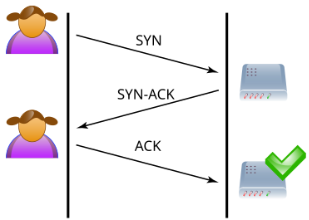
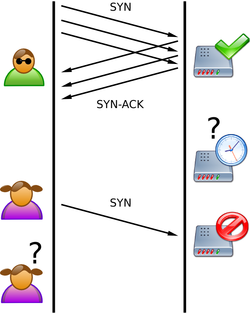
SYN DDOS攻擊介紹 :

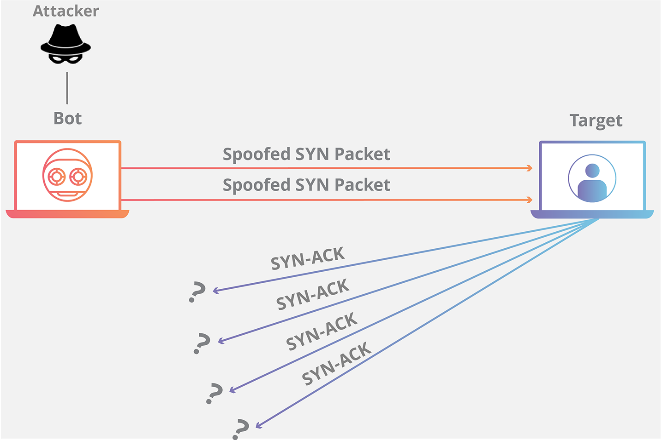
SYN flooding攻擊(又稱SYN 洪水攻擊)，為半開放式攻擊，顧名思義，就是利用送很多封包導致伺服器癱瘓的攻擊，是一種廣為人知的攻擊方式。駭客會透過消耗所有可用的伺服器資源，使伺服器無法用於合法請求。透過重複傳送初始連線要求 (SYN) 封包，攻擊者能夠淹沒目標伺服器上所有可用的連接埠，使目標裝置緩慢回應或完全不回應合法請求，下圖為正常收發的TCP三向交握。



目前有兩種攻擊方法，都與server不會收到ACK回應有關，惡意使用者可以跳過傳送最後的ACK資訊，如下圖，server在等待第三次交握(handshaking)時，會遲遲無法收到使用者發送的第三次ACK回應，導致重複等待，並重複收到同一個惡意使用者發送的SYN請求，導致server癱瘓，正常使用的user會使用不了服務。

