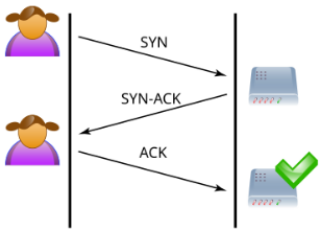
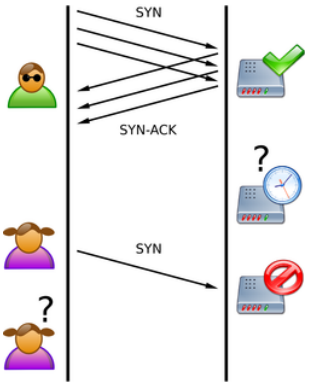
SYN DDOS 攻擊介紹 ：

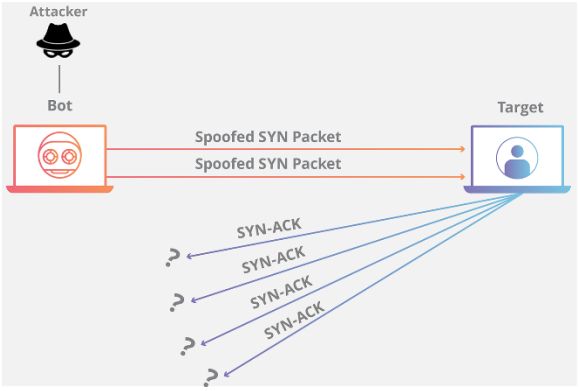
SYN flooding 攻擊(又稱 SYN 洪水攻擊)，為半開放式攻擊，顧名思義，就是利用送很多封包導致伺服器癱瘓的攻擊，是一種廣為人知的攻擊方式。駭客會透過消耗所有可用的伺服器資源，使伺服器無法用於合法請求。透過重複傳送初始連線要求 (SYN) 封包，攻擊者能夠淹沒目標伺服器上所有可用的連接埠，使目標裝置緩慢回應或完全不回應合法請求，下圖為正常收發的 TCP 三向交握。



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。

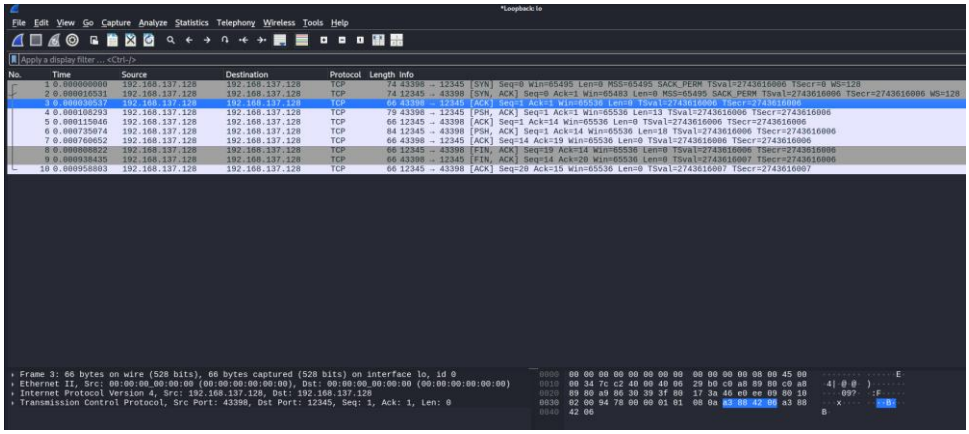


另一種攻擊方式是，惡意使用者會創造一個假的來源 IP 位址並傳送 SYN 請求，這讓 server 送 SYN-ACK 到偽造的 IP 位址，因此永不可能收到 ACK 回應，如下圖所示。



