回傳 27893 AWK 回去，代表接收到 27893，server 則會繼續傳送 (27893:29333, 29333:30773)直到結束。

最後是 UDP 的觀測，原本以為影音串流平台都是使用 UDP 作影片串流，但實測 youtube , twitch 等平台都沒有發現 UDP 封包的蹤跡。經過上網查詢後發現他們都已改用其他 TCP 協定做影音傳輸，所以我改為觀察 DNS server 的動作

以連線 www.twitch.com 為例:

```
root@Ryzen3600:/home/heisenberg# tcpdump -i enp4s0 -nnn -c 5 host 192.168.50.11 and udp and port 53
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:06:43.416233 IP 192.168.50.11.57162 > 192.168.50.1.53: 52045+ [1au] A? twitch.map.fastly.net. (50)
01:06:43.421507 IP 192.168.50.1.53 > 192.168.50.11.57162: 52045 1/0/1 A 199.232.46.167 (66)
```

這裡使用 tcpdump -i (指定網卡) enp4s0 (網卡名稱) -nnn (輸出詳細資料) -c5 (只收集 5 個封包) host 192.168.50.11 and udp and port 53 (指定 udp 和 53 接口)

從結果圖看，可以觀察到本機會使用 udp 傳送網址給 DNS server 查詢 ip，由於篩選條件為 udp，所以看不到 DNS server 利用 TCP 回傳的 ip 值。