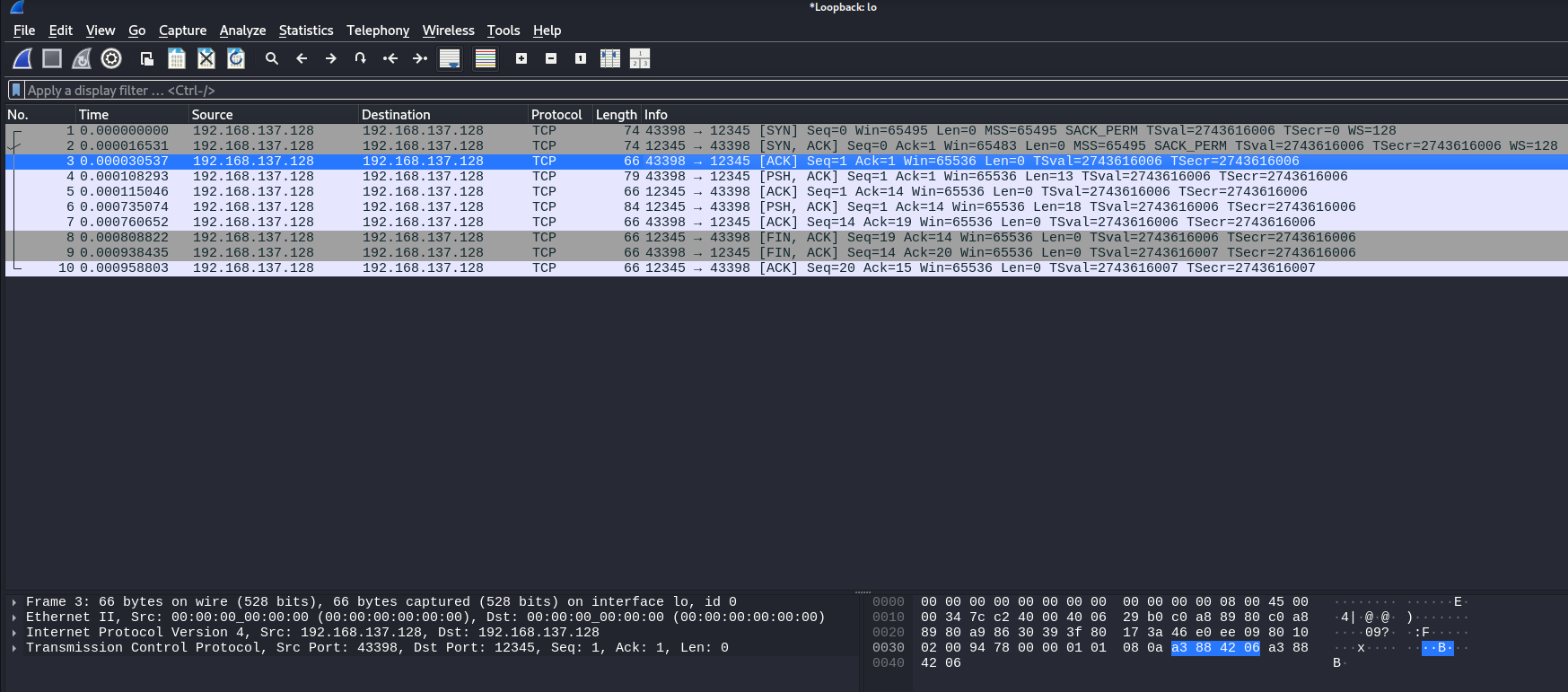


另一種攻擊方式是，惡意使用者會創造一個假的來源IP位址並傳送SYN請求，這讓server送SYN-ACK到偽造的IP位址，因此永不可能收到ACK回應，如下圖所示。



攻擊示範 :

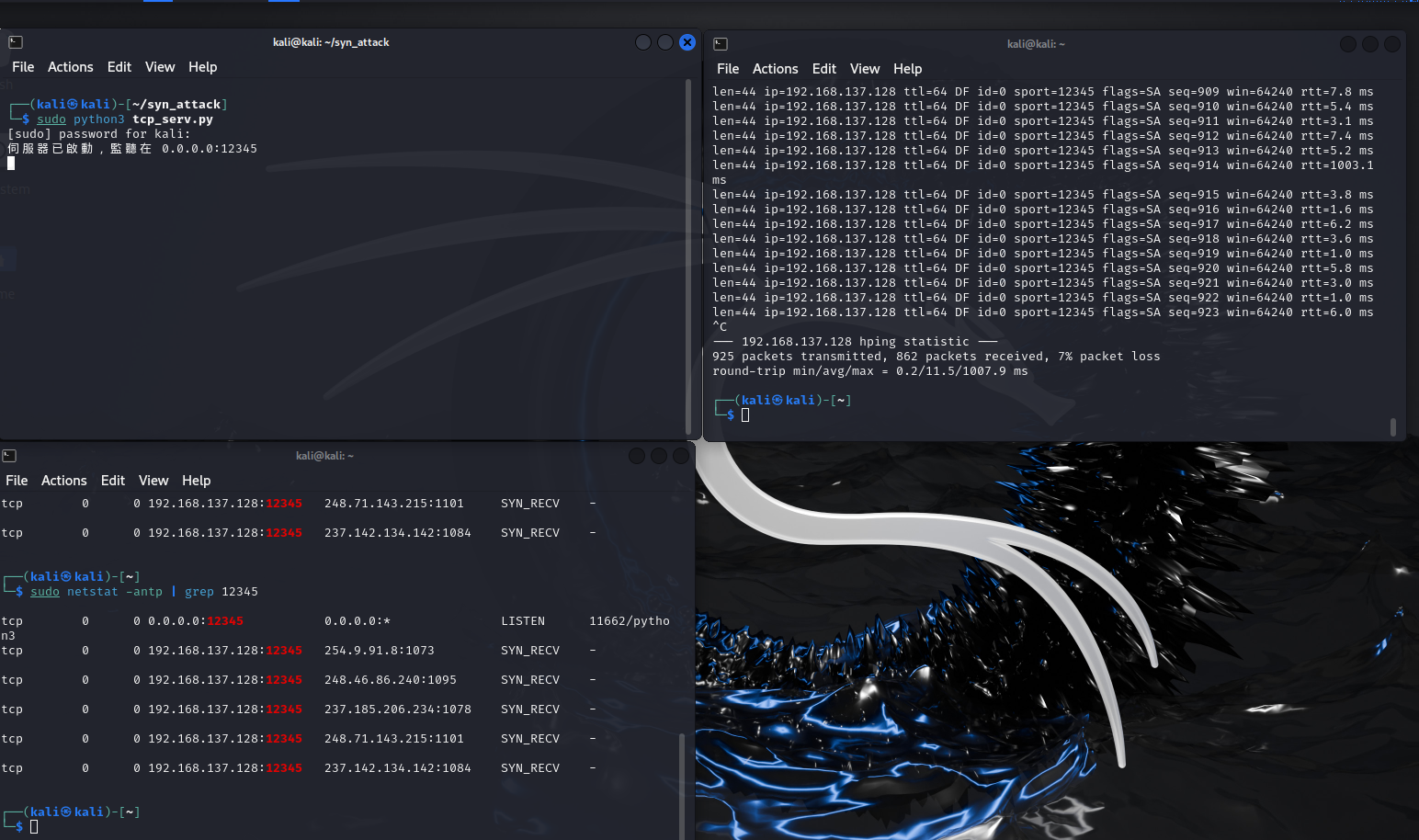
以下為正常交握的情況，做SYN請求，server回應SYN\_ACK，user再次回應ACK