攻擊示範 ：

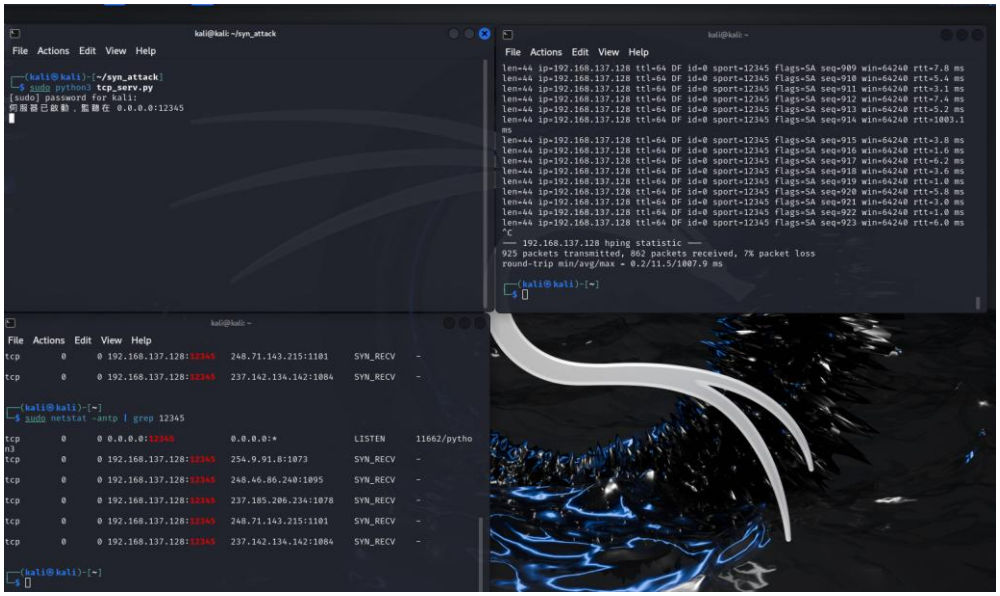
以下為正常交握的情況，做 SYN 請求，server 回應 SYN_ACK，user 再次回應 ACK



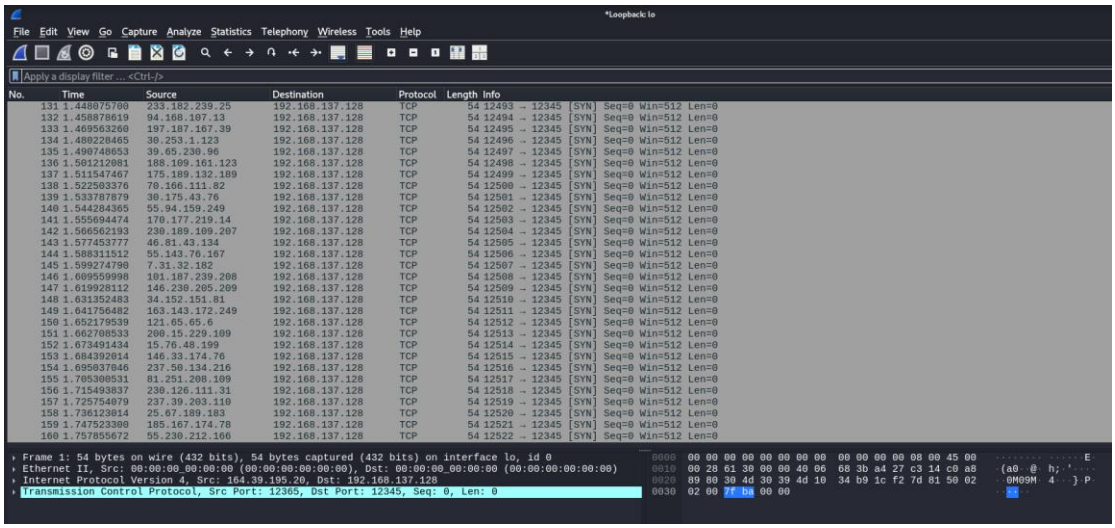
執行事先架設好的 server (含有漏洞)(左上 terminal)，利用 hping3 傳送封包進行 SYN flooding 攻擊(右上 terminal)，接著驗證 server 的 backlog 是否被塞滿(受到 ddos 攻擊)(左下 terminal)，可以看到 port 12345 的 server 收到了很多來自 random ip 的封包(server 目前只設定 5 個)，狀態都是 SYN_RECV，代表收到 SYN 請求，server 回應 SYN_ACK，但是 user 並未回傳 ACK 回應，導致 backlog 被塞爆，最終導致 server 癱瘓。

