

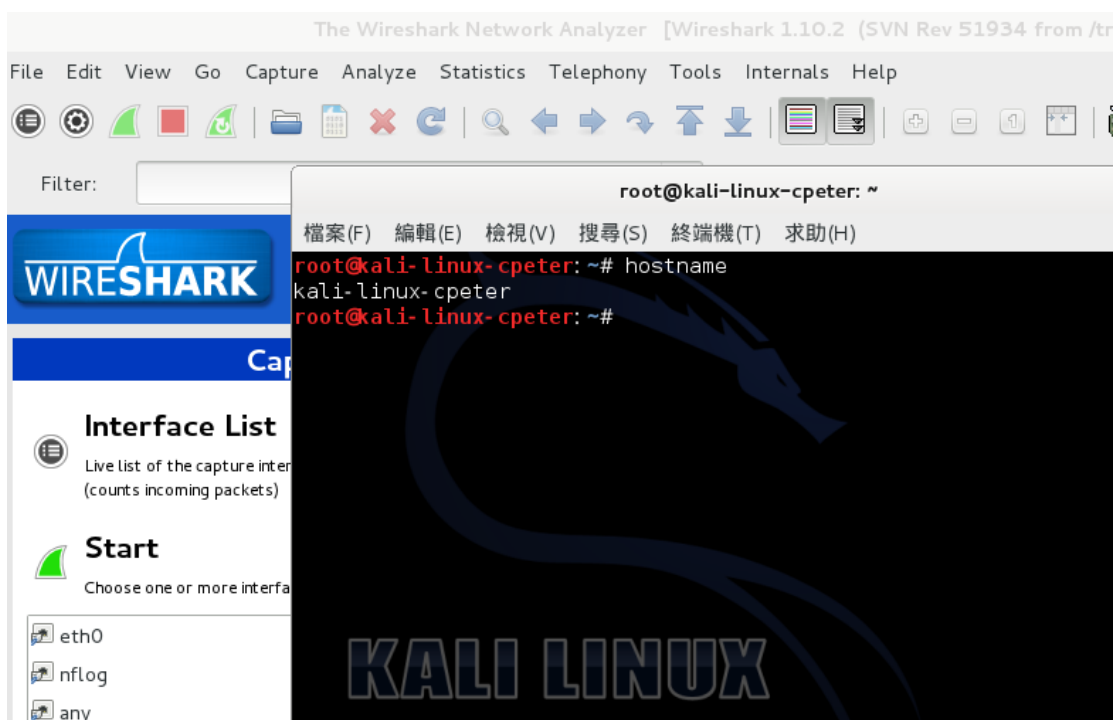
網路應用程式設計

Homework 1

B013040033

雷皓博

分析工具:Wireshark(在 VMware 裡的 kali-linux 環境下)



VMware

VM1(kali-linux)的 ip==192.168.79.130

```
root@kali-linux-cpeter: ~
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 終端機(T) 求助(H)
root@kali-linux-cpeter: ~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e0:5e:c2
          inet addr:192.168.79.130  Bcast:192.168.79.255
          inet6 addr: fe80::20c:29ff:fee0:5ec2/64 Scope:
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metr
          RX packets:3454 errors:0 dropped:0 overruns:0 ca
          TX packets:29 errors:0 dropped:0 overruns:0 ca
          collisions:0 txqueuelen:1000
          RX bytes:2137284 (2.0 MiB)  TX bytes:2703 (2.6
          Interrupt:19 Base address:0x2000
```

VM2(Ubuntu)的 ip==192.168.79.128(與 VM1 同網域)

```
cpeter@ubuntu: ~
cpeter@ubuntu:~$ ifconfid
No command 'ifconfid' found, did you mean:
  Command 'ifconfig' from package 'net-tools' (main)
ifconfid: command not found
cpeter@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:51:3f:96
          inet addr:192.168.79.128  Bcast:192.168.79.255
          inet6 addr: fe80::20c:29ff:fe51:3f96/64 Scope:
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metr
          RX packets:380 errors:0 dropped:0 overruns:0 f
          TX packets:372 errors:0 dropped:0 overruns:0 c
```

VM2 使用 firefox 瀏覽器 進入學校的網站

輸入學號 B013040033

密碼這裡輸入 netprog



VM1 監測到的其中一份 packet

(src)VM2(port 44836)連到(dst)學校 140.117.152.12(port 80)