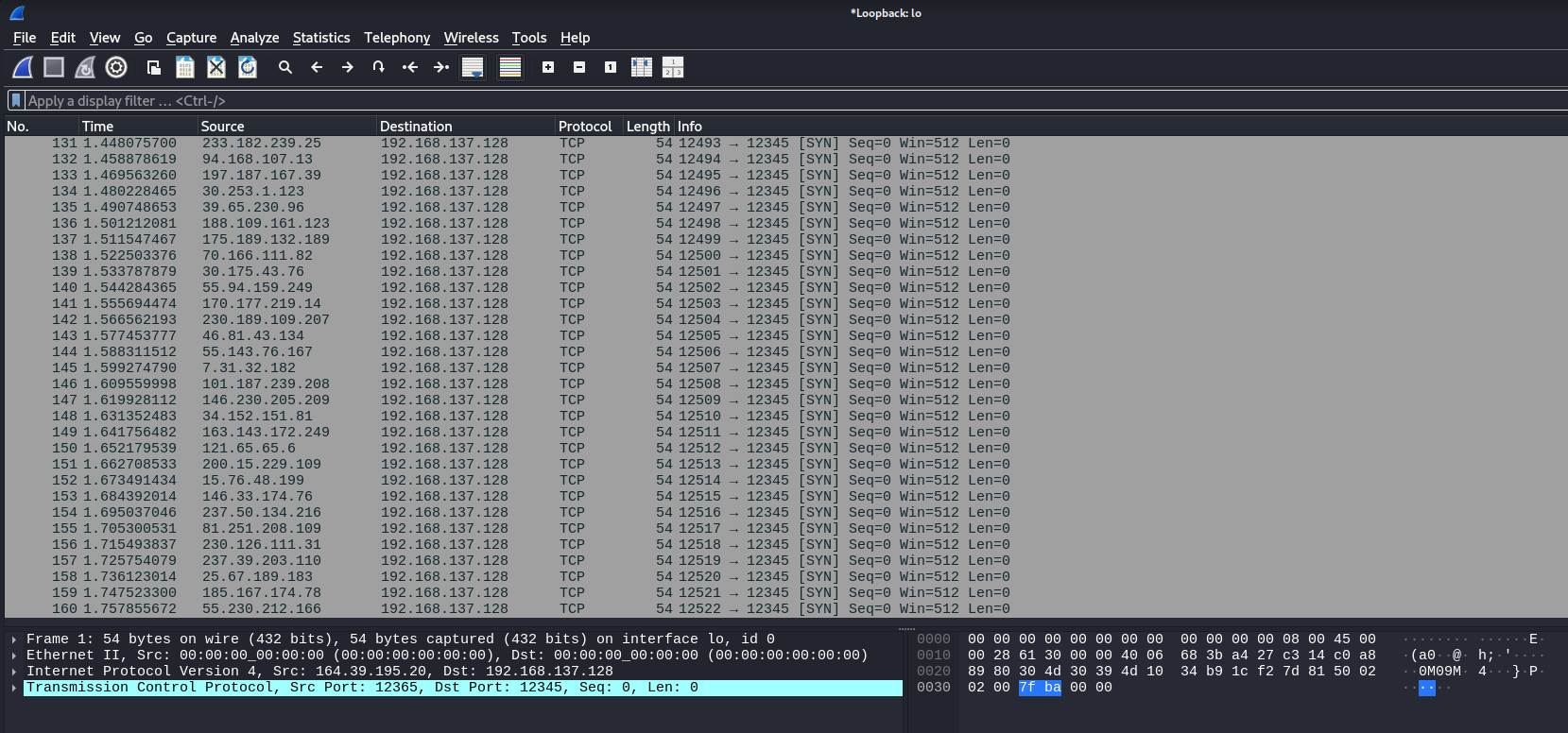
執行事先架設好的server (含有漏洞)(左上terminal)，利用hping3傳送封包進行SYN flooding攻擊(右上terminal)，接著驗證server的backlog是否被塞滿(受到ddos攻擊)(左下terminal)，可以看到port 12345的server 收到了很多來自random ip的封包(server目前只設定5個)，狀態都是SYN\_RECV，代表收到SYN請求，server回應SYN\_ACK，但是user並未回傳ACK回應，導致backlog被塞爆，最終導致server癱瘓。