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



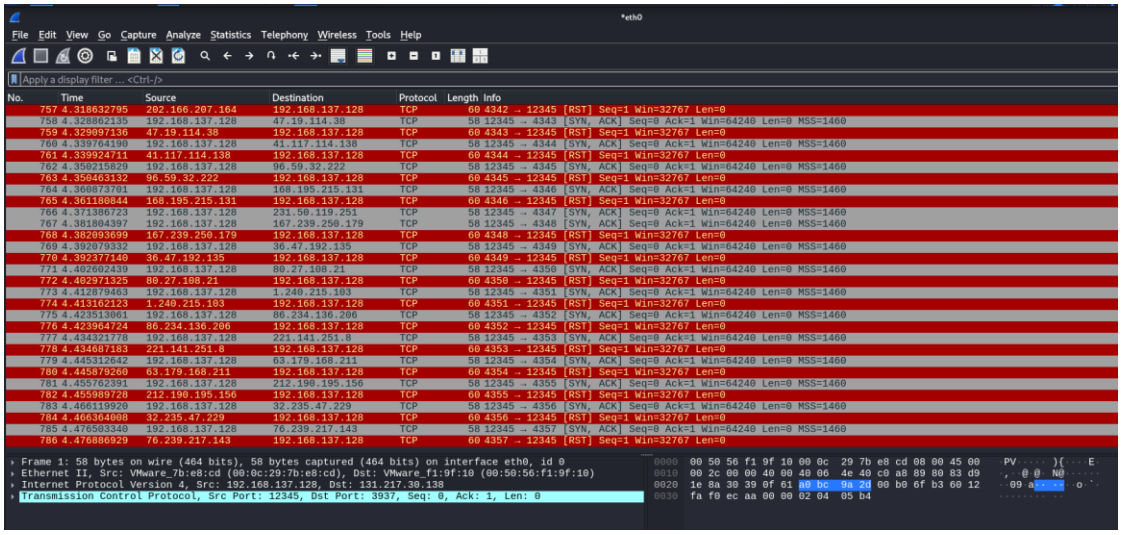
如下圖，server 在收到 SYN 請求後，不斷回應了 SYN_ACK，但是由於遲遲沒有收到 ACK 的回應，所以會有大量的 RST 封包出現，這個封包代表的意思是系統在 server 一直沒有收到 ACK 封包的情況下，自動清理這些大量的無效請求，來確保系統不會當機，也代表了系統資源正在逐漸被消耗。(測試 10 秒)

```
18    # 發動攻擊
19    ssh.exec_command(f"echo kali | sudo -S {command}", get_pty=True)
20
21    # 等待一段時間後強制結束
22    time.sleep(10)
23    # 結束攻擊
24    stdin, stdout, stderr = ssh.exec_command("echo kali | sudo -S pkill -9 -f hping3", get_pty=True)
25    stdout.channel.recv_exit_status()  # 等待 pkill 完成
26

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

[Running] python -u "c:\Users\benso\Documents\assignment\3下\駭客攻防\SYN_ms.py"
Connecting to slave...
Connected!
Launching SYN attack...
hping3 processes still running:
kali       17496  0.0  0.1   7692  3556 ?        Ss   09:04   0:00 zsh -c ps aux | grep hping3
kali       17498  0.0  0.1   6520  2188 ?        S    09:04   0:00 grep hping3

Stopped SYN attack from 192.168.137.128
```



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

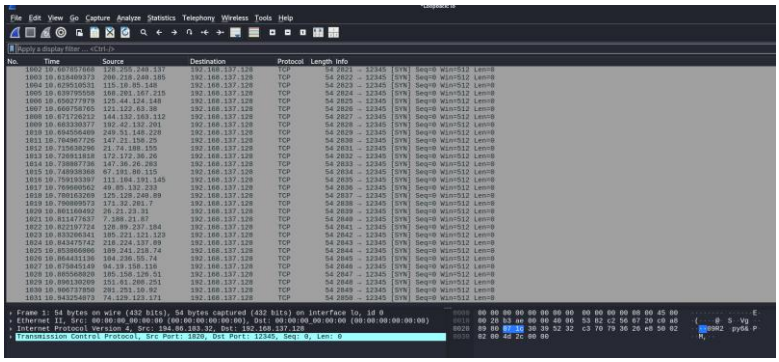
利用 Linux 上的防火墻管理工具 iptables 限制 input TCP 流量，接著匹配 TCP 三次交握過程中的第一個封包，針對 port 為 12345 且發送到本地端的封包，限制只有 5 個(每秒)且同時最多 10 個的封包可以通過系統並繼續處理。

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

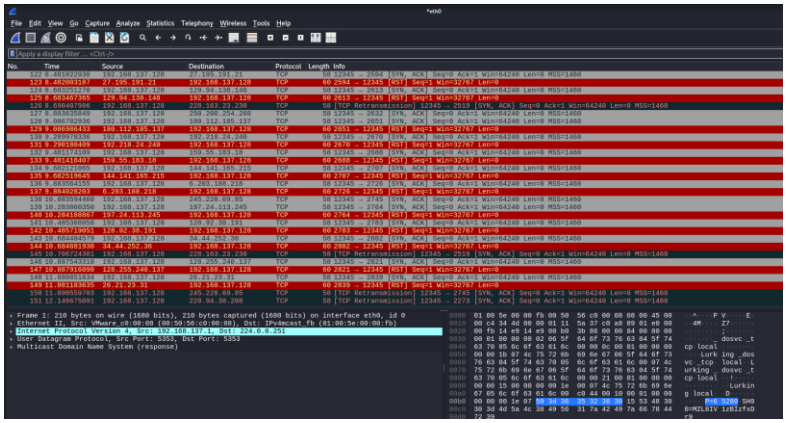
承上，將該條規則以外的封包進行無條件丟棄

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