Protocol is TCP

transport-layer segments 為 PSH, ACK

```
4426 2905.042355000 192.168.79.128 140.117.152.12 HTTP 630 POST /scoreqry/sco_query.asp HTTP/1.1 (appl
+ Frame 4426: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on interface 0
+ Ethernet II, Src: Vmware_51:3f:96 (00:0c:29:51:3f:96), Dst: Vmware_e5:cd:40 (00:50:56:e5:cd:40)
+ Internet Protocol Version 4, Src: 192.168.79.128 (192.168.79.128), Dst: 140.117.152.12 (140.117.152.12)
- Transmission Control Protocol, Src Port: 44836 (44836), Dst Port: http (80), Seq: 1, Ack: 1, Len: 576
  Source port: 44836 (44836)
  Destination port: http (80)
  [Stream index: 31]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 577 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Header length: 20 bytes
+ Flags: 0x018 PSH, ACK
  Window size value: 29200
  [Calculated window size: 29200]
  [Window size scaling factor: -2 (no window scaling used)]
+ Checksum: 0x0dce [validation disabled]
+ [SEQ/ACK analysis]
```

interesting things

VM1 用 wireshark 監測時可以看到 VM1 輸入的學號與密碼(明文)!!!!

```
192.168.79.128 140.117.152.12 HTTP 630 POST /scoreqry/sco_query.asp HTTP/
140.117.152.12 192.168.79.128 TCP 60 http... 44836 [ACK] Seq=1 Ack=577 W
70 65 3a 20 61 70 70 6c 69 63 61 74 t-Type: applicat
78 2d 77 77 77 2d 66 6f 72 6d 2d 75 ion/x-www-form-u
63 6f 64 65 64 0d 0a 43 6f 6e 74 65 rlen: code d..Conte
65 6e 67 74 68 3a 20 38 35 0d 0a 0d nt-Length: 85...
3d 42 30 31 33 30 34 30 30 33 33 26 .SID=B0130400336
57 44 3d 6e 65 74 70 72 6f 67 26 41 PASSWD=netprog&A
```

分析工具: Wireshark(win7 環境下)

Skype 聲音通話期間時 Protocol is UDP

而開始與結束通話時會有 TCP(three-way handshake 建立連線)

監測端及本機 ip==140.117.178.35(port 18790)

同學的 ip==140.117.178.34(port 27668)

```
C:\Users\user>ipconfig

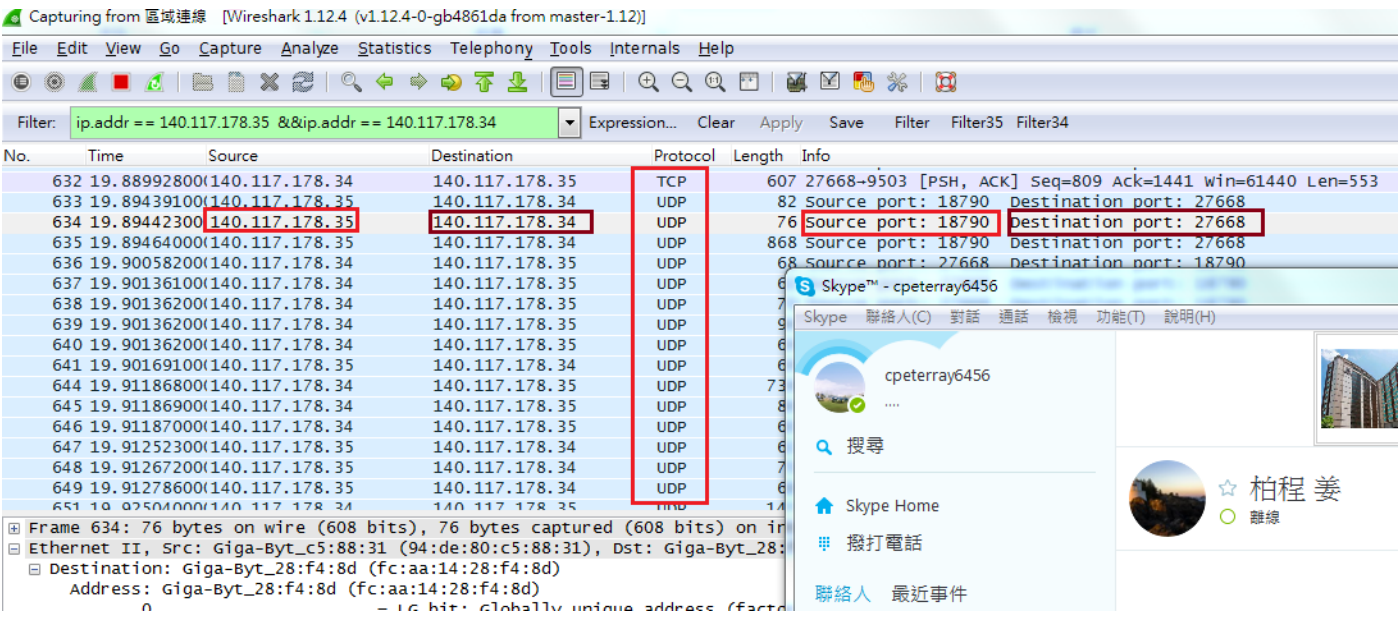
Windows IP 設定

乙太網路卡 區域連線:

    連線特定 DNS 尾碼 . . . . . : 
    IPv4 位址 . . . . . : 140.117.178.35
    子網路遮罩 . . . . . : 255.255.255.0
```