指令 : sudo hping3 -S -p 12345 -i u10000 --rand-source 本地ip

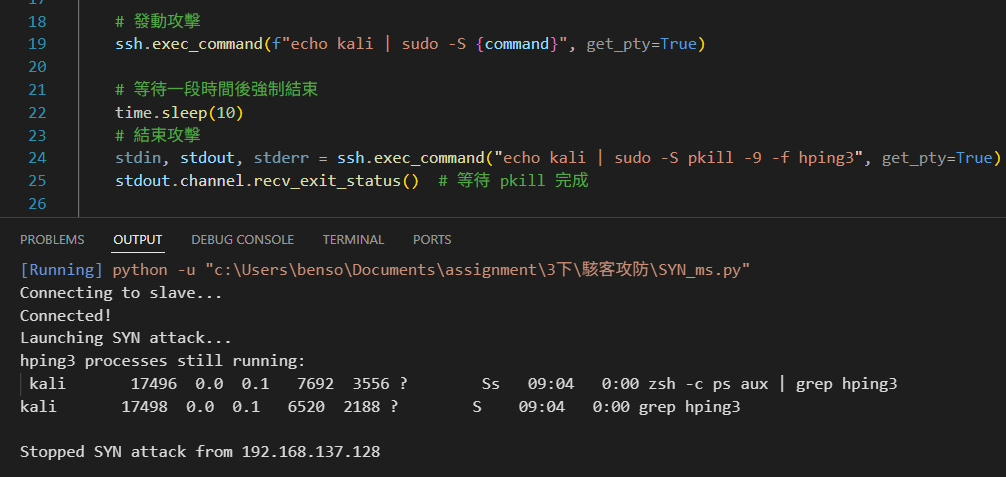
利用hping3發送SYN請求，設定port為12345，每隔 10000 微秒（即 0.01 秒，或 10 毫秒）傳送一個封包，並用隨機ip發送給指定的ip位置

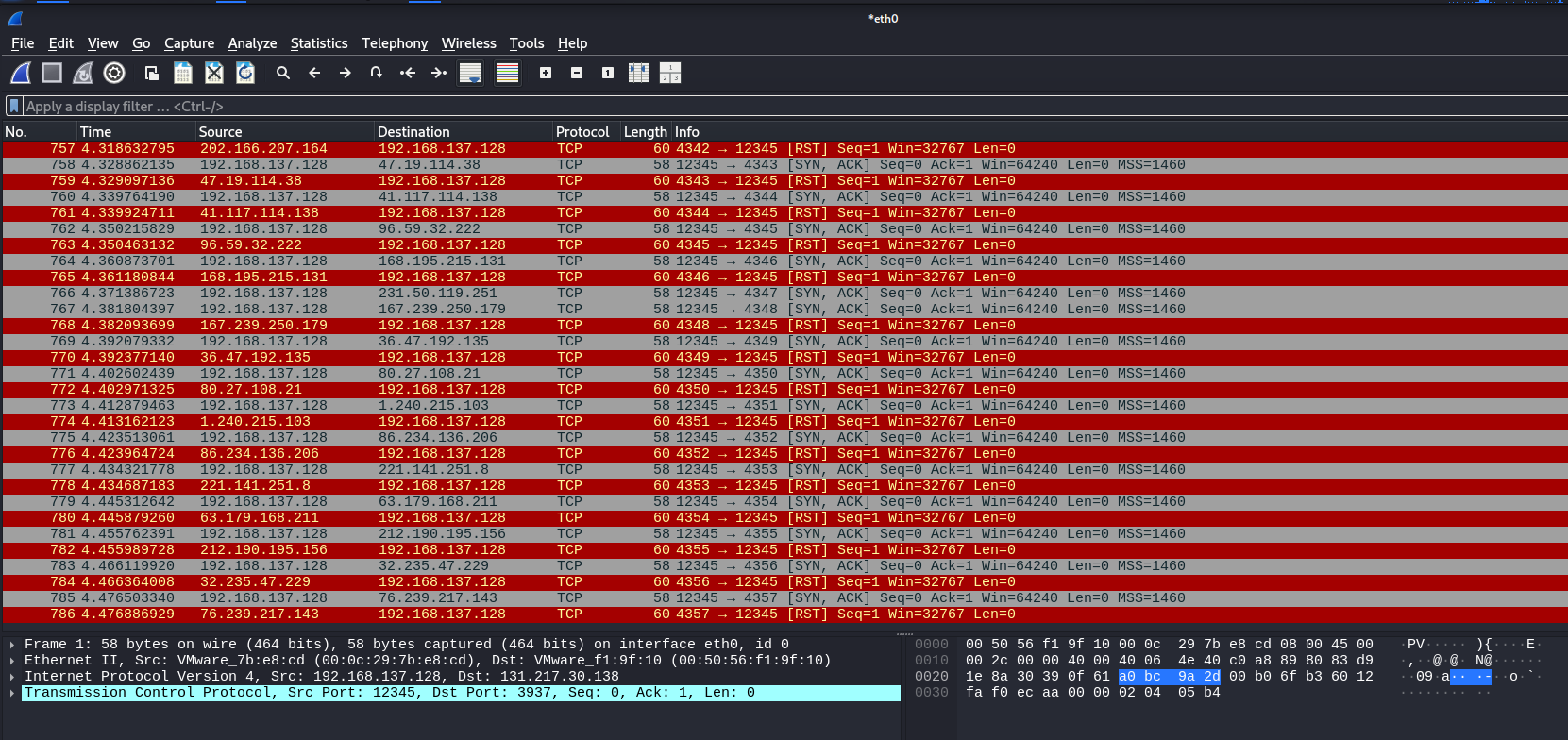


利用wireshark確認server是否受到攻擊，可以看到下圖，我正在利用hping3不斷發送SYN封包給server



如下圖，server在收到SYN請求後，不斷回應了SYN\_ACK，但是由於遲遲沒有收到ACK的回應，所以會有大量的RST封包出現，這個封包代表的意思是系統在server一直沒有收到ACK封包的情況下，自動清理這些大量的無效請求，來確保系統不會當機，也代表了系統資源正在逐漸被消耗。(測試10秒)





如何防禦 :

無法做到完全防禦，因為你無法全部拒絕SYN請求，這樣會導致其他正常使用的user無法傳送請求，但是可以透過一些措施來進行緩解，像是限制單位時間內的 SYN 封包數量、阻擋來源 IP 重複且頻繁送 SYN等等，我將示範限制單位時間內的 SYN 封包數量

指令 : sudo iptables -A INPUT -p tcp --syn --dport 12345 -m limit --limit 5/second --limit-burst 10 -j ACCEPT