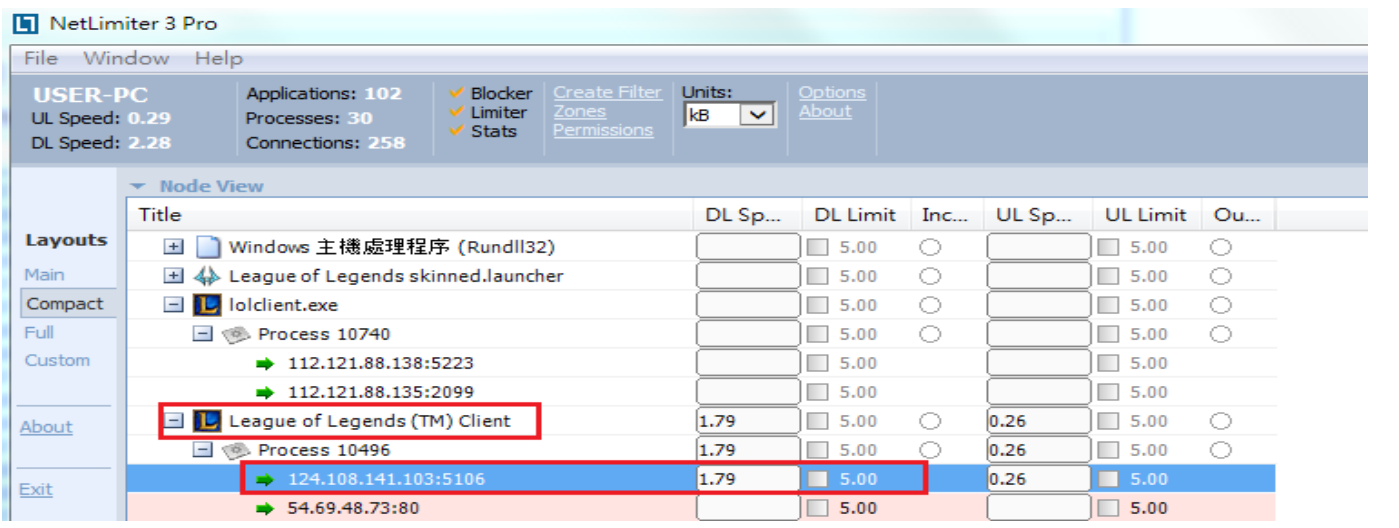
interesting things

使用 skype 時的 UDP 的 packet 非常多且極快且容量不大,我想大概是因為網路電話的傳輸是及時的.



分析工具:Wireshark(win7 環境下),NetLimiter3

LOL 先找出連到的(Playing)遊戲房間的 ip==124.108.141.103 port==5106



在 wireshark 上設 filter

(ip.addr == 140.117.178.35 && ip.addr == 124.108.141.103)

User ip=140.117.178.35

用來來查看在打 LOL 時的連線是怎麼樣的 Protocol

結果者主是 UDP 在傳輸 User 用的 port 是 55761

Filter:	ip.addr == 140.117.178.35 && ip.addr == 124.108.141.103	Expression...	Clear	Apply	Save	Filter	Filter35	Filter34
No.	Time	Source	Destination	Protocol	Length	Info		
128317	1667.621677	(124.108.141.103	140.117.178.35	UDP	526	Source port: 5106 Destination port: 55761		
128318	1667.622014	(140.117.178.35	124.108.141.103	UDP	56	Source port: 55761 Destination port: 5106		
128319	1667.640538	(124.108.141.103	140.117.178.35	UDP	191	Source port: 5106 Destination port: 55761		
128320	1667.640833	(140.117.178.35	124.108.141.103	UDP	56	Source port: 55761 Destination port: 5106		
128322	1667.678811	(124.108.141.103	140.117.178.35	UDP	412	Source port: 5106 Destination port: 55761		
128323	1667.679134	(140.117.178.35	124.108.141.103	UDP	56	Source port: 55761 Destination port: 5106		
128325	1667.704525	(124.108.141.103	140.117.178.35	UDP	736	Source port: 5106 Destination port: 55761		
128326	1667.704808	(140.117.178.35	124.108.141.103	UDP	64	Source port: 55761 Destination port: 5106		
128328	1667.724635	(140.117.178.35	124.108.141.103	UDP	66	Source port: 55761 Destination port: 5106		
128330	1667.739496	(124.108.141.103	140.117.178.35	UDP	201	Source port: 5106 Destination port: 55761		
128331	1667.739843	(140.117.178.35	124.108.141.103	UDP	56	Source port: 55761 Destination port: 5106		
128332	1667.782847	(124.108.141.103	140.117.178.35	UDP	155	Source port: 5106 Destination port: 55761		
128333	1667.783092	(140.117.178.35	124.108.141.103	UDP	56	Source port: 55761 Destination port: 5106		
128334	1667.802814	(124.108.141.103	140.117.178.35	UDP	289	Source port: 5106 Destination port: 55761		

interesting things

當初完全沒想到 LOL 是用 UDP, 看來在這種即時性很強的遊戲選擇 UDP 是一種不錯的選擇, 但是 UDP 感覺並不是很安全, 也可能像是之前的 LOL 的攻擊房間的外掛的成因