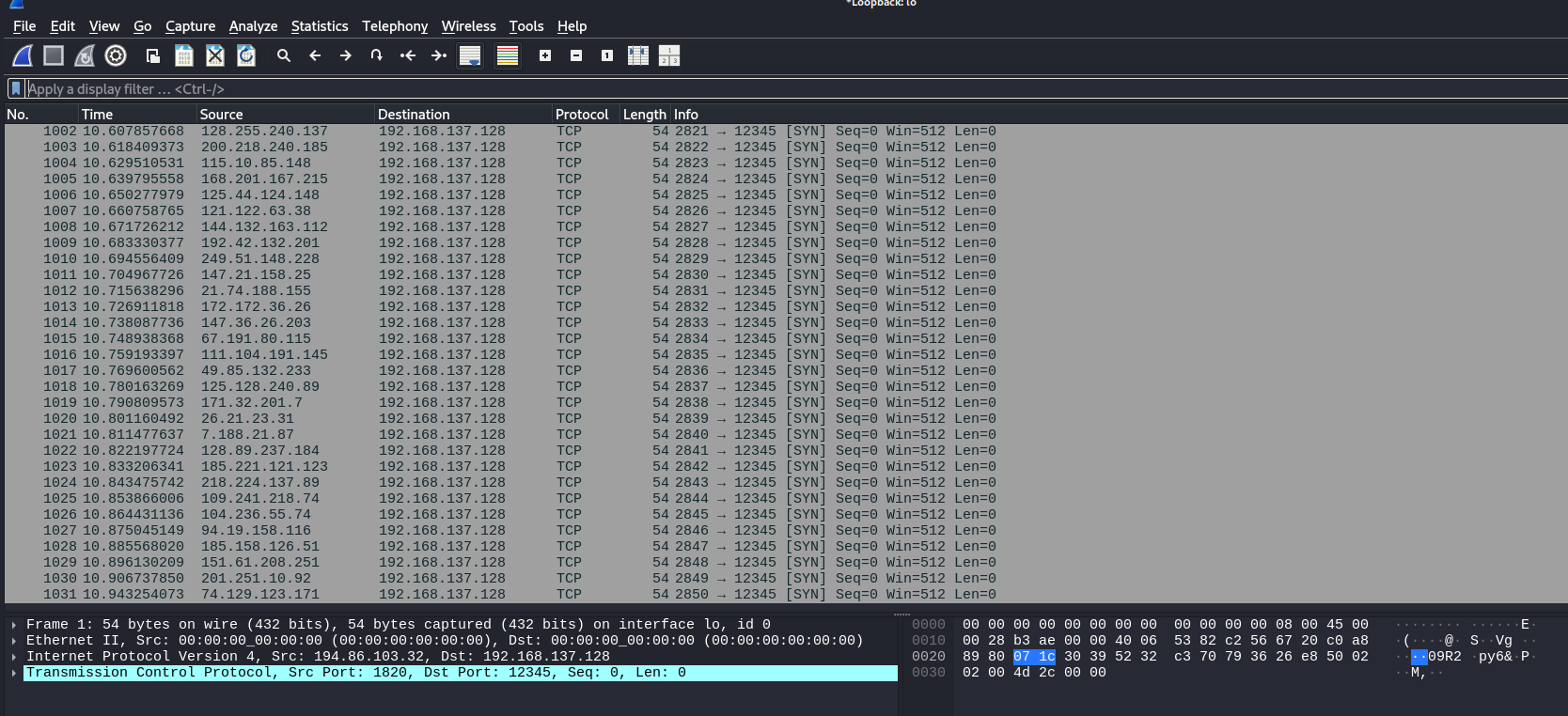
利用Linux上的防火墙管理工具iptables限制input TCP流量，接著匹配 TCP 三次交握過程中的第一個封包，針對port為12345且發送到本地端的封包，限制只有5個(每秒)且同時最多10個的封包可以通過系統並繼續處理。

sudo iptables -A INPUT -p tcp --syn --dport 12345 -j DROP

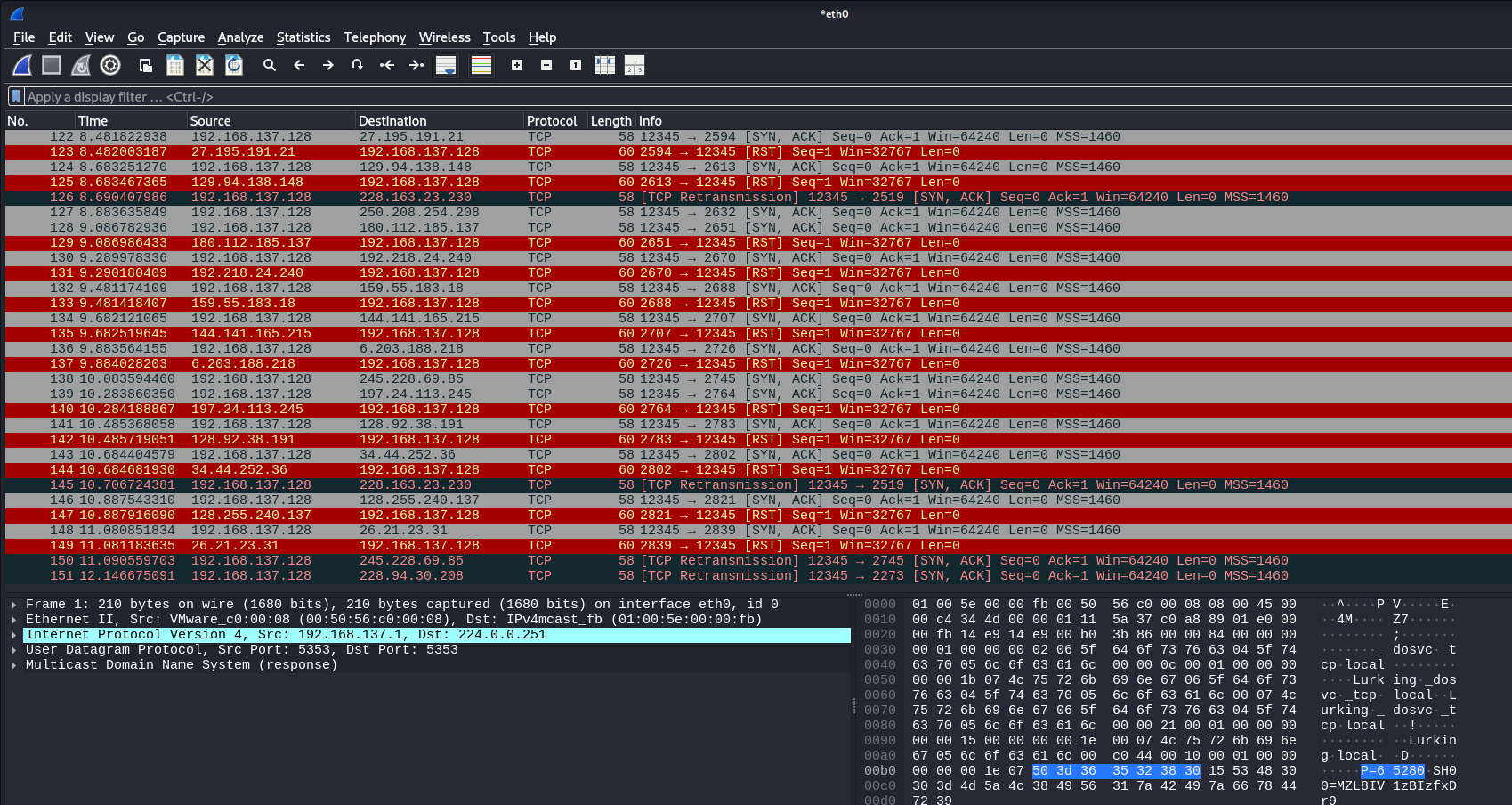
承上，將該條規則以外的封包進行無條件丟棄

這兩個指令加在一起就可以達到防禦的效果，在使用第一條規則後，剩下不符合第一條規則的封包就會利用第二條規則進行丟棄，以減少系統的負擔。

經過觀察wireshark，同樣在10秒內，可以看到發送的SYN請求數量還是有很多



但是透過下面這張圖可以看到，在透過指令的限制下，系統處理的SYN請求少了很多，由此可以防禦成功，在防禦之後可以減少系統的負擔



參考資料 :

<https://www.cnblogs.com/wpjamer/articles/10957629.html>

<https://www.cloudflare.com/zh-tw/learning/ddos/syn-flood-ddos-attack/>

<https://zh.wikipedia.org/zh-tw/SYN_flood>

<https://topic.alibabacloud.com/tc/a/brief-discussion-on-iptables-anti-syn-flood-attack-and-cc-attack_1_31_31056603.html>

<http://www.study-area.org/tips/syn_flood.htm>

攻擊影片demo :

<https://youtu.be/GrWaLU2tBQ4>